Vorwort

Von Erholungspause keine Spur - mit immer schnellerer Taktung prägen Trends und neue Technologien die Informationsverarbeitung in Behörden und Unternehmen. Konvergenz der Netze und Virtualisierung sind nur zwei der vielen Schlagwörter, mit denen sich Entscheider, Sicherheitsverantwortliche, Entwickler, Administratoren und letztendlich auch Anwender konfrontiert sehen. Dabei ist die Informationssicherheit längst kein Randaspekt mehr, sie wird vielmehr als integraler Bestandteil von Lösungen, Dienstleistungen und Technologien eingefordert.

Hierzu leisten die IT-Grundschutz-Kataloge einen handlungsorientierten Beitrag. Die vorliegende Fassung wurde gründlich überarbeitet und um wichtige neue Themen ergänzt. Internet-Telefonie, drahtlose Netze und Speichersysteme werden anhand von praxisbewährten Maßnahmen in eigenständigen Bausteinen behandelt. Hinzu kommen zahlreiche weitere Ergänzungen und Aktualisierungen, die auf der Grundlage des Anwenderbedarfs erarbeitet wurden.

Die Vielzahl an positiven Rückmeldungen zeigt auch, dass das BSI mit der neuen Struktur der IT-Grundschutz-Dokumente, dem Lebenszyklus-Konzept und den BSI-Standards zum IT-Grundschutz den richtigen Weg eingeschlagen hat. In der vorliegenden neuen Fassung der IT-Grundschutz-Kataloge wird dieser Ansatz deshalb konsequent weiter verfolgt.

Ich wünsche Ihnen viel Erfolg bei der praktischen Anwendung der IT-Grundschutz-Kataloge und ermutige Sie, auch weiterhin mit Kritik und Anregungen zur Weiterentwicklung des IT-Grundschutzes beizutragen.

Bonn, im November 2006

Dr. Udo Helmbrecht, Präsident des BSI

Hinweis:

Wird im Text die männliche Form verwendet, geschieht dies ausschließlich aus Gründen der leichteren Lesbarkeit.

Dankesworte

Aufgrund der jährlichen Bedarfsabfrage bei registrierten Anwendern werden die IT-Grundschutz-Kataloge bedarfsorientiert weiterentwickelt. Für die Mitarbeit bei der Weiterentwicklung des IT-Grundschutzes und die engagierte Unterstützung bei der Fortschreibung der 8. Ergänzungslieferung der IT-Grundschutz-Kataloge wird an dieser Stelle folgenden Beteiligten gedankt:

- Gesamtkoordination	Frau Isabel Münch, BSI
- Redaktionelle Bearbeitung und Hotline	Frau Elke Cäsar, BSI Frau Gabriele Scheer-Gumm, BSI
- Baustein B 5.13 SAP System	Herr Stefan Fünfrocken, Eurosec Martina Seiler, Eurosec Herr Michael Mehrhoff, BSI Herr Michael Förtsch, BSI
- Baustein B 3.108 Windows Server 2003	Herr Knud Brandis, PERSICON Information Risk Management GmbH Herr Willy Wauschkuhn, PERSICON Information Risk Management GmbH Prof. Dr. Rainer Rumpel, PERSICON Information Risk Management GmbH, Berufsakademie Berlin Herr Thomas Caspers, BSI Frau Dr. Lydia Tsintsifa, BSI
- Baustein B 3.303 Speichersysteme und Speichernetze	Herr Werner Metterhausen, VZM GmbH Frau Dr. Lydia Tsintsifa, BSI
- Baustein B 4.6 WLAN	Frau Isabel Münch, BSI Herr Michael Ruck, BSI Herr Berthold Ternes, BSI
- Baustein B 4.7 VoIP	Herr Dr. Harald Niggemann, BSI Herr Holger Schildt, BSI
- Überarbeitung Baustein B 5.7 Datenbanken	Jörg Stockmann, Atos Origin Andreas Sesterhenn, Atos Origin Herr Michael Förtsch, BSI Frau Petra Simons-Felwor, BSI
- Qualitätssicherung	Herr Gerhard Weck, INFODAS Herr Tobias Hödtke, BSI

Neben der Aktualisierung und Überarbeitung von Bausteinen wurden zahlreiche einzelne Gefährdungen und Maßnahmen an neue technische Entwicklungen, neue Bedrohungsszenarien und neue Entwicklungen in der IT-Sicherheit angepasst. Auch hier sei den Mitwirkenden gedankt.

Darüber hinaus sei allen gedankt, die sich durch konstruktive Kritik und praktische Verbesserungsvorschläge an der Verbesserung des IT-Grundschutzes und der IT-Grundschutz-Kataloge beteiligt haben.

Bei der Fortschreibung und Weiterentwicklung vorhergehender Versionen des IT-Grundschutzhandbuchs haben die nachfolgend aufgezählten Personen und Institutionen mitgewirkt. Auch ihnen sei hiermit Dank ausgesprochen:

- Atos Origin
  Herr Herbert Blaauw, Herr Matthias Mönter
  Herr Götz, Herr Jaster, Herr Pohl
- ConSecur GmbH
  Herr Nedon, Herr Eckardt
- Daimler-Benz AG
  Herr Heinle, Hr. Schlette
- Europäische Kommission
  GD Informationsgesellschaft
  Herr Achim Klabunde
- EUROSEC GmbH
  Herr FünfrockenHerr Vetter
  Herr Dr. Zieschang
- Evangelische Kirche von Westfalen,
  Das Landeskirchenamt
  Herr Huget
- Flughafen Düsseldorf GmbH
  Herr Andreas Peters
- GUIDE SHARE EUROPE
  Arbeitskreis "DATENSCHUTZ und DATENSICHERHEIT"
- Henkel KGaA
  Herr Rhefus
- HiSolutions Software GmbH
  Herr Alexander Geschonneck
- INFODAS
  Herr Dr. Weck
- Ingenieurbüro Mink
- Innenministerium des Landes
  Schleswig-Holstein
  Herr Kuhr
- Landesbeauftragter für den Datenschutz
  Saarland
  Herr Simon
- Microsoft Deutschland GmbH
  Thomas Obert, Lars Klinghammer
- Fa. Novell
- Fa. Oracle
- Röhm GmbH Chemische Fabrik
  Datenschutzbeauftragter Herr Güldemeister
- T-Systems International GmbH
  Herr Stephan Hüttinger, Herr Torsten Kullich,
  Herr Klaus Müller, Herr Stefan Morkovsky,
  Herr Axel Nennker
- Universität GH Essen, FB Wirtschaftinformatik
  Herr Prof. Dr. Voßbein
- Universitätsklinikum der TU Dresden
  Klinik für Orthopädie
  Herr Frank Heyne
- Verband der Chemischen Industrie e. V.
- Symantec Deutschland GmbH
  Herr Frank Bunn
- VZM GmbH
  Herr Bruno Hecht, Herr Werner Metterhausen,
  Herr Rainer von zur Mühlen
- Zentrale Datenverarbeitungsstelle für das Saarland
  Herr Müller

Folgende Autoren haben durch die Erstellung von Bausteinen ihr Fachwissen in die IT-Grundschutz-Kataloge einfließen lassen. Ihnen gebührt besonderer Dank, da ihr Engagement die Entstehung und Weiterentwicklung der IT-Grundschutz-Kataloge erst ermöglicht hat.

Bundesministerium des Innern: Herr Jörg-Udo Aden, Herr André Reisen, Herr Manfred Kramer

Bundesministerium für Bildung und Wissenschaft: Herr Frank Stefan Stumm

Bundesamt für Sicherheit in der Informationstechnik: Herr Rainer Belz, Herr Thomas Biere, Frau Steffi Botzelmann, Frau Elke Cäsar, Herr Thomas Caspers, Herr Björn Dehms, Herr Uwe Dornseifer, Herr Günther Ennen, Herr Olaf Erber, Herr Frank W. Felzmann, Herr Michael Förtsch, Herr Dr. Kai Fuhrberg, Herr Thomas Häberlen, Herr Dr. Dirk Häger, Herr Dr. Timo Hauschild, Herr Dr. Hartmut Isselhorst, Frau Angelika Jaschob, Herr Harald Kelter, Herr Kurt Klinner, Herr Dr. Christian Mrugalla, Frau Isabel Münch, Herr Dr. Harald Niggemann, Herr Robert Rasten, Frau Martina Rohde, Herr Michael Ruck, Frau Gabriele Scheer-Gumm, Herr Fabian Schelo, Herr Holger Schildt, Herr Dr. Willibald Schneider, Herr Heiner Schorn, Herr Dr. Ernst Schulte-Geers, Herr Carsten Schulz, Herr Bernd Schweda, Frau Petra Simons-Felwor, Frau Dr. Lydia Tsintsifa, Frau Katja Vogel, Herr Frank Weber, Herr Helmut Weisskopf

sowie

Herr Marcel Birkner

Herr Felix Stolte

Herr Dr. Stefan Wolf

Inhaltsverzeichnis - IT-Grundschutz-Kataloge

Schicht 2 Infrastruktur

Schicht 3 IT-Systeme

Schicht 4 Netze

Schicht 5 IT-Anwendungen

Gefährdungskataloge

Maßnahmenkataloge

Neues in Version 2006 der IT-Grundschutz-Kataloge

Bedarfsorientierte Weiterentwicklung

Aufgrund der jährlichen Bedarfsabfrage bei registrierten Anwendern wurden die IT-Grundschutz-Kataloge bedarfsorientiert weiterentwickelt. Die neuen Bausteine befassen sich mit folgenden Themen:

Sicherheit in SAP Systemen

Der Baustein B 5.13 *SAP System* fokussiert auf die Grundabsicherung von SAP-basierten Applikationen für Geschäftsprozesse auf Ebene der Basis-Administration. Hier werden die wichtigsten technischen Aspekte genannt, die aus Sicht der IT-Sicherheit bei der Planung und beim Einsatz von SAP Systemen zu beachten sind. Auf versionsbezogene Unterschiede verzichtet der Baustein, so dass er für mySAP ERP Systeme und für SAP R/3 Systeme eingesetzt werden kann. Auf die existierende und sehr umfangreiche SAP Dokumentation wird im Baustein verwiesen. Ziel des Bausteines ist es jedoch nicht, diese zu reproduzieren, sondern empfohlene sicherheitsrelevante Vorgehensweisen und beachtenswerte Besonderheiten darzustellen.

Speichersysteme und Speichernetze

Thema des Bausteins B 3.303 *Speichersysteme und Speichernetze* sind Systeme und Netze, die zentralisierten Speicher für Applikationen zur Verfügung stellen. Der Baustein enthält Sicherheitsempfehlungen, die bei der Planung und beim Einsatz von Storage Area Networks (SAN) und Network Attached Storage (NAS) Systemen in der Organisation zu beachten sind.

Windows Server 2003

Der Baustein B 3.108 *Windows Server 2003* ergänzt die Reihe von Bausteinen, die sich mit dem sicheren Einsatz von Windows-Betriebssystemen beschäftigen. Hier wird der Anwender auf konzeptionelle Sicherheitsaspekte, aber auch auf Sicherheitsempfehlungen zu konkreten Konfigurationseinstellungen hingewiesen.

Wireless LAN (WLAN)

Der Baustein B 4.6 *WLAN* behandelt den sicheren Einsatz von drahtlosen Netzen, die auf dem Standard IEEE 802.11 und dessen Erweiterungen basieren. Neben einem Überblick der Begrifflichkeiten bei WLANs werden Empfehlungen für Verschlüsselungs- und Authentisierungsmechanismen gegeben. Wichtige Teile sind die in der Planungsphase notwendige Konzeption eines WLANs und die Auswahl des richtigen WLAN-Standards. Darüber hinaus wurde auch an die Sensibilisierung und Schulung der Mitarbeiter und an eine Betreuung eines WLANs durch externe Dienstleister gedacht.

Voice over IP (VoIP)

Der Baustein B 4.7 *VoIP* beschäftigt sich mit dem sicheren Einsatz von VoIP in Netzen. Die in dem Baustein betrachteten Empfehlungen wirken den Problemen, die bei der Telefonie über ein Datennetz entstehen können, entgegen. Neben Grundlagen, wie einer Übersicht über die verbreiteten Signalisierungs- und Medientransportprotokolle, werden unter anderem Hinweise zur Integration von VoIP in vorhandene Datennetze sowie zur Administration und Konfiguration von VoIP-Komponenten gegeben.

Neue Maßnahmen und Gefährdungen

Außerdem sind verschiedene neue Maßnahmen und Gefährdungen aufgenommen worden, beispielsweise zu den Themen

- Verletzung von Brandschottungen / Änderung von Brandlasten

- Einbeziehung des Brandschutzbeauftragten in Baumaßnahmen
- Vermeidung elektrischer Zündquellen: Verwendung unzureichender Steckdosenleisten, verstaubte Lüfter, etc.
- Sicherer Einsatz virtueller IT-Systeme
- Umgang mit Ausnahmegenehmigungen
- Software-Entwicklung durch Endbenutzer
- Vertraulichkeitsvereinbarungen
- Einsatz zentraler, netzbasierter Authentisierungsdienste, z. B. RADIUS-Server

Aktualisierung und Überarbeitung

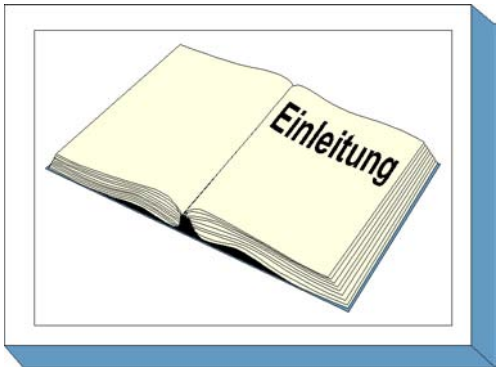
Der Baustein B 5.7 *Datenbanken* wurde überarbeitet, um technische Entwicklungen in den letzten Jahren zu berücksichtigen. So wurden die betrachteten Datenbankmodelle um das Netzwerkdatenbankmodell und das objektrelationale Datenbankmodell ergänzt. Auch der Datenbank-Zugriff über mobile Endgeräte (Mobiltelefone und PDAs) findet in dem aktualisierten Baustein Beachtung. Um Risiken durch SQL-Injections zu reduzieren, bietet der Baustein eine dedizierte neue Maßnahme, die eine Reihe von Sicherheitsempfehlungen hierzu vorstellt.

Darüber hinaus wurden zahlreiche einzelne Gefährdungen und Maßnahmen an neue technische Entwicklungen, neue Bedrohungsszenarien und neue Entwicklungen in der IT-Sicherheit angepasst.

Weitere strukturelle Veränderungen wurden in der aktualisierten Ausgabe nicht durchgeführt. Die Nummerierung bestehender Gefährdungen und Maßnahmen blieb erhalten, sodass ein im Vorjahr auf Basis der IT-Grundschutz-Kataloge erstelltes Sicherheitskonzept fortgeschrieben werden kann. Es empfiehlt sich dennoch, die ausgewählten Maßnahmen bei der Bearbeitung komplett zu lesen, um Ergänzungen berücksichtigen zu können und um das Wissen zur IT-Sicherheit aufzufrischen.

1 IT-Grundschutz - Basis für IT-Sicherheit

1.1 Warum ist IT-Sicherheit wichtig?



Weder ein Unternehmen noch eine Behörde sind mittlerweile ohne funktionierende Informationstechnik (IT) noch lebensfähig. Hierzu gehört auch, dass diese IT sicher betrieben wird. Ein anerkanntes Standardwerk, in dem für die verschiedensten IT-Umgebungen Empfehlungen zum sicheren Umgang mit Information und IT gegeben wird, sind die IT-Grundschutz-Kataloge.

Nahezu alle Geschäftsprozesse und Fachaufgaben werden mittlerweile elektronisch gesteuert. Große Mengen von Informationen werden dabei digital gespeichert, elektronisch verarbeitet und in lokalen und globalen sowie in privaten und öffentlichen Netzen übermittelt. Viele öffentliche oder privatwirtschaftliche Aufgaben und Vorhaben können ohne IT überhaupt nicht mehr oder im besten Fall nur noch teilweise durchgeführt werden. Damit sind viele Institutionen in Verwaltung und Wirtschaft von dem einwandfreien Funktionieren der eingesetzten IT abhängig. Die jeweiligen Behörden- und Unternehmensziele können nur bei ordnungsgemäßem und sicheren IT-Einsatz erreicht werden.

Mit der Abhängigkeit von der IT erhöht sich auch der potenzielle soziale Schaden durch den Ausfall von Informationstechnik. Da IT an sich nicht frei von Schwachstellen ist, besteht ein durchaus berechtigtes Interesse, die von der IT verarbeiteten Daten und Informationen zu schützen und die Sicherheit der IT zu planen, zu realisieren und zu kontrollieren.

Die Schäden durch IT-Fehlfunktionen können verschiedenen Kategorien zugeordnet werden. Am auffälligsten ist der Verlust der Verfügbarkeit: Läuft ein IT-System nicht, können keine Geldtransaktionen durchgeführt werden, Online-Bestellungen sind unmöglich, Produktionsprozesse stehen still. Häufig diskutiert ist auch der Verlust der Vertraulichkeit von Daten: Jeder Bürger weiß um die Notwendigkeit, seine personenbezogenen Daten vertraulich zu halten, jedes Unternehmen weiß, dass firmeninterne Daten über Umsatz, Marketing, Forschung und Entwicklung die Konkurrenz interessieren. Aber auch der Verlust der Integrität (Korrektheit von Daten) kann schwerwiegende Folgen haben: gefälschte oder verfälschte Daten führen zu Fehlbuchungen, Produktionsprozesse stoppen wegen fehlerhafter Lieferungen, falsche Entwicklungs- und Planungsdaten führen zu fehlerhaften Produkten. Seit einigen Jahren gewinnt auch der Verlust der Authentizität als ein Teilbereich der Integrität an Bedeutung: Daten werden einer falschen Person zugeordnet. Beispielsweise können Zahlungsanweisungen oder Bestellungen zu Lasten einer dritten Person verarbeitet werden, ungesicherte digitale Willenserklärungen können falschen Personen zugerechnet werden, die "digitale Identität" wird gefälscht.

Dabei wird diese Abhängigkeit von der Informationstechnik in Zukunft noch weiter zunehmen. Besonders erwähnenswert sind dabei folgende Entwicklungen:

- **Steigender Vernetzungsgrad:** IT-Systeme arbeiten heutzutage nicht mehr isoliert voneinander, sondern werden immer stärker vernetzt. Die Vernetzung ermöglicht es, auf gemeinsame Datenbestände zuzugreifen und intensive Formen der Kooperation über geographische Grenzen hinweg zu nutzen. Damit entsteht nicht nur eine Abhängigkeit von den einzelnen IT-Systemen, sondern in starkem Maße auch von den Datennetzen. Sicherheitsmängel eines IT-Systems können aber dadurch schnell globale Auswirkungen haben.

- **IT-Verbreitung und Durchdringung:** Immer mehr Bereiche werden durch Informationstechnik unterstützt, häufig, ohne dass dies auffällt. Die erforderliche Hardware wird zunehmend kleiner und günstiger, so dass kleine und kleinste IT-Einheiten in alle Bereiche des Alltags integriert werden können. So gibt es beispielsweise Jacken mit integrierten PDAs, RFIDs zur Steuerung von Besucher- oder Warenströmen, IT-gestützte Sensorik in Autos, um automatisch auf veränderte Umgebungsverhältnisse reagieren zu können. Die Kommunikation der verschiedenen IT-Komponenten untereinander findet dabei zunehmend drahtlos statt.
- **Verschwinden der Netzgrenzen**: Bis vor kurzem ließen sich IT-Anwendungen ganz klar auf die IT-Systeme und die Kommunikationsstrecken dazwischen begrenzen. Ebenso ließ sich sagen, an welchen Standorten und bei welcher Institution diese angesiedelt waren. Durch Globalisierung und die Zunahme von drahtloser und spontaner Kommunikation verschwinden diese Grenzen zunehmend.
- **Angriffe kommen schneller:** Die beste Vorbeugung gegen Computer-Viren, Würmer oder andere Angriffe auf IT-Systeme ist die frühzeitige Information über Sicherheitslücken und deren Beseitigung, z. B. durch Einspielen von Patches und Updates. Mittlerweile sinkt allerdings die Zeitspanne zwischen dem Bekanntwerden einer Sicherheitslücke und den ersten gezielten Massenangriffen darauf, so dass es immer wichtiger wird, ein gut aufgestelltes IT-Sicherheitsmanagement und Warnsystem zu haben.

Angesichts der vorgestellten Gefährdungspotentiale und der steigenden Abhängigkeit stellen sich damit für jede Institution, sei es ein Unternehmen oder eine Behörde, bezüglich IT-Sicherheit mehrere zentrale Fragen:

- Wie sicher ist die Informationstechnik einer Institution?
- Welche IT-Sicherheitsmaßnahmen müssen ergriffen werden?
- Wie müssen diese Maßnahmen konkret umgesetzt werden?
- Wie hält bzw. verbessert eine Institution das erreichte Sicherheitsniveau?
- Wie sicher ist die IT anderer Institutionen, mit denen eine Kooperation stattfindet?

Bei der Suche nach Antworten auf diese Fragen ist zu beachten, dass IT-Sicherheit nicht alleine eine technische Fragestellung ist. Um ein ausreichend sicheres IT-System betreiben zu können, sind neben den technischen auch organisatorische, personelle und baulich-infrastrukturelle Maßnahmen zu realisieren und insbesondere ist ein IT-Sicherheitsmanagement einzuführen, das die Aufgaben zur IT-Sicherheit konzipiert, koordiniert und überwacht.

Vergleicht man jetzt die IT-Systeme aller Institutionen im Hinblick auf obige Fragen, so kristallisiert sich eine besondere Gruppe von IT-Systemen heraus. Die IT-Systeme in dieser Gruppe lassen sich wie folgt charakterisieren:

- Es sind typische IT-Systeme, d. h. diese Systeme sind keine Individuallösungen, sondern sie sind weit verbreitet im Einsatz.
- Der Schutzbedarf der IT-Systeme bezüglich Vertraulichkeit, Integrität und Verfügbarkeit liegt im Rahmen des Normalmaßes.
- Zum sicheren Betrieb der IT-Systeme sind Standard-Sicherheitsmaßnahmen aus den Bereichen Infrastruktur, Organisation, Personal, Technik und Notfallvorsorge erforderlich.

Gelingt es, für diese Gruppe der "typischen" IT-Systeme den gemeinsamen Nenner aller Sicherheitsmaßnahmen, die Standard-Sicherheitsmaßnahmen, zu beschreiben, so würde dies die Beantwortung obiger Fragen für diese "typischen" IT-Systeme erheblich erleichtern. IT-Systeme, die außerhalb

dieser Gruppe liegen, seien es seltenere Individualsysteme oder IT-Systeme mit sehr hohem Schutzbedarf, können sich dann zwar an den Standard-Sicherheitsmaßnahmen orientieren, bedürfen letztlich aber einer individuellen Betrachtung.

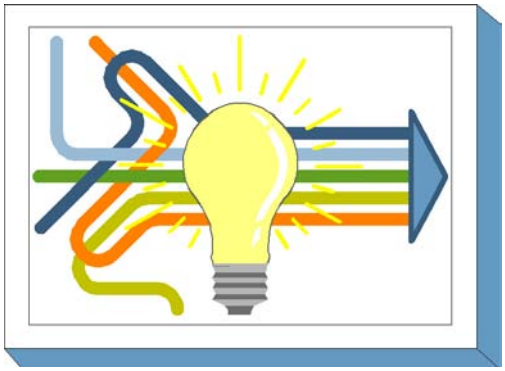
Die IT-Grundschutz-Kataloge beschreiben detailliert diese Standard-Sicherheitsmaßnahmen, die praktisch für jedes IT-System zu beachten sind. Sie umfassen:

- Standard-Sicherheitsmaßnahmen für typische IT-Systeme mit "normalem" Schutzbedarf,
- eine Darstellung der pauschal angenommenen Gefährdungslage,
- ausführliche Maßnahmenbeschreibungen als Umsetzungshilfe,
- eine Beschreibung des Prozesses zum Erreichen und Aufrechterhalten eines angemessenen IT-Sicherheitsniveaus und
- eine einfache Verfahrensweise zur Ermittlung des erreichten IT-Sicherheitsniveaus in Form eines Soll-Ist-Vergleichs.

Dabei ist die Resonanz sehr positiv. Auf den BSI-Webseiten findet sich ein Auszug aus der Liste derjenigen Institutionen, die IT-Grundschutz einsetzen. Sie stellt im Überblick dar, in welchen Branchen und in welchen Firmen bzw. Behörden IT-Grundschutz angewendet wird.

Da der IT-Grundschutz auch international großen Anklang findet, werden die IT-Grundschutz-Kataloge und das GSTOOL, aber auch die meisten anderen Dokumente zum IT-Grundschutz zusätzlich in englischer Sprache digital zur Verfügung gestellt.

1.2 IT-Grundschutz: Ziel, Idee und Konzeption



In den IT-Grundschutz-Katalogen werden Standard-Sicherheitsmaßnahmen für typische IT-Systeme empfohlen. Das Ziel dieser IT-Grundschutz-Empfehlungen ist es, durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den normalen Schutzbedarf angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Systeme und -Anwendungen dienen kann.

Um den sehr heterogenen Bereich der Informationstechnik einschließlich der Einsatzumgebung besser strukturieren und aufbereiten zu können, verfolgt der IT-Grundschutz das Baukastenprinzip. Die einzelnen Bausteine spiegeln typische Bereiche des IT-Einsatzes wider, wie beispielsweise Client-Server-Netze, bauliche Einrichtungen, Kommunikations- und Applikationskomponenten. In jedem Baustein wird zunächst die zu erwartende Gefährdungslage beschrieben, wobei sowohl die typischen Gefährdungen als auch die pauschalisierten Eintrittswahrscheinlichkeiten berücksichtigt werden. Diese Gefährdungslage bildet die Grundlage, um ein spezifisches Maßnahmenbündel aus den Bereichen Infrastruktur, Personal, Organisation, Hard- und Software, Kommunikation und Notfallvorsorge zu generieren.

Die Vorgehensweise nach IT-Grundschutz hilft dabei, IT-Sicherheitskonzepte einfach und arbeitsökonomisch zu erstellen. Bei der traditionellen Risikoanalyse werden zunächst die Bedrohungen ermittelt und mit Eintrittswahrscheinlichkeiten bewertet, um dann die geeigneten IT-Sicherheitsmaßnahmen auszuwählen und anschließend noch das verbleibende Restrisiko bewerten zu können. Bei einer Risikobewertung nach IT-Grundschutz wird hingegen nur ein Soll-Ist-Vergleich zwischen empfohlenen und bereits realisierten Maßnahmen durchgeführt. Dabei festgestellte fehlende und noch nicht umgesetzte Maßnahmen zeigen die Sicherheitsdefizite auf, die es durch die empfohlenen Maßnahmen zu beheben gilt. Erst bei einem signifikant höheren Schutzbedarf muss zusätzlich eine ergänzende Sicherheitsanalyse durchgeführt werden. Hierbei reicht es dann aber in der Regel aus, die Maßnahmenempfehlungen der IT-Grundschutz-Kataloge durch entsprechende individuelle, qualitativ höherwertige Maßnahmen, zu ergänzen. Eine einfache Vorgehensweise hierzu ist in dem BSI-Dokument "Risikoanalyse basierend auf IT-Grundschutz" beschrieben.

Auch wenn besondere Komponenten oder Einsatzumgebungen vorliegen, die in den IT-Grundschutz-Katalogen nicht hinreichend behandelt werden, bieten diese dennoch eine wertvolle Arbeitshilfe. Die dann notwendige ergänzende Analyse kann sich auf die spezifischen Gefährdungen und Sicherheitsmaßnahmen für diese Komponenten oder Rahmenbedingungen konzentrieren.

Bei den in den IT-Grundschutz-Katalogen aufgeführten Maßnahmen handelt es sich um Standard-Sicherheitsmaßnahmen, also um diejenigen Maßnahmen, die für die jeweiligen Bausteine nach dem Stand der Technik umzusetzen sind, um eine angemessene Basis-Sicherheit zu erreichen. Dabei stellen die Maßnahmen, die für die IT-Grundschutz-Zertifizierung gefordert werden, das Minimum dessen dar, was in jedem Fall vernünftigerweise an Sicherheitsvorkehrungen umzusetzen ist. Die als "zusätzlich" gekennzeichneten Maßnahmen haben sich ebenfalls in der Praxis bewährt, sie richten sich jedoch an Anwendungsfälle mit erhöhten Sicherheitsanforderungen.

Sicherheitskonzepte, die auf IT-Grundschutz basieren, können kompakt gehalten werden, da innerhalb des Konzepts jeweils nur auf die entsprechenden Maßnahmen in den IT-Grundschutz-Katalogen ver-

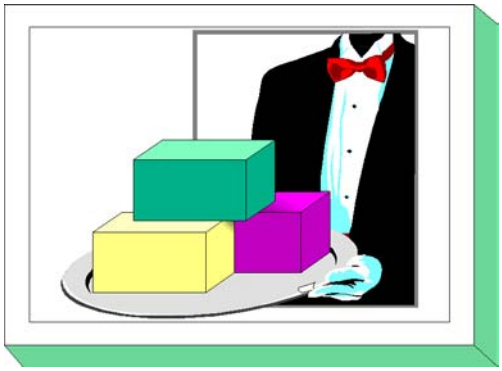
wiesen werden muss. Dies fördert die Verständlichkeit und die Übersichtlichkeit. Um die Maßnahmenempfehlungen leichter umsetzbar zu machen, sind die Sicherheitsmaßnahmen in den IT-Grundschutz-Katalogen detailliert beschrieben. Bei der verwendeten Fachterminologie wird darauf geachtet, dass die Beschreibungen für diejenigen verständlich sind, die die Maßnahmen realisieren müssen.

Um die Realisierung der Maßnahmen zu vereinfachen, werden die IT-Grundschutz-Kataloge ebenso wie die meisten Informationen rund um IT-Grundschutz auch in elektronischer Form zur Verfügung gestellt. Darüber hinaus wird die Realisierung der Maßnahmen auch durch Hilfsmittel und Musterlösungen unterstützt, die teilweise durch das BSI und teilweise auch von IT-Grundschutz-Anwendern bereitgestellt werden.

Da die Informationstechnik sehr innovativ ist und sich ständig weiterentwickelt, sind die vorliegenden Kataloge auf Aktualisierbarkeit und Erweiterbarkeit angelegt. Das Bundesamt für Sicherheit in der Informationstechnik aktualisiert auf der Grundlage von Anwenderbefragungen die IT-Grundschutz-Kataloge ständig und erweitert sie um neue Themen.

Das BSI bietet allen Anwendern die Möglichkeit der freiwilligen, selbstverständlich kostenfreien Registrierung an. Registrierte Anwender erhalten regelmäßig Informationen über aktuelle Themen des IT-Grundschutzes und der IT-Sicherheit. Die Registrierung ist außerdem die Grundlage für die Anwenderbefragungen. Nur durch den ständigen Erfahrungsaustausch mit den IT-Grundschutz-Anwendern ist eine bedarfsgerechte Weiterentwicklung möglich. Diese Bemühungen zielen letztlich darauf, aktuelle Empfehlungen zu typischen IT-Sicherheitsproblemen aufzeigen zu können. Maßnahmenempfehlungen, die nicht ständig aktualisiert und erweitert werden, veralten sehr schnell oder müssen so generisch gehalten werden, dass sie ihren eigentlichen Nutzen, Sicherheitslücken zu identifizieren und die konkrete Umsetzung zu vereinfachen, verfehlen.

1.3 Aufbau der IT-Grundschutz-Kataloge



Die IT-Grundschutz-Kataloge lassen sich in verschiedene Bereiche untergliedern, die zum besseren Verständnis hier kurz erläutert werden sollen:

Einstieg und Vorgehensweise

In diesem einleitenden Teil wird die Konzeption IT-Grundschutz und die Vorgehensweise zur Erstellung eines Sicherheitskonzepts nach IT-Grundschutz kurz vorgestellt. Eine ausführliche Beschreibung der Vorgehensweise nach IT-Grundschutz findet sich im BSI-Standard 100-2. Außerdem wird die Struktur der IT-Grundschutz-Kataloge und deren Nutzung erläutert.

IT-Sicherheitsmanagement

Die Planungs- und Lenkungsaufgabe, die erforderlich ist, um einen durchdachten und planmäßigen IT-Sicherheitsprozess aufzubauen und kontinuierlich umzusetzen, wird als IT-Sicherheitsmanagement bezeichnet.

Die Erfahrung zeigt, dass es ohne ein funktionierendes IT-Sicherheitsmanagement praktisch nicht möglich ist, ein durchgängiges und angemessenes IT-Sicherheitsniveau zu erzielen und zu erhalten. Daher wird im BSI-Standard 100-1 "Managementsysteme für Informationssicherheit (ISMS)" beschrieben, wie ein solches Managementsystem aufgebaut werden kann.

Aufbauend hierauf wird außerdem in Baustein B 1.0 der IT-Grundschutz-Kataloge beschrieben, wie ein effizientes IT-Sicherheitsmanagement aussehen sollte und welche Organisationsstrukturen dafür sinnvoll sind. Es wird außerdem ein systematischer Weg aufgezeigt, wie ein funktionierendes IT-Sicherheitsmanagement eingerichtet und im laufenden Betrieb weiterentwickelt werden kann.

Bausteine

Die Bausteine der IT-Grundschutz-Kataloge enthalten jeweils eine Kurzbeschreibung für die betrachteten Komponenten, Vorgehensweisen und IT-Systeme sowie einen Überblick über die Gefährdungslage und die Maßnahmenempfehlungen. Die Bausteine sind nach dem IT-Grundschutz-Schichtenmodell in die folgenden Kataloge gruppiert:

B 1: Übergeordnete Aspekte der IT-Sicherheit
B 2: Sicherheit der Infrastruktur
B 3: Sicherheit der IT-Systeme
B 4: Sicherheit im Netz
B 5: Sicherheit in Anwendungen

Gefährdungskataloge

Dieser Bereich enthält die ausführlichen Beschreibungen der Gefährdungen, die in den einzelnen Bausteinen als Gefährdungslage genannt wurden. Die Gefährdungen sind in fünf Kataloge gruppiert:

G 1: Höhere Gewalt
G 2: Organisatorische Mängel
G 3: Menschliche Fehlhandlungen
G 4: Technisches Versagen
G 5: Vorsätzliche Handlungen

Maßnahmenkataloge

Dieser Teil beschreibt die in den Bausteinen der IT-Grundschutz-Kataloge zitierten IT-Sicherheitsmaßnahmen ausführlich. Die Maßnahmen sind in sechs Maßnahmenkataloge gruppiert:

M 1: Infrastruktur
M 2: Organisation
M 3: Personal
M 4: Hard- und Software
M 5: Kommunikation
M 6: Notfallvorsorge

Aufbau der Bausteine

Die zentrale Rolle der IT-Grundschutz-Kataloge spielen die Bausteine, deren Aufbau im Prinzip gleich ist. Jeder Baustein beginnt mit einer kurzen Beschreibung der betrachteten Komponente, der Vorgehensweise bzw. des IT-Systems.

Im Anschluss daran wird die Gefährdungslage dargestellt. Die Gefährdungen sind dabei nach den genannten Bereichen Höhere Gewalt, Organisatorische Mängel, Menschliche Fehlhandlungen, Technisches Versagen und Vorsätzliche Handlungen unterteilt.

Um die Bausteine übersichtlich zu gestalten und um Redundanzen zu vermeiden, werden die Gefährdungstexte lediglich referenziert. Hier ein Beispiel für das Zitat einer Gefährdung innerhalb eines Bausteins:

- G 4.1 Ausfall der Stromversorgung

Im Kürzel G x.y steht der Buchstabe "G" für Gefährdung. Die Zahl x vor dem Punkt bezeichnet den Gefährdungskatalog (hier G 4 = Technisches Versagen) und die Zahl y nach dem Punkt bezeichnet die laufende Nummer der Gefährdung innerhalb des jeweiligen Katalogs. Es folgt der Titel der Gefährdung. Ein Einlesen in die Gefährdungen ist aus Gründen der Sensibilisierung und des Verständnisses der Maßnahmen empfehlenswert, aber für die Erstellung eines IT-Sicherheitskonzepts nach IT-Grundschutz nicht zwingend erforderlich.

Den wesentlichen Teil eines jeden Bausteins bilden die Maßnahmenempfehlungen, die sich an die Gefährdungslage anschließen. Zunächst erfolgen kurze Hinweise zum jeweiligen Maßnahmenbündel. So enthalten diese Ausführungen z. B. Hinweise zur folgerichtigen Reihenfolge bei der Realisierung der notwendigen Maßnahmen.

In jedem Baustein wird für das betrachtete Themengebiet vor der Maßnahmen-Liste eine Übersicht in Form eines "Lebenszyklus" gegeben, welche Maßnahmen in welcher Phase der Bearbeitung zu welchem Zweck umgesetzt werden sollten. In der Regel können die folgenden Phasen identifiziert werden, wobei für jede dieser Phasen typische Arbeiten angegeben sind, die im Rahmen einzelner Maßnahmen durchgeführt werden. Phasenübergreifend wirken dabei das IT-Sicherheitsmanagement und die Revision, die den gesamten Lebenszyklus begleiten und kontrollieren.

Phase	typische Tätigkeiten
Planung und Konzeption	- Definition des Einsatzzwecks - Festlegung von Einsatzszenarien - Abwägung des Risikopotentials - Dokumentation der Einsatzentscheidung - Erstellung des IT-Sicherheitskonzepts - Festlegung von Richtlinien für den Einsatz
Beschaffung (sofern erforderlich)	- Festlegung der Anforderungen an zu beschaffende Produkte (nach Möglichkeit auf Basis der Einsatzszenarien der Strategie-Phase) - Auswahl der geeigneten Produkte
Umsetzung	- Konzeption und Durchführung des Testbetriebs - Installation und Konfiguration entsprechend Sicherheitsrichtlinie - Schulung und Sensibilisierung aller Betroffenen
Betrieb	- Sicherheitsmaßnahmen für den laufenden Betrieb (z. B. Protokollierung) - Kontinuierliche Pflege und Weiterentwicklung - Änderungsmanagement - Organisation und Durchführung von Wartungsarbeiten - Audit
Aussonderung (sofern erforderlich)	- Entzug von Berechtigungen - Entfernen von Datenbeständen und Referenzen auf diese Daten - Sichere Entsorgung von Datenträgern
Notfallvorsorge	- Konzeption und Organisation der Datensicherung - Nutzung von Redundanz zur Erhöhung der Verfügbarkeit - Umgang mit Sicherheitsvorfällen - Erstellen eines Notfallplans

Es finden sich nicht in allen Bausteinen für jede Phase Maßnahmen. So findet sich beispielsweise im Baustein IIS-Server keine Maßnahme in der Beschaffungsphase, da dieser Baustein auf der Umsetzung des Bausteins Webserver basiert und hier die Auswahl eines Produkts bereits entschieden wurde.

Da alle Geschäftsprozesse, IT-Systeme und Einsatzbedingungen sich ständig ändern und weiterentwickelt werden, müssen die Phasen erfahrungsgemäß immer wieder durchlaufen werden. Dies sicherzustellen ist Aufgabe des IT-Sicherheitsmanagements.

Analog zu den Gefährdungen sind die Maßnahmen in die Maßnahmenkataloge Infrastruktur, Organisation, Personal, Hard- und Software, Kommunikation und Notfallvorsorge gruppiert. Wie bei den Gefährdungen wird hier ebenfalls nur auf die entsprechende Maßnahme referenziert. Hier ein Beispiel für das Zitat einer empfohlenen Maßnahme innerhalb eines Bausteins:

- M 1.15 (A) Geschlossene Fenster und Türen

Im Kürzel M x.y bezeichnet "M" eine Maßnahme, die Zahl x vor dem Punkt den Maßnahmenkatalog (hier M 1 = Infrastruktur). Die Zahl y nach dem Punkt ist die laufende Nummer der Maßnahme innerhalb des jeweiligen Katalogs.

Mit dem Buchstaben in Klammern - hier (A) - wird zu jeder Maßnahme die Qualifizierungsstufe angegeben, also eine Einstufung, ob diese Maßnahme für die IT-Grundschutz-Qualifizierung gefordert wird. Folgende Einstufungen sind vorgesehen:

A (Einstieg)	Diese Maßnahmen müssen für alle drei Ausprägungen der Qualifizierung nach IT-Grundschutz (Auditor-Testat "IT-Grundschutz Einstiegsstufe", Auditor-Testat "IT-Grundschutz Aufbaustufe" und ISO 27001-Zertifikat auf Basis von IT-Grundschutz) umgesetzt sein. Diese Maßnahmen sind essentiell für die Sicherheit innerhalb des betrachteten Bausteins. Sie sind vorrangig umzusetzen.
B (Aufbau)	Diese Maßnahmen müssen für das Auditor-Testat "IT-Grundschutz Aufbaustufe" und für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz umgesetzt sein. Sie sind besonders wichtig für den Aufbau einer kontrollierbaren IT-Sicherheit. Eine zügige Realisierung ist anzustreben.
C (Zertifikat)	Diese Maßnahmen müssen für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz umgesetzt sein. Sie sind wichtig für die Abrundung der IT-Sicherheit. Bei Engpässen können sie zeitlich nachrangig umgesetzt werden.
Z (zusätzlich)	Diese Maßnahmen müssen weder für ein Auditor-Testat noch für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz verbindlich umgesetzt werden. Sie stellen Ergänzungen dar, die vor allem bei höheren Sicherheitsanforderungen hilfreich sein können.

Um ein IT-Sicherheitskonzept nach IT-Grundschutz erstellen und den dabei notwendigen Soll-Ist-Vergleich durchführen zu können, ist es erforderlich, die Texte zu den jeweils in den identifizierten Bausteinen enthaltenen Maßnahmen im jeweiligen Maßnahmenkatalog sorgfältig zu lesen. Als Beispiel sei hier ein Auszug aus einer Maßnahme zitiert:

M 2.11 Regelung des Passwortgebrauchs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Benutzer

[Maßnahmentext ...]

Ergänzende Kontrollfragen:

- Sind die Benutzer über den korrekten Umgang mit Passwörtern unterrichtet worden?

[...]

Die Maßnahmentexte sind sinngemäß umzusetzen. Sie sind so geschrieben, dass sie auf möglichst viele Bereiche angewendet werden können. Bevor die Maßnahmenempfehlungen umgesetzt werden, ist immer zu überlegen, ob sie für die jeweilige Organisation oder IT-Umgebungen angepasst werden müssen. Alle Änderungen sollten dokumentiert werden, damit die Gründe auch später noch nachvollziehbar sind.

Neben der eigentlichen Empfehlung, wie die einzelnen Maßnahmen umzusetzen sind, werden Verantwortliche beispielhaft genannt. *Verantwortlich für die Initiierung* bezeichnet die Personen oder Rollen, die die Umsetzung einer Maßnahme typischerweise veranlassen sollten. *Verantwortlich für die Umsetzung* bezeichnet die Personen oder Rollen, die die Maßnahme realisieren sollten.

Weiterhin werden ergänzende Kontrollfragen angeführt, die das behandelte Thema abrunden und nochmals einen kritischen Blick auf die Umsetzung der Maßnahmen bewirken sollen. Diese ergänzenden Kontrollfragen erheben dabei jedoch keinen Anspruch auf Vollständigkeit.

Der Zusammenhang zwischen den für den IT-Grundschutz angenommenen Gefährdungen und den empfohlenen Maßnahmen kann den Maßnahmen-Gefährdungstabellen entnommen werden. Diese finden sich auf den Grundschutz-Seiten der BSI-Webseite. Für jeden Baustein gibt es eine Maßnahmen-Gefährdungstabelle.

Als Beispiel sei ein Auszug aus der Maßnahmen-Gefährdungstabelle für den Baustein B 2.10 *Mobiler Arbeitsplatz* angeführt:

Priorität/Siegel			G 1. 15	G 2. 1	G 2. 4	G 2. 47	G 2. 48	G 3. 3	G 3. 43	G 3. 44	G 5. 1	G 5. 2	G 5. 4	G 5. 71
M 1.15	1	A									X		X	
M 1.23	1	A									X		X	
M 1.45	1	A				X	X					X	X	X
M 1.46	1	Z											X	
M 1.61	1	A	X					X			X		X	X

Alle Tabellen haben einen einheitlichen Aufbau. In der Kopfzeile sind die im dazugehörigen Baustein aufgelisteten Gefährdungen mit ihren Nummern eingetragen. In der ersten Spalte finden sich entsprechend die Nummern der Maßnahmen wieder. In der zweiten Spalte ist eingetragen, welche Priorität die einzelne Maßnahme für den betrachteten Baustein besitzt. In der dritten Spalte ist notiert, welche Einstufung bezüglich einer Grundschutz-Qualifizierung die einzelne Maßnahme für den betrachteten Baustein besitzt.

Die übrigen Spalten beschreiben den Zusammenhang zwischen Maßnahmen und Gefährdungen. Ist in einem Feld ein "X" eingetragen, so bedeutet dies, dass die korrespondierende Maßnahme gegen die entsprechende Gefährdung wirksam ist. Diese Wirkung kann schadensvorbeugender oder schadensmindernder Natur sein.

Zu beachten ist, dass in den Maßnahmen-Gefährdungstabellen nur die wichtigsten Gefährdungen angeführt sind, gegen die eine bestimmte Maßnahme wirkt. Dies bedeutet insbesondere, dass eine Maßnahme nicht automatisch überflüssig wird, wenn alle in der Tabelle zugeordneten Gefährdungen in einem bestimmten Anwendungsfall nicht relevant sind. Ob auf eine Standard-Sicherheitsmaßnahme verzichtet werden kann, muss immer im Einzelfall anhand der vollständigen Sicherheitskonzeption und nicht nur anhand der Maßnahmen-Gefährdungstabelle geprüft und dokumentiert werden.

Abschließend sei erwähnt, dass sämtliche Bausteine, Gefährdungen, Maßnahmen, Tabellen und Hilfsmittel in elektronischer Form verfügbar sind. Diese Texte können bei der Erstellung eines IT-Sicherheitskonzeptes und bei der Realisierung von Maßnahmen weiterverwendet werden.

1.4 Anwendungsweisen der IT-Grundschutz-Kataloge

Für die erfolgreiche Etablierung eines kontinuierlichen und effektiven IT-Sicherheitsprozesses müssen eine ganze Reihe von Aktionen durchgeführt werden. Hierfür bieten die IT-Grundschutz-Vorgehensweise (siehe BSI-Standard 100-2) sowie die IT-Grundschutz-Kataloge Hinweise zur Methodik und praktische Umsetzungshilfen. Enthalten sind ferner Lösungsansätze für verschiedene, die IT-Sicherheit betreffende Aufgabenstellungen, beispielsweise IT-Sicherheitskonzeption, Revision und Zertifizierung. Je nach vorliegender Aufgabenstellung sind dabei unterschiedliche Anwendungsweisen des IT-Grundschutzes zweckmäßig. Dieser Abschnitt dient dazu, durch Querverweise auf die entsprechenden Kapitel der IT-Grundschutz-Vorgehensweise im BSI-Standard 100-2 den direkten Einstieg in die einzelnen Anwendungsweisen zu erleichtern.

IT-Sicherheitsprozess und IT-Sicherheitsmanagement

Die Abhängigkeit vom ordnungsgemäßen Funktionieren der Informationstechnik hat in den letzten Jahren sowohl in der öffentlichen Verwaltung als auch in der Privatwirtschaft stark zugenommen. Immer mehr Geschäftsprozesse werden auf die Informationstechnik verlagert oder mit ihr verzahnt. Ein Ende dieser Entwicklung ist nicht abzusehen. IT-Sicherheit ist daher als integraler Bestandteil der originären Aufgabe anzusehen. Der folgende Aktionsplan beinhaltet alle wesentlichen Schritte, die für einen kontinuierlichen IT-Sicherheitsprozess notwendig sind, und ist somit als eine planmäßig anzuwendende, begründete Vorgehensweise zu verstehen, wie ein angemessenes IT-Sicherheitsniveau erreicht und aufrechterhalten werden kann:

- Initiierung des IT-Sicherheitsprozesses
  - Übernahme der Verantwortung durch die Leitungsebene
  - Konzeption und Planung des IT-Sicherheitsprozesses
  - Erstellung der IT-Sicherheitsleitlinie
  - Aufbau einer geeigneten Organisationsstruktur für das IT-Sicherheitsmanagement
  - Bereitstellung von finanziellen, personellen und zeitlichen Ressourcen
- Erstellung einer IT-Sicherheitskonzeption
- Umsetzung der IT-Sicherheitskonzeption
  - Realisierung der IT-Sicherheitsmaßnahmen
  - Einbindung aller Mitarbeiter in den IT-Sicherheitsprozess
- Aufrechterhaltung der IT-Sicherheit im laufenden Betrieb und kontinuierliche Verbesserung

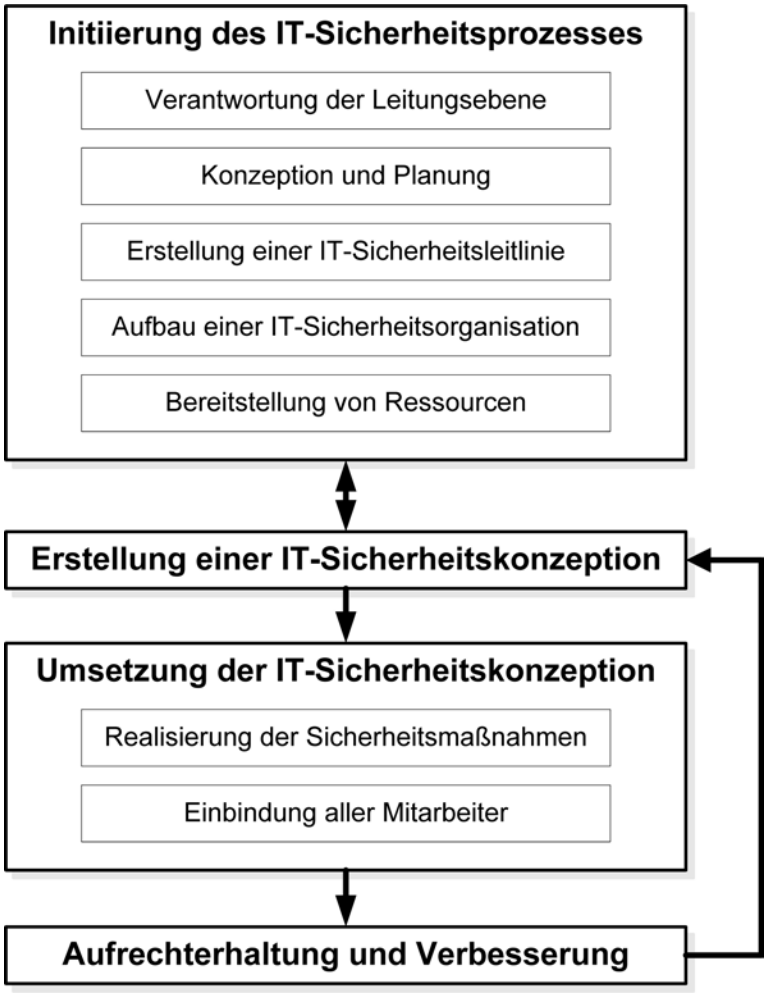


Abbildung: Initiierung des IT-Sicherheitsprozesses

Im Dokument IT-Grundschutz-Vorgehensweise wird dies ausführlich beschrieben. Außerdem wird im Baustein B 1.0 *IT-Sicherheitsmanagement* der IT-Sicherheitsprozess im Überblick dargestellt und es wird eine detaillierte Erläuterung der einzelnen Aktionen in Form empfohlener Standard-Maßnahmen gegeben.

Zur Erstellung der IT-Sicherheitskonzeption ist nach IT-Grundschutz eine Reihe von Schritten notwendig. Eine kurze Darstellung davon wird im Folgenden gegeben.

IT-Strukturanalyse

Unter einem IT-Verbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein IT-Verbund kann dabei als Ausprägung die gesamte IT einer Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungsnetz) oder gemeinsame Geschäftsprozesse bzw. IT-Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

Für die Erstellung eines IT-Sicherheitskonzepts und insbesondere für die Anwendung von IT-Grundschutz ist es erforderlich, die Struktur der vorliegenden Informationstechnik zu analysieren und zu dokumentieren. Aufgrund der heute üblichen starken Vernetzung von IT-Systemen bietet sich ein

Netztopologieplan als Ausgangsbasis für die Analyse an. Die folgenden Aspekte müssen berücksichtigt werden:

- die vorhandene Infrastruktur,
- die organisatorischen und personellen Rahmenbedingungen für den IT-Verbund,
- im IT-Verbund eingesetzte vernetzte und nicht-vernetzte IT-Systeme,
- die Kommunikationsverbindungen zwischen den IT-Systemen und nach außen,
- im IT-Verbund betriebene IT-Anwendungen.

Die einzelnen Schritte der IT-Strukturanalyse werden im Detail in Kapitel 4.1 der IT-Grundschutz-Vorgehensweise (BSI-Standard 100-2) in Form einer Handlungsanweisung beschrieben.

Schutzbedarfsfeststellung

Zweck der Schutzbedarfsfeststellung ist es zu ermitteln, welcher Schutz für die Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien "normal", "hoch" und "sehr hoch". Erläuterungen und praktische Hinweise zur Schutzbedarfsfeststellung sind Gegenstand von Kapitel 4.2 der IT-Grundschutz-Vorgehensweise.

Modellierung

Im nächsten Schritt müssen die Bausteine der IT-Grundschutz-Kataloge in einem Modellierungsschritt auf die Komponenten des vorliegenden IT-Verbunds abgebildet werden.

In Kapitel 4.3 der IT-Grundschutz-Vorgehensweise wird beschrieben, wie die Modellierung eines IT-Verbunds durch Bausteine aus den IT-Grundschutz-Katalogen vorgenommen werden sollte. Detaillierte Hinweise für die Verwendung des Schichtenmodells und die Modellierung nach IT-Grundschutz sind im Kapitel 2 der IT-Grundschutz-Kataloge enthalten. Wie der anschließende Soll-Ist-Vergleich anhand eines Basis-Sicherheitschecks durchgeführt werden sollte, wird in Kapitel 4.4 der IT-Grundschutz-Vorgehensweise beschrieben.

Basis-Sicherheitscheck

Der Basis-Sicherheitscheck ist ein Organisationsinstrument, welches einen schnellen Überblick über das vorhandene IT-Sicherheitsniveau bietet. Mit Hilfe von Interviews wird der Status Quo eines bestehenden (nach IT-Grundschutz modellierten) IT-Verbunds in Bezug auf den Umsetzungsgrad von Sicherheitsmaßnahmen der IT-Grundschutz-Kataloge ermittelt. Als Ergebnis liegt eine Übersicht vor, in dem für jede relevante Maßnahme der Umsetzungsstatus "entbehrlich", "ja", "teilweise" oder "nein" erfasst ist. Durch die Identifizierung von noch nicht oder nur teilweise umgesetzten Maßnahmen werden Verbesserungsmöglichkeiten für die Sicherheit der betrachteten Informationstechnik aufgezeigt. Kapitel 4.4 des BSI-Standards 100-2 beschreibt einen Aktionsplan für die Durchführung eines Basis-Sicherheitschecks. Dabei wird sowohl den organisatorischen Aspekten als auch den fachlichen Anforderungen bei der Projektdurchführung Rechnung getragen.

IT-Sicherheitsrevision

Die in den IT-Grundschutz-Katalogen enthaltenen Sicherheitsmaßnahmen können auch für die IT-Sicherheitsrevision genutzt werden. Hierzu wird die gleiche Vorgehensweise wie beim Basis-Sicherheitscheck empfohlen. Hilfreich und arbeitsökonomisch ist es, für jeden Baustein anhand der Maßnahmentexte eine speziell auf die eigene Institution angepasste Checkliste zu erstellen. Dies erleichtert die Revision und verbessert häufig die Reproduzierbarkeit der Ergebnisse.

Weiterführende IT-Sicherheitsmaßnahmen

Die Standard-Sicherheitsmaßnahmen nach IT-Grundschutz bieten im Normalfall einen angemessenen und ausreichenden Schutz. Insbesondere bei hohem oder sehr hohem Schutzbedarf kann es jedoch sinnvoll sein zu prüfen, ob zusätzlich oder ersatzweise höherwertige IT-Sicherheitsmaßnahmen erforderlich sind. Geeignete Maßnahmen für Bereiche mit höherem Schutzbedarf sollten über ergänzende Sicherheitsanalysen bzw. Risikoanalysen ausgewählt werden (siehe Kapitel 4.5 des BSI-Standards 100-2). Eine Methode hierfür ist die im BSI-Standard 100-3 "Risikoanalyse auf der Basis von IT-Grundschutz" beschriebene Vorgehensweise.

Umsetzung von IT-Sicherheitskonzepten

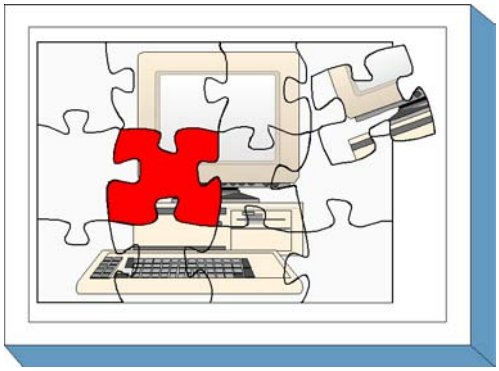
Damit das angestrebte IT-Sicherheitsniveau erreicht wird, müssen bestehende Schwachstellen ermittelt und alle erforderlichen Maßnahmen identifiziert werden. Diese sowie die Realisierungsplanung müssen in einem Sicherheitskonzept festgehalten werden. Vor allem müssen alle erforderlichen Maßnahmen auch konsequent umgesetzt werden. In Kapitel 4.6 des BSI-Standards zur IT-Grundschutz-Vorgehensweise wird beschrieben, was bei der Umsetzungsplanung von IT-Sicherheitsmaßnahmen beachtet werden muss.

Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz

Die Vorgehensweise nach IT-Grundschutz und die IT-Grundschutz-Kataloge werden nicht nur für die IT-Sicherheitskonzeption, sondern auch zunehmend als Referenz im Sinne eines Sicherheitsstandards verwendet. Durch eine Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz kann eine Institution nach innen und außen hin dokumentieren, dass sie sowohl ISO 27001 als auch IT-Grundschutz in der erforderlichen Tiefe umgesetzt hat.

Das Niveau der Qualifizierung wird dabei in drei verschiedene Stufen unterteilt, die sich sowohl im Hinblick auf die Güte (d. h. den erforderlichen Umsetzungsgrad der Sicherheitsmaßnahmen) als auch in Bezug auf die Vertrauenswürdigkeit unterscheiden. Das Eingangsniveau kann durch einen lizenzierten Auditor nachgewiesen werden, das höchste Niveau erfordert zusätzlich eine Prüfung durch eine Zertifizierungsstelle. Das Prüfungsschema für Zertifizierungen nach ISO 27001 auf Basis von IT-Grundschutz sowie das entsprechende Lizenzierungsschema für Auditoren sind auf dem Webserver des BSI erhältlich.

2 Schichtenmodell und Modellierung



2.1 Modellierung nach IT-Grundschutz

Bei der Umsetzung von IT-Grundschutz muss der betrachtete IT-Verbund mit Hilfe der vorhandenen Bausteine nachgebildet werden, also die relevanten Sicherheitsmaßnahmen aus den IT-Grundschutz-Katalogen zusammengetragen werden. Dafür müssen die IT-Strukturanalyse und eine Schutzbedarfsfeststellung vorliegen. Darauf aufbauend wird ein IT-Grundschutzmodell des IT-Verbunds erstellt, das aus verschiedenen, gegebenenfalls auch mehrfach verwendeten IT-Grundschutz-Bausteinen besteht und eine Abbildung zwischen den Bausteinen und den sicherheitsrelevanten Aspekten des IT-Verbunds beinhaltet.

Das erstellte IT-Grundschutzmodell ist unabhängig davon, ob der IT-Verbund aus bereits im Einsatz befindlichen IT-Systemen besteht oder ob es sich um einen IT-Verbund handelt, der sich erst im Planungsstadium befindet. Jedoch kann das Modell unterschiedlich verwendet werden:

- Das IT-Grundschutzmodell eines bereits realisierten IT-Verbunds identifiziert über die verwendeten Bausteine die relevanten Standard-Sicherheitsmaßnahmen. Es kann in Form eines **Prüfplans** benutzt werden, um einen Soll-Ist-Vergleich durchzuführen.
- Das IT-Grundschutzmodell eines geplanten IT-Verbunds stellt hingegen ein **Entwicklungskonzept** dar. Es beschreibt über die ausgewählten Bausteine, welche Standard-Sicherheitsmaßnahmen bei der Realisierung des IT-Verbunds umgesetzt werden müssen.

Die Einordnung der Modellierung und die möglichen Ergebnisse verdeutlicht das folgende Bild:

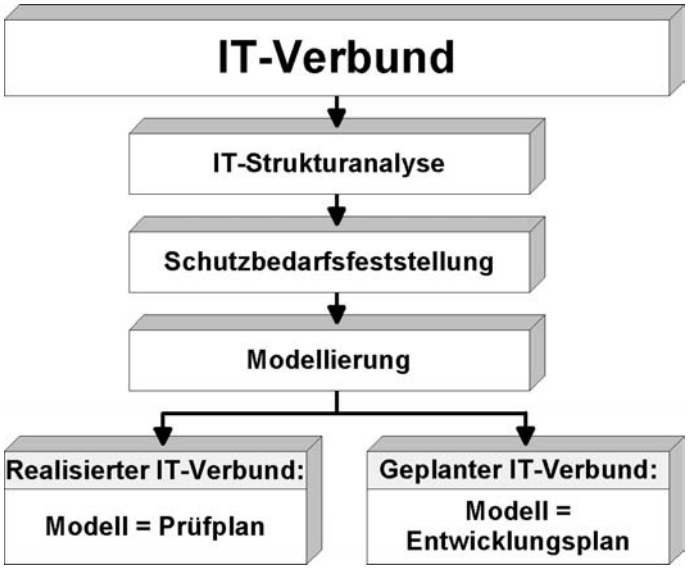


Abbildung: Ergebnis der Modellierung nach IT-Grundschutz

Typischerweise wird ein im Einsatz befindlicher IT-Verbund sowohl realisierte als auch in Planung befindliche Anteile besitzen. Das resultierende IT-Grundschutzmodell beinhaltet dann sowohl einen Prüfplan wie auch Anteile eines Entwicklungskonzepts.

Für die Abbildung eines im Allgemeinen komplexen IT-Verbunds auf die Bausteine der IT-Grundschutz-Kataloge bietet es sich an, die IT-Sicherheitsaspekte gruppiert nach bestimmten Themen zu betrachten.

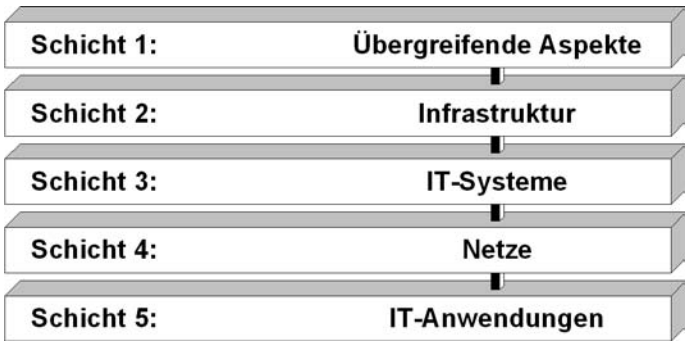


Abbildung: Schichten des IT-Grundschutzmodells

Die IT-Sicherheitsaspekte eines IT-Verbunds werden wie folgt den einzelnen Schichten zugeordnet:

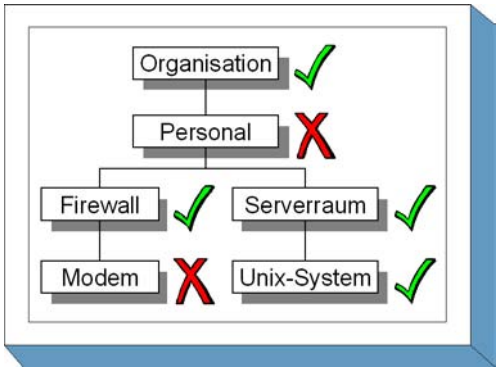
- **Schicht 1** umfasst die übergreifenden IT-Sicherheitsaspekte, die für sämtliche oder große Teile des IT-Verbunds gleichermaßen gelten. Dies betrifft insbesondere übergreifende Konzepte und die daraus abgeleiteten Regelungen. Typische Bausteine der Schicht 1 sind unter anderem IT-Sicherheitsmanagement, Organisation, Datensicherungskonzept und Computer-Virenschutzkonzept.
- **Schicht 2** befasst sich mit den baulich-physischen Gegebenheiten. In dieser Schicht werden Aspekte der infrastrukturellen Sicherheit zusammengeführt. Dies betrifft zum Beispiel die Bausteine Gebäude, Serverraum, Schutzschrank und häuslicher Arbeitsplatz.
- **Schicht 3** betrifft die einzelnen IT-Systeme des IT-Verbunds, die gegebenenfalls in Gruppen zusammengefasst wurden. Hier werden die IT-Sicherheitsaspekte sowohl von Clients als auch von Servern, aber auch von Einzelplatz-Systemen behandelt. In diese Schicht fallen beispielsweise die Bausteine TK-Anlage, Laptop sowie Client unter Windows 2000.
- **Schicht 4** betrachtet die Vernetzungsaspekte, die sich in erster Linie nicht auf bestimmte IT-Systeme, sondern auf die Netzverbindungen und die Kommunikation beziehen. Dazu gehören zum Beispiel die Bausteine Heterogene Netze, Modem sowie Remote Access.
- **Schicht 5** schließlich beschäftigt sich mit den eigentlichen IT-Anwendungen, die im IT-Verbund genutzt werden. In dieser Schicht können unter anderem die Bausteine E-Mail, Webserver, Faxserver und Datenbanken zur Modellierung verwendet werden.

Die Aufgabenstellung bei der Modellierung nach IT-Grundschutz besteht nun darin, für die Bausteine einer jeden Schicht zu entscheiden, ob und wie sie zur Abbildung des IT-Verbunds herangezogen werden können. Je nach betrachtetem Baustein können die Zielobjekte dieser Abbildung von unterschiedlicher Art sein: einzelne Geschäftsprozesse oder Komponenten, Gruppen von Komponenten, Gebäude, Liegenschaften, Organisationseinheiten, usw.

Nachfolgend wird die Vorgehensweise der Modellierung für einen IT-Verbund detailliert beschrieben. Dabei wird besonderer Wert auf die Randbedingungen gelegt, wann ein einzelner Baustein sinnvollerweise eingesetzt werden soll und auf welche Zielobjekte er anzuwenden ist.

Bei der Modellierung eines IT-Verbunds nach IT-Grundschutz kann das Problem auftreten, dass es Zielobjekte gibt, die mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet werden können. In diesem Fall sollte eine ergänzenden Sicherheitsanalyse durchgeführt werden, wie in der IT-Grundschutz-Vorgehensweise beschrieben.

2.2 Zuordnung anhand Schichtenmodell



Bei der Modellierung eines IT-Verbunds ist es zweckmäßig, die Zuordnung der Bausteine anhand des Schichtenmodells vorzunehmen. Daran anschließend folgt schließlich die Vollständigkeitsprüfung.

zu Schicht 1: Übergeordnete Aspekte der IT-Sicherheit

In dieser Schicht werden alle Aspekte des IT-Verbunds modelliert, die den technischen Komponenten übergeordnet sind. Im Vordergrund stehen dabei Konzepte und die von diesen Konzepten abgeleiteten Regelungen. Diese Aspekte sollten für den gesamten IT-Verbund einheitlich geregelt sein, so dass die entsprechenden Bausteine in den meisten Fällen nur einmal für den gesamten IT-Verbund anzuwenden sind. Dem IT-Sicherheitsmanagement, der Organisation des IT-Betriebs sowie der Schulung und Sensibilisierung des Personals kommt dabei eine besondere Bedeutung zu. Die Umsetzung der diesbezüglichen Maßnahmen ist von grundlegender Bedeutung für die sichere Nutzung von Informations- und Kommunikationstechnik. Unabhängig von den eingesetzten technischen Komponenten sind die entsprechenden Bausteine daher immer anzuwenden.

- Der Baustein B 1.0 *IT-Sicherheitsmanagement* ist für den gesamten IT-Verbund einmal anzuwenden. Ein funktionierendes IT-Sicherheitsmanagement ist die wesentliche Grundlage für die Erreichung eines angemessenen Sicherheitsniveaus. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.1 *Organisation* muss für jeden IT-Verbund mindestens einmal herangezogen werden. Wenn Teile des vorliegenden IT-Verbunds einer anderen Organisation(-seinheit) zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Organisation(-seinheit) getrennt angewandt werden. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.2 *Personal* muss für jeden IT-Verbund mindestens einmal herangezogen werden. Wenn Teile des vorliegenden IT-Verbunds einer anderen Organisation(-seinheit) zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Organisation(-seinheit) getrennt angewandt werden. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.3 *Notfallvorsorge-Konzept* ist zumindest dann anzuwenden, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert wurden, die einen hohen oder sehr hohen Schutzbedarf in Bezug auf Verfügbarkeit haben oder wenn größere IT-Systeme bzw. umfangreiche Netze betrieben werden. Bei der Bearbeitung des Bausteins ist besonderes Augenmerk auf diese Komponenten zu richten. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.4 *Datensicherungskonzept* ist für den gesamten IT-Verbund einmal anzuwenden.
- Der Baustein B 1.6 *Computer-Virenschutzkonzept* ist für den gesamten IT-Verbund einmal anzuwenden.

- Der Baustein B 1.7 *Kryptokonzept* ist zumindest dann anzuwenden, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert wurden, die einen hohen oder sehr hohen Schutzbedarf in Bezug auf Vertraulichkeit oder Integrität haben, oder wenn bereits kryptographische Verfahren im Einsatz sind.
- Der Baustein B 1.8 *Behandlung von Sicherheitsvorfällen* ist zumindest dann anzuwenden, wenn in der Schutzbedarfsfeststellung Komponenten identifiziert wurden, die einen hohen oder sehr hohen Schutzbedarf in Bezug auf einen der drei Grundwerte haben, oder wenn der Ausfall des gesamten IT-Verbunds einen Schaden in den Kategorien hoch oder sehr hoch zur Folge hat. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.9 *Hard- und Software-Management* muss für jeden IT-Verbund mindestens einmal herangezogen werden. Wenn Teile des vorliegenden IT-Verbunds einer anderen Organisation(-seinheit) zugeordnet sind und daher anderen Rahmenbedingungen unterliegen, sollte der Baustein auf jede Organisation(-seinheit) getrennt angewandt werden. Im Fall von Outsourcing gelten für die Anwendung dieses Bausteins besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.10 *Standardsoftware* ist zumindest einmal für den gesamten IT-Verbund anzuwenden. Gibt es innerhalb des IT-Verbunds Teilbereiche mit unterschiedlichen Anforderungen oder Regelungen für die Nutzung von Standardsoftware, sollte Baustein B 1.10 auf diese Teilbereiche jeweils getrennt angewandt werden.
- Der Baustein B 1.11 *Outsourcing* ist zumindest dann anzuwenden, wenn die folgenden Bedingungen alle erfüllt sind:
  - IT-Systeme, Anwendungen oder Geschäftsprozesse werden zu einem externen Dienstleister ausgelagert, und
  - die Bindung an den Dienstleister erfolgt auf längere Zeit, und
  - durch die Dienstleistung kann die IT-Sicherheit des Auftraggebers beeinflusst werden, und
  - im Rahmen der Dienstleistungen erbringt der Dienstleister auch regelmäßig nennenswerte IT-Sicherheitsmanagement-Tätigkeiten.

  Gibt es in einem IT-Verbund verschiedene ausgelagerte Komponenten bei unterschiedlichen Dienstleistern, ist der Baustein für jeden externen Dienstleister einmal anzuwenden. Für die Anwendung dieses Bausteins gelten besondere Regeln, die im BSI-Dokument "IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten" aufgeführt sind.
- Der Baustein B 1.12 *Archivierung* ist auf den IT-Verbund anzuwenden, wenn aufgrund interner oder externer Vorgaben eine Langzeitarchivierung elektronischer Dokumente erforderlich ist oder bereits ein System zur Langzeitarchivierung elektronischer Dokumente betrieben wird.
- Der Baustein B 1.13 *IT-Sicherheitssensibilisierung und -schulung* ist für den gesamten IT-Verbund einmal anzuwenden.

zu Schicht 2: Sicherheit der Infrastruktur

Die für den vorliegenden IT-Verbund relevanten baulichen Gegebenheiten werden mit Hilfe der Bausteine aus Schicht 2 "Sicherheit der Infrastruktur" modelliert. Jedem Gebäude, Raum oder Schutzschrank (bzw. Gruppen dieser Komponenten) wird dabei der entsprechende Baustein aus den IT-Grundschutz-Katalogen zugeordnet.

- Der Baustein B 2.1 *Gebäude* ist für jedes Gebäude bzw. jede Gebäudegruppe ein**m**al anzuwenden.

- Der Baustein B 2.2 *Verkabelung* ist in der Regel einmal pro Gebäude bzw. Gebäudegruppe anzuwenden (zusätzlich zum Baustein B 2.1). Falls bestimmte Teilbereiche - beispielsweise Serverraum oder Leitstand - in Bezug auf die Verkabelung Besonderheiten aufweisen, kann es jedoch zweckmäßig sein, Baustein B 2.2 an diesen Stellen gesondert anzuwenden.
- Der Baustein B 2.3 *Büroraum* ist auf jeden Raum bzw. jede Gruppe von Räumen anzuwenden, in denen Informationstechnik genutzt wird, für die jedoch keiner der Bausteine B 2.4, B 2.5, B 2.6, B 2.8, B 2.9, B 2.10 oder B 2.11 herangezogen wird.
- Der Baustein B 2.4 *Serverraum* ist auf jeden Raum bzw. jede Gruppe von Räumen anzuwenden, in denen Server oder TK-Anlagen betrieben werden. Server sind IT-Systeme, die Dienste im Netz zur Verfügung stellen. Für Räumlichkeiten, auf die der Baustein B 2.9 angewandt wird, muss nicht zusätzlich der Baustein B 2.4 herangezogen werden.
- Der Baustein B 2.5 *Datenträgerarchiv* ist auf jeden Raum bzw. jede Gruppe von Räumen anzuwenden, in denen Datenträger gelagert oder archiviert werden.
- Der Baustein B 2.6 *Raum für technische Infrastruktur* ist auf jeden Raum bzw. jede Gruppe von Räumen anzuwenden, in denen technische Geräte betrieben werden, die keine oder nur wenig Bedienung erfordern (z. B. Verteilerschrank, Netzersatzanlage).
- Der Baustein B 2.7 *Schutzschränke* ist auf jeden Schutzschrank bzw. jede Gruppe von Schutzschränken einmal anzuwenden. Schutzschränke können gegebenenfalls als Ersatz für einen dedizierten Serverraum dienen.
- Der Baustein B 2.8 *Häuslicher Arbeitsplatz* ist auf jeden häuslichen Arbeitsplatz bzw. jede Gruppe (falls entsprechende Gruppen definiert wurden) einmal anzuwenden.
- Der Baustein B 2.9 *Rechenzentrum* ist auf jedes Rechenzentrum einmal anzuwenden. Als Rechenzentrum werden Einrichtungen und Räumlichkeiten bezeichnet, die für den Betrieb einer größeren, zentral für mehrere Stellen eingesetzten Datenverarbeitungsanlage erforderlich sind. Für Räumlichkeiten, auf die der Baustein B 2.9 angewandt wird, muss nicht zusätzlich der Baustein B 2.4 herangezogen werden.
- Der Baustein B 2.10 *Mobiler Arbeitsplatz* ist immer dann anzuwenden, wenn Mitarbeiter häufig nicht mehr nur innerhalb der Räumlichkeiten des Unternehmens bzw. der Behörde arbeiten, sondern an wechselnden Arbeitsplätzen außerhalb. Typische Zielobjekte für den Baustein B 2.10 sind Laptops.
- Der Baustein B 2.11 *Besprechungs-, Veranstaltungs- und Schulungsräume* ist auf jeden solchen Raum bzw. jede Gruppe (falls entsprechende Gruppen definiert wurden) einmal anzuwenden.

zu Schicht 3: Sicherheit der IT-Systeme

Sicherheitsaspekte, die sich auf IT-Systeme beziehen, werden in dieser Schicht abgedeckt. Diese Schicht ist zur Übersichtlichkeit nach Servern, Clients, Netzkomponenten und Sonstiges sortiert.

Analog zum Bereich "Sicherheit der Infrastruktur" können die Bausteine des Bereichs "Sicherheit der IT-Systeme" sowohl auf einzelne IT-Systeme als auch auf Gruppen solcher IT-Systeme angewandt werden. Dies wird im Folgenden nicht mehr gesondert hervorgehoben.

Server

- Der Baustein B 3.101 *Allgemeiner Server* ist auf jedes IT-System anzuwenden, das Dienste (z. B. Datei- oder Druckdienste) als Server im Netz anbietet.

- Der Baustein B 3.102 *Server unter Unix* ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.103 *Server unter Windows NT* ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.104 *Server unter Novell Netware 3.x* ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.105 *Server unter Novell Netware Version 4.x* ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.106 *Server unter Windows 2000* ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.107 *S/390- und zSeries-Mainframe* ist auf jeden Großrechner anzuwenden, der vom Typ S/390 oder zSeries ist.
- Der Baustein B 3.108 *Windows Server 2003* ist auf jeden Server anzuwenden, der mit diesem Betriebssystem arbeitet.

Hinweis: Für jeden Server (und auch jeden Großrechner) muss neben dem Betriebssystem-spezifischen Baustein immer auch Baustein B 3.101 angewandt werden, da in diesem Baustein die plattformunabhängigen Sicherheitsaspekte für Server zusammengefasst sind.

Clients

- Der Baustein B 3.201 *Allgemeiner Client* ist auf jeden Client anzuwenden. Clients sind Arbeitsplatz-Computer, die regelmäßig oder zumindest zeitweise in einem Netz betrieben werden (im Gegensatz zu Einzelplatz-Systemen).
- Der Baustein B 3.202 *Allgemeines nicht vernetztes IT-System* ist auf jedes Einzelplatz-System anzuwenden. Einzelplatz-Systeme sind Arbeitsplatz-Computer, die gar nicht oder nur in Ausnahmefällen in einem Netz betrieben werden (im Gegensatz zu Clients).
- Der Baustein B 3.203 *Laptop* ist auf jeden mobilen Computer (Laptop) anzuwenden.
- Der Baustein B 3.204 *Client unter Unix* ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.205 *Client unter Windows NT* ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.206 *Client unter Windows 95* ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.207 *Client unter Windows 2000* ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.
- Der Baustein B 3.208 *Internet-PC* ist auf jeden Computer anzuwenden, der *ausschließlich* für die Nutzung von Internet-Diensten vorgesehen ist und *nicht* mit dem internen Netz der Institution verbunden ist. In diesem speziellen Szenario brauchen *keine weiteren Bausteine* der IT-Grundschutz-Kataloge auf diesen Computer (bzw. diese Gruppe) angewandt werden.
- Der Baustein B 3.209 *Client unter Windows XP* ist auf jeden Einzelplatz-Rechner oder Client anzuwenden, der mit diesem Betriebssystem arbeitet.

Hinweis: Für jeden Client muss neben dem Betriebssystem-spezifischen Baustein immer auch entweder Baustein B 3.201 oder Baustein B 3.202 angewandt werden, da in diesen Bausteinen die plattformunabhängigen Sicherheitsaspekte für Clients zusammengefasst sind.

Netzkomponenten

- Der Baustein B 3.301 *Sicherheitsgateway (Firewall)* ist immer anzuwenden, wenn unterschiedlich vertrauenswürdige Netze gekoppelt werden. Ein typischer Anwendungsfall ist die Absicherung einer Außenverbindung (z. B. beim Übergang eines internen Netzes zum Internet oder bei Anbindungen zu Netzen von Geschäftspartnern). Aber auch bei einer Kopplung von zwei organisationsinternen Netzen mit unterschiedlich hohem Schutzbedarf ist der Baustein anzuwenden, z. B. bei der Trennung des Bürokommunikationsnetzes vom Netz der Entwicklungsabteilung, wenn dort besonders vertrauliche Daten verarbeitet werden.
- Der Baustein B 3.302 *Router und Switches* ist in jedem aktiven Netz, das im vorliegenden IT-Verbund eingesetzt wird, anzuwenden.
- Der Baustein B 3.303 *Speichersysteme und Speichernetze* ist immer dann anzuwenden, wenn für die Datenspeicherung dedizierte Speichersysteme eingesetzt werden. Typische Zielobjekte für diesen Baustein sind NAS-Systeme (Network Attached Storage) und SAN-Systeme (Storage Area Networks).

Sonstiges

- Der Baustein B 3.401 *TK-Anlage* ist auf jede **TK-Anlage** bzw. auf jede entsprechende Gruppe anzuwenden.
- Der Baustein B 3.402 *Faxgerät* ist auf jedes **Faxgerät** bzw. auf jede entsprechende Gruppe anzuwenden.
- Der Baustein B 3.403 *Anrufbeantworter* ist auf jeden **Anrufbeantworter** bzw. auf jede entsprechende Gruppe anzuwenden.
- Der Baustein B 3.404 *Mobiltelefon* sollte mindestens einmal angewandt werden, wenn die Benutzung von Mobiltelefonen in der betrachteten Organisation(-seinheit) nicht grundsätzlich untersagt ist.

  Bestehen mehrere unterschiedliche Einsatzbereiche von Mobiltelefonen (beispielsweise mehrere Mobiltelefon-Pools), so ist der Baustein B 3.404 jeweils getrennt darauf anzuwenden.
- Der Baustein B 3.405 *PDA* sollte mindestens einmal angewandt werden, wenn die Benutzung von PDAs in der betrachteten Organisation(-seinheit) nicht grundsätzlich untersagt ist. Der Baustein B 3.201 *Allgemeiner Client* muss hier nicht zusätzlich angewandt werden.

zu Schicht 4: Sicherheit im Netz

In dieser Schicht werden Sicherheitsaspekte im Netz behandelt, die nicht an bestimmten IT-Systemen (z. B. Servern) festgemacht werden können. Vielmehr geht es um Sicherheitsaspekte, die sich auf die Netzverbindungen und die Kommunikation zwischen den IT-Systemen beziehen.

Um die Komplexität zu verringern, ist es sinnvoll, bei der Untersuchung statt des Gesamtnetzes Teilbereiche jeweils einzeln zu betrachten. Die hierzu erforderliche Aufteilung des Gesamtnetzes in Teilnetze sollte anhand der beiden folgenden Kriterien vorgenommen werden:

- Im Rahmen der Schutzbedarfsfeststellung sind Verbindungen identifiziert worden, über die bestimmte Daten auf keinen Fall transportiert werden dürfen. Diese Verbindungen bieten sich als

"Schnittstellen" zwischen Teilnetzen an, d. h. die Endpunkte einer solchen Verbindung sollten in verschiedenen Teilnetzen liegen. Umgekehrt sollten Verbindungen, die Daten mit hohem oder sehr hohem Schutzbedarf transportieren, möglichst keine Teilnetzgrenzen überschreiten. Dies führt zu einer Definition von Teilnetzen mit möglichst einheitlichem Schutzbedarf.

- Komponenten, die nur über eine Weitverkehrsverbindung miteinander verbunden sind, sollten nicht demselben Teilnetz zugeordnet werden, d. h. Teilnetze sollten sich nicht über mehrere Standorte oder Liegenschaften erstrecken. Dies ist sowohl aus Gründen der Übersichtlichkeit als auch im Hinblick auf eine effiziente Projektdurchführung wünschenswert.

Falls diese beiden Kriterien nicht zu einer geeigneten Aufteilung des Gesamtnetzes führen (beispielsweise weil einige resultierende Teilnetze zu groß oder zu klein sind), kann die Aufteilung in Teilnetze alternativ auch auf organisatorischer Ebene erfolgen. Dabei werden die Zuständigkeitsbereiche der einzelnen Administratoren(-Teams) als Teilnetze betrachtet.

Es ist nicht möglich, eine grundsätzliche Empfehlung darüber zu geben, welche Aufteilung in Teilnetze zu bevorzugen ist, falls die oben angegebenen Anforderungen mit dem vorliegenden IT-Verbund grundsätzlich nicht vereinbar sind. Stattdessen sollte im Einzelfall entschieden werden, welche Aufteilung des Gesamtnetzes im Hinblick auf die anzuwendenden Bausteine der IT-Grundschutz-Kataloge am praktikabelsten ist.

- Der Baustein B 4.1 *Heterogene Netze* ist in der Regel auf jedes Teilnetz einmal anzuwenden. Falls die Teilnetze klein sind und mehrere Teilnetze in der Zuständigkeit des gleichen Administratoren-Teams liegen, kann es jedoch ausreichend sein, den Baustein B 4.1 auf diese Teilnetze insgesamt einmal anzuwenden.
- Der Baustein B 4.2 *Netz- und Systemmanagement* ist auf jedes Netz- bzw. Systemmanagement-System anzuwenden, das im vorliegenden IT-Verbund eingesetzt wird.
- Der Baustein B 4.3 *Modem* ist auf alle Außenverbindungen anzuwenden, die über Modems realisiert sind.
- Der Baustein B 4.4 *Remote Access* ist pro entfernter Zugriffsmöglichkeit auf das interne Netz, die nicht über eine dedizierte Standleitung erfolgt, einmal anzuwenden (z. B. Telearbeit, Anbindung von Außendienstmitarbeitern über analoge Wählleitungen, ISDN oder Mobiltelefon).
- Der Baustein B 4.5 *LAN-Anbindung eines IT-Systems über ISDN* ist auf alle Außenverbindungen anzuwenden, die über ISDN realisiert sind.
- Der Baustein B 4.6 *WLAN* ist auf alle Kommunikationsnetze anzuwenden, die gemäß der Standard-Reihe IEEE 802.11 und deren Erweiterungen realisiert sind.
- Der Baustein B 4.7 *VoIP (Voice over Internet Protocol)* ist auf alle Kommunikationsnetze anzuwenden, in denen VoIP-Technologie zum Einsatz kommt. Tauschen leitungsvermittelnde TK-Anlagen Informationen untereinander über ein IP-Netz aus, ist der Baustein B 4.7 *VoIP* ebenfalls anzuwenden.

zu Schicht 5: Sicherheit in Anwendungen

In der untersten Schicht des zu modellierenden IT-Verbunds erfolgt die Nachbildung der Anwendungen. Moderne Anwendungen beschränken sich nur selten auf ein einzelnes IT-System. Insbesondere behörden- bzw. unternehmensweite Kernanwendungen sind in der Regel als Client-Server-Applikationen realisiert. In vielen Fällen greifen Server selbst wieder auf andere, nachgeschaltete Server, z. B. Datenbank-Systeme, zu. Die Sicherheit der Anwendungen muss daher unabhängig von den IT-Systemen und Netzen betrachtet werden.

- Der Baustein B 5.1 *Peer-to-Peer-Dienste* ist auf jeden Client anzuwenden, der Peer-to-Peer-Dienste (beispielsweise freigegebene Verzeichnisse) im Netz anbietet.
- Der Baustein B 5.2 *Datenträgeraustausch* sollte für jede Anwendung einmal herangezogen werden, die als Datenquelle für einen Datenträgeraustausch dient oder auf diesem Wege eingegangene Daten weiterverarbeitet.
- Der Baustein B 5.3 *E-Mail* ist auf jedes E-Mail-System (intern oder extern) des betrachteten IT-Verbunds anzuwenden.
- Der Baustein B 5.4 *Webserver* ist auf jeden WWW-Dienst (z. B. Intranet oder Internet) des betrachteten IT-Verbunds anzuwenden.
- Der Baustein B 5.5 *Lotus Notes* ist auf jedes Workgroup-System, das auf dem Produkt Lotus Notes basiert, bzw. auf jede entsprechende Gruppe im IT-Verbund einmal anzuwenden.
- Der Baustein B 5.6 *Faxserver* ist auf jeden Faxserver bzw. auf jede entsprechende Gruppe anzuwenden.
- Der Baustein B 5.7 *Datenbanken* sollte pro Datenbanksystem bzw. pro Gruppe von Datenbanksystemen einmal angewandt werden.
- Der Baustein B 5.8 *Telearbeit* ist zusätzlich auf jedes IT-System anzuwenden, das für Telearbeit verwendet wird.
- Der Baustein B 5.9 *Novell eDirectory* sollte auf jeden Verzeichnisdienst, der mit Hilfe von Novell eDirectory realisiert ist, einmal angewandt werden.
- Der Baustein B 5.10 *Internet Information Server* ist - zusätzlich zu Baustein B 5.4 - auf jeden WWW-Dienst anzuwenden, der mit diesem Produkt betrieben wird.
- Der Baustein B 5.11 *Apache Webserver* ist - zusätzlich zu Baustein B 5.4 - auf jeden WWW-Dienst anzuwenden, der mit diesem Produkt betrieben wird.
- Der Baustein B 5.12 *Exchange 2000 / Outlook 2000* ist - zusätzlich zu Baustein B 5.3 - auf jedes Workgroup- oder E-Mail-System anzuwenden, das auf Microsoft Exchange bzw. Outlook basiert.
- Der Baustein B 5.13 *SAP System* ist auf jede Applikation für Geschäftsprozesse (oder Gruppe solcher Applikationen) anzuwenden, die auf Software des Herstellers SAP basiert.

Prüfung auf Vollständigkeit

Abschließend muss überprüft werden, ob die Modellierung des Gesamtsystems vollständig ist und keine Lücken aufweist. Es wird empfohlen, hierzu erneut den Netzplan oder eine vergleichbare Übersicht über den IT-Verbund heranzuziehen und die einzelnen Komponenten systematisch durchzugehen. Jede Komponente muss entweder einer Gruppe zugeordnet oder einzeln modelliert worden sein.

Falls das Gesamtnetz in der Schicht 4 in Teilnetze aufgeteilt wurde, muss geprüft werden, ob

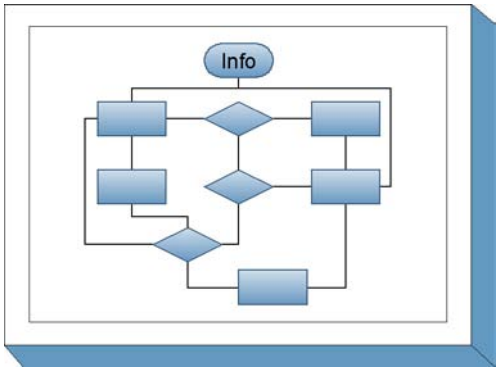
- jedes Teilnetz vollständig nachgebildet wurde und
- durch die Summe aller Teilnetze das Gesamtnetz vollständig dargestellt wird.

Wichtig ist, dass nicht nur alle Hard- und Software-Komponenten in technischer Hinsicht nachgebildet sind, sondern dass auch die zugehörigen organisatorischen, personellen und infrastrukturellen Aspekte vollständig abgedeckt sind.

Falls sich bei der Überprüfung Lücken in der Modellierung zeigen, sind die entsprechenden fehlenden Bausteine hinzuzufügen. Andernfalls besteht die Gefahr, dass wichtige Bestandteile des

Gesamtsystems oder wichtige Sicherheitsaspekte bei der Anwendung des IT-Grundschutzes nicht berücksichtigt werden.

3 Rollen



In den Maßnahmen der IT-Grundschutz-Kataloge werden neben der eigentlichen Empfehlung, wie die einzelnen Maßnahmen umzusetzen sind, Verantwortliche für die Initiierung bzw. für die Umsetzung dieser Maßnahmen beispielhaft genannt. Da die Bezeichnungen der hier als Verantwortliche genannten Personen oder Rollen nicht in allen Organisationen einheitlich sind, wird für eine leichtere Zuordnung in diesem Kapitel eine kurze Beschreibung der wesentlichen Rollen dargestellt.

Verantwortliche	**Rollenbeschreibung**
Administrator	Ein Administrator ist zuständig für Einrichtung, Betrieb, Überwachung und Wartung eines IT-Systems.
Anwendungsentwickler	Ein Anwendungsentwickler ist ein mit der Planung, Entwicklung, Test oder Pflege von Programmen betrauter Experte.
Archivverwalter	Der Archivverwalter ist verantwortlich für Einrichtung, Betrieb, Überwachung und Wartung eines Archivsystems auf fachlicher Ebene.
Bauausführende Firma	Dies sind Firmen, die Bauleistungen aller Art im Auftrag der IT-betreibenden Organisation oder der dazu Beauftragten ausführen. Dies können klassische Baugewerke, Elektrogewerke aber auch die Errichtung von Einrichtungen der Gefahrenmeldetechnik (Errichterfirma) sein.
Bauleiter	Ein Bauleiter ist für die Umsetzung von Baumaßnahmen verantwortlich.
Behörden-/Unternehmensleitung	Dies bezeichnet die Leitungsebene der Institution bzw. der betrachteten Organisationseinheit.
Benutzer	Ein Benutzer ist ein Mitarbeiter des Unternehmens bzw. der Behörde, der informationstechnische Systeme im Rahmen der Erledigung seiner Aufgaben benutzt. IT-Benutzer und Benutzer sind hierbei als Synonyme zu betrachten, da heutzutage nahezu jeder Mitarbeiter eines Unternehmens bzw. einer Behörde informationstechnische Systeme während der Erledigung seiner Aufgaben benutzt.
Beschaffer	Dies bezeichnet einen Mitarbeiter der Beschaffungsstelle, der verantwortlich ist für die Beschaffung von Betriebsmitteln oder IT-Systemen.
Beschaffungsstelle	Die Beschaffungsstelle initiiert und überwacht Beschaffungen. Öffentliche Einrichtungen wickeln ihre Beschaffungen nach vorgeschriebenen Verfahren ab.

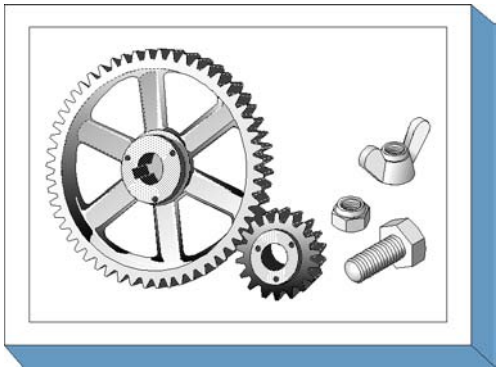
Brandschutzbeauftragter	Ein Brandschutzbeauftragter ist Ansprechpartner und Verantwortlicher in allen Fragen des Brandschutzes. Er ist u. a. zuständig für die Erstellung von Brandrisikoanalysen, Aus- und Fortbildung der Beschäftigten, teilweise auch für Wartung und Instandhaltung der Brandschutzeinrichtungen.
Datenschutzbeauftragter	Ein Datenschutzbeauftragter ist eine von der Behörden- bzw. Unternehmensleitung bestellte Person, die für den datenschutzrechtlich korrekten bzw. gesetzeskonformen Umgang mit personenbezogenen Daten im Unternehmen bzw. in der Behörde verantwortlich ist.
Entwickler	Mit Entwickler wird im Kontext des IT-Grundschutzes eine Person bezeichnet, die Software, Hardware oder ganze Systeme entwirft, die aus mehreren Software- und Hardware-Komponenten bestehen können. In der Software-Entwicklung erfolgt durch ihn typischerweise das Design und die Programmierung, dabei wird eine Programmiersprache eingesetzt. In der Hardware-Entwicklung erfolgt durch den Entwickler das Design, die Herstellung der Hardware wird in der Regel durch einen Hardware-Hersteller geleistet.
Errichterfirma	Es handelt sich hierbei um ein Unternehmen, das Gewerke oder aber auch Gebäude erstellt.
Fachabteilung	Eine Fachabteilung ist ein Teil einer Behörde bzw. eines Unternehmens, welche fachspezifische Aufgaben zu erledigen hat. Bei Bundes- und Landesbehörden ist eine Abteilung die übergeordnetete Organisationsform mehrerer Referate, die inhaltlich zusammengehören.
Fachverantwortliche	Der Fachverantwortliche ist inhaltlich für ein oder mehrere IT-Verfahren verantwortlich (so ist z. B. der Leiter des Referats "Vertrieb" der Fachverantwortliche für die Anwendung "automatisierter Vertrieb").
Fax-Verantwortlicher	Der Fax-Verantwortliche ist für alle organisatorischen und technischen Regelungen verantwortlich, die die Fax-Nutzung innerhalb einer Organisationseinheit betreffen.
Haustechnik	Haustechnik bezeichnet die Organisationseinheit, die für die Einrichtungen der Infrastruktur in einem Gebäude oder in einer Liegenschaft verantwortlich ist. Betreute Gewerke können dabei z. B. sein: Elektrotechnik, Melde- und Steuerungstechnik, Sicherungstechnik, IT-Netze (Physikalischer Teil), Heizungs- und Sanitärtechnik, Aufzüge etc.
Innerer Dienst	Der Innere Dienst ist eine Organisationseinheit, die alle zentralen Dienste für die Mitarbeiter koordiniert, z. B. Poststelle, Kopierer, Fahrdienst, Botendienst, Beseitigung technischer Störungen, Gebäudereinigung, Bereitstellung von Betriebsmitteln etc.
IT-Betreuer	Zu den Aufgaben von IT-Betreuern zählen u. a. die Entgegennahme und Bearbeitung von Benutzeranfragen zu Problemen rund um die IT-Ausstattung.

IT-Sicherheitsbeauftragter	Ein IT-Sicherheitsbeauftragter ist eine von der Behörden- bzw. Unternehmensleitung ernannte Person, die im Auftrag der Leitungsebene die Aufgabe IT-Sicherheit koordiniert und und innerhalb der Behörde bzw. des Unternehmens vorantreibt.
IT-Sicherheitsmanagement	IT-Sicherheitsmanagement ist die Leitungs- und Koordinierungsaufgabe, die für eine angemessene IT-Sicherheit im Unternehmen bzw. in der Behörde sorgt. Dieser Begriff wird jedoch häufig auch für Personen verwendet, die diese Leitungsaufgabe wahrnehmen.
IT-Sicherheitsmanagement-Team	Das IT-Sicherheitsmanagement-Team unterstützt den IT-Sicherheitsbeauftragten, indem es übergreifende Maßnahmen in der Gesamtorganisation koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt.
IT-Verfahrensverantwortlicher	Ein IT-Verfahrensverantwortlicher ist für den korrekten Ablauf eines oder mehrere spezieller IT-Verfahren verantwortlich, z. B. für die elektronische Lagerhaltung, etc.
Leiter Beschaffung	Hiermit ist der Leiter der Beschaffungsstelle oder der Organisationseinheit gemeint, die für die Beschaffung zuständig ist.
Leiter Entwicklung	Dies bezeichnet den Leiter einer Entwicklungsabteilung für Hard- bzw. Software oder den Projektleiter eines Entwicklerteams.
Leiter Fachabteilung	Dies bezeichnet den Leiter einer Fachabteilung.
Leiter Haustechnik	Hiermit ist der Verantwortliche für die Haustechnik gemeint.
Leiter Innerer Dienst	Dies bezeichnet den Leiter des Inneren Dienstes bzw. den Verantwortlichen für die Bereitstellung zentraler Dienste.
Leiter IT	Hiermit ist der Leiter der IT-Abteilung bzw. das für die Informationstechnik zuständige Management gemeint.
Leiter Organisation	Dies bezeichnet den Leiter der Organisationseinheit, die u. a. für Regelung und Überwachung des allgemeinen Betriebs sowie für Planung, Organisation und Durchführung aller Verwaltungsdienstleistungen verantwortlich ist.
Leiter Personal	Hiermit ist der Leiter der Personalabteilung bzw. der für Personalfragen zuständigen Organisationseinheit gemeint.
Mitarbeiter	Ein Mitarbeiter ist Mitglied einer Fachabteilung, einer Behörde oder eines Unternehmens.
Notfall-Verantwortliche	Der Notfall-Verantwortliche ist von der Behörden- bzw. Unternehmensleitung autorisiert darüber zu entscheiden, ob es sich bei einer bestimmten Situation um einen Notfall handelt. Weiterhin ist er für die Einleitung der erforderlichen Notfallmaßnahmen verantwortlich.

Personalabteilung	Die Personalabteilung ist unter Anderem für folgende Aufgaben zuständig: - Personalwirtschaftliche Grundfragen - Personalbedarfsplanung - Personalangelegenheiten der Mitarbeiter - Soziale Betreuung der Mitarbeiter - Allgemeine Zusammenarbeit mit der Personalvertretung
Personalrat/Betriebsrat	Der Personal- bzw. Betriebsrat (Personalvertretung) ist für die Interessenvertretung der Mitarbeiter gegenüber der Behörden- bzw. Unternehmensleitung zuständig.
Planer	Mit dem allgemeinen Begriff "Planer" werden Rollen wie "Netzplaner" und "Bauplaner" zusammengefasst. Gemeint sind also Personen, die verantwortlich sind für die Planung und Konzeption bestimmter Aufgaben.
Poststelle	Die Poststelle ist die Sammelstelle einer Behörde oder eines Unternehmens für ankommende und ausgehende Post. Zu den Aufgabengebieten können auch Fax- und E-Mail-Dienstleistungen sowie das Scannen eingehender Dokumente im Rahmen eines elektronischen Workflows gehören.
Pressestelle	Die Pressestelle ist zuständig für alle ein- und ausgehenden Kontakte zu Presse und Medien. In vielen Fällen werden dort auch Anfragen von Privatpersonen und Firmen bearbeitet.
Revisor	Ein Revisor kontrolliert, ob die geplanten Maßnahmen adäquat umgesetzt wurden.
Telearbeiter	Ein Telearbeiter nimmt seine Tätigkeiten außerhalb der Büroräume des Unternehmens oder der Behörde wahr und verfügt über eine kommunikationstechnische Anbindung an die IT des Arbeit- bzw. Auftraggebers.
Tester	Tester sind Personen, die gemäß eines Testplans nach vorher festgelegten Verfahren und Kriterien eine neue oder veränderte Software bzw. Hardware testen und die Testergebnisse mit den erwarteten Ergebnissen vergleichen.
TK-Anlagen-Verantwortlicher	Der TK-Anlagen-Verantwortliche ist für den ordnungsgemäßen Betrieb der Telekommunikationsanlagen und für entsprechende Regelungen verantwortlich.
Verantwortliche der einzelnen IT-Anwendungen	Der Verantwortliche für die einzelne IT-Anwendung ist nicht nur für den reibungslosen Betrieb der IT-Anwendung zuständig, sondern auch für die Initiierung und Umsetzung von IT-Sicherheitsmaßnahmen für diese Anwendung.

Verantwortliche für die Datensicherung	Der Verantwortliche für die Datensicherung ist zuständig für die Erstellung, Pflege, regelmäßige Aktualisierung und Umsetzung eines Datensicherungskonzeptes.
Vorgesetzte	Als Vorgesetzte werden die Mitarbeiter einer Institution bezeichnet, die gegenüber anderen, ihnen zugeordneten Mitarbeitern weisungsbefugt sind.

4 Glossar und Begriffsdefinitionen



In diesem Glossar werden einige wichtige Begriffe rund um Informationssicherheit und IT-Grundschutz erläutert.

Administrator

Ein Administrator verwaltet und betreut Rechner sowie Computernetze. Er installiert Betriebssysteme und Anwendungsprogramme, richtet neue Benutzerkennungen ein und verteilt die für die Arbeit notwendigen Rechte. Dabei hat er im Allgemeinen weitreichende oder sogar uneingeschränkte Zugriffsrechte auf die betreuten Rechner oder Netze.

Angriff

Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

Application-Level-Gateway (ALG)

Die Funktionen eines Sicherheitsgateways auf Anwendungsebene werden von den so genannten Application-Level-Gateways (ALG) übernommen. Implizit nehmen ALGs auch Funktionen auf den ISO-/OSI-Schichten 1 bis 3 wahr. ALGs, auch Sicherheitsproxies genannt, unterbrechen den direkten Datenstrom zwischen Quelle und Ziel. Bei einer Kommunikationsbeziehung zwischen Client und Server über einen Proxy hinweg nimmt der Proxy die Anfragen des Clients entgegen und leitet sie an den Server weiter. Bei einem Verbindungsaufbau in umgekehrter Richtung, also vom Server zum Client, verfährt der Proxy analog.

Sämtliche Kommunikationsbeziehungen zwischen den beiden Rechnern verlaufen in diesem Fall also mittelbar über den Proxy. Diese Kommunikationsform ermöglicht es einem Proxy beispielsweise bestimmte Protokollbefehle zu filtern.

Authentisierung (englisch authentication)

Authentisierung bezeichnet den Nachweises eines Kommunikationspartners, dass er tatsächlich derjenige ist, der er vorgibt zu sein. Dies kann unter Anderem durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen.

Einige Autoren unterscheiden im Deutschen zwischen den Begriffen Authentisierung, Authentifizierung und Authentikation. Mit Authentisierung wird dann die Vorlage eines Nachweises zur Identifikation bezeichnet, mit Authentifizierung die Überprüfung dieses Nachweises. Um den Text verständlich zu halten, verzichtet der IT-Grundschutz auf diese Unterscheidung.

Authentizität

Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.

Autorisierung

Bei einer Autorisierung wird geprüft, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtigt ist.

Basis-Sicherheitscheck

Der Begriff bezeichnet gemäß IT-Grundschutz die Überprüfung, ob die nach IT-Grundschutz empfohlenen Maßnahmen in einer Organisation bereits umgesetzt sind und welche grundlegenden IT-Sicherheitsmaßnahmen noch fehlen.

Baustein

Der Begriff dient zur Strukturierung von Empfehlungen der IT-Grundschutz-Kataloge. Bausteine sind die Einheiten innerhalb einer Schicht (z. B. IT-Systeme, Netze). Sie beschreiben teils technische Komponenten (wie Verkabelung), teils organisatorische Verfahren (wie Notfallvorsorge-Konzept) und besondere Einsatzformen (wie Häuslicher Arbeitsplatz). In jedem Baustein werden die betrachtete IT-Komponente und die Gefährdungslage beschrieben sowie organisatorische und technische Sicherheitsmaßnahmen empfohlen.

Bedrohung (englisch threat)

Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann. Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen. Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung.

Benutzerkennung (häufig auch Benutzerkonto)

Die Benutzerkennung ist der Name, mit dem sich der Benutzer einem IT-System gegenüber identifiziert. Dies kann der tatsächliche Name sein, ein Pseudonym, eine Abkürzung oder eine Kombination aus Buchstaben und/oder Ziffern.

Biometrie

Unter Biometrie ist die automatisierte Erkennung von Personen anhand ihrer körperlichen Merkmale zu verstehen. Diese kann genutzt werden, um Benutzer auf Grundlage besonderer Merkmale eindeutig zu authentisieren. Eine oder mehrere der folgenden biometrischen Merkmale können beispielsweise für eine Authentisierung verwendet werden:

- Iris
- Fingerabdruck
- Gesichtsproportionen
- Stimme und Sprachverhalten
- Handschrift
- Tippverhalten am Rechner

Blackbox-Test

Bei Blackbox-Tests wird das Verhalten von Außentätern simuliert, wobei vorausgesetzt wird, dass der Angreifer keine oder nur oberflächliche Informationen über sein Angriffsziel hat.

Browser

Mit Browser (von "to browse", auf deutsch: schmökern, blättern, umherstreifen) wird Software zum Zugriff auf das World Wide Web bezeichnet. Das Programm interpretiert die ankommenden Daten und stellt sie als Text und Bild auf dem Bildschirm dar.

Business Continuity Management

Business Continuity Management (BCM) bezeichnet alle organisatorischen, technischen und personellen Maßnahmen, die zur Fortführung des Kerngeschäfts einer Behörde oder eines Unternehmens nach Eintritt eines Notfalls bzw. eines Sicherheitsvorfalls dienen. Weiterhin unterstützt BCM die sukzessive Fortführung der Geschäftsprozesse bei länger anhaltenden Ausfällen oder Störungen.

Client

Als Client wird Soft- oder Hardware bezeichnet, die bestimmte Dienste von einem Server in Anspruch nehmen kann. Häufig steht der Begriff Client für einen Arbeitsplatzrechner, der in einem Netz auf Daten und Programme von Servern zugreift.

Computer-Virus

Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.)

Datenschutz

Mit Datenschutz wird der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit).

Datenschutz-Management

Mit Datenschutz-Management werden die Prozesse bezeichnet, die notwendig sind, um die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicher zu stellen.

Datensicherheit

Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein modernerer Begriff dafür ist "IT-Sicherheit".

Datensicherung (englisch Backup)

Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt.

Datensicherung umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren.

Ordnungsgemäße Datensicherung bedeutet, dass die getroffenen Maßnahmen in Abhängigkeit von der Datensensitivität eine sofortige oder kurzfristige Wiederherstellung des Zustandes von Systemen, Daten, Programmen oder Prozeduren nach erkannter Beeinträchtigung der Verfügbarkeit, Integrität oder Konsistenz aufgrund eines schadenswirkenden Ereignisses ermöglichen. Die Maßnahmen umfassen dabei mindestens die Herstellung und Erprobung der Rekonstruktionsfähigkeit von Kopien der Software, Daten und Prozeduren in definierten Zyklen und Generationen.

Demilitarisierte Zone (DMZ)

Eine DMZ ist ein Zwischennetz, das an Netzübergängen gebildet wird, aber weder zu dem einen, noch zu dem anderen Netz gehört. Sie stellt ein eigenes Netz dar, das nicht so stark gesichert ist wie das eigentlich zu schützende Netz.

DMZ werden bei einfachen Sicherheitsgateways üblicherweise an einer dritten Schnittstelle des Paketfilters erzeugt. Besteht das Sicherheitsgateway aus Paketfilter - Application-Level-Gateway - Paketfilter, dient in der Regel eine weitere Schnittstelle des Application-Level-Gateways (ALG) als DMZ-Schnittstelle. Verfügen Paketfilter oder ALG über mehr als drei Schnittstellen, können weitere DMZ gebildet werden.

Digitale Signatur

Eine digitale Signatur ist eine Kontrollinformation, die an eine Nachricht oder Datei angehängt wird, mit der folgende Eigenschaften verbunden sind:

- Anhand einer digitalen Signatur kann eindeutig festgestellt werden, wer diese erzeugt hat, und
- es ist authentisch überprüfbar, ob die Datei, an die die digitale Signatur angehängt wurde, identisch ist mit der Datei, die tatsächlich signiert wurde.

Ergänzende Sicherheitsanalyse

Diese Analyse ist nach IT-Grundschutz erforderlich, wenn Zielobjekte des betrachteten IT-Verbunds einen erhöhten Schutzbedarf haben, nicht geeignet modelliert werden können oder in untypischen Einsatzszenarien betrieben werden. Die Vorgehensweise hierzu ist im BSI-Standard 100-2 "IT-Grundschutz-Vorgehensweise" beschrieben. Die ergänzende Sicherheitsanalyse dient dazu festzustellen, für welche Teile des IT-Verbunds eine Risikoanalyse notwendig ist.

Firewall

Eine Firewall (besser mit Sicherheitsgateway bezeichnet) ist ein System aus soft- und hardwaretechnischen Komponenten, um IP-Netze sicher zu koppeln (siehe Sicherheitsgateway).

Gefahr

"Gefahr" wird oft als übergeordneter Begriff gesehen, wohingegen unter "Gefährdung" eine genauer beschriebene Gefahr (räumlich und zeitlich nach Art, Größe und Richtung bestimmt) verstanden wird. Beispiel: Die Gefahr ist ein Datenverlust. Datenverlust kann unter anderem durch eine defekte Festplatte oder einen Dieb entstehen, der die Festplatte stiehlt. Die Gefährdungen sind dann "defekter Datenträger" und "Diebstahl von Datenträgern". Diese Unterscheidung wird aber in der Literatur nicht durchgängig gemacht und ist eher von akademischer Bedeutung, so dass es sinnvoll ist, "Gefahr" und "Gefährdung" als gleichbedeutend aufzufassen.

Gefährdung (englisch applied threat)

Eine Gefährdung ist eine Bedrohung, die konkret auf ein Objekt über eine Schwachstelle einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt.

Sind beispielsweise Computer-Viren eine Bedrohung oder eine Gefährdung für Anwender, die im Internet surfen? Nach der oben gegebenen Definition lässt sich feststellen, dass alle Anwender prinzipiell durch Computer-Viren im Internet bedroht sind. Der Anwender, der eine virenverseuchte Datei herunterlädt, wird von dem Computer-Virus gefährdet, wenn sein Computer anfällig für diesen Computer-Viren-Typ ist. Für Anwender mit einem wirksamen Schutzprogramm, einer Konfiguration, die das Funktionieren des Computer-Virus verhindert, oder einem Betriebssystem, das den Virencode nicht ausführen kann, bedeutet das geladene Schadprogramm hingegen keine Gefährdung.

Gefährdungskataloge

Gefährdungskataloge sind Teil der IT-Grundschutz-Kataloge und enthalten Beschreibungen möglicher Gefährdungen der Informationstechnik. Sie sind in die Schadensursachen höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen und vorsätzliche Handlungen gegliedert.

Grundwerte der IT-Sicherheit

Der IT-Grundschutz betrachtet die drei Grundwerte der IT-Sicherheit: Vertraulichkeit, Verfügbarkeit und Integrität.

Jedem Anwender steht es natürlich frei, bei der Schutzbedarfsfeststellung weitere Grundwerte zu betrachten, wenn dies in seinem individuellem Anwendungsfall hilfreich ist. Weitere generische Oberbegriffe der IT-Sicherheit sind zum Beispiel:

- Authentizität
- Verbindlichkeit
- Zuverlässigkeit
- Nichtabstreitbarkeit

Informationssicherheit

Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Der Begriff "Informationssicherheit" statt IT-Sicherheit ist daher umfassender und wird daher zunehmend verwendet. Da aber in der Literatur noch überwiegend der Begriff "IT-Sicherheit" zu finden ist, wird er auch in dieser sowie in anderen Publikationen des IT-Grundschutzes weiterhin verwendet.

Informationssicherheitsmanagement

Die Planungs- und Lenkungsaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen, wird als Informationssicherheitsmanagement bezeichnet. Aus den gleichen Gründen, die oben für die Begriffe "Informationssicherheit" und "IT-Sicherheit" genannt sind, wird im IT-Grundschutz meist der kürzere Begriff "IT-Sicherheitsmanagement" verwendet.

Informationstechnik (IT)

Informationstechnik (IT) umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen.

Infrastruktur

Beim IT-Grundschutz werden unter Infrastruktur die für IT genutzten Gebäude, Räume, Energieversorgung, Klimatisierung und die Verkabelung verstanden. Die IT-Systeme und Netzkoppelelemente gehören nicht dazu.

Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Information" wird dabei für "Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt

der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

Intranet

Ein Intranet ist ein internes Netz, das sich unter vollständiger Kontrolle des Netzbetreibers (also der jeweiligen Behörde oder des Unternehmens) befindet. Meist werden Zugriffe aus anderen Netzen (wie dem Internet) durch eine Firewall abgesichert.

IT-Grundschutz

IT-Grundschutz bezeichnet eine Methodik zum Aufbau eines Sicherheitsmanagementsystems sowie zur Absicherung von IT-Verbünden über Standard-Sicherheitsmaßnahmen. Außerdem wird mit IT-Grundschutz der Zustand bezeichnet, in dem die vom BSI empfohlenen Standard-Sicherheitsmaßnahmen für IT-Systeme mit normalem Schutzbedarf umgesetzt sind.

IT-Grundschutzanalyse

Zu einer IT-Grundschutzanalyse gehören die Modellierung mit der Ermittlung der notwendigen Sicherheitsmaßnahmen und der Basis-Sicherheitscheck, in dem ein Soll-Ist-Vergleich den aktuellen Umsetzungsgrad von Sicherheitsmaßnahmen in einem Unternehmen oder einer Behörde beschreibt.

IT-Sicherheit

IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.

Es gibt drei Grundwerte der IT-Sicherheit: Vertraulichkeit, Verfügbarkeit und Integrität. Jedem Anwender steht es natürlich frei, bei der Schutzbedarfsfeststellung weitere Grundwerte zu betrachten, wenn dies in seinem individuellem Anwendungsfall hilfreich ist. Weitere generische Oberbegriffe der IT-Sicherheit sind zum Beispiel:

- Authentizität
- Verbindlichkeit
- Zuverlässigkeit
- Nichtabstreitbarkeit

IT-Sicherheitsbeauftragter

Person mit eigener Fachkompetenz zur IT-Sicherheit in einer Stabsstelle eines Unternehmens oder einer Behörde, der für alle IT-Sicherheitsfragen, Mitwirkung im IT-Sicherheitsprozess und IT-Sicherheitsmanagement-Team zuständig ist, die IT-Sicherheitsleitlinie, das IT-Sicherheitskonzept und andere Konzepte z. B. für Notfallvorsorge koordinierend erstellt und deren Umsetzung plant und überprüft.

IT-Sicherheitskonzept

Ein IT-Sicherheitskonzept dient zur Umsetzung der IT-Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das IT-Sicherheitskonzept ist das zentrale Dokument im IT-Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete IT-Sicherheitsmaßnahme muss sich letztlich darauf zurückführen lassen.

IT-Sicherheitskonzeption

Die Erstellung einer IT-Sicherheitskonzeption ist eine der zentralen Aufgaben des IT-Sicherheitsmanagements. Aufbauend auf den Ergebnissen von IT-Strukturanalyse und Schutzbedarfsfeststellung werden hier die erforderlichen IT-Sicherheitsmaßnahmen identifiziert und im IT-Sicherheitskonzept dokumentiert.

IT-Sicherheitsmanagement

IT-Sicherheitsmanagement ist die Planungs-, Lenkungs- und Kontrollaufgabe, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen. Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.

IT-Strukturanalyse

In einer IT-Strukturanalyse werden die erforderlichen Informationen über den ausgewählten IT-Verbund, die IT-Anwendungen, IT-Systeme, Netze, Räume, Gebäude und Verbindungen erfasst und so aufbereitet, dass sie die weiteren Schritte gemäß IT-Grundschutz unterstützen.

IT-Verbund

Unter einem IT-Verbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein IT-Verbund kann dabei als Ausprägung die gesamte IT einer Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungsnetz) oder gemeinsame IT-Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

Kumulationseffekt

Der Kumulationseffekt beschreibt, dass sich der Schutzbedarf eines IT-Systems erhöhen kann, wenn durch Kumulation mehrerer (z. B. kleinerer) Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden entstehen kann. Ein Auslöser kann auch sein, dass mehrere IT-Anwendungen bzw. eine Vielzahl sensitiver Informationen auf einem IT-System verarbeitet werden, so dass durch Kumulation von Schäden der Gesamtschaden höher sein kann.

Maßnahmenkataloge

In den IT-Grundschutz-Katalogen werden zu jedem Baustein passende Maßnahmen empfohlen. Diese sind in Katalogen zusammengefasst, die in Infrastruktur, Organisation, Personal, Hardware/Software, Kommunikation und Notfallvorsorge gegliedert sind.

Maximum-Prinzip

Nach dem Maximum-Prinzip bestimmt der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf eines Geschäftsprozesses, einer Anwendung bzw. eines IT-Systems.

Modellierung

Bei der Vorgehensweise nach IT-Grundschutz wird bei der Modellierung der betrachtete IT-Verbund eines Unternehmens oder einer Behörde mit Hilfe der Bausteine aus den IT-Grundschutz-Katalogen nachgebildet. Hierzu enthält Kapitel 2.2 der IT-Grundschutz-Kataloge für jeden Baustein einen Hinweis, auf welche Zielobjekte er anzuwenden ist und welche Voraussetzungen dabei gegebenenfalls zu beachten sind.

Netzplan

Ein Netzplan ist eine graphische Übersicht über die Komponenten eines Netzes und ihrer Verbindungen.

Nichtabstreitbarkeit (englisch non repudiation):

Hierbei liegt der Schwerpunkt auf der Nachweisbarkeit gegenüber Dritten. Ziel ist es zu gewährleisten, dass der Versand und Empfang von Daten und Informationen nicht in Abrede gestellt werden kann. Es wird unterschieden zwischen

- Nichtabstreitbarkeit der Herkunft: Es soll einem Absender einer Nachricht unmöglich sein, das Absenden einer bestimmten Nachricht nachträglich zu bestreiten.
- Nichtabstreitbarkeit des Erhalts: Es soll einem Empfänger einer Nachricht unmöglich sein, den Erhalt einer gesendeten Nachricht nachträglich zu bestreiten.

Paketfilter

Paketfilter sind IT-Systeme mit spezieller Software, die den ein- und ausgehenden Datenverkehr in einem Netz anhand spezieller Regeln filtern. Aufgabe eines Paketfilters ist es, Datenpakete anhand der Informationen in den Header-Daten der UDP/IP- bzw. TCP/IP-Schicht (z. B. IP-Adresse und Portnummer) weiterzuleiten oder zu verwerfen. Diese Entscheidung treffen Paketfilter anhand der vom Anwender vorgegebenen Filterregeln. Vielfach bieten die Paketfilter auch eine Möglichkeit zur "Network Address Translation" (NAT), bei der die Absender-Adressen von IP-Paketen durch eine IP-Adresse des Paketfilters ersetzt wird. Dadurch wird die Netzstruktur des zu schützenden Netzes verdeckt.

Patch

Ein Patch (vom englischen "patch", auf deutsch: Flicken) ist ein kleines Programm, das Softwarefehler wie z. B. Sicherheitslücken in Anwendungsprogrammen oder Betriebssystemen behebt.

Penetrationstest

Ein Penetrationstest ist ein gezielter, in der Regel simulierter, Angriffsversuch auf ein IT-System. Er wird als Wirksamkeitsprüfung vorhandener Sicherheitsmaßnahmen eingesetzt.

Proxy

Ein Proxy ist eine Art Stellvertreter in Netzen. Er nimmt Daten von einer Seite an und leitet sie an eine andere Stelle im Netz weiter. Mittels eines Proxys lassen sich Datenströme filtern und gezielt weiterleiten.

Qualifizierungsstufe

Die IT-Grundschutz-Methodik sieht drei Qualifizierungsstufen vor: "A" für die IT-Grundschutz-Einstiegsstufe, "B" für die IT-Grundschutz-Aufbaustufe, "C" für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz. Mit "Z" werden Maßnahmen bezeichnet, die Ergänzungen darstellen, die vor allem bei höheren Sicherheitsanforderungen hilfreich sein können.

Revision

Revision ist die systematische Überprüfung der Eignung und Einhaltung vorgegebener (Sicherheits-) Richtlinien. Die Revision sollte unabhängig und neutral sein.

Risiko

Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab.

Risiko wird auch häufig definiert als die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens.

Im Unterschied zu "Gefährdung" umfasst der Begriff "Risiko" bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.

Risikoanalyse (englisch Risk Assessment/Analysis)

Mit einer Risikoanalyse wird untersucht, welche schädigenden Ereignisse eintreten können, wie wahrscheinlich das Eintreten eines schädigenden Ereignisses ist und welche negativen Folgen der Schaden hätte.

Schadfunktion

Mit Schadfunktion wird eine vom Anwender ungewünschte Funktion bezeichnet, die die IT-Sicherheit unbeabsichtigt oder bewusst gesteuert gefährden kann.

Schutzbedarf

Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.

Schutzbedarfsdefinitionen

Dies sind auf die jeweils betrachtete Institution angepasste Kriterien, anhand derer entschieden werden kann, welche Schutzbedarfskategorie auf eine IT-Komponente anzuwenden ist.

Schutzbedarfsfeststellung

Bei der Schutzbedarfsfeststellung wird der Schutzbedarf der Geschäftsprozesse, der verarbeiteten Informationen und der IT-Komponenten bestimmt. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung der IT-Sicherheits-Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien "normal", "hoch" und "sehr hoch".

Schwachstelle (englisch vulnerability)

Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.

Server

Als Server wird Soft- oder Hardware bezeichnet, die bestimmte Dienste anderen (nämlich Clients) anbietet. Typischerweise wird damit ein Rechner bezeichnet, der seine Hardware- und Software-Ressourcen in einem Netz anderen Rechnern zugänglich macht. Beispiele sind Applikations-, Daten-, Web- oder E-Mail-Server. Zu häufiger Verwirrung führen X-Server, da ein X-Server-Prozess typischerweise auf einem Arbeitsplatzrechner, also einem Client in einem Server-Client-Netz, läuft.

Sicherheitsgateway

Ein Sicherheitsgateway (oft auch Firewall genannt) ist ein System aus soft- und hardware-technischen Komponenten. Es gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer IT-Sicherheitsrichtlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei im Wesentlichen, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden.

Sicherheitskonzept

In einem Sicherheitskonzept werden die konzeptionellen Sicherheitsanforderungen systematisch festgelegt und das Vorgehen zu ihrer Umsetzung in Maßnahmen beschrieben.

Sicherheitsmaßnahme

Mit Sicherheitsmaßnahme (kurz Maßnahme) werden alle Aktionen bezeichnet, die dazu dienen, um Sicherheitsrisiken zu steuern und um diesen entgegenzuwirken. Dies schließt sowohl organisatorische, als auch personelle, technische oder infrastrukturelle Sicherheitsmaßnahmen ein. Synonym werden auch die Begriffe Sicherheitsvorkehrung oder Schutzmaßnahme benutzt. Als englische Übersetzung wurde "safeguard", "security measure" oder "measure" gewählt. Im englischen Sprachraum wird neben "safeguard" außerdem häufig der Begriff "control" verwendet.

Sicherheitsrichtlinie (englisch Security Policy)

In einer Sicherheitsrichtlinie werden Schutzziele und allgemeine Sicherheitsmaßnahmen im Sinne offizieller Vorgaben eines Unternehmens oder einer Behörde formuliert. Detaillierte Sicherheitsmaßnahmen sind in einem umfangreicheren Sicherheitskonzept enthalten.

Sicherheitspolitik

Hierbei handelt es sich um eine falsche Übersetzung des englischen Begriffs "Security Policy", siehe Sicherheitsrichtlinie.

Standardsoftware

Unter Standardsoftware wird Software (Programme, Programm-Module, Tools etc.) verstanden, die für die Bedürfnisse einer Mehrzahl von Kunden am Markt und nicht speziell vom Auftragnehmer für den Auftraggeber entwickelt wurde, einschließlich der zugehörigen Dokumentation. Sie zeichnet sich außerdem dadurch aus, dass sie vom Anwender selbst installiert werden soll und dass nur geringer Aufwand für die anwenderspezifische Anpassung notwendig ist.

Starke Authentisierung

Starke Authentisierung bezeichnet die Kombination von zwei Authentisierungstechniken, wie Passwort plus Transaktionsnummern (Einmalpasswörter) oder plus Chipkarte. Daher wird dies auch häufig als Zwei-Faktor-Authentisierung bezeichnet.

Trojanisches Pferd

Ein Trojanisches Pferd, oft auch (eigentlich fälschlicherweise) kurz Trojaner genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung.

Verbindlichkeit

Unter Verbindlichkeit werden die IT-Sicherheitsziele Authentizität und Nichtabstreitbarkeit zusammengefasst. Bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.

Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Verschlüsselung

Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation - die Zurückgewinnung des Klartextes aus dem Geheimtext - wird Entschlüsselung genannt.

Verteilungseffekt

Der Verteilungseffekt kann sich auf den Schutzbedarf relativierend auswirken, wenn zwar eine IT-Anwendung einen hohen Schutzbedarf besitzt, ihn aber deshalb nicht auf ein betrachtetes IT-System überträgt, weil auf diesem IT-System nur unwesentliche Teilbereiche der IT-Anwendung laufen.

Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

VLAN

Virtuelle lokale Netze (Virtual LANs, VLANs) werden zur logischen Strukturierung von Netzen verwendet. Dabei wird innerhalb eines physikalischen Netzes eine logische Netzstruktur abgebildet, indem funktionell zusammengehörende Arbeitsstationen und Server zu einem virtuellen Netz verbunden werden.

VPN

Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft des Internet) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können unter Zuhilfenahme kryptographischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner sicher authentisieren werden, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

Der Begriff VPN wird oft als Bezeichnung für verschlüsselte Verbindungen verwendet, zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden, beispielsweise spezielle Funktionen des genutzten Transportprotokolls.

Wert (englisch asset)

Werte sind alles, was wichtig für eine Institution ist (Vermögen, Wissen, Gegenstände, Gesundheit).

WLAN

Mit WLAN werden drahtlose Netze bezeichnet, die auf der als IEEE 802.11 bezeichneten Gruppe von Standards basieren, die vom Institute of Electrical and Electronics Engineers (IEEE) spezifiziert wurden.

Zertifikat

Der Begriff Zertifikat wird in der Informationssicherheit in verschiedenen Bereichen mit unterschiedlichen Bedeutungen verwendet. Zu unterscheiden sind vor allem:

- IT-Grundschutz-Zertifikat: Damit kann dokumentiert werden, dass für den betrachteten IT-Verbund alle relevanten Sicherheitsmaßnahmen gemäß IT-Grundschutz-Vorgehensweise realisiert wurden. Dieses Zertifizierungsverfahren wurde durch die ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz (siehe unten) abgelöst.
- ISO 27001-Zertifikate: Der ISO-Standard 27001 "Information technology - Security techniques - Information security management systems requirements specification" ermöglicht eine Zertifizierung des IT-Sicherheitsmanagements.
- ISO 27001-Zertifikate auf der Basis von IT-Grundschutz: Seit Anfang 2006 können ISO 27001-Zertifikate auf der Basis von IT-Grundschutz beim BSI beantragt werden. Voraussetzung für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist eine Überprüfung durch einen vom BSI lizenzierten ISO 27001-Grundschutz-Auditor. Zu den Aufgaben eines ISO 27001-Grundschutz-Auditors gehört eine Sichtung der von der Institution erstellten Referenzdokumente, die Durchführung einer Vor-Ort-Prüfung und die Erstellung eines Audit-Reports. Die Zertifizierungsstelle BSI stellt aufgrund des Audit-Reports fest, ob die notwendigen IT-Sicherheitsmaßnahmen umgesetzt sind, erteilt im positiven Falle ein Zertifikat und veröffentlicht es.
- Zertifikat (Schlüsselzertifikat): Ein Schlüsselzertifikat ist eine elektronische Bescheinigung, mit der Signaturprüfschlüssel einer Person zugeordnet werden. Bei digitalen Signaturen wird ein Zertifikat als Bestätigung einer vertrauenswürdigen dritten Partei benötigt, um nachzuweisen, dass die zur Erzeugung der Digitalen Signatur eingesetzten kryptographischen Schlüssel wirklich zu dem Unterzeichnenden gehören.
- Zertifikat (IT-Sicherheitszertifikat, CC-Zertifikat): Zertifiziert wird nach international anerkannten IT-Sicherheitskriterien, wie z. B. den Common Criteria (ISO/IEC 15408). Auf dieser Basis können Produkte und Systeme unterschiedlichster Art evaluiert werden. Eine wesentliche Voraussetzung ist jedoch, dass die am Ende des Verfahrens im Zertifikat zu bestätigenden Sicherheitseigenschaften im Zusammenhang mit der Wahrung von Vertraulichkeit, Verfügbarkeit und Integrität stehen.
- Zertifikat von Schutzprofilen (Profil-Zertifikate): Mit Schutzprofilen wird bei den Common Criteria Anwendergruppen und Herstellern die Möglichkeit gegeben, produktklassentypische und dienstleistungsspezifische Sicherheitsanforderungen festzulegen. Die Berücksichtigung von Schutzprofilen bei der Produktentwicklung erleichtert deren Evaluierung und führt zu Produkten, die in besonderem Maße den anwenderspezifischen Anforderungen entsprechen. Auch Schutzprofile können evaluiert und zertifiziert werden.

Zugang

Mit Zugang wird die Nutzung von IT-Systemen, System-Komponenten und Netzen bezeichnet.

Zugangsberechtigungen erlauben somit einer Person, bestimmte Ressourcen wie IT-Systeme bzw. System-Komponenten und Netze zu nutzen.

Zugriff

Mit Zugriff wird die Nutzung von Informationen bzw. Daten bezeichnet.

Über Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind, Informationen, Daten oder auch IT-Anwendungen, zu nutzen oder Transaktionen auszuführen.

Zutritt

Mit Zutritt wird das Betreten von abgegrenzten Bereichen wie z. B. Räumen oder geschützen Arealen in einem Gelände bezeichnet.

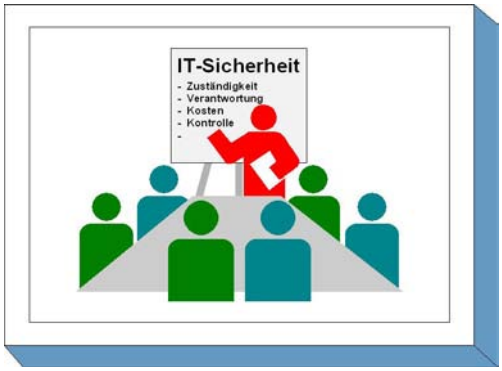
Zutrittsberechtigungen erlauben somit Personen, bestimmte Umgebungen zu betreten, also beispielsweise ein Gelände, ein Gebäude oder definierte Räume eines Gebäudes.

1 Übergreifende Aspekte

In der Schicht Übergreifende Aspekte sind folgende Bausteine enthalten:

B 1.0 IT-Sicherheitsmanagement
B 1.1 Organisation
B 1.2 Personal
B 1.3 Notfallvorsorge-Konzept
B 1.4 Datensicherungskonzept
B 1.5 Datenschutz
B 1.6 Computer-Viren-Schutzkonzept
B 1.7 Kryptokonzept
B 1.8 Behandlung von Sicherheitsvorfällen
B 1.9 Hard- und Software-Management
B 1.10 Standardsoftware
B 1.11 Outsourcing
B 1.12 Archivierung
B 1.13 IT-Sicherheitssensibilisierung und -schulung

B 1.0 IT-Sicherheitsmanagement



Beschreibung

Die sichere Verarbeitung von Informationen ist heutzutage für nahezu alle Unternehmen und Behörden von existenzieller Bedeutung. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Für den Schutz der Informationen reicht es nicht aus, nur technische Sicherheitslösungen einzusetzen. Ein angemessenes IT-Sicherheitsniveau kann nur durch geplantes und organisiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden. Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von Sicherheitsmaßnahmen ist eine systematische Vorgehensweise. Diese Planungs-, Lenkungs- und Kontrollaufgabe wird als Informationssicherheitsmanagement oder auch als IT-Sicherheitsmanagement bezeichnet.

Der Begriff Informationssicherheit ist umfassender als der Begriff IT-Sicherheit und wird daher zunehmend verwendet. Da IT-Sicherheit aber in dieser sowie in anderen Publikationen ein eingeführter Begriff ist, wird er im folgenden auch weiterhin verwendet.

Ein funktionierendes IT-Sicherheitsmanagement muss in die existierenden Managementstrukturen einer jeden Institution eingebettet werden. Daher ist es praktisch nicht möglich, eine für jede Institution unmittelbar anwendbare Organisationsstruktur für das IT-Sicherheitsmanagement anzugeben. Vielmehr werden häufig Anpassungen an spezifische Gegebenheiten erforderlich sein.

Dieser Baustein soll aufzeigen, wie ein funktionierendes IT-Sicherheitsmanagement eingerichtet und im laufenden Betrieb weiterentwickelt werden kann. Er beschreibt dazu sinnvolle Schritte eines systematischen IT-Sicherheitsprozesses und gibt Anleitungen zur Erstellung eines umfassenden IT-Sicherheitskonzeptes. Der Baustein baut auf dem BSI-Standard 100-1 *Managementsysteme für Informationssicherheit* und BSI-Standard 100-2 *Vorgehensweise nach IT-Grundschutz* auf und fasst die wichtigsten Aspekte zum IT-Sicherheitsmanagement hieraus zusammen.

Gefährdungslage

Gefährdungen im Umfeld des IT-Sicherheitsmanagements können vielfältiger Natur sein. Stellvertretend für diese Vielzahl der Gefährdungen wird in diesem Baustein die folgende typische Gefährdung betrachtet:

Organisatorischer Mängel:

- G 2.66 Unzureichendes IT-Sicherheitsmanagement
- G 2.105 Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen
- G 2.106 Störung der Geschäftsabläufe aufgrund von IT-Sicherheitsvorfällen
- G 2.107 Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes IT-Sicherheitsmanagement

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Im Rahmen des IT-Sicherheitsmanagements sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über den Aufbau geeigneter Organisationsstrukturen bis hin zur regelmäßigen Revision. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Einer der Grundpfeiler zur Erreichung eines angemessenen Sicherheitsniveaus ist, dass die Leitungsebene hinter den Sicherheitszielen steht und sich ihrer Verantwortung für IT-Sicherheit bewusst ist. Die Leitungsebene muss den IT-Sicherheitsprozess initiieren, steuern und kontrollieren, damit dieser in der Institution auch in allen Bereichen umgesetzt wird (siehe M 2.336 *Übernahme der Gesamtverantwortung für IT-Sicherheit durch die Leitungsebene*).

Weiterhin muss ein kontinuierlicher IT-Sicherheitsprozess etabliert und eine für die jeweilige Institution passende IT-Sicherheitsstrategie festgelegt werden (siehe M 2.335 *Festlegung der IT-Sicherheitsziele und -strategie*). Die Leitungsebene muss hierfür wie für alle weiteren Sicherheitsfragen eine Person als Hauptverantwortlichen benennen. Diese ist dafür zuständig, eine geeignete Organisationsstruktur für IT-Sicherheit aufzubauen und aufrechtzuerhalten (siehe M 2.193 *Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit*). Als eine der ersten Aktionen sollte eine IT-Sicherheitsleitlinie erstellt werden (siehe M 2.192 *Erstellung einer IT-Sicherheitsleitlinie*).

IT-Sicherheit muss in allen Bereichen der Institution gelebt werden (siehe M 2.337 *Integration der IT-Sicherheit in organisationsweite Abläufe und Prozesse*). Dazu gehört neben der Erarbeitung eines IT-Sicherheitskonzepts (siehe M 2.195 *Erstellung eines IT-Sicherheitskonzepts*) auch die Integration der Mitarbeiter in den Sicherheitsprozess (siehe M 2.197 *Integration der Mitarbeiter in den Sicherheitsprozess*) sowie die Erstellung von zielgruppengerechten IT-Sicherheitsrichtlinien (siehe M 2.338 *Erstellung von zielgruppengerechten IT-Sicherheitsrichtlinien*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "IT-Sicherheitsmanagement" vorgestellt.

Planung und Konzeption

- M 2.192 (A) Erstellung einer IT-Sicherheitsleitlinie
- M 2.335 (A) Festlegung der IT-Sicherheitsziele und -strategie
- M 2.336 (A) Übernahme der Gesamtverantwortung für IT-Sicherheit durch die Leitungsebene

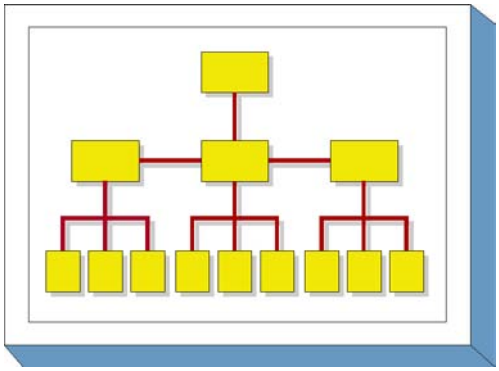
Umsetzung

- M 2.193 (A) Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit
- M 2.195 (A) Erstellung eines IT-Sicherheitskonzepts
- M 2.197 (A) Integration der Mitarbeiter in den Sicherheitsprozess
- M 2.337 (A) Integration der IT-Sicherheit in organisationsweite Abläufe und Prozesse
- M 2.338 (Z) Erstellung von zielgruppengerechten IT-Sicherheitsrichtlinien
- M 2.339 (Z) Wirtschaftlicher Einsatz von Ressourcen für IT-Sicherheit

Betrieb

- M 2.199 (A) Aufrechterhaltung der IT-Sicherheit
- M 2.200 (C) Managementreporte und -bewertungen der IT-Sicherheit
- M 2.201 (C) Dokumentation des IT-Sicherheitsprozesses
- M 2.340 (A) Beachtung rechtlicher Rahmenbedingungen
- M 2.380 (C) Ausnahmegenehmigungen

B 1.1 Organisation



Beschreibung

In diesem Baustein werden allgemeine und übergreifende Maßnahmen im Organisationsbereich aufgeführt, die als organisatorische Standardmaßnahmen zur Erreichung eines Mindestschutzniveaus erforderlich sind. Spezielle Maßnahmen organisatorischer Art, die in unmittelbarem Zusammenhang mit anderen Maßnahmen stehen (z. B. LAN-Administration), werden in den entsprechenden Bausteinen aufgeführt. Auf das ordnungsgemäße Management informationstechnischer Komponenten (Hardware oder Software) ausgerichtete Standard-Sicherheitsmaßnahmen befinden sich im Baustein B 1.9 *Hard- und Software-Management*.

Gefährdungslage

In diesem Baustein werden für den IT-Grundschutz die folgenden typischen Gefährdungen betrachtet:

Höhere Gewalt:
- G 1.4 Feuer
- G 1.5 Wasser
- G 1.7 Unzulässige Temperatur und Luftfeuchte

Organisatorischer Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.3 Fehlende, ungeeignete, inkompatible Betriebsmittel
- G 2.5 Fehlende oder unzureichende Wartung
- G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.8 Unkontrollierter Einsatz von Betriebsmitteln

Menschliche Fehlhandlungen
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal

Technisches Versagen:
- G 4.1 Ausfall der Stromversorgung
- G 4.2 Ausfall interner Versorgungsnetze
- G 4.3 Ausfall vorhandener Sicherungseinrichtungen

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.3 Unbefugtes Eindringen in ein Gebäude
- G 5.4 Diebstahl
- G 5.5 Vandalismus
- G 5.6 Anschlag
- G 5.12 Abhören von Telefongesprächen und Datenübertragungen
- G 5.13 Abhören von Räumen
- G 5.16 Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal
- G 5.17 Gefährdung bei Wartungsarbeiten durch externes Personal
- G 5.68 Unberechtigter Zugang zu den aktiven Netzkomponenten
- G 5.102 Sabotage

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Ein Mindestschutzniveau kann nur erreicht werden, wenn übergreifende Regelungen zur IT-Sicherheit verbindlich festgelegt werden. Hierzu sind eine Reihe von Maßnahmen umzusetzen, beginnend mit Festlegung und Zuweisung von verantwortlichen Personen für einzelne IT-Objekte (z. B. Anwendungen, IT-Komponenten) über entsprechende organisatorische Handlungsanweisungen bis hin zur Behandlung von schützenswerten Betriebsmitteln. Die Schritte, die dabei im Sinne eines kontinuierlichen IT-Sicherheitsprozesses durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Für die Initiierung und die Umsetzung der sich aus den Sicherheitszielen und Sicherheitsrichtlinien ergebenden Prozesse sind organisatorische und personelle Festlegungen zu treffen. Hierbei sind gegebenenfalls die Mitbestimmungsrechte des Personal- bzw. Betriebsrates zu wahren (siehe M 2.40 *Rechtzeitige Beteiligung des Personal-/Betriebsrates*). Die verschiedenen Organisationsebenen und die hier tätigen Personen benötigen konkrete Handlungsanweisungen und Verantwortlichkeiten zur Abwicklung der sie betreffenden Prozesse (siehe M 2.225 *Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten*).

Die strategischen Überlegungen sind in einem Betriebskonzept bezüglich ihrer Umsetzung im Unternehmen bzw. in der Behörde zu detaillieren.

Der Einsatz der erforderlichen Betriebsmittel ist auf die Aufgabenerfüllung und die Sicherheitsanforderungen abzustimmen und über eine Betriebsmittelverwaltung (siehe M 2.2 *Betriebsmittelverwaltung*) zu dokumentieren. Diese muss vollständig sein und durch entsprechende Prozesse auch jederzeit aktuell gehalten werden.

Voraussetzung für eine funktionierende IT-Infrastruktur, die auch auf Störungen adäquat reagieren kann, sind Regelungen für Ersatzteilbeschaffung, Reparaturen und Wartungsarbeiten (siehe M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*). In Wartungsverträgen ist die terminliche und inhaltliche Wartung einzelner IT-Systeme (oder Gruppen) verbindlich zu regeln, ebenso wie die erforderlichen Zugänge (Remote, vor Ort) und die an die Sicherheitsanforderungen angepassten Reaktionszeiten des mit der Wartung beauftragten Personals.

Die Aufgabenverteilung und die hierfür erforderlichen Funktionen (siehe M 2.5 *Aufgabenverteilung und Funktionstrennung*) sind so zu strukturieren, dass operative und kontrollierende Funktionen auf verschiedene Personen verteilt werden, um Interessenskonflikte bei den handelnden Personen zu minimieren oder ganz auszuschalten.

Betrieb

Die festgelegten Konzeptionen werden in konkrete Handlungsanweisungen gefasst und für den Betrieb verbindlich verabschiedet. Mitarbeiterbezogene Regelungen müssen hierbei die komplette Laufbahn eines Mitarbeiters im Unternehmen vom Eintritt bis zum Austritt betrachten. Durch Anwendung des Need-to-Know-Prinzips und des Vier-Augen-Prinzips ist sicher zu stellen, das Berechtigungen auf den verschiedenen Ebenen (z. B. Zutritt zu Räumen, Zugang zu IT-Systemen) zielgerichtet vergeben werden und auch praktikabel sind (siehe M 2.6 *Vergabe von Zutrittsberechtigungen* und M 2.7 *Vergabe von Zugangsberechtigungen*).

Diese Berechtigungen sind zu dokumentieren und durch verschiedene Methoden zu unterstützen, wie z. B. kontrollierte und nachweisbare Ausgabe von Schlüsseln nur an Berechtigte (siehe M 2.14 *Schlüsselverwaltung*), Authentisierung von Zugriffen, Zutrittskontrollsysteme für speziell gesicherte Bereiche und Kontrolle der Aktionen Betriebsfremder (siehe M 2.16 *Beaufsichtigung oder Begleitung von Fremdpersonen*). Die Zuordnung von Personen oder Personengruppen zu Rollen erleichtert die Verwaltung von Berechtigungen (siehe M 2.8 *Vergabe von Zugriffsrechten*). Werden Regelungen bewusst oder unbewusst verletzt, so müssen die hieraus ableitbaren Informations- und Eskalationsprozesse den Mitarbeitern bekannt sein, so dass eine zielgerichtete Reaktion auf die Verletzung erfolgen kann (siehe M 2.39 *Reaktion auf Verletzungen der Sicherheitspolitik*).

Aussonderung

Betriebs- und Sachmittel, die besonderen Schutzbedingungen unterliegen, sind so zu entsorgen, dass keine Rückschlüsse auf ihre Verwendung oder Inhalte gemacht werden können (siehe M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*). Hierzu sind entsprechende Regelungen, gegebenenfalls auch mit externen Firmen, zu treffen. Entsprechende Bestimmungen des Datenschutzes sind zu beachten.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Organisation" vorgestellt:

Planung und Konzeption

- M 2.1 (A) Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz
- M 2.2 (C) Betriebsmittelverwaltung
- M 2.4 (B) Regelungen für Wartungs- und Reparaturarbeiten
- M 2.5 (A) Aufgabenverteilung und Funktionstrennung
- M 2.40 (A) Rechtzeitige Beteiligung des Personal-/Betriebsrates
- M 2.225 (B) Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten
- M 2.393 (A) Regelung des Informationsaustausches

Betrieb

- M 2.6 (A) Vergabe von Zutrittsberechtigungen
- M 2.7 (A) Vergabe von Zugangsberechtigungen
- M 2.8 (A) Vergabe von Zugriffsrechten
- M 2.14 (A) Schlüsselverwaltung
- M 2.16 (B) Beaufsichtigung oder Begleitung von Fremdpersonen
- M 2.18 (Z) Kontrollgänge
- M 2.37 (Z) "Der aufgeräumte Arbeitsplatz"
- M 2.39 (B) Reaktion auf Verletzungen der Sicherheitsvorgaben
- M 2.177 (Z) Sicherheit bei Umzügen

Aussonderung

- M 2.13 (A) Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln

B 1.2 Personal

Beschreibung

In diesem Baustein werden die übergeordneten IT-Grundschutzmaßnahmen erläutert, die im Bereich Personalwesen standardmäßig durchgeführt werden sollten. Beginnend mit der Einstellung von Mitarbeitern bis hin zu deren Ausscheiden ist eine Vielzahl von Maßnahmen erforderlich. Personelle Empfehlungen, die an eine bestimmte Funktion gebunden sind, wie z. B. die Ernennung des Systemadministrators eines LAN, werden in den IT-spezifischen Bausteinen angeführt.

Gefährdungslage

In diesem Baustein werden für den IT-Grundschutz die folgenden typischen Gefährdungen betrachtet:

Höhere Gewalt:
- G 1.1 Personalausfall
- G 1.2 Ausfall des IT-Systems

Organisatorische Mängel:
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.7 Unerlaubte Ausübung von Rechten

Menschliche Fehlhandlungen:
- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.36 Fehlinterpretation von Ereignissen
- G 3.37 Unproduktive Suchzeiten
- G 3.43 Ungeeigneter Umgang mit Passwörtern
- G 3.44 Sorglosigkeit im Umgang mit Informationen

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.20 Missbrauch von Administratorrechten
- G 5.23 Computer-Viren
- G 5.42 Social Engineering
- G 5.43 Makro-Viren
- G 5.80 Hoax
- G 5.104 Ausspähen von Informationen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für das in einem Unternehmen oder einer Behörde tätige Personal sind eine Reihe von Maßnahmen umzusetzen, beginnend mit einer geregelten Einarbeitung neuer Mitarbeiter, über Schulungen, die den Umgang mit der IT betreffen, bis hin zu einem geregelten Ausscheiden eines Mitarbeiters. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Umsetzung

Das Unternehmen bzw. die Behörde muss neuen Mitarbeitern bestehende Regelungen und Handlungsanweisungen bekannt machen (siehe M 3.1 *Geregelte Einarbeitung/Einweisung neuer Mitarbeiter*, damit diese zügig in die bestehenden Prozesse integriert werden können. Ebenso ist es unerlässlich, alle Mitarbeiter über Veränderungen dieser Regelungen und ihre spezifischen Auswirkungen auf einen Prozess oder auf den einzelnen Mitarbeiter zu unterrichten. Insbesondere bei sicherheitskritischen Betriebsumgebungen empfiehlt es sich, die Mitarbeiter entsprechend zu verpflichten (siehe M 3.2 *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*) und die Vertrauenswürdigkeit von Mitarbeitern bestätigen zu lassen (siehe M 3.33 *Sicherheitsüberprüfung von Mitarbeitern*). Besonderes Gewicht ist hierbei auf die Vertrauenswürdigkeit von Personen mit besonderen Funktionen und Berechtigungen zu legen (siehe M 3.10 *Auswahl eines vertrauenswürdigen Administrators und Vertreters*.

Betrieb

Die Motivation aller Mitarbeiter, IT-Sicherheit in den Betriebsprozessen zu akzeptieren und auch eigenverantwortlich umzusetzen, muss durch geeignete Schulungen (siehe M 3.5 *Schulung zu IT-Sicherheitsmaßnahmen*) und durch detaillierte Kenntnisse der Anwendungen (siehe M 3.4 *Schulung vor Programmnutzung*) auf fachlicher Ebene motiviert und gefördert werden. Hierbei kommt der Ausbildung des Administrations- und Wartungspersonals (siehe M 3.11 *Schulung des Wartungs- und Administrationspersonals*) ein besonderer Stellenwert zu, da dieser Personenkreis aufgrund seiner weitgehenden Rechte im Umgang mit der IT eine hohe Verantwortung trägt.

Um eine kontinuierliche Verfügbarkeit wichtiger Prozesse zu erreichen, muss dafür gesorgt werden, dass Schlüsselpositionen immer besetzt sind, wenn dies von den Abläufen her gefordert wird (siehe M 3.3 *Vertretungsregelungen*).

Kommunikationsprobleme, persönliche Probleme, schlechtes Betriebsklima, weitreichende organisatorische Veränderungen und Ähnliches sind ebenfalls Faktoren, die zu Sicherheitsrisiken führen können. Für solche Fälle sollten Vertrauenspersonen und Anlaufstellen eingerichtet sein (siehe M 3.7 *Anlaufstelle bei persönlichen Problemen*).

Funktionsänderungen

Bei Mitarbeitern, die die Institution verlassen oder andere Funktionen übernehmen, müssen bestehende Regelungen mit erhöhter Sorgfalt umgesetzt werden (siehe M 3.6 *Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern*). Bei kurzfristig ausscheidenden Mitarbeitern kann ein potentielles Risiko vorhanden sein, dass unberechtigterweise vertrauliche Informationen mitgenommen werden oder erst im nachhinein gezielte Manipulationen an IT-Objekten und Daten bemerkt werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Personal" vorgestellt:

Planung und Konzeption

- M 3.51 (Z) Geeignetes Konzept für Personaleinsatz und -qualifizierung

Beschaffung

- M 3.50 (Z) Auswahl von Personal

Umsetzung

- M 3.1 (A) Geregelte Einarbeitung/Einweisung neuer Mitarbeiter
- M 3.2 (A) Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
- M 3.10 (A) Auswahl eines vertrauenswürdigen Administrators und Vertreters
- M 3.33 (Z) Sicherheitsüberprüfung von Mitarbeitern
- M 3.55 (C) Vertraulichkeitsvereinbarungen

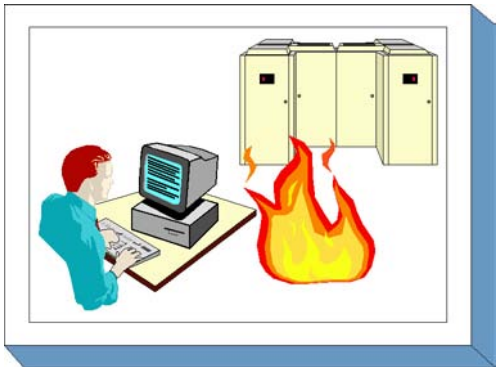
Betrieb

- M 3.3 (A) Vertretungsregelungen
- M 3.4 (A) Schulung vor Programmnutzung
- M 3.5 (A) Schulung zu IT-Sicherheitsmaßnahmen
- M 3.7 (Z) Anlaufstelle bei persönlichen Problemen
- M 3.8 (Z) Vermeidung von Störungen des Betriebsklimas
- M 3.11 (A) Schulung des Wartungs- und Administrationspersonals

Aussonderung

- M 3.6 (A) Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern

B 1.3 Notfallvorsorge-Konzept



Beschreibung

Die Notfallvorsorge umfasst Maßnahmen, die auf die Wiederherstellung der Betriebsfähigkeit nach (technisch bedingtem bzw. durch fahrlässige oder vorsätzliche Handlungen herbeigeführten) Ausfall eines IT-Systems ausgerichtet sind. Abhängig vom Zeitpunkt der Realisierung dieser Maßnahmen lassen sich die weiter unten beschriebenen Phasen der Notfallvorsorge unterscheiden.

Um eine unter Wirtschaftlichkeitsgesichtspunkten angemessene Notfallvorsorge betreiben zu können, müssen die entstehenden Kosten dem potentiellen Schaden (Kosten aufgrund mangelnder Verfügbarkeit im Notfall) gegenübergestellt und bewertet werden. Als Kosten sind zu betrachten:

- Kosten für die Erstellung eines Notfallvorsorgekonzeptes,
- Kosten für die Realisierung und Aufrechterhaltung der den IT-Betrieb begleitenden Notfallvorsorgemaßnahmen,
- Kosten für Notfallübungen und
- Kosten für die Wiederherstellung der Betriebsfähigkeit.

In diesem Baustein soll ein systematischer Weg aufgezeigt werden, wie ein Notfall-Handbuch erstellt und dessen Anwendung geübt werden kann. Der Aufwand zur Erstellung eines Notfallhandbuchs einschließlich der notwendigen begleitenden Maßnahmen ist beträchtlich. Daher kann dieser Baustein insbesondere für

- IT-Systeme mit hohen Verfügbarkeitsanforderungen,
- größere IT-Systeme (Großrechner, Server, umfangreiche Netze) oder
- eine größere Anzahl räumlich konzentrierter IT-Systeme

sinnvoll eingesetzt werden.

Gefährdungslage

In diesem Baustein wird für den IT-Grundschutz die folgende Gefährdung stellvertretend für alle Gefährdungen betrachtet, durch die ein Ausfall herbeigeführt werden kann:

Höhere Gewalt

- G 1.2 Ausfall des IT-Systems

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für die Erstellung eines Notfallvorsorge-Konzepts sind eine Reihe von Maßnahmen umzusetzen, beginnend mit einer strategischen Planung über die Einbeziehung der relevanten Geschäftsprozesse bis hin zu konkreten Maßnahmen für die IT-Systeme, die diesen Prozessen zugeordnet sind. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Für die verschiedenen Geschäftsprozesse bzw. Organisationseinheiten sind individuelle Notfallvorsorge-Konzepte zu erstellen, die die jeweils spezifischen Gegebenheiten abbilden. Für den Bereich der IT werden die geeigneten und wirtschaftlich angemessenen Maßnahmen identifiziert. Auf Basis der in der Schutzbedarfsfeststellung erhobenen Anforderungen an die Verfügbarkeit werden die erforderlichen präventiven Maßnahmen während des Betriebes eines IT-Systems (z. B. Rauchverbot, unterbrechungsfreie Stromversorgung, Wartung, Datensicherung) definiert (siehe M 6.1 *Erstellung einer Übersicht über Verfügbarkeitsanforderungen*), um Notfälle zu vermeiden bzw. die Schäden aufgrund von Notfällen zu vermindern.

Ist als Ergebnis der Verfügbarkeitsanforderungen eine Ausweichmöglichkeit für den IT-Betrieb erforderlich, so sind im Notfallhandbuch die Bedingungen und Prozeduren eines temporären oder permanenten Ausweichbetriebs zu beschreiben (siehe M 6.6 *Untersuchung interner und externer Ausweichmöglichkeiten*). Das Notfallhandbuch (siehe M 6.3 *Erstellung eines Notfall-Handbuches*) muss so ausgestaltet sein, dass kritische Geschäftsprozesse und IT-Objekte innerhalb der geforderten Zeiten wieder zur Verfügung stehen. Insbesondere sind personelle Schlüsselpositionen und deren Aufgaben und Befugnisse zu dokumentieren. Darüber hinaus wird in den Notfallplänen, die Bestandteile eines Notfallhandbuchs sind, festgeschrieben, welche Maßnahmen bei Eintreten eines Notfalls durchgeführt werden müssen. Das Notfallhandbuch muss aufgrund technischer, organisatorischer und personeller Veränderungen immer aktuell gehalten werden. Die Notfallvorsorgemaßnahmen für die verschiedenen IT-Bereiche müssen im Notfallhandbuch so beschrieben werden, dass sie von einem sachverständigen Dritten ausgeführt werden können.

Umsetzung

Das Notfallhandbuch muss an die spezifische IT-Situation des Unternehmens bzw. der Behörde angepasst sein. In Form detaillierter Übersichten sind die verantwortlichen und handelnden Personen (siehe M 6.7 *Regelung der Verantwortung im Notfall*), die zu treffenden Entscheidungen, die Sofortmaßnahmen bei Feststellung eines Notfalls (siehe M 6.8 *Alarmierungsplan*) und die Handlungsanweisungen für spezielle Ereignisse festzuschreiben. Es beschreibt die präventiven Maßnahmen (siehe M 6.13 *Erstellung eines Datensicherungsplans*), sowie die Maßnahmen zur Schadenstabilisierung, zur Wiederherstellung der IT-Systeme (siehe M 6.11 *Erstellung eines Wiederanlaufplans*) sowie Ersatzbeschaffungsmaßnahmen.

Das Notfallhandbuch muss im Notfall schnell erreichbar und transportabel sein. Bei ausschließlich elektronischer Speicherung des Dokumentes oder wenn es in einer werkzeuggestützten Form vorliegt, ist die Bereitstellung eines oder mehrerer Notfall-Notebooks erforderlich.

Betrieb

Von besonderer Bedeutung ist die Durchführung von Notfallübungen, um die Umsetzung der im Notfallhandbuch aufgeführten Maßnahmen einzuüben und deren Effizienz zu steigern (siehe M 6.12 *Durchführung von Notfallübungen*). Zusätzlich sollte das für den Notfall erforderliche Schlüsselpersonal durch Sensibilierungs- und Trainingsmaßnahmen kontinuierlich ausgebildet werden. Werden Notfall-Notebooks verwendet, so müssen diese kurzfristig einsetzbar sein.

Planung und Konzeption

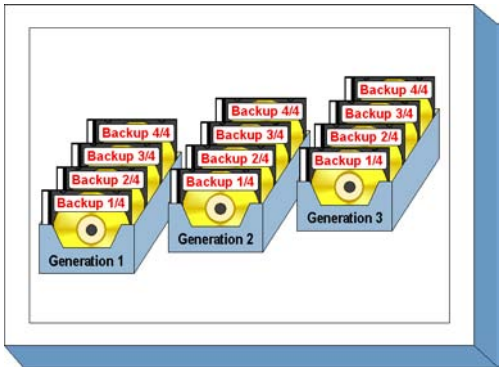
- M 6.1 (A) Erstellung einer Übersicht über Verfügbarkeitsanforderungen
- M 6.2 (A) Notfall-Definition, Notfall-Verantwortlicher
- M 6.3 (C) Erstellung eines Notfall-Handbuches
- M 6.75 (Z) Redundante Kommunikationsverbindungen

Beschaffung
- M 6.14 (B) Ersatzbeschaffungsplan
- M 6.15 (Z) Lieferantenvereinbarungen

Umsetzung
- M 6.4 (B) Dokumentation der Kapazitätsanforderungen der IT-Anwendungen
- M 6.5 (B) Definition des eingeschränkten IT-Betriebs
- M 6.6 (B) Untersuchung interner und externer Ausweichmöglichkeiten
- M 6.7 (A) Regelung der Verantwortung im Notfall
- M 6.8 (A) Alarmierungsplan
- M 6.9 (C) Notfall-Pläne für ausgewählte Schadensereignisse
- M 6.10 (C) Notfall-Plan für DFÜ-Ausfall
- M 6.11 (B) Erstellung eines Wiederanlaufplans
- M 6.13 (A) Erstellung eines Datensicherungsplans
- M 6.16 (Z) Abschließen von Versicherungen

Betrieb
- M 6.12 (C) Durchführung von Notfallübungen

B 1.4 Datensicherungskonzept



Beschreibung

Durch technisches Versagen, versehentliches Löschen oder durch Manipulation können gespeicherte Daten unbrauchbar werden bzw. verloren gehen. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen.

Die Konzeption einer angemessenen und funktionstüchtigen Datensicherung bedarf allerdings aufgrund der Komplexität einer geordneten Vorgehensweise. In diesem Baustein wird ein Weg beschrieben, wie für ein IT-System ein Datensicherungskonzept erstellt werden kann.

Gefährdungslage

Für die mittels eines Datensicherungskonzepts zu schützenden Daten wird für den IT-Grundschutz folgende typische Gefährdung angenommen:

Technisches Versagen:
- G 4.13 Verlust gespeicherter Daten

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Um eine effektive Datensicherung einzurichten, sind eine Reihe von Schritten zu durchlaufen. Diese sind in der Maßnahme M 6.33 *Entwicklung eines Datensicherungskonzepts* beschrieben und werden durch die dort aufgeführten Maßnahmen erläutert. Daher sollte mit der Umsetzung der Maßnahme M 6.33 begonnen werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Datensicherungskonzept" vorgestellt, das vor allem für größere IT-Systeme oder IT-Systeme mit großem Datenvolumen sinnvoll ist. Die Bearbeitung der Maßnahmen sollte in der angegebenen Reihenfolge geschehen, um systematisch ein Datensicherungskonzept zu erarbeiten.

Planung und Konzeption
- M 6.33 (B) Entwicklung eines Datensicherungskonzepts
- M 6.34 (B) Erhebung der Einflussfaktoren der Datensicherung
- M 6.35 (B) Festlegung der Verfahrensweise für die Datensicherung
- M 6.36 (A) Festlegung des Minimaldatensicherungskonzeptes

Beschaffung
- M 2.137 (A) Beschaffung eines geeigneten Datensicherungssystems

Umsetzung
- M 2.41 (A) Verpflichtung der Mitarbeiter zur Datensicherung
- M 6.21 (C) Sicherungskopie der eingesetzten Software
- M 6.37 (A) Dokumentation der Datensicherung

Betrieb

- M 6.20 (A) Geeignete Aufbewahrung der Backup-Datenträger
- M 6.22 (A) Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
- M 6.32 (A) Regelmäßige Datensicherung

Notfallvorsorge

- M 6.41 (A) Übungen zur Datenrekonstruktion

B 1.5 Datenschutz

Beschreibung

Aufgabe des Datenschutzes ist es, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen ("informationelles Selbstbestimmungsrecht").

Aufgrund der engen Verflechtung von Datenschutz und IT-Sicherheit sollte es Ziel eines IT-Grundschutz-Bausteins zum Thema "Datenschutz" sein, einerseits die Rahmenbedingungen für den Datenschutz praxisgerecht aufzubereiten und andererseits die Verbindung zur IT-Sicherheit über den IT-Grundschutz aufzubauen.

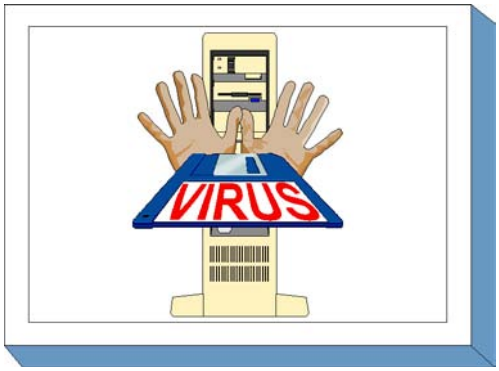
Ein Vorschlag für ein solches IT-Grundschutz-Baustein "Datenschutz" wurde federführend vom Bundesbeauftragten für den Datenschutz gemeinsam mit dem Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder erstellt. Es richtet sich an die öffentlichen Stellen des Bundes und der Länder, die privaten Anbieter von Telekommunikationsdiensten und Postdienstleistungen.

Dieser Vorschlag kann beim Bundesbeauftragten für den Datenschutz per E-Mail angefordert werden unter der Adresse:

poststelle@bfdi.bund.de

Darüber hinaus kann dieser Vorschlag auch auf dem Internet-Server des Bundesbeauftragten für den Datenschutz unter der Adresse *www.bfdi.bund.de* nachgelesen werden. In Vorbereitung befindet sich darüber hinaus eine Download-Möglichkeit dieses Vorschlagbausteins, das für die Lose-Blattsammlung der IT-Grundschutz-Kataloge vorformatiert ist.

B 1.6 Computer-Viren-Schutzkonzept



Beschreibung

Ziel eines Computer-Viren-Schutzkonzeptes ist es, geeignete Maßnahmen zum Schutz vor Schadprogrammen zusammenzustellen. Es soll gewährleistet sein, dass das Auftreten von Computer-Viren verhindert oder so früh wie möglich erkannt wird. Zusätzlich sind Maßnahmen zu benennen, die Schäden minimieren helfen, wenn ein Schadprogramm nicht rechtzeitig entdeckt werden konnte. Wesentlich ist die konsequente Anwendung der Maßnahmen und die ständige Aktualisierung der eingesetzten technischen Methoden. Diese Forderung begründet sich durch die täglich neu auftretenden Computer-Viren bzw. der Variation schon bekannter Computer-Viren. Durch die Weiterentwicklung von Betriebssystemen, Programmiersprachen und Anwendungssoftware entstehen weitere mögliche Angriffspotentiale für Computer-Viren, so dass rechtzeitig geeignete Gegenmaßnahmen eingeleitet werden müssen.

Wenn Behörden oder Unternehmen an öffentliche Kommunikationsnetze angeschlossen sind, ist die Gefahr durch Computer-Viren besonders groß. Die eingesetzten Rechner müssen daher permanent auf Computer-Viren kontrolliert werden.

Um für eine Gesamtorganisation einen effektiven Computer-Virenschutz zu erreichen, wird in diesem Baustein die Vorgehensweise zur Erstellung und Realisierung eines Viren-Schutzkonzeptes in einzelnen Schritten erläutert. Maßnahmenempfehlungen zum Computer-Virenschutz für einzelne IT-Systeme finden sich in den systemspezifischen Bausteinen.

Gefährdungslage

Für den IT-Grundschutz werden bezüglich Computer-Viren die folgenden typischen Gefährdungen betrachtet:

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.3 Fehlende, ungeeignete, inkompatible Betriebsmittel
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.8 Unkontrollierter Einsatz von Betriebsmitteln
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- G 2.26 Fehlendes oder unzureichendes Test- und Freigabeverfahren

Menschliche Fehlhandlungen:
- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.44 Sorglosigkeit im Umgang mit Informationen

Technisches Versagen:
- G 4.22 Software-Schwachstellen oder -Fehler

Vorsätzliche Handlungen:
- G 5.2 Manipulation an Daten oder Software
- G 5.21 Trojanische Pferde

- G 5.23 Computer-Viren
- G 5.43 Makro-Viren
- G 5.80 Hoax
- G 5.127 Spyware

Maßnahmenempfehlungen

Bei der Erstellung eines Computer-Viren-Schutzkonzepts (siehe M 2.154 *Erstellung eines Computer-Virenschutzkonzept,*) muss zunächst ermittelt werden, welche der vorhandenen oder geplanten IT-Systeme in das Computer-Viren-Schutzkonzept einzubeziehen sind (siehe M 2.155 *Identifikation potentiell von Computer-Viren betroffener IT-Systeme*). Für diese IT-Systeme müssen die für die Umsetzung von Sicherheitsmaßnahmen relevanten Einflussfaktoren betrachtet werden. Darauf aufbauend können dann die technischen und organisatorischen Maßnahmen ausgewählt werden. Hierzu ist insbesondere die Auswahl geeigneter technischer Gegenmaßnahmen wie Computer-Viren-Suchprogramme zu beachten (siehe M 2.156 *Auswahl einer geeigneten Computer-Virenschutz-Strategie* und M 2.157 *Auswahl eines geeigneten Computer-Viren-Suchprogramms*). Neben der Einrichtung eines Meldewesens (siehe M 2.158 *Meldung von Computer-Virusinfektionen*) und der Koordinierung der Aktualisierung eingesetzter Schutzprodukte (siehe M 2.159 *Aktualisierung der eingesetzten Computer-Viren-Suchprogramme*) sind für die Umsetzung des Konzeptes eine Reihe von Regelungen zu vereinbaren (siehe M 2.11 *Regelung des Passwortgebrauchs*), in denen zusätzlich notwendige Maßnahmen zum Virenschutz festgelegt werden.

Eine der wichtigsten Vorbeugemaßnahmen gegen Schäden durch Computer-Viren ist die regelmäßige Datensicherung (siehe M 6.32 *Regelmäßige Datensicherung*).

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Planung und Konzeption

- M 2.154 (A) Erstellung eines Computer-Virenschutzkonzepts
- M 2.155 (A) Identifikation potentiell von Computer-Viren betroffener IT-Systeme
- M 2.156 (A) Auswahl einer geeigneten Computer-Virenschutz-Strategie
- M 2.160 (A) Regelungen zum Computer-Virenschutz

Beschaffung

- M 2.157 (A) Auswahl eines geeigneten Computer-Viren-Suchprogramms

Umsetzung

- M 4.84 (A) Nutzung der BIOS-Sicherheitsmechanismen

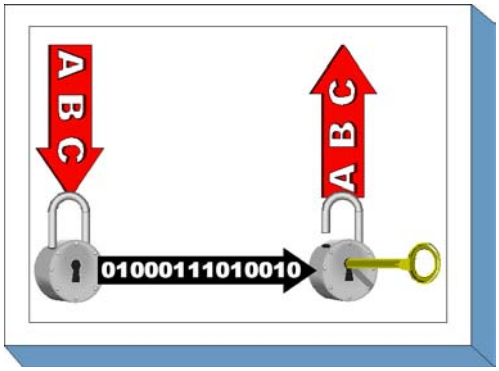
Betrieb

- M 2.158 (A) Meldung von Computer-Virusinfektionen
- M 2.159 (A) Aktualisierung der eingesetzten Computer-Viren-Suchprogramme
- M 2.224 (A) Vorbeugung gegen Trojanische Pferde
- M 4.3 (A) Regelmäßiger Einsatz eines Anti-Viren-Programms
- M 4.33 (A) Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
- M 4.253 (A) Schutz vor Spyware

Notfallvorsorge

- M 6.23 (A) Verhaltensregeln bei Auftreten eines Computer-Virus

B 1.7 Kryptokonzept



Beschreibung

Dieser Baustein beschreibt eine Vorgehensweise, wie in einer heterogenen Umgebung sowohl die lokal gespeicherten Daten als auch die zu übertragenen Daten wirkungsvoll durch kryptographische Verfahren und Techniken geschützt werden können. Dazu wird beschrieben, wie und wo in einer heterogenen Umgebung kryptographische Verfahren und die entsprechenden Komponenten eingesetzt werden können. Da beim Einsatz kryptographischer Verfahren sehr viele komplexe Einflussfaktoren zu betrachten sind, sollte hierfür ein Kryptokonzept erstellt werden.

In diesem Baustein wird daher beschrieben, wie ein Kryptokonzept erstellt werden kann. Beginnend mit der Bedarfsermittlung und der Erhebung der Einflussfaktoren geht es über die Auswahl geeigneter kryptographischer Lösungen und Produkte bis hin zur Sensibilisierung und Schulung der Anwender und zur Krypto-Notfallvorsorge.

Dieser Baustein kann auch herangezogen werden, wenn nur ein kryptographisches Produkt für eines der möglichen Einsatzfelder ausgewählt werden soll. Dann können einige der im folgenden beschriebenen Schritte ausgelassen werden und nur die für das jeweilige Einsatzfeld relevanten Teile bearbeitet werden.

Für die Umsetzung dieses Bausteins sollte ein elementares Verständnis der grundlegenden kryptographischen Mechanismen vorhanden sein. Ein Überblick über kryptographische Grundbegriffe findet sich in M 3.23 *Einführung in kryptographische Grundbegriffe*.

Gefährdungslage

Kryptographische Verfahren werden eingesetzt zur Gewährleistung von

- Vertraulichkeit,
- Integrität,
- Authentizität und
- Nichtabstreitbarkeit.

Daher werden für den IT-Grundschutz primär die folgenden Gefährdungen für kryptographische Verfahren betrachtet:

- G 4.33 Schlechte oder fehlende Authentikation
- G 5.27 Nichtanerkennung einer Nachricht
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.85 Integritätsverlust schützenswerter Informationen

Werden kryptographische Verfahren eingesetzt, sollten für den IT-Grundschutz zusätzlich folgende Gefährdungen betrachtet werden:

Organisatorische Mängel:

- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.19 Unzureichendes Schlüsselmanagement bei Verschlüsselung

Menschliche Fehlhandlungen:
- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- G 3.32 Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptographischen Verfahren
- G 3.33 Fehlbedienung von Kryptomodulen

Technisches Versagen:
- G 4.22 Software-Schwachstellen oder -Fehler
- G 4.34 Ausfall eines Kryptomoduls
- G 4.35 Unsichere kryptographische Algorithmen
- G 4.36 Fehler in verschlüsselten Daten

Vorsätzliche Handlungen:
- G 5.81 Unautorisierte Benutzung eines Kryptomoduls
- G 5.82 Manipulation eines Kryptomoduls
- G 5.83 Kompromittierung kryptographischer Schlüssel
- G 5.84 Gefälschte Zertifikate

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Darüber hinaus sind im Bereich kryptographische Verfahren im wesentlichen die folgenden Schritte durchzuführen:

1. Entwicklung eines Kryptokonzepts (siehe M 2.161 *Entwicklung eines Kryptokonzepts*)

   Der Einsatz kryptographischer Verfahren wird von einer großen Zahl von Einflussfaktoren bestimmt. Das IT-System, das Datenvolumen, das angestrebte Sicherheitsniveau und die Verfügbarkeitsanforderungen sind einige dieser Faktoren. Daher sollte zunächst ein Konzept entwickelt werden, in dem alle Einflussgrößen und Entscheidungskriterien für die Wahl eines konkreten kryptographischen Verfahrens und der entsprechenden Produkte berücksichtigt werden und das gleichzeitig unter Kostengesichtspunkten wirtschaftlich vertretbar ist.

2. Ermittlung der Anforderungen an die kryptographischen Verfahren

   Es muss ein Anforderungskatalog erstellt werden, in dem die Einflussgrößen und die Entscheidungskriterien beschrieben werden, die einem Einsatz von kryptographischen Verfahren zugrunde liegen (siehe M 2.162 *Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte* und M 2.163 *Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte*). Kryptographische Verfahren können auf den verschiedenen Schichten des ISO/OSI-Schichtenmodells eingesetzt werden. Je nach den festgestellten Anforderungen oder Gefährdungen ist der Einsatz auf bestimmten Schichten zu empfehlen (siehe auch M 4.90 *Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells*).

3. Auswahl geeigneter kryptographischer Verfahren (siehe M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*)

   Bei der Auswahl von kryptographischen Verfahren steht zunächst die Frage, ob symmetrische, asymmetrische oder hybride Algorithmen geeignet sind, im Vordergrund und dann die Mechanismenstärke. Anschließend sind geeignete Produkte zu bestimmen.

4. Auswahl eines geeigneten kryptographischen Produktes (siehe M 2.165 *Auswahl eines geeigneten kryptographischen Produktes*)

   Nachdem alle Rahmenbedingungen bestimmt worden sind, muss ein Produkt ausgewählt werden, das die im Kryptokonzept dargelegte Sicherheitsfunktionalität bietet. Ein solches Produkt, im folgenden kurz Kryptomodul genannt, kann dabei aus Hardware, Software, Firmware oder aus einer diesbezüglichen Kombination sowie der zur Durchführung der Kryptoprozesse notwendigen Bauteilen wie Speicher, Prozessoren, Busse, Stromversorgung etc. bestehen. Ein Kryptomodul kann zum Schutz von sensiblen Daten bzw. Informationen in unterschiedlichsten Rechner- oder Telekommunikationssystemen Verwendung finden.

5. Geeigneter Einsatz der Kryptomodule (siehe M 2.166 *Regelung des Einsatzes von Kryptomodulen*)

   Auch im laufenden Betrieb müssen eine Reihe von Sicherheitsanforderungen an ein Kryptomodul gestellt werden. Neben der Sicherheit der durch das Kryptomodul zu schützenden Daten geht es schwerpunktmäßig auch darum, das Kryptomodul selbst gegen unmittelbare Angriffe und Fremdeinwirkung zu schützen.

6. Die sicherheitstechnischen Anforderungen an die IT-Systeme, auf denen die kryptographischen Verfahren eingesetzt werden, sind den jeweiligen systemspezifischen Bausteinen zu entnehmen.

7. Notfallvorsorge, hierzu gehören

   - die Datensicherung bei Einsatz kryptographischer Verfahren (siehe M 6.56 *Datensicherung bei Einsatz kryptographischer Verfahren*), also die Sicherung der Schlüssel, der Konfigurationsdaten der eingesetzten Produkte, der verschlüsselten Daten,
   - die Informationsbeschaffung über sowie die Reaktion auf Sicherheitslücken.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Kryptokonzept" vorgestellt. Auf eine Wiederholung von Maßnahmen anderer Bausteine wird hier verzichtet.

Planung und Konzeption

- M 2.161 (A) Entwicklung eines Kryptokonzepts
- M 2.162 (A) Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte
- M 2.163 (A) Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte
- M 2.164 (A) Auswahl eines geeigneten kryptographischen Verfahrens
- M 2.166 (A) Regelung des Einsatzes von Kryptomodulen
- M 3.23 (A) Einführung in kryptographische Grundbegriffe
- M 4.90 (A) Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells

Beschaffung

- M 2.165 (A) Auswahl eines geeigneten kryptographischen Produktes
- M 4.85 (Z) Geeignetes Schnittstellendesign bei Kryptomodulen
- M 4.88 (A) Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen

Umsetzung

- M 2.46 (A) Geeignetes Schlüsselmanagement
- M 4.86 (A) Sichere Rollenteilung und Konfiguration der Kryptomodule
- M 4.87 (Z) Physikalische Sicherheit von Kryptomodulen
- M 4.89 (Z) Abstrahlsicherheit

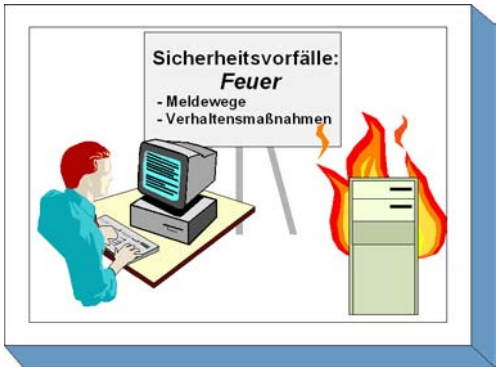
Notfallvorsorge

- M 6.56 (A) Datensicherung bei Einsatz kryptographischer Verfahren

Viele andere Bausteine enthalten Maßnahmen, die das Thema kryptographische Verfahren berühren und die als Realisierungsbeispiele betrachtet werden können. Dazu gehören z. B.:

- M 4.29 *Einsatz eines Verschlüsselungsproduktes für tragbare PCs*
- M 4.30 *Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen*
- M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*
- M 4.41 *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*
- M 4.72 *Datenbank-Verschlüsselung*
- M 5.33 *Absicherung der per Modem durchgeführten Fernwartung*
- M 5.34 *Einsatz von Einmalpasswörtern*
- M 5.36 *Verschlüsselung unter Unix und Windows NT*
- M 5.50 *Authentisierung mittels PAP/CHAP*
- M 5.52 *Sicherheitstechnische Anforderungen an den Kommunikationsrechner*
- M 5.63 *Einsatz von GnuPG oder PGP*
- M 5.64 *Secure Shell*
- M 5.66 *Verwendung von SSL*

B 1.8 Behandlung von Sicherheitsvorfällen



Beschreibung

Um die IT-Sicherheit im laufenden Betrieb aufrecht zu erhalten, ist es notwendig, die Behandlung von Sicherheitsvorfällen (Incident Handling) konzipiert und eingeübt zu haben. Als Sicherheitsvorfall wird dabei ein Ereignis bezeichnet, das Auswirkungen nach sich ziehen kann, die einen großen Schaden anrichten können. Um Schäden zu verhüten bzw. zu begrenzen, sollte die Behandlung der Sicherheitsvorfälle zügig und effizient ablaufen. Wenn hierbei auf ein vorgegebenes Verfahren aufgesetzt werden kann, können Reaktionszeiten minimiert werden. Die möglichen Schäden bei einem Sicherheitsvorfall können dabei sowohl die Vertraulichkeit oder Integrität von Daten als auch die Verfügbarkeit betreffen.

Ein besonderer Bereich der Behandlung von Sicherheitsvorfällen ist dabei das Notfallvorsorge-Konzept (siehe Baustein B 1.3 *Notfallvorsorge-Konzept*). In einem Notfallvorsorge-Konzept wird konkret für bestimmte IT-Systeme der Ausfall kritischer Komponenten vorab analysiert und eine Vorgehensweise zur Aufrechterhaltung oder Wiederherstellung der Verfügbarkeit festgelegt.

Sicherheitsvorfälle können zum Beispiel ausgelöst werden durch

- Benutzerfehlverhalten, das zu Datenverlust oder sicherheitskritischer Änderung von Systemparametern führt,
- Auftreten von Sicherheitslücken in Hard- oder Softwarekomponenten,
- massenhaftes Auftreten von Computer-Viren,
- Hacking von Internet-Servern,
- Offenlegung vertraulicher Daten,
- Personalausfall oder
- kriminelle Handlungen (etwa Einbruch, Diebstahl oder Erpressung mit IT-Bezug).

Alle Arten von Sicherheitsvorfällen müssen angemessen angegangen werden. Dies gilt sowohl für solche Sicherheitsvorfälle, gegen die man sich konkret rüsten kann, wie z. B. Computer-Viren, als auch solche, die die Organisation unerwartet treffen.

In diesem Baustein soll ein systematischer Weg aufgezeigt werden, wie ein Konzept zur Behandlung von Sicherheitsvorfällen erstellt und wie dessen Umsetzung und Einbettung innerhalb eines Unternehmens bzw. einer Behörde sichergestellt werden kann. Der Aufwand zur Erstellung und Umsetzung eines solchen Konzepts ist nicht gering. Daher sollte dieses Baustein vor allem bei größeren IT-Systemen und/oder solchen mit hoher Relevanz für die Behörde bzw. das Unternehmen beachtet werden.

Gefährdungslage

Sicherheitsvorfälle können durch eine Vielzahl von Gefährdungen ausgelöst werden. Eine große Sammlung von Gefährdungen, die kleinere oder größere Sicherheitsvorfälle verursachen können, findet sich in den Gefährdungskatalogen.

Ein großer Schaden kann durch diese Gefährdungen dann ausgelöst werden, wenn dafür keine angemessene Herangehensweise vorgesehen ist. In diesem Baustein wird daher stellvertretend für alle Gefährdungen, die sich im Umfeld von Sicherheitsvorfällen ereignen können, folgende Gefährdung betrachtet:

- G 2.62 Ungeeigneter Umgang mit Sicherheitsvorfällen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Um ein effektives System zur Behandlung von Sicherheitsvorfällen einzurichten, sind eine Reihe von Schritten zu durchlaufen. Diese sind in der Maßnahme M 6.58 *Etablierung eines Managementsystems zur Behandlung von Sicherheitsvorfällen* beschrieben und werden durch die daran anschließenden Maßnahmen erläutert. Daher sollte mit der Umsetzung der Maßnahme M 6.58 *Etablierung eines Managementsystems zur Behandlung von Sicherheitsvorfällen* begonnen werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Behandlung von Sicherheitsvorfällen" vorgestellt.

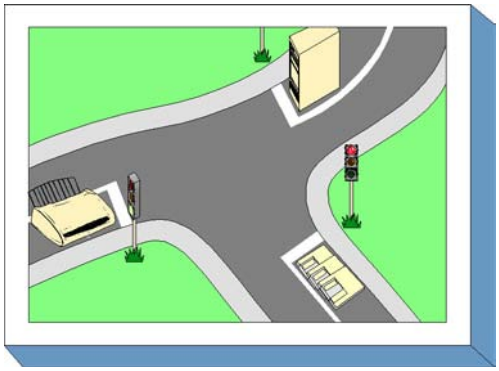
Planung und Konzeption

- M 6.58 (A) Etablierung eines Managementsystems zur Behandlung von Sicherheitsvorfällen
- M 6.59 (A) Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen
- M 6.60 (A) Verhaltensregeln und Meldewege bei Sicherheitsvorfällen
- M 6.61 (C) Eskalationsstrategie für Sicherheitsvorfälle
- M 6.62 (B) Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen
- M 6.67 (Z) Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle

Betrieb

- M 6.63 (A) Untersuchung und Bewertung eines Sicherheitsvorfalls
- M 6.64 (A) Behebung von Sicherheitsvorfällen
- M 6.65 (A) Benachrichtigung betroffener Stellen
- M 6.66 (B) Nachbereitung von Sicherheitsvorfällen
- M 6.68 (C) Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen

B 1.9 Hard- und Software-Management



Beschreibung

Um den notwendigen und erwünschten Sicherheitsgrad für die gesamte IT-Organisation zu erreichen, genügt es nicht, nur die einzelnen IT-Komponenten zu sichern. Es ist vielmehr erforderlich, auch alle Abläufe und Vorgänge, die diese IT-Systeme berühren, so zu gestalten, dass das angestrebte IT-Sicherheitsniveau erreicht und beibehalten wird. Es sind daher für alle diese Vorgänge Regelungen einzuführen und zu pflegen, die die Wirksamkeit der Sicherheitsmaßnahmen gewährleisten.

Den Schwerpunkt dieses Bausteins bilden dabei Regelungen, die sich spezifisch auf informationstechnische Hardware- oder Software-Komponenten beziehen, mit dem Ziel, einen ordnungsgemäßen IT-Betrieb in Bezug auf Management bzw. Organisation sicherzustellen. Sicherheit sollte integrierter Bestandteil des gesamten Lebenszyklus eines IT-Systems bzw. eines Produktes sein.

Gefährdungslage

In diesem Baustein werden für den IT-Grundschutz die folgenden typischen Gefährdungen betrachtet:

Höhere Gewalt:

- G 1.1 Personalausfall
- G 1.2 Ausfall des IT-Systems
- G 1.4 Feuer
- G 1.5 Wasser
- G 1.8 Staub, Verschmutzung

Organisatorischer Mängel:

- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- G 2.10 Nicht fristgerecht verfügbare Datenträger
- G 2.15 Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
- G 2.21 Mangelhafte Organisation des Wechsels zwischen den Benutzern
- G 2.22 Fehlende Auswertung von Protokolldaten
- G 2.67 Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten

Menschliche Fehlhandlungen:

- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.5 Unbeabsichtigte Leitungsbeschädigung
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.11 Fehlerhafte Konfiguration von sendmail
- G 3.17 Kein ordnungsgemäßer PC-Benutzerwechsel

- G 3.35 Server im laufenden Betrieb ausschalten
- G 3.44 Sorglosigkeit im Umgang mit Informationen

Technisches Versagen:
- G 4.8 Bekanntwerden von Softwareschwachstellen
- G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
- G 4.13 Verlust gespeicherter Daten
- G 4.22 Software-Schwachstellen oder -Fehler
- G 4.31 Ausfall oder Störung von Netzkomponenten
- G 4.35 Unsichere kryptographische Algorithmen
- G 4.38 Ausfall von Komponenten eines Netz- und Systemmanagementsystems
- G 4.39 Software-Konzeptionsfehler
- G 4.43 Undokumentierte Funktionen

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.9 Unberechtigte IT-Nutzung
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.26 Analyse des Nachrichtenflusses
- G 5.43 Makro-Viren
- G 5.68 Unberechtigter Zugang zu den aktiven Netzkomponenten
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.82 Manipulation eines Kryptomoduls
- G 5.83 Kompromittierung kryptographischer Schlüssel
- G 5.84 Gefälschte Zertifikate
- G 5.87 Web-Spoofing

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Ein IT-Verbund besteht aus einer Vielzahl von IT-Komponenten, die zunächst als Einzelkomponenten gemäß der Maßnahmenvorschläge aus den entsprechenden Bausteinen abgesichert werden sollten. Damit für alle eingesetzten IT-Komponenten das gleiche Sicherheitsniveau erreicht wird, sollten durch das Hard- und Software-Management einheitliche Regelungen vorgegeben werden.

Im Rahmen des Hard- und Software-Managements sind unabhängig von der Art der eingesetzten IT-Komponenten eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Aspekte der IT-Sicherheit müssen frühzeitig in die strategische Ausrichtung und die Beschaffung von IT-Systemen mit einfließen, da sie ganz konkrete Auswirkungen auf die Aufgabendurchführung und den Ablauf von Geschäftsprozessen haben. Hierbei müssen die definierten Sicherheitsanforderungen für die bereits vorhandenen IT-Systeme sowie die Anforderungen aus den geplanten Einsatzszenarien konsolidiert werden (siehe M 2.214 *Konzeption des IT-Betriebs*). Die Beschaffung und der Einsatz von Hardware und Software erfordern spezifische Regelungen für die verschiedenen Benutzer.

Hierbei müssen die für einen sicheren Geschäftsablauf erforderlichen Sicherheitsparameter der IT-Systeme den Benutzern transparent gemacht werden (siehe M 2.223 *Sicherheitsvorgaben für die Nutzung von Standardsoftware*). Trotz intensiver Schulung müssen die Benutzer im laufenden Betrieb hinsichtlich Funktionalität der Programme und Sicherheit sowie bei auftretenden Problemen zielgerichtet und zügig unterstützt werden (siehe M 2.12 *Betreuung und Beratung von IT-Benutzern*). Hierzu sind Benutzerbetreuer und Help-Desks einzurichten.

Die für den sicheren Betrieb aller IT-Komponenten notwendigen Maßnahmen müssen in einer Sicherheitsrichtlinie festgelegt werden. Die Einhaltung des darin spezifizierten Sicherheitsniveaus erfordert neben den technischen Maßnahmen auch ein umfangreiches Regelwerk für den Benutzer, das diesem Hilfestellung und eine verbindliche und präzise Anleitung gibt. Potentielle Risikofaktoren und Schwachstellen wie Passwörter, Fremdpersonal, nicht freigegebene IT-Komponenten, Zugang zu den IT-Systemen müssen durch organisatorische Regelungen (siehe M 2.226 *Regelungen für den Einsatz von Fremdpersonal*) oder durch eine Kombination von organisatorischen und technischen Maßnahmen (siehe M 2.11 *Regelung des Passwortgebrauchs*) minimiert werden. Die Benutzer müssen regelmäßig für den sorgfältigen Umgang mit sicherheitskritischen Informationen und IT-Komponenten sensibilisiert werden (siehe M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*).

Der effiziente und sichere Betrieb heterogener Netze erfordert strikte Richtlinien hinsichtlich Test, Installation und Dokumentation neuer Hardware und Software (siehe M 2.216 *Genehmigungsverfahren für IT-Komponenten*) sowie eine effiziente Benutzerverwaltung (siehe M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*). Der physikalische Zugang zu IT-Systemen sowie eine Authentisierung der Benutzer gegenüber den Anwendungen und Systemen (siehe M 2.220 *Richtlinien für die Zugriffs- bzw. Zugangskontrolle*) sollte grundsätzlich unter Beachtung des Need-to-Know-Prinzips erfolgen.

Der Einsatz von externen Datenträgern kann ein hohes Sicherheitsrisiko darstellen, da vermeintliche Sicherheitsbarrieren häufig einfach ausgehebelt werden können. Regelungen der Verwendung, Kennzeichnung und Prüfungen - z. B. auf Viren - für Disketten, CD-ROMs, Memory-Sticks und andere über USB anschließbare Geräte für den Datenaustausch, dienen ebenfalls zur Aufrechterhaltung eines sicheren IT-Betriebs (siehe M 2.3 *Datenträgerverwaltung*).

Aufgabe des Änderungsmanagements ist es, Änderungen an den aktuellen Konfigurationen einem formalen Dokumentations- und Freigabeprozess zu unterziehen (siehe M 2.221 *Änderungsmanagement*). Sicherheitskritische Aspekte müssen hierbei ebenso bewertet werden wie die Durchführung nach dem Vier-Augen-Prinzip und die aktuelle Dokumentation der Änderungen. Hierzu gehört auch, dass nur zugelassene Komponenten zum Einsatz kommen dürfen, da sonst ein kontrollierbarer Betrieb nicht möglich ist (siehe M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*).

Beschaffung

Für die Beschaffung von IT-Systemen müssen die aus dem Konzept resultierenden Anforderungen an die jeweiligen Produkte formuliert und basierend darauf die Auswahl der geeigneten Produkte getroffen werden. Der formalen Freigabe eines neuen Produktes (siehe M 2.62 *Software-Abnahme- und Freigabe-Verfahren*) sollte eine funktionale Prüfung und eine Konsistenzprüfung hinsichtlich der geforderten Sicherheitseigenschaften vorausgehen (siehe M 4.65 *Test neuer Hard- und Software*).

Umsetzung

Die Umsetzung der Sicherheitsrichtlinie für den Betrieb erfordert Festlegungen für Sicherheitsmaßnahmen im Rahmen der Installation und ersten Konfiguration (siehe M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien) sowie für den laufenden Betrieb der IT-Systeme. Die strukturierte

Datenhaltung mit konsequenter Trennung von Programm- und Arbeitsdateien (siehe M 2.138 *Strukturierte Datenhaltung*) sollte auf einer weitgehend einheitlichen Konfiguration der Systeme aufsetzen. Diese wiederum unterstützt eine zentral durchführbare Systemverwaltung (siehe M 2.69 *Einrichtung von Standardarbeitsplätzen*).

Die Sicherstellung einer durchgängigen Systemadministration - auch in Ausfallzeiten wie bei Krankheit oder Urlaub - lässt sich durch entsprechende Vertretungsregelungen erreichen (siehe M 2.26 *Ernennung eines Administrators und eines Vertreters*). Die Kompetenzen des Vertreters müssen transparent gemacht werden.

Die Dokumentation der Systemkonfiguration muss aktuell und verständlich sein und sollte werkzeugunterstützt erfolgen (siehe M 2.25 *Dokumentation der Systemkonfiguration*). Neben den physikalischen IT-Komponenten sind auch die logischen Netzstrukturen sowie die Rollen und Zugriffsrechte zu dokumentieren.

Betrieb

Durch die Systemadministration ist der laufende Betrieb mit unterschiedlichen Schwerpunkten aufrecht zu erhalten. Die durch Migration, Ausfall und Neuanschaffung erforderlichen Änderungen des IT-Bestandes (siehe M 4.78 Sorgfältige Durchführung von Konfigurationsänderungen) müssen nach erfolgter Freigabe im IT-Bestandsverzeichnis zeitnah nachgeführt werden (siehe M 2.34 *Dokumentation der Veränderungen an einem bestehenden System* und M 2.219 *Kontinuierliche Dokumentation der Informationsverarbeitung*).

Die laufende Beobachtung und Auswertung des Betriebes (siehe M 2.10 *Überprüfung des Hard- und Software-Bestandes* und M 2.64 *Kontrolle der Protokolldateien*) hinsichtlich Konformität und eventuellen Sicherheitsverletzungen sowie die Durchführung der entsprechenden Sicherheitsmaßnahmen (siehe M 2.215 *Fehlerbehandlung*) erfordern eine permanente Informationsbeschaffung über entsprechende Updates der unterschiedlichen Hersteller (siehe M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*). Durch Einspielen der erforderlichen Sicherheitspatches sollte die geforderte Sicherheit auch schon präventiv erreicht werden.

Die für die Bereiche Organisation und Personal festgelegten Sicherheitsmaßnahmen müssen durch Kontrollen auf ihre Anwendbarkeit, Akzeptanz und Wirksamkeit hin untersucht werden (M 2.182 *Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen*).

Aussonderung

Bei der Außerbetriebnahme von IT-Systemen ist dafür zu sorgen, dass wichtige Daten nicht verloren gehen, sondern vor der Abgabe bzw. Verschrottung der IT-Systeme gesichert werden (siehe Maßnahme M 4.234 *Aussonderung von IT-Systemen*). Fast noch wichtiger ist es jedoch, die Datenträger dieser Systeme anschließend so gründlich zu löschen (siehe Maßnahme M 2.167 *Sicheres Löschen von Datenträgern*), dass nicht im Nachhinein Unbefugte auf sensible Daten Zugriff erhalten, da in der Regel nach der Aussonderung keine Kontrolle darüber besteht, was mit den IT-Systemen weiter geschieht.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Hard- und Software-Management" vorgestellt:

Planung und Konzeption

- M 2.3 (B) Datenträgerverwaltung
- M 2.9 (A) Nutzungsverbot nicht freigegebener Hard- und Software
- M 2.11 (A) Regelung des Passwortgebrauchs
- M 2.12 (C) Betreuung und Beratung von IT-Benutzern
- M 2.24 (Z) Einführung eines IT-Passes

- M 2.30 (A) Regelung für die Einrichtung von Benutzern / Benutzergruppen
- M 2.214 (A) Konzeption des IT-Betriebs
- M 2.216 (C) Genehmigungsverfahren für IT-Komponenten
- M 2.217 (B) Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
- M 2.218 (C) Regelung der Mitnahme von Datenträgern und IT-Komponenten
- M 2.220 (A) Richtlinien für die Zugriffs- bzw. Zugangskontrolle
- M 2.221 (B) Änderungsmanagement
- M 2.223 (B) Sicherheitsvorgaben für die Nutzung von Standardsoftware
- M 2.226 (A) Regelungen für den Einsatz von Fremdpersonal
- M 2.392 (A) Sicherer Einsatz virtueller IT-Systeme
- M 4.133 (Z) Geeignete Auswahl von Authentikationsmechanismen
- M 4.134 (C) Wahl geeigneter Datenformate
- M 5.68 (Z) Einsatz von Verschlüsselungsverfahren zur Netzkommunikation
- M 5.77 (Z) Bildung von Teilnetzen
- M 5.87 (C) Vereinbarung über die Anbindung an Netze Dritter
- M 5.88 (C) Vereinbarung über Datenaustausch mit Dritten

Beschaffung

- M 2.62 (B) Software-Abnahme- und Freigabe-Verfahren

Umsetzung

- M 1.29 (Z) Geeignete Aufstellung eines IT-Systems
- M 1.32 (B) Geeignete Aufstellung von Druckern und Kopierern
- M 2.25 (A) Dokumentation der Systemkonfiguration
- M 2.26 (A) Ernennung eines Administrators und eines Vertreters
- M 2.38 (B) Aufteilung der Administrationstätigkeiten
- M 2.69 (B) Einrichtung von Standardarbeitsplätzen
- M 2.111 (A) Bereithalten von Handbüchern
- M 2.138 (B) Strukturierte Datenhaltung
- M 2.204 (A) Verhinderung ungesicherter Netzzugänge
- M 4.1 (A) Passwortschutz für IT-Systeme
- M 4.65 (C) Test neuer Hard- und Software
- M 4.7 (A) Änderung voreingestellter Passwörter
- M 4.84 (A) Nutzung der BIOS-Sicherheitsmechanismen
- M 4.135 (A) Restriktive Vergabe von Zugriffsrechten auf Systemdateien

Betrieb

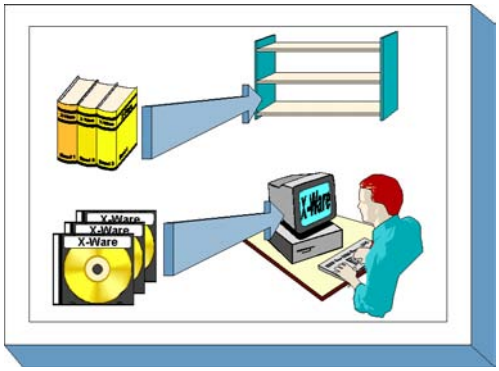
- M 1.46 (Z) Einsatz von Diebstahl-Sicherungen
- M 2.10 (C) Überprüfung des Hard- und Software-Bestandes
- M 2.22 (Z) Hinterlegen des Passwortes
- M 2.31 (A) Dokumentation der zugelassenen Benutzer und Rechteprofile
- M 2.34 (A) Dokumentation der Veränderungen an einem bestehenden System
- M 2.35 (B) Informationsbeschaffung über Sicherheitslücken des Systems
- M 2.64 (A) Kontrolle der Protokolldateien
- M 2.65 (C) Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
- M 2.110 (A) Datenschutzaspekte bei der Protokollierung
- M 2.182 (A) Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen
- M 2.215 (B) Fehlerbehandlung
- M 2.219 (A) Kontinuierliche Dokumentation der Informationsverarbeitung
- M 3.26 (A) Einweisung des Personals in den sicheren Umgang mit IT
- M 4.78 (A) Sorgfältige Durchführung von Konfigurationsänderungen

- M 4.107 (B) Nutzung von Hersteller-Ressourcen
- M 4.109 (Z) Software-Reinstallation bei Arbeitsplatzrechnern
- M 4.254 (Z) Sicherer Einsatz von drahtlosen Tastaturen und Mäusen

Aussonderung
- M 2.167 (B) Sicheres Löschen von Datenträgern
- M 4.234 (B) Aussonderung von IT-Systemen

Notfallvorsorge
- M 6.27 (C) Sicheres Update des BIOS

B 1.10 Standardsoftware



Beschreibung

Unter Standardsoftware wird Software verstanden, die auf dem Markt angeboten wird und im Allgemeinen über den Fachhandel, z. B. über Kataloge, erworben werden kann. Sie zeichnet sich dadurch aus, dass sie vom Anwender selbst installiert werden soll und dass nur geringer Aufwand für die anwenderspezifische Anpassung notwendig ist.

In diesem Baustein wird eine Vorgehensweise für den Umgang mit Standardsoftware unter Sicherheitsgesichtspunkten dargestellt. Dabei wird der gesamte Lebenszyklus von Standardsoftware betrachtet: Erstellung eines Anforderungskataloges, Vorauswahl eines geeigneten Produktes, Test, Freigabe, Installation, Lizenzverwaltung und Deinstallation.

Das Qualitätsmanagementsystem des Entwicklers der Standardsoftware fällt nicht in den Anwendungsbereich dieses Bausteins. Es wird vorausgesetzt, dass die Entwicklung der Software unter Beachtung gängiger Qualitätsstandards erfolgte.

Die beschriebene Vorgehensweise dient der Orientierung, um einen Sicherheitsprozess bezüglich Standardsoftware zu etablieren. Gegebenenfalls kann die hier aufgezeigte Vorgehensweise auch zum Vergleich mit einem bereits eingeführten Verfahren herangezogen werden.

Gefährdungslage

Für den IT-Grundschutz von "Standardsoftware" werden die folgenden typischen Gefährdungen betrachtet:

Höhere Gewalt:
- G 1.2 Ausfall des IT-Systems

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.3 Fehlende, ungeeignete, inkompatible Betriebsmittel
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.26 Fehlendes oder unzureichendes Test- und Freigabeverfahren
- G 2.27 Fehlende oder unzureichende Dokumentation
- G 2.28 Verstöße gegen das Urheberrecht
- G 2.29 Softwaretest mit Produktionsdaten
- G 2.67 Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten

Menschliche Fehlhandlungen:
- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten
- G 3.17 Kein ordnungsgemäßer PC-Benutzerwechsel

Technisches Versagen:
- G 4.7 Defekte Datenträger

- G 4.8 Bekanntwerden von Softwareschwachstellen
- G 4.22 Software-Schwachstellen oder -Fehler

Vorsätzliche Handlungen:
- G 5.2 Manipulation an Daten oder Software
- G 5.9 Unberechtigte IT-Nutzung
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.43 Makro-Viren

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Standardsoftware sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung des Einsatzes über die Beschaffung bis zu ihrer Außerbetriebnahme. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Vor der Auswahl einer bestimmten Standardsoftware sollte ein Anforderungskatalog erstellt werden, anhand dessen ein Produkt nach objektiven und nachvollziehbaren Kriterien ausgewählt werden kann, so dass man ein gewisses Vertrauen haben kann, dass ein einigermaßen optimales Produkt zum Einsatz kommt. In dieser Phase sollten bei komplexeren Produkten auch die Verantwortlichen für deren Beschaffung und Einsatz festgelegt werden.

Beschaffung

Für die Beschaffung kann anhand der konkreten Vorgaben des Anforderungskatalogs geprüft werden, welches der am Markt vorhandenen Produkte die am besten geeignete Funktionalität aufweist.

Umsetzung

Durch Tests in angemessener Tiefe ist sicherzustellen, dass das ausgewählte Produkt über die in der Dokumentation angegebene Funktionalität auch tatsächlich verfügt. Sofern das Produkt auf breiter Basis einzusetzen ist, muss es in die vorhandenen Installationsverfahren eingebunden werden, und die Installation selbst ist zu dokumentieren. Eine Nutzung in der Fläche darf erst erfolgen, wenn das Produkt nach erfolgreichem Durchlaufen der Tests und nach Abschluss der Vorbereitungsarbeiten dafür freigegeben wurde.

Betrieb

Die Kontrolle der installierten Versionen und die Nachverfolgung der verfügbaren Lizenzen und deren Abgleich mit der installierten Anzahl der Produkte ist eine permanente Aufgabe während der Nutzung der Standardsoftware.

Aussonderung

Eine saubere Deinstallation von Standardsoftware erfordert häufig umfangreiche und komplexe Arbeiten, in einzelnen Fällen bis hin zur Neuinstallation von Rechnern.

Nachfolgend wird das Maßnahmenbündel für den Baustein "Standardsoftware" vorgestellt. Je nach Art und Umfang der jeweiligen Standardsoftware muss erwogen werden, ob einzelne Maßnahmen nur reduziert umgesetzt werden. Die Maßnahmen M 2.79 bis M 2.89 stellen in der angegebenen Reihenfolge eine umfassende Beschreibung dar, wie der Lebenszyklus von Standardsoftware gestaltet werden kann. Sie werden durch die anderen genannten Maßnahmen ergänzt.

Planung und Konzeption
- M 2.79 (A) Festlegung der Verantwortlichkeiten im Bereich Standardsoftware
- M 2.80 (A) Erstellung eines Anforderungskatalogs für Standardsoftware
- M 2.82 (B) Entwicklung eines Testplans für Standardsoftware
- M 2.378 (Z) System-Entwicklung
- M 2.379 (Z) Software-Entwicklung durch Endbenutzer
- M 4.34 (Z) Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen

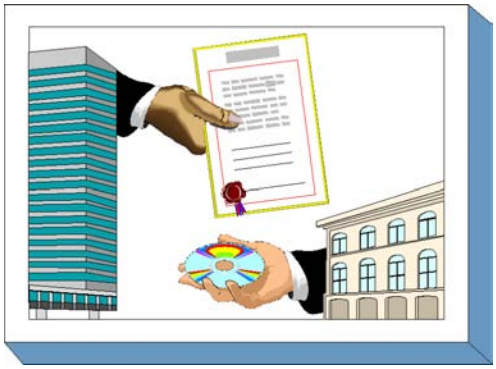
Beschaffung
- M 2.66 (Z) Beachtung des Beitrags der Zertifizierung für die Beschaffung
- M 2.81 (A) Vorauswahl eines geeigneten Standardsoftwareproduktes

Umsetzung
- M 2.83 (B) Testen von Standardsoftware
- M 2.84 (A) Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware
- M 2.85 (A) Freigabe von Standardsoftware
- M 2.86 (B) Sicherstellen der Integrität von Standardsoftware
- M 2.87 (A) Installation und Konfiguration von Standardsoftware
- M 2.90 (A) Überprüfung der Lieferung
- M 4.42 (Z) Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung

Betrieb
- M 2.88 (A) Lizenzverwaltung und Versionskontrolle von Standardsoftware

Aussonderung
- M 2.89 (C) Deinstallation von Standardsoftware

B 1.11 Outsourcing



Beschreibung

Beim Outsourcing werden Arbeits- oder Geschäftsprozesse einer Organisation ganz oder teilweise zu externen Dienstleistern ausgelagert. Outsourcing kann sowohl Nutzung und Betrieb von Hardware und Software, aber auch Dienstleistungen betreffen. Dabei ist es unerheblich, ob die Leistung in den Räumlichkeiten des Auftraggebers oder in einer externen Betriebsstätte des Outsourcing-Dienstleisters erbracht wird. Typische Beispiele sind der Betrieb eines Rechenzentrums, einer Applikation, einer Webseite oder des Wachdienstes. *Outsourcing* ist ein Oberbegriff, der oftmals durch weitere Begriffe ergänzt wird: *Tasksourcing* bezeichnet das Auslagern von Teilbereichen. Werden Dienstleistungen mit Bezug zur IT-Sicherheit ausgelagert, wird von *Security Outsourcing* oder *Managed Security Services* gesprochen. Beispiele sind die Auslagerung des Firewall-Betriebs, die Überwachung des Netzes, Virenschutz oder der Betrieb eines Virtual Private Networks (VPN). Unter *Application Service Provider* (ASP) versteht man einen Dienstleister, der auf seinen eigenen Systemen einzelne Anwendungen oder Software für seine Kunden betreibt (E-Mail, SAP-Anwendungen, Archivierung, Web-Shops, Beschaffung). Auftraggeber und Dienstleister sind dabei über das Internet oder ein VPN miteinander verbunden. Beim *Application Hosting* ist ebenfalls der Betrieb von Anwendungen an einen Dienstleister ausgelagert, jedoch gehören im Gegensatz zum ASP-Modell die Anwendungen noch dem jeweiligen Kunden. Da die Grenzen zwischen klassischem Outsourcing und reinem ASP in der Praxis zunehmend verschwimmen, wird im Folgenden nur noch der Oberbegriff Outsourcing verwendet.

Das Auslagern von Geschäfts- und Produktionsprozessen ist ein etablierter Bestandteil heutiger Organisationsstrategien. Speziell in den letzten beiden Jahrzehnten hat sich der Trend zum Outsourcing enorm verstärkt, und dieser scheint auch für die nächste Zukunft ungebrochen. Es gibt aber inzwischen auch publizierte Beispiele für gescheiterte Outsourcing-Projekte, wo der Auftraggeber den Outsourcing-Vertrag gekündigt hat und die ausgelagerten Geschäftsprozesse wieder in Eigenregie betreibt (Insourcing).

Die Gründe für Outsourcing sind vielfältig: die Konzentration einer Organisation auf ihre Kernkompetenzen, die Möglichkeit einer Kostenersparnis (z. B. keine Anschaffungs- oder Betriebskosten für IT-Systeme), der Zugriff auf spezialisierte Kenntnisse und Ressourcen, die Freisetzung interner Ressourcen für andere Aufgaben, die Straffung der internen Verwaltung, die verbesserte Skalierbarkeit der Geschäfts- und Produktionsprozesse, die Erhöhung der Flexibilität sowie der Wettbewerbsfähigkeit einer Organisation sind nur einige Beispiele.

Beim Auslagern von IT-gestützten Organisationsprozessen werden die IT-Systeme und Netze der auslagernden Organisation und ihres Outsourcing-Dienstleisters in der Regel eng miteinander verbunden, so dass Teile von internen Geschäftsprozessen unter Leitung und Kontrolle eines externen Dienstleisters ablaufen. Ebenso findet auf personeller Ebene ein intensiver Kontakt statt.

Durch die enge Verbindung zum Dienstleister und die entstehende Abhängigkeit von der Dienstleistungsqualität ergeben sich Risiken für den Auftraggeber, durch die im schlimmsten Fall sogar die Geschäftsgrundlage des Unternehmens oder der Behörde vital gefährdet werden können. (Beispielsweise könnten sensitive Organisationsinformationen gewollt oder ungewollt nach außen preisgegeben werden.) Der Betrachtung von Sicherheitsaspekten und der Gestaltung vertraglicher Regelungen zwischen Auftraggeber und Outsourcing-Dienstleister kommt im Rahmen eines Outsourcing-Vorhabens somit eine zentrale Rolle zu.

Den Schwerpunkt dieses Bausteins bilden daher Maßnahmen, die sich mit IT-Sicherheitsaspekten des Outsourcing beschäftigen. Dazu zählen ebenfalls geeignete Maßnahmen zur Kontrolle der vertraglich vereinbarten Ziele und Leistungen sowie der IT-Sicherheitsmaßnahmen.

Gefährdungslage

Die Gefährdungslage eines Outsourcing-Vorhabens ist ausgesprochen vielschichtig. Die Entscheidung über das Auslagern einer speziellen Aktivität beeinflusst nachhaltig die strategische Ausrichtung der Organisation, die Definition ihrer Kernkompetenzen, die Ausgestaltung der Wertschöpfungskette und betrifft viele weitere wesentliche Belange eines Organisationsmanagements. Es sollten daher alle Anstrengungen unternommen werden, um Fehlentwicklungen des Unternehmens oder der Behörde frühzeitig zu erkennen und zu verhindern.

Die Gefährdungen können parallel auf physikalischer, technischer und auch menschlicher Ebene existieren und sind nachfolgend in den einzelnen Gefährdungskatalogen aufgeführt. Um die jeweils existierenden Risiken quantitativ bewerten zu können, müssen zuvor die organisationseigenen Werte und Informationen entsprechend ihrer strategischen Bedeutung für die Organisation beurteilt und klassifiziert werden.

Höhere Gewalt:
- G 1.10 Ausfall eines Weitverkehrsnetzes

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.26 Fehlendes oder unzureichendes Test- und Freigabeverfahren
- G 2.47 Ungesicherter Akten- und Datenträgertransport
- G 2.66 Unzureichendes IT-Sicherheitsmanagement
- G 2.67 Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten
- G 2.83 Fehlerhafte Outsourcing-Strategie
- G 2.84 Unzulängliche vertragliche Regelungen mit einem externen Dienstleister
- G 2.85 Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens
- G 2.86 Abhängigkeit von einem Outsourcing-Dienstleister
- G 2.88 Störung des Betriebsklimas durch ein Outsourcing-Vorhaben
- G 2.89 Mangelhafte IT-Sicherheit in der Outsourcing-Einführungsphase
- G 2.90 Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister
- G 2.93 Unzureichendes Notfallvorsorgekonzept beim Outsourcing

Menschliche Fehlhandlungen:
- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer

Technisches Versagen:
- G 4.33 Schlechte oder fehlende Authentikation
- G 4.34 Ausfall eines Kryptomoduls
- G 4.48 Ausfall der Systeme eines Outsourcing-Dienstleisters

Vorsätzliche Handlungen:
- G 5.10 Missbrauch von Fernwartungszugängen
- G 5.20 Missbrauch von Administratorrechten
- G 5.42 Social Engineering
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.85 Integritätsverlust schützenswerter Informationen
- G 5.107 Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Ein ausgelagerter IT-Verbund kann sowohl aus Komponenten bestehen, die sich ausschließlich im Einflussbereich des Outsourcing-Dienstleisters befinden, als auch aus Komponenten beim Auftraggeber. In der Regel gibt es in diesem Fall Schnittstellen zur Verbindung der Systeme. Für jedes Teilsystem und für die Schnittstellenfunktionen muss IT-Grundschutz gewährleistet sein.

Ein Outsourcing-Vorhaben besteht aus mehreren Phasen, die im Folgenden kurz dargestellt sind.

Phase 1: Strategische Planung des Outsourcing-Vorhabens

Schon im Rahmen der strategischen Entscheidung, ob und in welcher Form ein Outsourcing-Vorhaben umgesetzt wird, müssen die sicherheitsrelevanten Gesichtspunkte herausgearbeitet werden. In der Maßnahme M 2.250 *Festlegung einer Outsourcing-Strategie* werden die wesentlichen Punkte vorgestellt, die zu beachten sind.

Phase 2: Definition der wesentlichen Sicherheitsanforderungen

Wenn die Entscheidung zum Outsourcing gefallen ist, müssen die wesentlichen übergeordneten Sicherheitsanforderungen für das Outsourcing-Vorhaben festgelegt werden. Diese Sicherheitsanforderungen sind die Basis für das Ausschreibungsverfahren (siehe M 2.251 *Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben*).

Phase 3: Auswahl des Outsourcing-Dienstleisters

Der Wahl des Outsourcing-Dienstleisters kommt eine besondere Bedeutung zu (siehe M 2.252 *Wahl eines geeigneten Outsourcing-Dienstleisters*).

Phase 4: Vertragsgestaltung

Auf Basis des Pflichtenheftes muss nun ein Vertrag mit dem Partner ausgehandelt werden, der die gewünschten Leistungen inklusive Qualitätsstandards und Fristen im Einklang mit der vorhandenen Gesetzgebung festschreibt. Diese Verträge werden häufig als Service Level Agreements (SLA) bezeichnet. In diesem Vertrag müssen auch die genauen Modalitäten der Zusammenarbeit geklärt sein: Ansprechpartner, Reaktionszeiten, IT-Anbindung, Kontrolle der Leistungen, Ausgestaltung der IT-Sicherheitsvorkehrungen, Umgang mit vertraulichen Informationen, Verwertungsrechte, Weitergabe von Information an Dritte etc. (siehe hierzu M 2.253 *Vertragsgestaltung mit dem Outsourcing-Dienstleister*).

Phase 5: Erstellung eines IT-Sicherheitskonzepts für den ausgelagerten IT-Verbund

In enger Zusammenarbeit müssen Auftraggeber und Outsourcing-Dienstleister ein detailliertes Sicherheitskonzept (M 2.254 *Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben*), das ein Notfallvorsorgekonzept (M 6.83 *Notfallvorsorge beim Outsourcing*) enthält, erstellen.

Phase 5 wird in der Regel erst nach Beendigung der Migrationsphase abgeschlossen werden können, weil sich während der Migration der IT-Systeme und Anwendungen immer wieder neue Erkenntnisse ergeben, die in das IT-Sicherheitskonzept eingearbeitet werden müssen.

Phase 6: Migrationsphase

Besonders sicherheitskritisch ist die Migrations- oder Übergangsphase, die deshalb einer sorgfältigen Planung bedarf (siehe M 2.255 *Sichere Migration bei Outsourcing-Vorhaben*).

Phase 7: Planung und Sicherstellen des laufenden Betriebs

Wenn der Outsourcing-Dienstleister die Systeme bzw. Geschäftsprozesse übernommen hat, sind verschiedene Maßnahmen, wie regelmäßige Kontrollen und Durchführung von Systemwartungen, zur Aufrechterhaltung der IT-Sicherheit im laufenden Betrieb notwendig (siehe M 2.256 *Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing*-Betrieb). Diese müssen im Vorfeld entsprechend geplant werden. Notfall- und Eskalationsszenarien müssen unbedingt in der Planung mit berücksichtigt werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Outsourcing" vorgestellt.

Planung und Konzeption
- M 2.40 (Z) Rechtzeitige Beteiligung des Personal-/Betriebsrates
- M 2.42 (A) Festlegung der möglichen Kommunikationspartner
- M 2.226 (A) Regelungen für den Einsatz von Fremdpersonal
- M 2.250 (A) Festlegung einer Outsourcing-Strategie
- M 2.251 (A) Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben
- M 2.254 (A) Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben

Beschaffung
- M 2.252 (A) Wahl eines geeigneten Outsourcing-Dienstleisters

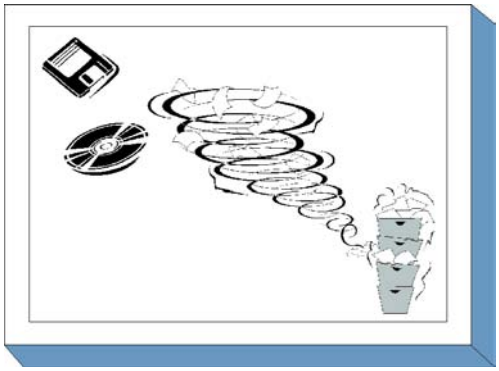
Umsetzung
- M 2.253 (A) Vertragsgestaltung mit dem Outsourcing-Dienstleister
- M 2.255 (A) Sichere Migration bei Outsourcing-Vorhaben
- M 5.87 (A) Vereinbarung über die Anbindung an Netze Dritter
- M 5.88 (A) Vereinbarung über Datenaustausch mit Dritten

Betrieb
- M 2.221 (A) Änderungsmanagement
- M 2.256 (A) Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb
- M 3.33 (Z) Sicherheitsüberprüfung von Mitarbeitern

Aussonderung
- M 2.307 (A) Geordnete Beendigung eines Outsourcing-Dienstleistungsverhältnisses

Notfallvorsorge
- M 6.70 (A) Erstellen eines Notfallplans für den Ausfall des RAS-Systems
- M 6.83 (A) Notfallvorsorge beim Outsourcing

B 1.12 Archivierung



Beschreibung

Die Abbildung von Geschäftsprozessen und -unterlagen in elektronische Dokumente erfordert eine geeignete Ablage der entstehenden Daten für die spätere Verwendung, deren Wiederfinden und Aufbereitung. Dies betrifft sowohl Datensätze als auch elektronische Repräsentationen papierner Geschäftsdokumente und Belege. Die dauerhafte und unveränderbare Speicherung von elektronischen Dokumenten und anderen Daten wird als Archivierung bezeichnet.

Die Archivierung ist als Teil eines Dokumentenmanagement-Prozesses zu sehen. Neben der Erzeugung, Bearbeitung und Verwaltung elektronischer Dokumente spielt die dauerhafte Speicherung (Archivierung) eine besondere Rolle, denn es wird üblicherweise erwartet, dass einerseits die Dokumente bis zum Ablauf einer vorgegebenen Aufbewahrungsfrist verfügbar sind und andererseits deren Vertraulichkeit- und Integrität gewahrt bleibt. Unter Umständen sollen elektronische Dokumente zeitlich unbegrenzt verfügbar sein.

Die technische Ausgestaltung dieses Prozesses erfolgt über Dokumentenmanagement- und Archivsysteme (siehe Abbildung). In diesem Baustein werden ausschließlich elektronische Archivsysteme betrachtet.

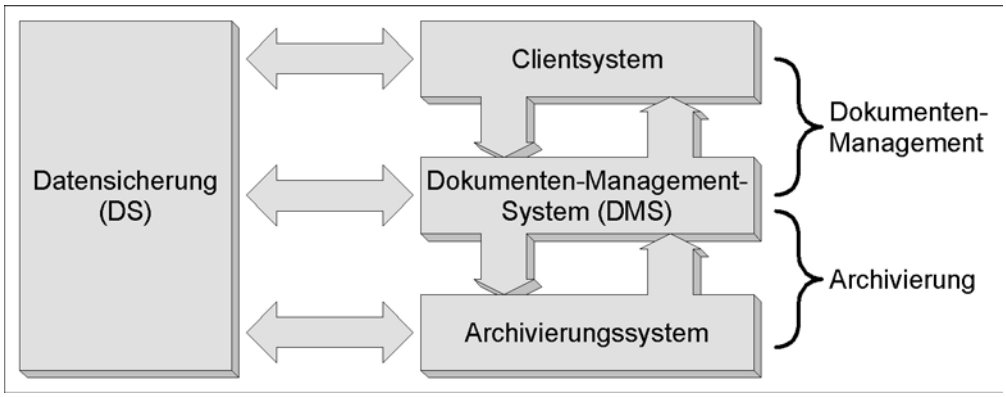


Abbildung: Technische Ausgestaltung der Archivierung über Dokumentenmanagement- und Archivierungssysteme

Die Spannweite der Realisierungsmöglichkeiten eines solchen Archivsystems umfasst:

- kleine Archivsysteme, z. B. bestehend aus einen Archivserver mit angeschlossenem Massenspeicher (wie Festplatte oder Jukebox), bis hin zu
- komplexen, gegebenenfalls weltweit verteilten Archivsystemen zur organisationsweiten Archivierung von relevanten Geschäftsdaten, bestehend aus:
  - zentralen Archivserver-Komponenten mit RAID-Systemen, Jukeboxen oder der Anbindung an Storage Area Networks (SAN) für das zentrale Speichern von Dateien,
  - WORM-Medien für die revisionssichere, unveränderbare Speicherung von Daten,
  - Komponenten zur Indizierung von Dateien, Recherche und zur Umwandlung von Speicherformaten (Rendition),

- dezentralen Cache-Servern für den schnellen Zugriff auf häufig benötigte Daten,
- Client-Software, die einen direkten Zugriff auf Daten des Archivs erlaubt (z. B. auch aus Office-Anwendungen heraus).

Es ist zweckmäßig, elektronische Archive gegenüber Systemen zur Datensicherung abzugrenzen. Bei einer Datensicherung werden Kopien der System- und Nutzdaten angelegt. Die gesicherten Daten werden hierbei physikalisch vom IT-System getrennt und gefahrengeschützt gelagert. Elektronische Archive dagegen sind regelmäßig in den laufenden Systembetrieb eingebunden. Dabei werden üblicherweise große Mengen von Nutzdaten (elektronischen Dokumenten) abgelegt, die aus dem elektronischen Archivsystem heraus jederzeit abgerufen werden können. Bei besonderem Aufbau (z. B. die redundante Auslegung der Speicherkomponenten und eine entsprechende räumliche Anordnung) können größere Archivsysteme teilweise die Funktionalität der Datensicherung (der Nutzdaten) übernehmen.

In diesem Baustein soll ein systematischer Weg aufgezeigt werden, wie ein Konzept zur elektronischen Archivierung erstellt und wie der Aufbau eines Archivsystems und dessen Einbettung innerhalb eines Unternehmens bzw. einer Behörde sichergestellt werden kann. Der Aufwand zur Erstellung und Umsetzung eines solchen Konzepts ist nicht gering. Dieser Baustein sollte immer dann angewandt werden, wenn die zu archivierenden Daten langfristig für die Behörde bzw. das Unternehmen relevant sind.

Gefährdungslage

Für die bei der elektronischen Archivierung zu betrachtenden Archivsysteme sowie die zugehörigen Organisationsprozesse werden im Rahmen des IT-Grundschutzes die folgenden typischen Gefährdungen angenommen:

Höhere Gewalt:
- G 1.2 Ausfall des IT-Systems
- G 1.7 Unzulässige Temperatur und Luftfeuchte
- G 1.9 Datenverlust durch starke Magnetfelder
- G 1.14 Datenverlust durch starkes Licht

Organisatorische Mängel:
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.72 Unzureichende Migration von Archivsystemen
- G 2.73 Fehlende Revisionsmöglichkeit von Archivsystemen
- G 2.74 Unzureichende Ordnungskriterien für Archive
- G 2.75 Mangelnde Kapazität von Archivdatenträgern
- G 2.76 Unzureichende Dokumentation von Archivzugriffen
- G 2.77 Unzulängliche Übertragung von Papierdaten in elektronische Archive
- G 2.78 Unzulängliche Auffrischung von Datenbeständen bei der Archivierung
- G 2.79 Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung
- G 2.80 Unzureichende Durchführung von Revisionen bei der Archivierung
- G 2.81 Unzureichende Vernichtung von Datenträgern bei der Archivierung
- G 2.82 Fehlerhafte Planung des Aufstellungsortes von Speicher- und Archivsystemen

Menschliche Fehlhandlungen:
- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten
- G 3.35 Server im laufenden Betrieb ausschalten
- G 3.54 Verwendung ungeeigneter Datenträger bei der Archivierung
- G 3.55 Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsystemen

Technisches Versagen:

- G 4.7 Defekte Datenträger
- G 4.13 Verlust gespeicherter Daten
- G 4.20 Datenverlust bei erschöpftem Speichermedium
- G 4.26 Ausfall einer Datenbank
- G 4.30 Verlust der Datenbankintegrität/-konsistenz
- G 4.31 Ausfall oder Störung von Netzkomponenten
- G 4.45 Verzögerte Archivauskunft
- G 4.46 Fehlerhafte Synchronisierung von Indexdaten bei der Archivierung
- G 4.47 Veralten von Kryptoverfahren

Vorsätzliche Handlungen:

- G 5.2 Manipulation an Daten oder Software
- G 5.6 Anschlag
- G 5.29 Unberechtigtes Kopieren der Datenträger
- G 5.82 Manipulation eines Kryptomoduls
- G 5.83 Kompromittierung kryptographischer Schlüssel
- G 5.85 Integritätsverlust schützenswerter Informationen
- G 5.102 Sabotage
- G 5.105 Verhinderung der Dienste von Archivsystemen
- G 5.106 Unberechtigtes Überschreiben oder Löschen von Archivmedien

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Darüber hinaus wird die im Folgenden beschriebene Vorgehensweise für die Einführung und den Betrieb von elektronischen Archivsystemen empfohlen. Bereits bei der Planung ist zu berücksichtigen, dass die eingesetzten Archivsysteme und -medien im Lauf der Zeit technologisch und physikalisch veralten werden. Daher schließt sich an eine Planungs- und Einführungs-/Betriebsphase eine Migrationsphase an, in der das bestehende Archivsystem oder Teile davon durch neue Technologien und Komponenten ersetzt werden. Die Migrationsphase umfasst auch die Übertragung der archivierten Daten und Dokumente in zukünftig verwendete Datenformate.

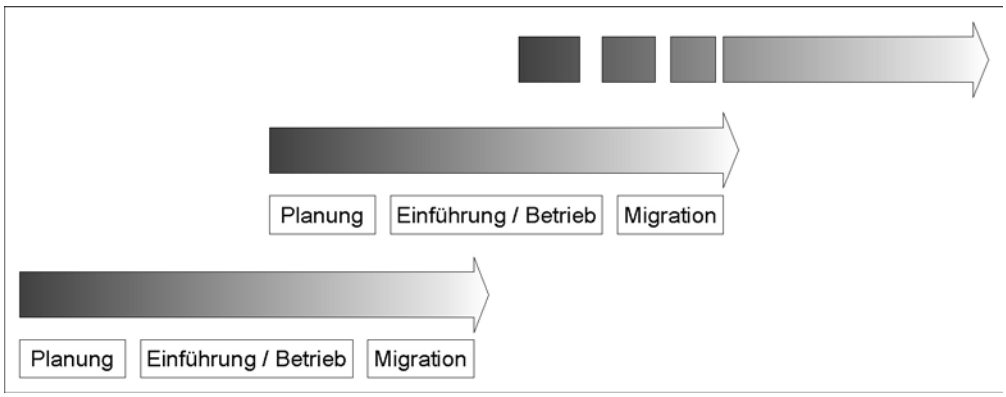


Abbildung: Planung von Migrationsschritten innerhalb der Archivierungssystem-Planung

Die einzelnen Phasen und die darin umzusetzenden Maßnahmen sind nachfolgend kurz erläutert.

1. Planungsphase

In der Planungsphase muss die Zielsetzung , die mit dem Einsatz des Archivsystems verbunden ist, formuliert werden (siehe M 2.242 *Zielsetzung der elektronischen Archivierung*). Hierbei müssen die relevanten organisatorischen, rechtlichen und technischen Anforderungen ermittelt werden, wobei auch abgeschätzt werden muss, wie sich die Anforderungen während der erwarteten Laufzeit des einzuführenden Archivsystems entwickeln werden (siehe M 2.244, M 2.245 und M 2.246). Die Ergebnisse müssen in einem Archivierungskonzept niedergelegt werden (siehe M 2.243).

2. Einführung und Betrieb

Bei der Einführung eines Archivsystems ist zunächst ein System auszuwählen, das den ermittelten Anforderungen genügt. Darüber hinaus sind der Aufstellungsort des Systems sowie der Lagerungsort der Archivmedien festzulegen (siehe M 4.168, M 4.169, M 4.170, M 1.59, M 1.60).

Neben dem Archivsystem als solches muss ein geeignetes übergeordnetes Dokumentenmanagement-System zur Verwaltung der Inhalte des Archivs eingeführt werden (siehe M 2.258, M 2.259).

Es müssen die Regelungen für die Nutzung des Archivsystems sowie den Einsatz digitaler Signaturen festgelegt und die Administratoren und Benutzer geschult werden (siehe M 2.262, M 2.265, M 3.34, M 3.35).

Um die Ordnungsmäßigkeit langfristig sicherstellen zu können, ist der Archivierungsprozess kontinuierlich zu überwachen und auf Korrektheit zu prüfen. Darüber hinaus ist sicherzustellen, dass zu jedem Zeitpunkt genügend Medien zur Archivierung verfügbar sind (siehe M 2.257, M 2.260 M 2.263, M 4.171, M 4.172, M 4.173, M 6.84).

In Abhängigkeit der konkret eingesetzten Archivsoftware müssen auch die in Baustein B 5.7 *Datenbanken* beschriebenen Maßnahmen umgesetzt werden.

3. Migrationsphase

Die Migrationsphase wird häufig durch Ereignisse wie die folgenden ausgelöst:

- Bei Systemkomponenten oder Datenformaten hat ein Technologiewechsel stattgefunden, daher sollten die Entwicklungen in diesem Bereich beobachtet werden (siehe M 2.261 *Regelmäßige Marktbeobachtung von Archivsystemen*).
- Systemkomponenten, insbesondere Datenträger, sind überaltert und müssen durch neue ersetzt werden (siehe M 2.266 *Regelmäßige Erneuerung technischer Archivsystem-Komponenten*).
- Die Nutzungskriterien für das Archivsystem haben sich geändert.
- Kryptographische Verfahren, Produkte bzw. Schlüssel müssen durch neue abgelöst werden (siehe M 2.264 *Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung*).

Nachfolgend wird das Maßnahmenbündel für den Einsatz elektronischer Archivsysteme vorgestellt:

Planung und Konzeption

- M 2.242 (A) Zielsetzung der elektronischen Archivierung
- M 2.243 (A) Entwicklung des Archivierungskonzepts
- M 2.244 (A) Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung
- M 2.245 (A) Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung
- M 2.246 (A) Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung
- M 2.259 (Z) Einführung eines übergeordneten Dokumentenmanagements

- M 2.262 (A) Regelung der Nutzung von Archivsystemen
- M 2.265 (Z) Geeigneter Einsatz digitaler Signaturen bei der Archivierung

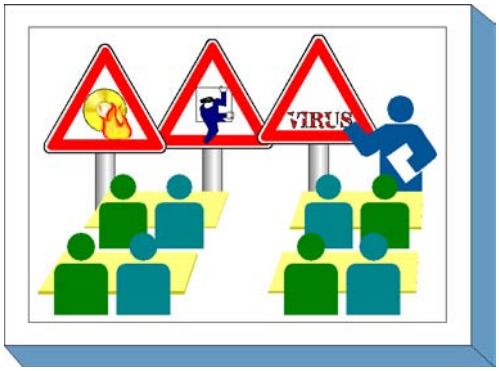
Beschaffung
- M 4.168 (A) Auswahl eines geeigneten Archivsystems
- M 4.169 (A) Verwendung geeigneter Archivmedien
- M 4.170 (A) Auswahl geeigneter Datenformate für die Archivierung von Dokumenten

Umsetzung
- M 1.59 (B) Geeignete Aufstellung von Speicher- und Archivsystemen
- M 2.266 (C) Regelmäßige Erneuerung technischer Archivsystem-Komponenten
- M 3.2 (A) Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
- M 3.34 (A) Einweisung in die Administration des Archivsystems
- M 3.35 (A) Einweisung der Benutzer in die Bedienung des Archivsystems

Betrieb
- M 1.60 (A) Geeignete Lagerung von Archivmedien
- M 2.257 (C) Überwachung der Speicherressourcen von Archivmedien
- M 2.258 (A) Konsistente Indizierung von Dokumenten bei der Archivierung
- M 2.260 (B) Regelmäßige Revision des Archivierungsprozesses
- M 2.261 (B) Regelmäßige Marktbeobachtung von Archivsystemen
- M 2.263 (A) Regelmäßige Aufbereitung von archivierten Datenbeständen
- M 2.264 (B) Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung
- M 4.171 (A) Schutz der Integrität der Index-Datenbank von Archivsystemen
- M 4.172 (C) Protokollierung der Archivzugriffe
- M 4.173 (B) Regelmäßige Funktions- und Recoverytests bei der Archivierung

Notfallvorsorge
- M 6.84 (A) Regelmäßige Datensicherung der System- und Archivdaten

B 1.13 IT-Sicherheitssensibilisierung und -schulung



Beschreibung

Um IT-Sicherheitsmaßnahmen wirkungsvoll umsetzen zu können, muss in einem Unternehmen bzw. einer Behörde eine IT-Sicherheitskultur aufgebaut und ein IT-Sicherheitsbewußtsein gebildet werden. Alle Mitarbeiter müssen davon überzeugt sein, dass IT-Sicherheit einen wesentlichen Teil des Erfolges der jeweiligen Organisation ausmacht. Dazu muss auch kommuniziert werden, warum bestimmte IT-Sicherheitsmaßnahmen notwendig und sinnvoll sind. Ebenso muss allen Mitarbeitern bekannt sein, was von ihnen im Hinblick auf IT-Sicherheit erwartet wird und wie sie in sicherheitskritischen Situationen reagieren sollten. Dies setzt in vielen Bereichen eine langfristige Verhaltensänderung der Mitarbeiter voraus und kann nur in einem langen und kontinuierlichen Prozess erreicht werden. Einmalige Schulungen oder Sensibilisierungsveranstaltungen reichen hier nicht aus.

Informierte und geschulte Mitarbeiter sind Voraussetzungen dafür, dass eine Behörde oder ein Unternehmen die gesteckten Ziele erreichen kann. Außerdem wird durch Information und Schulung sichergestellt, dass alle Mitarbeiter die Folgen und Auswirkungen ihrer Tätigkeit im beruflichen und privaten Umfeld einschätzen können. Ziel der IT-Sicherheitssensibilisierung ist es, das Bewusstsein der Mitarbeiter für Sicherheitsprobleme zu schärfen. Durch Schulungen zur IT-Sicherheit wird den Mitarbeitern die notwendige Kompetenz zur IT-Sicherheit vermittelt, die sie bei der Ausführung ihrer Fachaufgaben benötigen. Es ist sicherzustellen, dass alle Mitarbeiter die Abläufe kennen und wissen, an wen sie sich wenden müssen, falls Sicherheitsfragen auftreten oder Sicherheitsprobleme gelöst werden müssen.

Damit die Durchführung von Schulungs- und Sensibilisierungsmaßnahmen auch nachhaltig unterstützt wird, ist es wichtig, dass das Management auf die Bedeutung der IT-Sicherheit aufmerksam gemacht wird. Dieser Baustein ist also grundsätzlich für alle zu empfehlen, die für die IT-Sicherheit in einer Institution (egal welcher Größe) verantwortlich sind.

In diesem Baustein wird daher beschrieben, wie ein effektives Schulungs- und Sensibilisierungsprogramm zur IT-Sicherheit aufgebaut und aufrechterhalten werden kann.

Gefährdungslage

Für den IT-Grundschutz werden in diesem Baustein die folgenden typische Gefährdungen betrachtet:

Organisatorische Mängel

- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.102 Unzureichende Sensibilisierung für IT-Sicherheit
- G 2.103 Unzureichende Schulung der Mitarbeiter

Menschliche Fehlhandlungen:

- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.44 Sorglosigkeit im Umgang mit Informationen
- G 3.77 Mangelhafte Akzeptanz von IT-Sicherheitsmaßnahmen

Vorsätzliche Handlungen:
- G 5.2 Manipulation an Daten oder Software
- G 5.9 Unberechtigte IT-Nutzung
- G 5.19 Missbrauch von Benutzerrechten
- G 5.20 Missbrauch von Administratorrechten
- G 5.42 Social Engineering
- G 5.104 Ausspähen von Informationen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Um eine umfassende Sensibilisierung für IT-Sicherheitsfragen in einer Institution zu erreichen, sollte ein Programm aufgebaut werden, das unter anderem Schulungen, Trainingsprogramme, Sicherheitskampagnen und andere Aktivitäten beinhalten kann. Damit dieses wirkungsvoll realisiert wird, sind eine Reihe von Schritten zu durchlaufen.

Planung und Konzeption

Die Unterstützung der Leitung ist für den gesamten IT-Sicherheitsprozess notwendig. Dies setzt voraus, dass diese die Bedeutung der IT-Sicherheit hinreichend bekannt ist. In M 3.44 *Sensibilisierung des Managements für IT-Sicherheit* wird beschrieben, wie dies erreicht werden kann.

Zunächst muss das Schulungs- und Sensibilisierungsprogramm strategisch vorbereitet und geplant werden. Die hierfür notwendigen Schritte sind in der Maßnahme M 2.312 *Konzeption eines Schulungs- und Sensibilisierungsprogramms zur IT-Sicherheit* beschrieben und werden durch die daran anschließenden Maßnahmen erläutert. Daher sollte mit der Umsetzung der Maßnahme M 2.312 begonnen werden.

Die Basis jedes Schulungsprogramms sind die Sicherheitsleitlinie und die Sicherheitsrichtlinien, die sowohl übergreifend als auch themenbezogen innerhalb einer Behörde oder eines Unternehmens existieren sollten (siehe M 2.192 *Erstellung einer IT-Sicherheitsleitlinie*).

Beschaffung

Für die Durchführung von Schulungs- und Sensibilisierungsprogrammen wird internes oder externes Personal benötigt, das die Sensibilisierungs- und Schulungsmaßnahmen vorbereiten und durchführen kann, siehe dazu M 3.48 *Auswahl von Trainern oder Schulungsanbietern*.

Umsetzung

Für die Durchführung von Schulungs- und Sensibilisierungsmaßnahmen werden diverse Ressourcen benötigt, beispielsweise Personal für Konzeption und Durchführung oder Räumlichkeiten für Schulungen. Besondere Sicherheitsaspekte, die bei der Gestaltung von Schulungsräumen zu beachten sind, finden sich in Baustein B 2.11 *Besprechungs-, Veranstaltungs- und Schulungsräume*.

Schulungsinhalte zur IT-Sicherheit müssen je nach Zielgruppe geeignet ausgewählt werden, siehe M 3.45 *Planung von Schulungsinhalten zur IT-Sicherheit.*

Betrieb, Kontinuierliche Pflege und Weiterentwicklung

Ein stets unabdingbarer Bestandteil der Schulungen zur IT-Sicherheit ist dabei der Umgang mit IT (siehe M 3.4 *Schulung vor Programmnutzung*, M 3.11 *Schulung des Wartungs- und Administrationspersonals*, M 3.26 *Einweisung des Personals in den sicheren Umgang mit IT* und weitere themenspezifische Maßnahmen).

Bei der Einführung neuer Techniken sollten die Mitarbeiter frühzeitig über diese informiert sowie für Gefahrenpotentiale und Sicherheitsmaßnahmen sensibilisiert werden, damit die neuen Techniken auch ordnungsgemäß eingesetzt werden.

Wie die Organisation die Bildung eines IT-Sicherheitsbewußtseins bei den Mitarbeitern fördern kann, wird in M 2.198 *Sensibilisierung der Mitarbeiter für IT-Sicherheit* und M 3.47 *Durchführung von Planspielen zur IT-Sicherheit* beschrieben.

Es sollte zu Sicherheitsfragen auch immer geeignete Ansprechpartner geben, siehe M 3.46 *Ansprechpartner zu Sicherheitsfragen*.

Nachfolgend wird das Maßnahmenbündel für den Bereich "IT-Sicherheitssensibilisierung und -schulung" vorgestellt. Auf eine Wiederholung von Maßnahmen anderer Bausteine wird hier aus Redundanzgründen verzichtet.

Planung und Konzeption
- M 2.312 (A) Konzeption eines Schulungs- und Sensibilisierungsprogramms zur IT-Sicherheit
- M 3.44 (A) Sensibilisierung des Managements für IT-Sicherheit

Beschaffung
- M 3.48 (A) Auswahl von Trainern oder Schulungsanbietern

Umsetzung
- M 3.45 (A) Planung von Schulungsinhalten zur IT-Sicherheit
- M 3.5 (A) Schulung zu IT-Sicherheitsmaßnahmen
- M 3.46 (A) Ansprechpartner zu Sicherheitsfragen
- M 3.49 (B) Schulung zur Vorgehensweise nach IT-Grundschutz

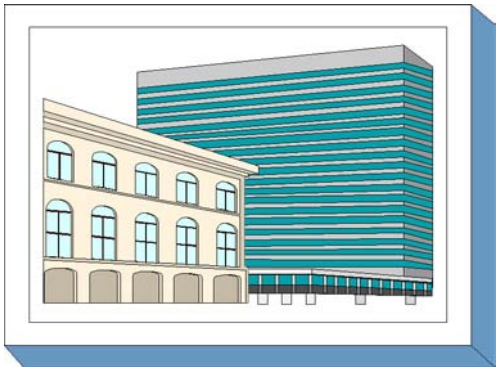
Betrieb
- M 2.198 (A) Sensibilisierung der Mitarbeiter für IT-Sicherheit
- M 3.4 (A) Schulung vor Programmnutzung
- M 3.11 (A) Schulung des Wartungs- und Administrationspersonals
- M 3.26 (A) Einweisung des Personals in den sicheren Umgang mit IT
- M 3.47 (Z) Durchführung von Planspielen zur IT-Sicherheit

2 Infrastruktur

In der Schicht Infrastruktur sind folgende Bausteine enthalten:

B 2.1 Gebäude
B 2.2 Verkabelung
B 2.3 Büroraum
B 2.4 Serverraum
B 2.5 Datenträgerarchiv
B 2.6 Raum für technische Infrastruktur
B 2.7 Schutzschränke
B 2.8 Häuslicher Arbeitsplatz
B 2.9 Rechenzentrum
B 2.10 Mobiler Arbeitsplatz
B 2.11 Besprechungs-, Veranstaltungs- und Schulungsräume

B 2.1 Gebäude



Beschreibung

Das Gebäude umgibt die aufgestellte Informationstechnik und gewährleistet somit einen äußeren Schutz. Weiterhin ermöglichen die Infrastruktureinrichtungen des Gebäudes erst den IT-Betrieb. Daher ist einerseits das Bauwerk, also Wände, Decken, Böden, Dach, Fenster und Türen zu betrachten und andererseits alle gebäudeweiten Versorgungseinrichtungen wie Strom, Wasser, Gas, Heizung, Rohrpost etc. Die Verkabelung in einem Gebäude wird in Baustein B 2.2 *Verkabelung* gesondert betrachtet, die TK-Anlage in Baustein B 3.401 *TK-Anlage*.

Gefährdungslage

Für den IT-Grundschutz eines Gebäudes werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.3 Blitz
- G 1.4 Feuer
- G 1.5 Wasser

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen

Menschliche Fehlhandlungen:
- G 3.85 Verletzung von Brandschottungen

Technisches Versagen:
- G 4.1 Ausfall der Stromversorgung
- G 4.2 Ausfall interner Versorgungsnetze
- G 4.3 Ausfall vorhandener Sicherungseinrichtungen

Vorsätzliche Handlungen:
- G 5.3 Unbefugtes Eindringen in ein Gebäude
- G 5.4 Diebstahl
- G 5.5 Vandalismus
- G 5.6 Anschlag

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Bei der Nutzung von Gebäuden für den Betrieb von IT-Systemen sind hinsichtlich der IT-Sicherheit bei bestimmten Maßnahmen unterschiedliche Vorgehensweisen zu verfolgen. Bei einem Neubau können erforderliche Maßnahmen zu einem großen Teil schon in der Planungsphase durchgeführt werden. Wenn es sich dagegen um eine Anmietung oder die Nutzung eines bestehenden Gebäudes handelt, was eventuell mit Erweiterungs- bzw. Umbaumaßnahmen verbunden sein kann, sind die Möglichkeiten zur Realisierung einer adäquaten IT-Sicherheit oft viel stärker eingeschränkt.

Planungsphase

Bei der Raumbelegungsplanung ist M 1.8 *Raumbelegung unter Berücksichtigung von Brandlasten* sowie, im Falle einer Nutzung eines bestehenden Gebäudes, M 1.13 *Anordnung schützenswerter Gebäudeteile* anzuwenden. Entsprechend der geplanten Raumnutzung sind die zu erwartenden elektrischen Anschlusswerte zu bestimmen (siehe M 1.3 *Angepasste Aufteilung der Stromkreise)*.

Bauphase und Vorbereitung für Nutzung

Während der Bauphase sind alle in der Planungsphase als erforderlich bewerteten Schutzmaßnahmen umzusetzen. In der Bauphase sind in jedem Fall die Maßnahmen M 1.1 *Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften* und M 1.6 *Einhaltung von Brandschutzvorschriften* anzuwenden. M 1.2 *Regelungen für Zutritt zu Verteilern* sowie M 2.14 *Schlüsselverwaltung* sind spätestens beim Einzug in ein Gebäude festzulegen. Ebenso ist eine Zutrittsregelung und ein Zutrittskontrollkonzept gemäß M 2.17 *Zutrittsregelung und -kontrolle* erforderlich.

Gebäudenutzung

Während der Gebäudenutzungsphase ist insbesondere die regelmäßige Anwendung von M 2.15 *Brandschutzbegehungen* vorzusehen, womit die Einhaltung der vorgegebenen Vorschriften zum Brandschutz überwacht wird.Durch die Anwendung und regelmäßige Überwachung der Maßnahme M 1.15 *Geschlossene Fenster und Türen* ist sicherzustellen, dass sich nur befugte Personen im Gebäude aufhalten und dass zumindest eine elementare Vorsorge gegen Einbrüche getroffen wird.

Notfallvorsorge

Um für den Notfall gerüstet zu sein, ist ein Alarmierungsplan zu erstellen, und in regelmäßigen Abständen sind auch Notfallübungen durchzuführen, da andernfalls zu erwarten ist, dass bei einem Notfall falsche Entscheidungen getroffen werden bzw. Unklarheit über die notwendigen Operationen herrscht (siehe M 6.17 *Alarmierungsplan und Brandschutzübungen*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "Gebäude" vorgestellt:

Planung und Konzeption

- M 1.3 (A) Angepasste Aufteilung der Stromkreise
- M 1.4 (B) Blitzschutzeinrichtungen
- M 1.5 (Z) Galvanische Trennung von Außenleitungen
- M 1.7 (A) Handfeuerlöscher
- M 1.8 (A) Raumbelegung unter Berücksichtigung von Brandlasten
- M 1.10 (Z) Verwendung von Sicherheitstüren und -fenstern
- M 1.11 (A) Lagepläne der Versorgungsleitungen
- M 1.12 (A) Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
- M 1.13 (Z) Anordnung schützenswerter Gebäudeteile
- M 1.14 (Z) Selbsttätige Entwässerung
- M 1.16 (Z) Geeignete Standortauswahl
- M 1.18 (Z) Gefahrenmeldeanlage
- M 1.19 (Z) Einbruchsschutz
- M 2.334 (Z) Auswahl eines geeigneten Gebäudes

Umsetzung

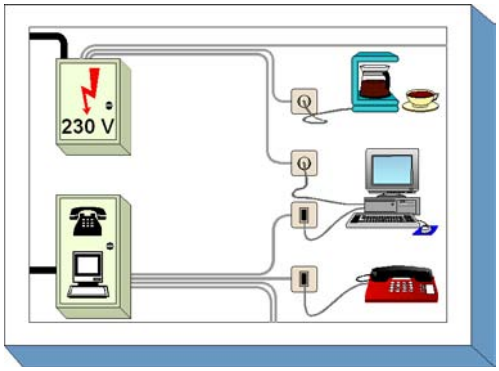
- M 1.1 (A) Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
- M 1.2 (A) Regelungen für Zutritt zu Verteilern
- M 1.6 (A) Einhaltung von Brandschutzvorschriften
- M 1.17 (Z) Pförtnerdienst
- M 2.17 (A) Zutrittsregelung und -kontrolle

Betrieb
- M 1.15 (A) Geschlossene Fenster und Türen
- M 2.14 (A) Schlüsselverwaltung
- M 2.15 (B) Brandschutzbegehungen
- M 2.391 (A) Frühzeitige Information des Brandschutzbeauftragten

Aussonderung
- M 2.308 (Z) Auszug aus Gebäuden

Notfallvorsorge
- M 6.17 (A) Alarmierungsplan und Brandschutzübungen

B 2.2 Verkabelung



Beschreibung

Die Verkabelung von IT-Systemen umfasst alle Kabel und passiven Komponenten (Rangier-/Spleißverteiler) der Netze vom evtl. vorhandenen Übergabepunkt aus einem Fremdnetz (Telefon, ISDN) bis zu den Anschlusspunkten der Netzteilnehmer. Aktive Netzkomponenten (Repeater, Sternkoppler, Bridges etc.) sind nicht Bestandteil dieses Kapitels.

Gefährdungslage

Für den IT-Grundschutz der Verkabelung werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.4 Feuer
- G 1.6 Kabelbrand

Organisatorische Mängel:
- G 2.11 Unzureichende Trassendimensionierung
- G 2.12 Unzureichende Dokumentation der Verkabelung
- G 2.13 Unzureichend geschützte Verteiler
- G 2.32 Unzureichende Leitungskapazitäten

Menschliche Fehlhandlungen:
- G 3.4 Unzulässige Kabelverbindungen
- G 3.5 Unbeabsichtigte Leitungsbeschädigung

Technisches Versagen:
- G 4.4 Leitungsbeeinträchtigung durch Umfeldfaktoren
- G 4.5 Übersprechen
- G 4.21 Ausgleichsströme auf Schirmungen
- G 4.62 Verwendung unzureichender Steckdosenleisten
- G 4.63 Verstaubte Lüfter

Vorsätzliche Handlungen:
- G 5.7 Abhören von Leitungen
- G 5.8 Manipulation an Leitungen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für die Verkabelung sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Umsetzung bis zum Betrieb und zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt. Wie beim Gebäude, so ist auch hier zu beachten, dass die Einflussmöglichkeiten beim Einzug in ein schon bestehendes Gebäude auch bei der Absicherung der Verkabelung wesentlich geringer sind als bei der Errichtung eines Neubaus.

Planung und Konzeption

In der Planungsphase werden die Grundlagen für eine leistungsfähige, gut abgesicherte Verkabelung gelegt, indem die Netzstruktur festgelegt (siehe Maßnahme M 5.2 Auswahl einer geeigneten Netz-Topographie) und in das Gebäude eingepasst wird (siehe Maßnahme M 1.21 Ausreichende Trassendimensionierung). Die mechanischen und elektrischen Eigenschaften der Verkabelung werden weitgehend durch die Auswahl der einzusetzenden Kabeltypen festgelegt. Bei der Planung sollte nach Möglichkeit auch darauf geachtet werden, dass Leitungen und über das Gebäude verteilte Schaltschränke gegen Missbrauch in geeigneter Weise physisch gesichert werden.

Umsetzung

Ein wesentliches Element des Brandschutzes ist die richtige Installation von Kabelkanälen, die durch eine fehlende Brandabschottung erhebliche Risiken verursachen können. Beim Einbau der Verkabelung ist auch auf eine ausführliche und korrekte Dokumentation zu achten, da es im Nachhinein meist sehr schwierig oder sogar unmöglich ist festzustellen, wo Kabel verlaufen und was sie verbinden.

Betrieb

Um das Aufschalten unzulässiger Geräte zu verhindern, sollten jeweils nur die Verbindungen und Anschlussdosen aktiviert sein, die tatsächlich benötigt werden, und durch regelmäßige Kontrollen sollte nach Möglichkeit sichergestellt werden, dass diese Aktivierung auch den tatsächlichen Erfordernissen entspricht.

Notfallvorsorge

Sofern erhöhte Anforderungen an die Verfügbarkeit gestellt werden, sollte die Verkabelung, gegebenenfalls einschließlich der externen Anschlüsse, so redundant ausgelegt werden, dass ein Schaden an einer einzigen Stelle nicht zu einem Totalausfall des gesamten Netzes führen kann.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Verkabelung" vorgestellt:

Planung und Konzeption

- M 1.20 (A) Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht (bei Verkabelung neuer Netze)
- M 1.21 (A) Ausreichende Trassendimensionierung (bei Verkabelung neuer Netze)
- M 1.22 (Z) Materielle Sicherung von Leitungen und Verteilern
- M 5.2 (A) Auswahl einer geeigneten Netz-Topographie
- M 5.3 (A) Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht

Umsetzung

- M 1.9 (A) Brandabschottung von Trassen
- M 1.39 (Z) Verhinderung von Ausgleichsströmen auf Schirmungen
- M 2.19 (B) Neutrale Dokumentation in den Verteilern
- M 5.4 (A) Dokumentation und Kennzeichnung der Verkabelung
- M 5.5 (A) Schadensmindernde Kabelführung (bei Verkabelung neuer Netze)
- M 1.64 (A) Vermeidung elektrischer Zündquellen

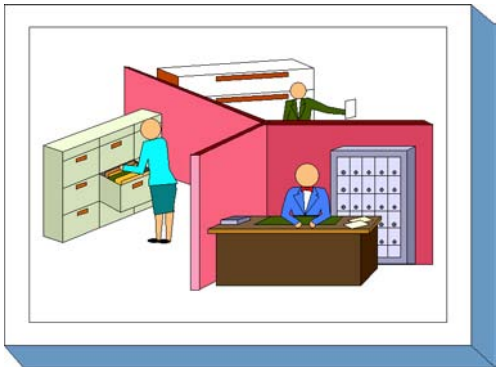
Betrieb

- M 2.20 (Z) Kontrolle bestehender Verbindungen
- M 5.1 (B) Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen

Notfallvorsorge

- M 6.18 (Z) Redundante Leitungsführung

B 2.3 Büroraum



Beschreibung

Der Büroraum ist ein Raum, in dem sich ein oder mehrere Mitarbeiter aufhalten, um dort der Erledigung ihrer Aufgaben eventuell auch IT-unterstützt nachzugehen. Diese Aufgaben können aus den verschiedensten Tätigkeiten bestehen: Erstellung von Schriftstücken, Bearbeitung von Karteien und Listen, Durchführung von Besprechungen und Telefonaten, Lesen von Akten und sonstigen Unterlagen.

Wird jedoch ein Büroraum überwiegend zur Archivierung von Datenträgern genutzt, ist zusätzlich Baustein B 2.5 *Datenträgerarchiv* zu beachten. Ist in einem Büroraum ein Server (z. B. für ein LAN, oder eine TK-Anlage) aufgestellt, sind zusätzlich die Maßnahmen aus Baustein B 2.4 *Serverraum* zu beachten.

Gefährdungslage

Für den IT-Grundschutz eines Büroraums werden folgende typische Gefährdungen angenommen:

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen
- G 2.14 Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen

Menschliche Fehlhandlungen:
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.5 Vandalismus

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Büroräume sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung bis hin zu ihrer Nutzung. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Beschaffung

In Büros mit Publikumsverkehr sollten Diebstahlsicherungen zum Schutz von Notebooks vorgesehen werden, da andernfalls die Gefahr relativ groß ist, dass solche Geräte in einem unbewachten Augenblick "verschwinden". Ein hinreichend dreister Täter braucht nicht viel Zeit, um sich ein Notebook oder einen Organizer zu verschaffen und den Raum damit zu verlassen.

Umsetzung

Auch für Büroräume sollte festgelegt werden, wer unter welchen Bedingungen Zutritt erhält. Insbesondere ist zu entscheiden, für welche Büros Publikumsverkehr vorgesehen wird und welche nur den Mitarbeitern des Unternehmens oder der Behörde offen stehen.

Betrieb

Unter Beachtung der Zutrittsregelungen und des Zutrittsschutzes zum Gebäude ist auch festzulegen, ob Büros bei Abwesenheit der Mitarbeiter grundsätzlich zu verschließen sind. Je nach den baulichen Gegebenheiten muss auch dafür gesorgt werden, dass kein Zutritt über einen Balkon bzw. durch ein ungesichertes Fenster möglich ist.

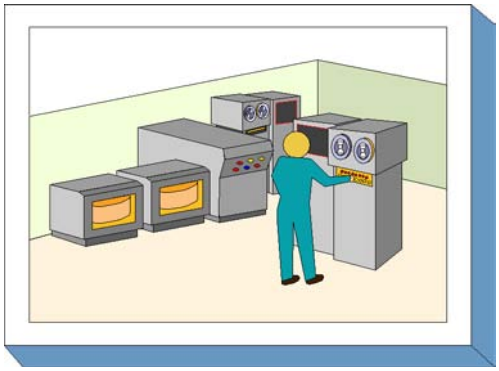
Nachfolgend wird das Maßnahmenbündel für den Bereich "Büroraum" vorgestellt:

Planung und Konzeption
- M 3.9 (Z) Ergonomischer Arbeitsplatz

Umsetzung
- M 2.17 (A) Zutrittsregelung und -kontrolle

Betrieb
- M 1.15 (A) Geschlossene Fenster und Türen
- M 1.23 (A) Abgeschlossene Türen
- M 1.46 (Z) Einsatz von Diebstahl-Sicherungen

B 2.4 Serverraum



Beschreibung

Der Serverraum dient in erster Linie zur Unterbringung von Servern, z. B. eines LAN-Servers, eines Unix-Zentralrechners oder eines Servers für eine TK-Anlage. Darüber hinaus können dort serverspezifische Unterlagen, Datenträger in kleinem Umfang oder weitere Hardware (Sternkoppler, Protokolldrucker, Klimatechnik) vorhanden sein.

In einem Serverraum ist kein ständig besetzter Arbeitsplatz eingerichtet, er wird nur sporadisch und zu kurzfristigen Arbeiten betreten. Zu beachten ist jedoch, dass im Serverraum aufgrund der Konzentration von IT-Geräten und Daten ein deutlich höherer Schaden eintreten kann als zum Beispiel in einem Büroraum.

Gefährdungslage

Für den IT-Grundschutz eines Serverraumes werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.4 Feuer
- G 1.5 Wasser
- G 1.7 Unzulässige Temperatur und Luftfeuchte
- G 1.16 Ausfall von Patchfeldern durch Brand

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen

Technisches Versagen:
- G 4.1 Ausfall der Stromversorgung
- G 4.2 Ausfall interner Versorgungsnetze
- G 4.6 Spannungsschwankungen/Überspannung/Unterspannung

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.3 Unbefugtes Eindringen in ein Gebäude
- G 5.4 Diebstahl
- G 5.5 Vandalismus

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Bei der Auswahl und Gestaltung eines Serverraums sind eine Reihe infrastruktureller und organisatorischer Maßnahmen umzusetzen, die in M 1.58 *Technische und organisatorische Vorgaben für Serverräume* beschrieben sind. Dabei sind bei bestimmten Maßnahmen unterschiedliche Vorgehensweisen zu verfolgen, je nachdem, ob ein Serverraum in einem neu zu errichtenden Gebäude eingerichtet werden soll oder ob es sich um eine Anmietung oder die Nutzung eines bestehenden Gebäudes

handelt. In diesem zweiten Fall sind die Möglichkeiten zur Realisierung einer adäquaten IT-Sicherheit oft viel stärker eingeschränkt. Die Schritte, die bei der Gestaltung eines Serverraums durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Bei der Planung von Serverräumen ist durch eine Reihe von Maßnahmen zur Installation der Stromversorgung, einer eventuell notwendigen Klimatisierung und zum Brandschutz dafür zu sorgen, dass eine hinreichende physische Sicherheit bereitgestellt wird. Dazu gehört auch, dass nach Möglichkeit keine wasserführenden Leitungen in einem Serverraum vorhanden sein sollten, da Undichtigkeiten größere Schäden bis hin zum Ausfall des gesamten IT-Verbundes verursachen können. Bei erhöhten Verfügbarkeitsanforderungen sollten für Serverräume hinreichende Redundanzen in der technischen Infrastruktur geplant werden, um die Überbrückung einzelner Ausfälle zu ermöglichen.

Umsetzung

Nur diejenigen Personen, die zur Durchführung ihrer Aufgaben direkten Zugriff auf Server und sonstige im Serverraum installierte Geräte wie Kommunikationsverteiler, Firewalls etc. benötigen, sollten Zutritt zu einem Serverraum erhalten, und ein Rauchverbot sollte dort selbstverständlich sein.

Betrieb

Serverräume sollten grundsätzlich immer verschlossen sein, wenn sie nicht besetzt sind.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Serverraum" vorgestellt:

Planung und Konzeption

- M 1.3 (A) Angepasste Aufteilung der Stromkreise
- M 1.7 (A) Handfeuerlöscher
- M 1.10 (C) Verwendung von Sicherheitstüren und -fenstern
- M 1.18 (Z) Gefahrenmeldeanlage
- M 1.24 (C) Vermeidung von wasserführenden Leitungen
- M 1.25 (B) Überspannungsschutz
- M 1.26 (Z) Not-Aus-Schalter
- M 1.27 (B) Klimatisierung
- M 1.28 (B) Lokale unterbrechungsfreie Stromversorgung
- M 1.31 (Z) Fernanzeige von Störungen
- M 1.52 (Z) Redundanzen in der technischen Infrastruktur
- M 1.58 (A) Technische und organisatorische Vorgaben für Serverräume
- M 1.62 (C) Brandschutz von Patchfeldern

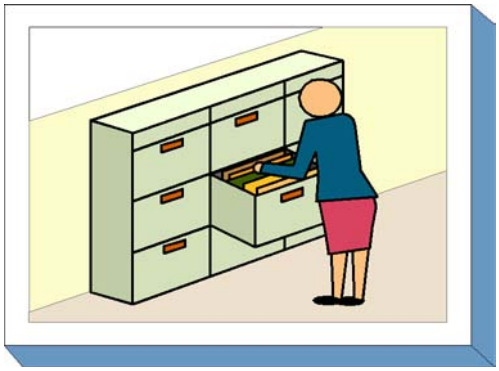
Umsetzung

- M 2.17 (A) Zutrittsregelung und -kontrolle
- M 2.21 (A) Rauchverbot

Betrieb

- M 1.15 (A) Geschlossene Fenster und Türen
- M 1.23 (A) Abgeschlossene Türen

B 2.5 Datenträgerarchiv



Beschreibung

Das Datenträgerarchiv dient der Lagerung von Datenträgern jeder Art. Im Rahmen des IT-Grundschutzes werden an den Archivraum hinsichtlich des Brandschutzes keine erhöhten Anforderungen gestellt. Der Brandschutz kann entsprechend den Bedürfnissen des IT-Betreibers durch die Behältnisse, in denen die Datenträger aufbewahrt werden, realisiert werden.

Bei zentralen Datenträgerarchiven und Datensicherungsarchiven ist die Nutzung von Datensicherungsschränken (siehe Baustein 2.7) empfehlenswert, um den Brandschutz, den Schutz gegen unbefugten Zugriff und die Durchsetzung von Zugangsberechtigungen zu unterstützen.

Der Baustein 2.5 Datenträgerarchiv eignet sich grundsätzlich auch für Papier-, Film- oder sonstige Akten, auch wenn er nicht primär auf diesen Anwendungsfall ausgerichtet ist. Einige Empfehlungen in den zugeordneten Maßnahmen müssen dann entsprechend uminterpretiert werden.

Gefährdungslage

Für den IT-Grundschutz eines Datenträgerarchivs werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.4 Feuer
- G 1.5 Wasser
- G 1.7 Unzulässige Temperatur und Luftfeuchte
- G 1.8 Staub, Verschmutzung

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen

Vorsätzliche Handlungen:
- G 5.3 Unbefugtes Eindringen in ein Gebäude
- G 5.4 Diebstahl
- G 5.5 Vandalismus

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für das Datenträgerarchiv sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption bis zum täglichen Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Die Grundstruktur des Datenträgerarchivs und damit die wesentlichen Randbedingungen seiner Nutzung werden bei der Planung und Konzeption festgelegt. Hier bestehen naturgemäß bei der Einrichtung eines neuen Gebäudes größere Freiheiten. Wenn ein Datenträgerarchiv in einem schon existierenden Gebäude installiert werden soll, sind die verbleibenden Möglichkeiten der Strukturierung bei der Nutzung eines Gebäudes meist nur noch gering, vor allem bei angemieteten Gebäuden.

Mit der Auswahl des Raumes, in dem das Archiv untergebracht wird, stehen dessen Schutzeigenschaften schon zu einem großen Teil fest, und nachträgliche Korrekturen wie die Entfernung wasserführender Leitungen sind oft nur noch mit erheblichem Aufwand zu realisieren. Notwendige technische Installationen wie eine Klimatisierung oder der Einsatz einer Gefahrenmeldeanlage sollten daher nach Möglichkeit schon bei der Planung oder Auswahl des Datenträgerarchivs vorgesehen werden.

Umsetzung

Vor der Inbetriebnahme des Datenträgerarchivs sind organisatorische Regelungen festzulegen, die einen geordneten und sicheren Betrieb unterstützen.

Betrieb

Im laufenden Betrieb ist durch entsprechende Kontrolle zu gewährleisten, dass die vorgesehenen Regelungen in der Praxis tatsächlich angewendet werden. Hierzu gehört vor allem, dass gewährleistet wird, dass nur die Personen Zutritt haben, die dazu berechtigt sind, und dass das Archiv abgeschlossen ist, solange sich dort niemand aufhält.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Datenträgerarchiv" vorgestellt:

Planung und Konzeption

- M 1.7 (A) Handfeuerlöscher
- M 1.10 (C) Verwendung von Sicherheitstüren und -fenstern
- M 1.18 (Z) Gefahrenmeldeanlage
- M 1.24 (Z) Vermeidung von wasserführenden Leitungen
- M 1.27 (Z) Klimatisierung

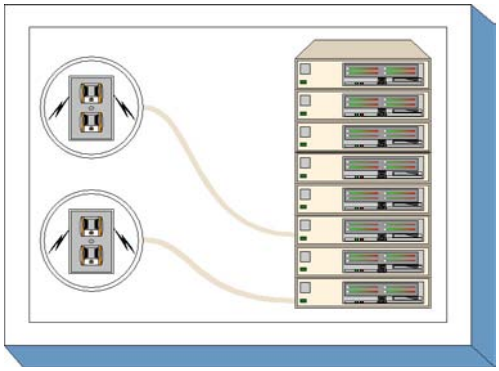
Umsetzung

- M 2.17 (A) Zutrittsregelung und -kontrolle
- M 2.21 (A) Rauchverbot

Betrieb

- M 1.15 (A) Geschlossene Fenster und Türen
- M 1.23 (A) Abgeschlossene Türen

B 2.6 Raum für technische Infrastruktur



Beschreibung

In Räumen für technische Infrastruktur sind in der Regel solche Geräte und Einrichtungen untergebracht, die keine oder nur eine seltene Bedienung durch einen Menschen benötigen. In der Regel wird es sich um Verteiler interner Versorgungsnetze handeln (z. B. Postkabeleingangsraum, Hochspannungsübergaberaum, Mittelspannungsübergaberaum, Niederspannungshauptverteiler). Eventuell werden in diesen Räumen auch die Sicherungen der Elektroversorgung untergebracht. Auch die Aufstellung sonstiger Geräte (USV, Sternkoppler, etc.) ist vorstellbar. Selbst ein Netzserver kann, wenn er keinen eigenen Raum hat (Baustein B 2.4 *Serverraum*), hier untergebracht sein.

Gefährdungslage

Für den IT-Grundschutz eines Raums für technische Infrastruktur werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.4 Feuer
- G 1.5 Wasser
- G 1.7 Unzulässige Temperatur und Luftfeuchte

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen

Technisches Versagen:
- G 4.1 Ausfall der Stromversorgung
- G 4.2 Ausfall interner Versorgungsnetze
- G 4.6 Spannungsschwankungen/Überspannung/Unterspannung

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.3 Unbefugtes Eindringen in ein Gebäude
- G 5.4 Diebstahl
- G 5.5 Vandalismus

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Infrastrukturräume sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung bis hin zum laufenden Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Bei der Planung von Infrastrukturräumen ist durch eine Reihe von Maßnahmen zur Installation der Stromversorgung, einer eventuell notwendigen Klimatisierung und zum Brandschutz dafür zu sorgen, dass eine hinreichende physische Sicherheit bereitgestellt wird. Dazu gehört auch, dass nach

Möglichkeit keine wasserführenden Leitungen in einem solchen, meist unbesetzten, Raum vorhanden sein sollten, da Undichtigkeiten größere Schäden bis hin zum Ausfall des gesamten IT-Verbundes verursachen können. Bei erhöhten Sicherheitsanforderungen sollten Infrastrukturräume darüber hinaus durch besonders gesicherte Türen und Fenster auch gegen gewaltsames Eindringen geschützt werden, da sie oft bevorzugte Angriffsziele darstellen.

Umsetzung

Nur diejenigen Personen, die mit den entsprechenden technischen Wartungsaufgaben betraut sind, sollten Zutritt zu einem Infrastrukturraum erhalten, und ein Rauchverbot sollte dort selbstverständlich sein.

Betrieb

Räume für die technische Infrastruktur sollten grundsätzlich immer verschlossen sein, wenn die dort aufgestellten Geräte nicht so in Schränken verschlossen sind, dass keine unbefugte Nutzung möglich ist.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Raum für technische Infrastruktur" vorgestellt:

Planung und Konzeption

- M 1.3 (A) Angepasste Aufteilung der Stromkreise
- M 1.7 (A) Handfeuerlöscher
- M 1.10 (Z) Verwendung von Sicherheitstüren und -fenstern
- M 1.18 (Z) Gefahrenmeldeanlage
- M 1.24 (Z) Vermeidung von wasserführenden Leitungen
- M 1.25 (A) Überspannungsschutz
- M 1.26 (Z) Not-Aus-Schalter
- M 1.27 (B) Klimatisierung
- M 1.31 (Z) Fernanzeige von Störungen

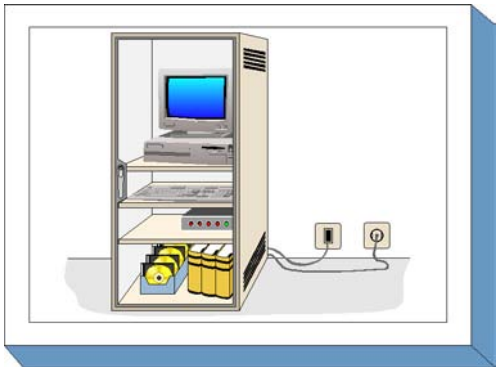
Umsetzung

- M 2.17 (A) Zutrittsregelung und -kontrolle
- M 2.21 (A) Rauchverbot

Betrieb

- M 1.15 (A) Geschlossene Fenster und Türen
- M 1.23 (A) Abgeschlossene Türen

B 2.7 Schutzschränke



Beschreibung

Schutzschränke dienen zur Aufbewahrung von Datenträgern jeder Art oder zur Unterbringung von informationstechnischen Geräten ("Serverschrank"). Diese Schutzschränke sollen den Inhalt gegen unbefugten Zugriff und/oder gegen die Einwirkung von Feuer oder schädigenden Stoffen (z. B. Staub) schützen. Sie können als Ersatz für einen Serverraum oder ein Datenträgerarchiv (siehe Bausteine B 2.4 und B 2.5) eingesetzt werden, wenn die vorhandenen räumlichen oder organisatorischen Gegebenheiten eigene Räume nicht zulassen. Sollen ausschließlich Datenträger und inaktive IT-Geräte aufbewahrt werden, ist hierfür ein entsprechend geeigneter Datensicherungsschrank auf Grundlage der Normen EN 1047-1 und EN 1047-2 vorzuziehen.

Darüber hinaus können Schutzschränke auch in Serverräumen oder Datenträgerarchiven eingesetzt werden, um die Schutzwirkung der Räume zu erhöhen. Sie sind auch zu empfehlen, wenn in einem Serverraum Server aus unterschiedlichen Organisationsbereichen aufgestellt sind, die dem jeweils anderen Administrator nicht zugänglich sein sollen.

Um mit einem Schutzschrank einen mit den dedizierten Räumen vergleichbaren Schutz zu erreichen, sind eine Reihe von Maßnahmen, beginnend mit der geeigneten Auswahl bis zur Aufstellung und Nutzungsregelung, notwendig. Diese werden im vorliegenden Baustein vorgestellt.

Gefährdungslage

Für den IT-Grundschutz von Schutzschränken werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.4 Feuer
- G 1.5 Wasser
- G 1.7 Unzulässige Temperatur und Luftfeuchte (nur Serverschrank)
- G 1.8 Staub, Verschmutzung

Organisatorische Mängel:
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen

Menschliche Fehlhandlungen:
- G 3.21 Fehlbedienung von Codeschlössern

Technisches Versagen:
- G 4.1 Ausfall der Stromversorgung (nur Serverschrank)
- G 4.2 Ausfall interner Versorgungsnetze (nur Serverschrank)
- G 4.3 Ausfall vorhandener Sicherungseinrichtungen
- G 4.4 Leitungsbeeinträchtigung durch Umfeldfaktoren

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.4 Diebstahl
- G 5.5 Vandalismus

- G 5.16 Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal
- G 5.17 Gefährdung bei Wartungsarbeiten durch externes Personal
- G 5.53 Bewusste Fehlbedienung von Schutzschränken aus Bequemlichkeit

Maßnahmenempfehlungen

Zur Realisierung des IT-Grundschutzes wird empfohlen, die notwendigen Maßnahmenbündel ("Bausteine") gemäß den Ergebnissen der Modellierung auszuwählen.

Für Auswahl und Einsatz von Schutzschränken sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption über die Beschaffung bis hin zu ihrer Nutzung. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Vor der Beschaffung eines Schutzschranks sollte zunächst ein Konzept erstellt werden, das auf den Anforderungen aus den geplanten Einsatzszenarien beruht (siehe M 2.311 *Planung von Schutzschränken*).

Beschaffung

Die Maßnahme M 2.95 *Beschaffung geeigneter Schutzschränke* nennt die wesentlichen Kriterien, die bei der Auswahl eines Schutzschranks zu beachten sind.

Umsetzung

Nur diejenigen Personen, die mit den entsprechenden technischen Wartungsaufgaben betraut sind, sollten Zutritt zum Schutzschrank erhalten, und sie sollten eine entsprechende Einweisung in die Bedienung des Schutzschranks erhalten. Ein Rauchverbot sollte für den Schutzschrankraum selbstverständlich sein. Hinweise für die Aufstellung eines Schutzschranks gibt die Maßnahme M 1.40 *Geeignete Aufstellung von Schutzschränken*.

Betrieb

Schutzschrankräume sollten grundsätzlich immer verschlossen sein, wenn die Schränke selbst nicht so ausgelegt sind, dass sie auch in ungeschützten Umgebungen aufgestellt werden können. Es ist darauf zu achten, dass die Schutzschränke immer korrekt verschlossen sind. Insbesondere bei Verwendung von Zahlenschlössern ist auf deren korrekte Bedienung zu achten.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Schutzschränke" vorgestellt.

Planung und Konzeption

- M 1.7 (B) Handfeuerlöscher
- M 1.18 (Z) Gefahrenmeldeanlage
- M 1.24 (Z) Vermeidung von wasserführenden Leitungen
- M 1.25 (B) Überspannungsschutz
- M 1.26 (A) Not-Aus-Schalter
- M 1.27 (B) Klimatisierung
- M 1.28 (B) Lokale unterbrechungsfreie Stromversorgung
- M 1.31 (Z) Fernanzeige von Störungen
- M 1.41 (Z) Schutz gegen elektromagnetische Einstrahlung
- M 2.311 (A) Planung von Schutzschränken

Beschaffung

- M 2.95 (A) Beschaffung geeigneter Schutzschränke

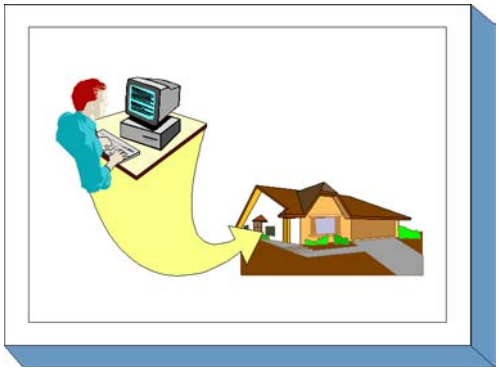
Umsetzung

- M 1.40 (A) Geeignete Aufstellung von Schutzschränken
- M 2.17 (C) Zutrittsregelung und -kontrolle
- M 2.21 (A) Rauchverbot
- M 3.20 (A) Einweisung in die Bedienung von Schutzschränken

Betrieb

- M 1.15 (A) Geschlossene Fenster und Türen
- M 2.96 (A) Verschluss von Schutzschränken
- M 2.97 (A) Korrekter Umgang mit Codeschlössern (falls vorhanden)

B 2.8 Häuslicher Arbeitsplatz



Beschreibung

Werden dienstliche Aufgaben in der häuslichen Umgebung und nicht in Räumen des Unternehmens bzw. der Behörde wahrgenommen, sind Sicherheitsmaßnahmen zu ergreifen, die eine mit einem Büroraum vergleichbare Sicherheitssituation erreichen lassen. Bei einem häuslichen Arbeitsplatz kann nicht die infrastrukturelle Sicherheit, wie sie in einer gewerblichen oder behördlichen Büroumgebung anzutreffen ist, vorausgesetzt werden. Besucher oder Familienangehörige haben oftmals Zutritt zu diesem Arbeitsplatz. In diesem Baustein werden die typischen Gefährdungen und Maßnahmen für einen häuslichen Arbeitsplatz beschrieben. Dieser häusliche Arbeitsplatz kann zum Beispiel im Rahmen der Telearbeit, bei freien Mitarbeitern und für Selbständige eingesetzt werden.

Gefährdungslage

Für den IT-Grundschutz des häuslichen Arbeitsplatzes werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.5 Wasser

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen
- G 2.14 Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
- G 2.47 Ungesicherter Akten- und Datenträgertransport
- G 2.48 Ungeeignete Entsorgung der Datenträger und Dokumente

Menschliche Fehlhandlungen:
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.3 Unbefugtes Eindringen in ein Gebäude
- G 5.69 Erhöhte Diebstahlgefahr am häuslichen Arbeitsplatz
- G 5.70 Manipulation durch Familienangehörige und Besucher
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den häuslichen Arbeitsplatz sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Nutzung bis zur Entsorgung sensibler Datenträger und Ausdrucke. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Die Maßnahme M 1.44 *Geeignete Einrichtung eines häuslichen Arbeitsplatzes* nennt die grundlegenden Gestaltungsmöglichkeiten, die bei der Einrichtung eines Arbeitsplatzes in häuslicher Umgebung beachtet werden sollten.

Umsetzung

Für die kontrollierte Nutzung eines häuslichen Arbeitsplatzes ist zu regeln, welche Informationen zwischen dem Unternehmen bzw. der Behörde und dem häuslichen Arbeitsplatz hin und her transportiert werden dürfen und welche Schutzvorkehrungen dabei zu treffen sind.

Betrieb

Auch bei der Nutzung eines häuslichen Arbeitsplatzes ist die übliche Arbeitsdisziplin zu wahren. Dazu gehören Ordnung am Arbeitsplatz, die Einhaltung der vom Arbeitgeber vorgesehenen Regelungen über die Arbeitsumgebung und eine sichere Aufbewahrung der Arbeitsmaterialien. Der häusliche Arbeitsplatz sollte auch so abgeschlossen werden, dass er keinem unzumutbaren Einbruchsrisiko ausgesetzt ist.

Aussonderung

Gerade am häuslichen Arbeitsplatz ist es wichtig, Datenträger und Ausdrucke sorgsam zu entsorgen und nicht einfach in den Hausmüll zu werfen.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Häuslicher Arbeitsplatz" vorgestellt.

Planung und Konzeption

- M 1.19 (Z) Einbruchsschutz
- M 1.44 (A) Geeignete Einrichtung eines häuslichen Arbeitsplatzes
- M 3.9 (Z) Ergonomischer Arbeitsplatz

Umsetzung

- M 2.112 (A) Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution

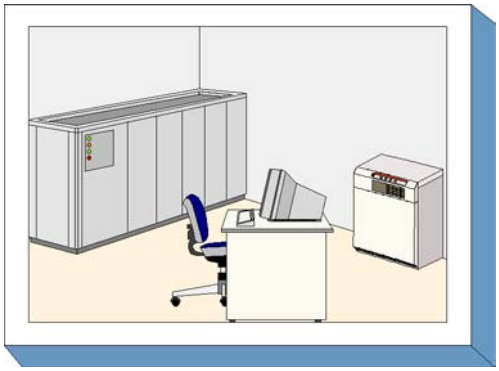
Betrieb

- M 1.15 (A) Geschlossene Fenster und Türen
- M 1.23 (A) Abgeschlossene Türen
- M 1.45 (A) Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
- M 2.37 (C) "Der aufgeräumte Arbeitsplatz"
- M 2.136 (A) Einhaltung von Regelungen bzgl. Arbeitsplatz und Arbeitsumgebung

Aussonderung

- M 2.13 (A) Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln

B 2.9 Rechenzentrum



Beschreibung

Bedingt durch erhöhte Verfügbarkeitsanforderungen, aber auch durch Forderungen nach einheitlichen Administrationskonzepten, meist unter dem Druck zusätzlicher Personaleinsparungen, ist eine Tendenz zur Zentralisierung der geschäftskritischen Produktiv-Hardware einer Behörde bzw. eines Unternehmens zu verzeichnen. Die Anforderungen an die Leistungsfähigkeit dieser Systeme und der Netzumgebung sind insbesondere dort gestiegen, wo zeitkritische Zugriffe auf zentrale Datenbanken realisiert werden müssen. Um diesem gestiegenen Leistungsbedarf gerecht zu werden und zusätzlich mittelfristig entsprechende Reserven vorzuhalten, haben auch Unternehmen mittlerer Größe, die bislang ausschließlich auf ein verteiltes Client-Server-Konzept vertrauten, ihre IT-Landschaft durch Rechenzentren ergänzt oder teilweise ersetzt.

Als Rechenzentrum werden die für den Betrieb einer größeren, zentral für mehrere Stellen eingesetzten Datenverarbeitungsanlage erforderlichen Einrichtungen (Rechner-, Speicher-, Druck-, Robotersysteme usw.) und Räumlichkeiten (Rechnersaal, Archiv, Lager, Aufenthaltsraum usw.) bezeichnet. Ein Rechenzentrum ist entweder ständig personell besetzt (Schichtdienst) oder es existiert in bedienerlosen Zeiten eine Rufbereitschaft (mit oder ohne Fernadministrationsmöglichkeit). In der Regel stützt sich die Datenverarbeitung eines Unternehmens nicht ausschliesslich auf die zentralen IT-Geräte in einem Rechenzentrum, sondern auf eine Vielzahl damit verbundener dezentraler IT-Systeme. In einem Rechenzentrum kann aufgrund der Konzentration von IT-Geräten und Daten jedoch ein deutlich höherer Schaden eintreten als bei dezentraler Datenverarbeitung. In jedem Fall ist beim Einsatz einer Großrechenanlage der Baustein Rechenzentrum anzuwenden.

Gegenstand dieses Bausteins ist ein Rechenzentrum mittlerer Art und Güte. Die Sicherheitsanforderungen liegen zwischen denen eines Serverraums oder "Serverparks" und denen von Hochsicherheitsrechenzentren, wie sie beispielsweise im Bankenbereich eingesetzt werden. Neben den hier aufgeführten Standard-Sicherheitsmaßnahmen, die sich in der Praxis bewährt haben, sind in den meisten Fällen jedoch weitere, individuelle IT-Sicherheitsmaßnahmen erforderlich, die die konkreten Anforderungen und das jeweilige Umfeld berücksichtigen (hierzu kann beispielsweise die Risikoanalyse basierend auf IT-Grundschutz verwendet werden). Gefährdungen aus den Bereichen Terrorismus oder höhere Gewalt wird durch die hier beschriebenen Standard-Sicherheitsmaßnahmen nur begrenzt Rechnung getragen.

Der Baustein richtet sich einerseits an Leser, die ein Rechenzentrum betreiben und im Rahmen einer Revision prüfen möchten, ob sie geeignete Standard-Sicherheitsmaßnahmen umgesetzt haben. Auf der anderen Seite kann der Baustein Rechenzentrum auch dazu verwendet werden, überblicksartig die IT-Sicherheitsmaßnahmen abzuschätzen, die bei einer Zentralisierung der IT in einem mittleren Rechenzentrum für einen sicheren Betrieb umgesetzt werden müssen. Um den Baustein überschaubar zu halten, wurde bewusst auf technische Details und planerische Größen verzichtet. Der Neubau eines Rechenzentrums sollte auch von großen IT-Abteilungen nicht ohne Hilfe eines erfahrenen Planungsstabes bzw. einer versierten Planungs- und Beratungsfirma in Betracht gezogen werden. Beim Outsourcing von Rechenzentrumsleistungen kann dieser Baustein dazu benutzt werden, die angebotenen Leistungen im Hinblick auf deren Sicherheitsniveau zu prüfen.

Im Gegensatz zum Schutzbedarf eines Serverraums (siehe dort) werden viele IT-Sicherheitsmaßnahmen für ein Rechenzentrum nicht als optional, sondern obligatorisch empfohlen. Dazu gehören beispielsweise eine angemessene Gefahrenmeldeanlage und eine alternative Stromversorgung. Für einen sicheren IT-Betrieb ist eine Brandfrühesterkennung durch Objektüberwachung der eingesetzten Hardware und des Doppelbodens effektiv und kostengünstig. Eine Raumlöschung richtet sich in erster Linie auf den Erhalt des Gebäudes.

Gefährdungslage

Für den IT-Grundschutz eines Rechenzentrums werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.2 Ausfall des IT-Systems
- G 1.3 Blitz
- G 1.4 Feuer
- G 1.5 Wasser
- G 1.6 Kabelbrand
- G 1.7 Unzulässige Temperatur und Luftfeuchte
- G 1.8 Staub, Verschmutzung
- G 1.11 Technische Katastrophen im Umfeld
- G 1.12 Beeinträchtigung durch Großveranstaltungen
- G 1.13 Sturm
- G 1.16 Ausfall von Patchfeldern durch Brand

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen
- G 2.11 Unzureichende Trassendimensionierung
- G 2.12 Unzureichende Dokumentation der Verkabelung

Technisches Versagen:
- G 4.1 Ausfall der Stromversorgung
- G 4.2 Ausfall interner Versorgungsnetze
- G 4.3 Ausfall vorhandener Sicherungseinrichtungen

Vorsätzliche Handlungen:
- G 5.3 Unbefugtes Eindringen in ein Gebäude
- G 5.4 Diebstahl
- G 5.5 Vandalismus
- G 5.6 Anschlag
- G 5.16 Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal
- G 5.17 Gefährdung bei Wartungsarbeiten durch externes Personal
- G 5.68 Unberechtigter Zugang zu den aktiven Netzkomponenten
- G 5.102 Sabotage

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Bei der Auswahl und Gestaltung eines Rechenzentrums sind eine Reihe infrastruktureller und organisatorischer Maßnahmen umzusetzen, die in M 1.49 *Technische und organisatorische Vorgaben für das Rechenzentrum* beschrieben sind. Dabei sind bei bestimmten Maßnahmen unterschiedliche Vorgehensweisen zu verfolgen, je nachdem, ob ein Rechenzentrum in einem neu zu errichtenden Gebäude eingerichtet werden soll oder ob es sich um eine Anmietung oder die Nutzung eines bestehenden Gebäudes handelt. In diesem zweiten Fall sind die Möglichkeiten zur Realisierung einer adäquaten IT-Sicherheit oft viel stärker eingeschränkt. Die Schritte, die bei der Gestaltung eines Rechenzentrums durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Bei der Planung eines Rechenzentrums ist durch eine Reihe von Maßnahmen zur Installation der Stromversorgung und Klimatisierung und zum Brandschutz dafür zu sorgen, dass eine hinreichende physische Sicherheit bereitgestellt wird. Dazu gehört auch, dass nach Möglichkeit keine wasserführenden Leitungen in einem Rechenzentrum vorhanden sein sollten, da Undichtigkeiten größere Schäden bis hin zum Ausfall des gesamten IT-Verbundes verursachen können. Zum physischen Schutz gehört dabei auch, dass die Lage des Rechenzentrums im Gebäude möglichst unter Sicherheitsgesichtspunkten in einem eigenen Brandabschnitt und ohne Kenntlichmachung nach außen gewählt wird.

In der Regel sollten auch hinreichende Redundanzen in der technischen Infrastruktur sowie eine Sekundär-Energieversorgung geplant werden, um die Überbrückung einzelner Ausfälle zu ermöglichen. Durch Installation von Überwachungsmaßnahmen, Fernanzeige von Störungen und einer geeigneten Löschtechnik ist Vorsorge zu treffen, dass eventuelle Schäden möglichst frühzeitig erkannt werden können und geeignete Maßnahmen so schnell eingeleitet werden können, dass die Schadensausbreitung so gering wie möglich ist.

Umsetzung

Nur diejenigen Personen, die zur Durchführung ihrer Aufgaben direkten Zugriff auf Server und sonstige im Rechenzentrum installierte Geräte wie Kommunikationsverteiler, Firewalls etc. benötigen, sollten Zutritt erhalten. Die Reinigung der Räume ist detailliert so zu regeln, dass nur vertrauenswürdiges Personal, und auch dieses möglichst nur unter Überwachung, Zutritt erhält. Ein Rauchverbot sollte dort ebenso selbstverständlich sein wie die Verfügbarkeit aktueller Infrastruktur- und Baupläne. Größere Mengen von Druckerpapier sind außerhalb des Rechenzentrums, in einem anderen Brandabschnitt zu lagern, um die Brandlast zu reduzieren.

Betrieb

Rechenzentren sollten grundsätzlich immer verschlossen sein, wenn sie nicht besetzt sind.

Notfallvorsorge

Da Schutzmaßnahmen, die nicht geübt werden, im Notfall nicht korrekt funktionieren, sind regelmäßige Brandschutzübungen erforderlich, zumal diese auch helfen, die Aktualität des Alarmierungsplans sicherzustellen. Um nach einem größeren Schaden schnell wieder Zugriff auf lebenswichtige Daten zu erhalten, sollten diese regelmäßig in einem separaten Notfallarchiv gesichert werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Rechenzentrum" vorgestellt:

Planung und Konzeption

- M 1.49 (A) Technische und organisatorische Vorgaben für das Rechenzentrum

Stromversorgung
- M 1.3 (A) Angepasste Aufteilung der Stromkreise
- M 1.25 (A) Überspannungsschutz
- M 1.56 (A) Sekundär-Energieversorgung

Brandschutz
- M 1.7 (A) Handfeuerlöscher
- M 1.10 (C) Verwendung von Sicherheitstüren und -fenstern
- M 1.26 (B) Not-Aus-Schalter
- M 1.47 (B) Eigener Brandabschnitt
- M 1.48 (B) Brandmeldeanlage
- M 1.50 (C) Rauchschutz
- M 1.54 (Z) Brandfrühesterkennung / Löschtechnik
- M 1.62 (C) Brandschutz von Patchfeldern

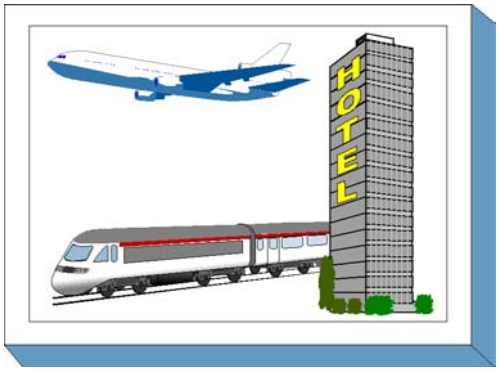
Gebäudeschutz
- M 1.12 (A) Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
- M 1.13 (Z) Anordnung schützenswerter Gebäudeteile
- M 1.18 (B) Gefahrenmeldeanlage
- M 1.24 (C) Vermeidung von wasserführenden Leitungen
- M 1.27 (B) Klimatisierung
- M 1.31 (Z) Fernanzeige von Störungen
- M 1.52 (Z) Redundanzen in der technischen Infrastruktur
- M 1.53 (Z) Videoüberwachung
- M 1.55 (Z) Perimeterschutz

Umsetzung
- M 1.51 (A) Brandlastreduzierung
- M 1.57 (A) Aktuelle Infrastruktur- und Baupläne
- M 2.17 (A) Zutrittsregelung und -kontrolle
- M 2.21 (A) Rauchverbot
- M 2.212 (B) Organisatorische Vorgaben für die Gebäudereinigung
- M 2.213 (A) Wartung der technischen Infrastruktur

Betrieb
- M 1.15 (A) Geschlossene Fenster und Türen
- M 1.23 (A) Abgeschlossene Türen

Notfallvorsorge
- M 6.16 (Z) Abschließen von Versicherungen
- M 6.17 (A) Alarmierungsplan und Brandschutzübungen
- M 6.74 (Z) Notfallarchiv

B 2.10 Mobiler Arbeitsplatz



Beschreibung

IT-Benutzer werden immer mobiler und können, dank immer kleinerer und leistungsfähigerer Geräte, nahezu überall arbeiten. Daher werden dienstliche Aufgaben häufig nicht mehr nur in Räumen des Unternehmens bzw. der Behörde wahrgenommen, sondern an wechselnden Arbeitsplätzen in unterschiedlichen Umgebungen, beispielsweise im Hotelzimmer, in der Eisenbahn oder beim Kunden.

In solchen Umgebungen kann aber nicht die infrastrukturelle Sicherheit, wie sie in einer gewerblichen oder behördlichen Büroumgebung anzutreffen ist, vorausgesetzt werden. Daher sind Sicherheitsmaßnahmen zu ergreifen, die eine mit einem Büroraum vergleichbare Sicherheitssituation erreichen lassen.

In diesem Baustein werden die typischen Gefährdungen und Maßnahmen für einen mobilen Arbeitsplatz beschrieben.

Gefährdungslage

Für den IT-Grundschutz eines mobilen Arbeitsplatzes werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.15 Beeinträchtigung durch wechselnde Einsatzumgebung

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.47 Ungesicherter Akten- und Datenträgertransport
- G 2.48 Ungeeignete Entsorgung der Datenträger und Dokumente

Menschliche Fehlhandlungen:
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.43 Ungeeigneter Umgang mit Passwörtern
- G 3.44 Sorglosigkeit im Umgang mit Informationen

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen

Maßnahmenempfehlungen:

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Auch für mobile Arbeitsplätze sind eine Reihe von Maßnahmen umzusetzen. Auch diese sollten angelehnt an das Lebenszyklus-Modell durchlaufen werden.

Planung und Konzeption

Die Maßnahme M 1.61 *Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes* die grundlegenden Gestaltungsmöglichkeiten, die bei der Einrichtung eines Arbeitsplatzes in fremder Umgebung beachtet werden sollten.

Umsetzung

Für alle Arbeiten unterwegs ist zu regeln, welche Informationen außerhalb des Unternehmen bzw. der Behörde transportiert und bearbeitet werden dürfen und welche Schutzvorkehrungen dabei zu treffen sind. Dabei ist auch zu klären, unter welchen Rahmenbedingungen Mitarbeiter mit mobilen IT-Systemen Zugriff auf interne Daten ihrer Institution nehmen können.

Betrieb

Beim mobilen Arbeiten müssen nicht nur die mitgenommenen IT-Systeme (z. B. Laptop, PDA, Handy), sondern auch die unterwegs bearbeiteten Informationen sorgfältig behandelt werden. Dazu gehören die Einhaltung der vom Arbeitgeber vorgesehenen Regelungen über die Arbeitsumgebung und eine sichere Aufbewahrung der Arbeitsmaterialien.

Aussonderung

Gerade in fremden Umgebungen ist es wichtig, Datenträger und Ausdrucke sorgsam zu entsorgen und nicht einfach in den Hausmüll zu werfen.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Mobiler Arbeitsplatz" vorgestellt.

Planung und Konzeption

- M 1.61 (A) Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes
- M 2.218 (A) Regelung der Mitnahme von Datenträgern und IT-Komponenten
- M 2.309 (C) Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung

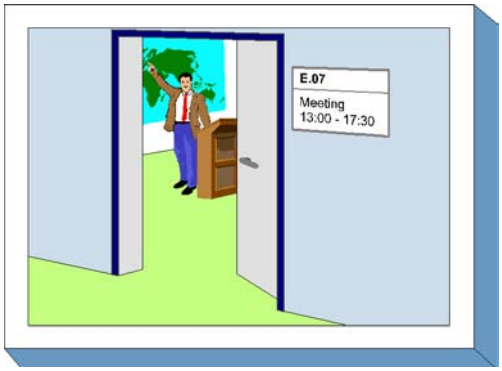
Betrieb

- M 1.15 (A) Geschlossene Fenster und Türen
- M 1.23 (A) Abgeschlossene Türen
- M 1.45 (A) Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
- M 1.46 (Z) Einsatz von Diebstahl-Sicherungen
- M 2.37 (C) "Der aufgeräumte Arbeitsplatz"
- M 2.136 (A) Einhaltung von Regelungen bzgl. Arbeitsplatz und Arbeitsumgebung
- M 2.389 (Z) Sichere Nutzung von Hotspots
- M 4.251 (A) Arbeiten mit fremden IT-Systemen

Aussonderung

- M 2.13 (A) Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln

B 2.11 Besprechungs-, Veranstaltungs- und Schulungsräume



Beschreibung

Besprechungs-, Veranstaltungs- und Schulungsräume zeichnen sich im wesentlichen dadurch aus, dass sie

- von wechselnden Personen bzw. Personenkreisen genutzt werden,
- sowohl durch eigenes Personal als auch durch Externe genutzt werden,
- eine in sich geschlossene Nutzung mit dem gleichen Kreis nutzende Personen meist nur kurze Zeit andauert, wenige Stunden bis zu wenigen Tagen,
- mitgebrachte IT-Systeme gemeinsam mit eigener IT betrieben werden (z. B. fremder Laptop am eigenen Beamer),
- die dort genutzten Informationen in der Regel lokal (z. B. auf Laptop oder mobilem Datenträger) vorhanden sind oder aus einem eigens eingerichteten Test- oder Trainingsnetz zur Verfügung gestellt werden. Teilweise ist sogar ein Anschluss an das LAN vorhanden, so dass auf institutionsinterne Daten zugegriffen werden kann.

Aus diesen extrem unterschiedlichen Nutzungen heraus ergibt sich eine Gefährdungslage, die kaum mit denen anderer Räume vergleichbar ist. Das Hauptaugenmerk ist dabei, neben den üblichen Gefährdungen für Räume aller Art, auf die Gefährdung durch den "Spieltrieb" anwesender Personen zu legen.

Gefährdungslage

Für den IT-Grundschutz von Besprechungs-, Veranstaltungs- und Schulungsräumen werden folgende Gefährdungen angenommen:

Organisatorische Mängel:

- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.14 Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
- G 2.104 Inkompatibilität zwischen fremder und eigener IT

Menschliche Fehlhandlungen:

- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.78 Fliegende Verkabelung

Technisches Versagen:

- G 4.1 Ausfall der Stromversorgung
- G 4.2 Ausfall interner Versorgungsnetze

Vorsätzliche Handlungen:

- G 5.4 Diebstahl

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Planung und Konzeption

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

- Die Nutzungsmöglichkeiten von Besprechungs-, Veranstaltungs- und Schulungsräumen variieren sehr stark. Da hiervon auch die erforderlichen Sicherheitsmaßnahmen abhängen, sollte zunächst eine Nutzungsübersicht erstellt werden, das die geplanten Einsatzszenarien berücksichtigt (siehe M 2.331 *Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen*).
- Basierend auf dem Nutzungskonzept sollten geeignete Räumlichkeiten ausgewählt und ausgestattet werden (siehe M 2.332 *Einrichtung von Besprechungs-, Veranstaltungs- und Schulungsräumen*).
- Wenn auf LANs oder das Internet zugegriffen werden soll, müssen die Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen sorgfältig abgesichert werden (siehe M 5.124 *Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen*).

Umsetzung

Es müssen Sicherheitsregelungen für Besprechungs-, Veranstaltungs- und Schulungsräume festgelegt sowie technisch und organisatorisch umgesetzt werden. Alle Mitarbeiter müssen darüber informiert werden, welche Nutzungsregelungen zu beachten sind (siehe M 2.333 *Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen*).

Betrieb

Auch in Besprechungs-, Veranstaltungs- und Schulungsräumen muss mit den Einrichtungen und der vorhandenen Technik sorgfältig umgegangen werden. Dazu gehören die Einhaltung der von der Institution vorgesehenen Regelungen über die Arbeitsumgebung und eine sichere Aufbewahrung der Arbeitsmaterialien.

Aussonderung

Gerade in Besprechungs-, Veranstaltungs- und Schulungsräumen mit häufig wechselnden Benutzern ist es wichtig, Arbeitsmaterialien wie Datenträger und Papiere sorgsam zu entsorgen und nicht einfach liegen zu lassen.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Besprechungs-, Veranstaltungs- und Schulungsräume" vorgestellt.

Planung und Konzeption

- M 2.331 (A) Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen
- M 2.332 (B) Einrichtung von Besprechungs-, Veranstaltungs- und Schulungsräumen
- M 3.9 (Z) Ergonomischer Arbeitsplatz
- M 5.77 (Z) Bildung von Teilnetzen
- M 5.124 (C) Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen

Umsetzung

- M 1.6 (A) Einhaltung von Brandschutzvorschriften
- M 2.69 (B) Einrichtung von Standardarbeitsplätzen
- M 2.204 (A) Verhinderung ungesicherter Netzzugänge
- M 2.333 (A) Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen
- M 4.252 (C) Sichere Konfiguration von Schulungsrechnern

Betrieb

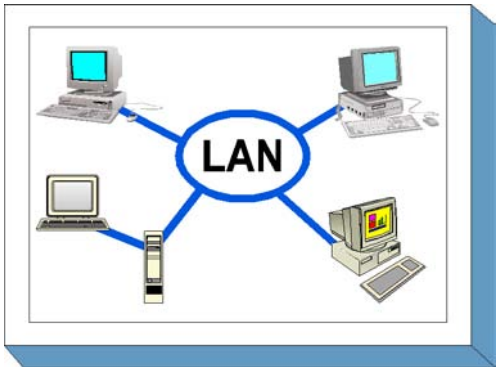
- M 1.15 (A) Geschlossene Fenster und Türen
- M 2.16 (B) Beaufsichtigung oder Begleitung von Fremdpersonen
- M 4.109 (C) Software-Reinstallation bei Arbeitsplatzrechnern
- M 4.293 (Z) Sicherer Betrieb von Hotspots

3 IT-Systeme

In der Schicht IT-Systeme sind folgende Bausteine enthalten:

B 3.101 Allgemeiner Server
B 3.102 Server unter Unix
B 3.103 Server unter Windows NT
B 3.104 Server unter Novell Netware 3.x
B 3.105 Server unter Novell Netware Version 4.x
B 3.106 Server unter Windows 2000
B 3.107 S/390- und zSeries-Mainframe
B 3.108 Windows Server 2003
B 3.201 Allgemeiner Client
B 3.202 Allgemeines nicht vernetztes IT-System
B 3.203 Laptop
B 3.204 Client unter Unix
B 3.205 Client unter Windows NT
B 3.206 Client unter Windows 95
B 3.207 Client unter Windows 2000
B 3.208 Internet-PC
B 3.209 Client unter Windows XP
B 3.301 Sicherheitsgateway (Firewall)
B 3.302 Router und Switches
B 3.303 Speichersysteme und Speichernetze
B 3.401 TK-Anlage
B 3.402 Faxgerät
B 3.403 Anrufbeantworter
B 3.404 Mobiltelefon
B 3.405 PDA

B 3.101 Allgemeiner Server



Beschreibung

Server sind IT-Systeme, die Dienste (Services) für andere IT-Systeme (Clients) im Netz anbieten. Sie werden typischerweise in zentralen, besonders gesicherten Räumlichkeiten betrieben, beispielsweise in einem Serverraum oder einem Rechenzentrum, und nicht als Arbeitsplatzrechner genutzt. Für Server stehen unterschiedliche Betriebssysteme zur Verfügung, unter anderem Unix bzw. Linux, Microsoft Windows und Novell Netware. Dieser Baustein betrachtet Sicherheitsaspekte, die unabhängig vom eingesetzten Betriebssystem für Server relevant sind. Für betriebssystemspezifische Sicherheitsaspekte existieren in den IT-Grundschutz-Katalogen eigenständige Bausteine, die zusätzlich auf die jeweils betroffenen Server anzuwenden sind. Die netzspezifischen Aspekte des Servereinsatzes werden im Baustein B 4.1 *Heterogene Netze* behandelt.

Gefährdungslage

Wie jedes IT-System ist auch ein Server vielfältigen Gefahren ausgesetzt. Generell gilt, dass die Gefährdungslage einzelner Rechner immer auch vom Einsatzszenario, beispielsweise der Nutzung als Dateiserver, Terminalserver bzw. Authentisierungsserver, abhängt und diese Einzelgefährdungen auch in die Gefährdung des Gesamtsystems eingehen.

Für den IT-Grundschutz eines Servers werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.1 Personalausfall
- G 1.2 Ausfall des IT-Systems

Organisatorische Mängel:
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- G 2.25 Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten

Menschliche Fehlhandlungen:
- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.5 Unbeabsichtigte Leitungsbeschädigung
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.31 Unstrukturierte Datenhaltung

Technisches Versagen:
- G 4.1 Ausfall der Stromversorgung
- G 4.6 Spannungsschwankungen/Überspannung/Unterspannung
- G 4.7 Defekte Datenträger
- G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
- G 4.13 Verlust gespeicherter Daten

- G 4.22 Software-Schwachstellen oder -Fehler
- G 4.39 Software-Konzeptionsfehler

Vorsätzliche Handlungen:

- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.7 Abhören von Leitungen
- G 5.9 Unberechtigte IT-Nutzung
- G 5.15 "Neugierige" Mitarbeiter
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.19 Missbrauch von Benutzerrechten
- G 5.20 Missbrauch von Administratorrechten
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.26 Analyse des Nachrichtenflusses
- G 5.40 Abhören von Räumen mittels Rechner mit Mikrofon
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.75 Überlastung durch eingehende E-Mails
- G 5.85 Integritätsverlust schützenswerter Informationen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den erfolgreichen Aufbau eines Servers sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Installation bis zum Betrieb. Ein besonderes Gewicht ist dabei auf die konzeptionellen Planungsmaßnahmen zu legen, wenn der Server im Rahmen des Aufbaus eines neuen servergestützten Netzes installiert wird. Sofern die Installation dagegen als Ausbau eines schon existierenden Netzes erfolgt, können sich die Planungsmaßnahmen häufig darauf beschränken, auf die Konformität des neuen Servers mit den schon vorhandenen Strukturen zu achten. Die Maßnahmen zur Beschaffung und zum Betrieb des Servers sind dagegen in jedem Fall umzusetzen. Die Schritte, die zum Schutz eines Servers zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Im Vorfeld der eigentlichen Planung ist die generelle Architektur des Netzes festzulegen bzw. zu analysieren, aus der sich im Allgemeinen auch Vorgaben für die einzusetzenden Betriebssysteme (Server und Client) ergeben. Insbesondere ist dabei festzulegen, welche Ziele mit dem aufzubauenden Server verfolgt werden. Dazu sind die voraussichtlichen Einsatzszenarien zu beschreiben und der Einsatzzweck zu definieren.

Falls ein neues Netz aufgebaut wird, ist zunächst die Struktur des Netzes insgesamt zu planen, wobei Fragen wie die Festlegung einer Netztopographie und die Entscheidung über den Grad der Serverzentrierung (Terminalserver, "klassische" Client-Server-Architektur oder Nutzung von Peer-to-Peer-Funktionalität) zu klären sind. Hier sind die Maßnahmen des Bausteins B 1.9 *Hard- und Software-Management* heranzuziehen.

In einem weiteren Schritt folgt die Festlegung der auf der Ebene der Server und der Clients verwendeten Betriebssysteme und gegebenenfalls auch die Auswahl spezifischer Varianten (z. B. Windows XP gegenüber Windows 2000 oder Linux gegenüber einer herstellerspezifischen Variante von Unix).

Falls ein neues Netz aufgebaut wird, muss als genaue technische Grundlage für die weiteren Arbeiten der detaillierte Aufbau des Netzes geplant werden. Anzahl und Zusammenspiel der vorgesehenen Server sind festzulegen. Die Aufgaben der Server und die Art ihrer Nutzung durch die Clients sind zu bestimmen. Anhand der Anforderungen an die Verfügbarkeit muss festgelegt werden, bis zu welchem Grad redundante Strukturen im Netz vorzusehen sind. Hier sind auch die notwendigen Vorgaben für die Infrastruktur (vor allem Klimatisierung und Stromversorgung, siehe dazu M 1.28 *Lokale unterbrechungsfreie Stromversorgung*) festzulegen. Parallel dazu ist eine allgemeine Sicherheitsrichtlinie zu erarbeiten (siehe M 2.316 *Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server*), die anschließend durch systemspezifische Sicherheitsrichtlinien und detaillierte Richtlinien für den Einsatz der Hard- und Software im Netz zu ergänzen ist (siehe dazu die Bausteine zu den einzelnen Server-Betriebssystemen).

Beschaffung

Im nächsten Schritt muss die Beschaffung der Software und eventuell zusätzlich benötigter Hardware erfolgen. Aufbauend auf Einsatzszenarien sind die Anforderungen an zu beschaffende Produkte zu formulieren und basierend darauf die Auswahl der geeigneten Produkte zu treffen. Mit der Beschaffung dieser Produkte ist dann die Grundlage für die Arbeiten des nächsten Schrittes gelegt.

Umsetzung

Die Benutzer bzw. die Administratoren haben einen wesentlichen Einfluss auf die Sicherheit eines Servers. Vor der tatsächlichen Inbetriebnahme müssen die Benutzer und Administratoren daher für den Umgang bzw. die Nutzung des aufzubauenden Servers geschult werden. Insbesondere für Administratoren empfiehlt sich aufgrund der Komplexität in der Planung und in der Verwaltung eine intensive Schulung. Die Administratoren sollen dabei detaillierte Systemkenntnisse erwerben, so dass eine konsistente und korrekte Systemverwaltung gewährleistet ist. Benutzern sollte insbesondere die Nutzung der verfügbaren Sicherheitsmechanismen vermittelt werden. Hier sind die Maßnahmen des Bausteins B 1.13 *IT-Sicherheitssensibilisierung und -schulung* heranzuziehen.

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt wurden, kann die Installation und Inbetriebnahme des Servers erfolgen. Dabei sind die folgenden Maßnahmen zu beachten:

- Schon die Installation und Grundkonfiguration eines Servers muss mit besonderer Sorgfalt durchgeführt werden, um schwer reparierbare Fehler von vornherein zu vermeiden. Allgemeine Hinweise hierzu finden sich in M 2.318 *Sichere Installation eines Servers* und M 4.237 *Sichere Grundkonfiguration eines IT-Systems*.

  Neben den allgemeinen Maßnahmen, die in diesem Baustein beschrieben sind, sind jeweils auch die weitergehenden Maßnahmen, die in den betreffenden Bausteinen für das jeweilige Betriebssystem empfohlen werden, umzusetzen.

- Nach der Installation und Grundkonfiguration der Server müssen gegebenenfalls übergeordnete Verwaltungsstrukturen konfiguriert werden. Dabei kommt unter anderem auch zum Tragen, für welchen Einsatzzweck die einzelnen Server geplant sind, beispielsweise als Dateiserver, Druckserver oder, im Falle von Thin Clients, als Terminalserver. Hier ist insbesondere die Maßnahme M 2.138 *Strukturierte Datenhaltung* wichtig, um einen kontrollierbaren Betrieb des Servers gewährleisten zu können.

  - Nachdem die Installation und Grundkonfiguration des Servers abgeschlossen ist, kann die eigentliche Serversoftware installiert und konfiguriert werden. Die dafür notwendigen Schritte unterscheiden sich je nach Art und Einsatzzweck der Software teilweise erheblich und werden teilweise in eigenen Bausteinen behandelt. Prinzipiell wird empfohlen, für die Installation und Konfiguration der Serversoftware analog wie für die

Konfiguration des Betriebssystems selbst vorzugehen:

- Erstellung eines Installationskonzepts
- Falls mehrere Server mit ähnlichen Einsatzgebieten und Konfiguration installiert werden sollen: Erstellen einer Referenzinstallation
- Installation, Grundkonfiguration und Aktualisierung
- Test

Detailliertere Hinweise für die Sicherheit verschiedener Server-Anwendungen finden sich in den Bausteinen der Schicht 5.

Betrieb

Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:

- Client-Server-Netze ändern sich sehr häufig. Dabei muss bei jeder Änderung sichergestellt werden, dass die Sicherheit auch nach der Änderung nicht beeinträchtigt wird. Die dabei im Detail zu beachtenden Aspekte sind in den Bausteinen zu den jeweiligen Serverbetriebssystemen enthalten. Dabei ist zu berücksichtigen, dass auch der Entzug von Berechtigungen sowie das Löschen nicht mehr benötigter Datenbestände so geregelt wird, dass durch veraltete Strukturen keine Sicherheitslücken entstehen. Eine wesentliche Hilfe ist dabei eine effiziente, umfassende Systemverwaltung, die sich jederzeit auf aktuelle Informationen über den Zustand des Systems und seiner Rechtestrukturen abstützen kann (siehe dazu M 4.24 *Sicherstellung einer konsistenten Systemverwaltung* und M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*).
- Ein Mittel im Rahmen der Aufrechterhaltung der Sicherheit eines Servers ist die Überwachung des Systems bzw. seiner Einzelkomponenten. Die hier relevanten Maßnahmen finden sich in, M 4.93 *Regelmäßige Integritätsprüfung*, M 5.8 *Regelmäßiger Sicherheitscheck des Netzes* und M 5.9 *Protokollierung am Server*. Dabei spielen auch insbesondere Datenschutzaspekte eine Rolle. Die häufigen Sicherheitslücken der meisten Client-Server-Systeme und die Vielzahl von Angriffen, die sich gegen diese Schwächen richten, fordern von den Administratoren, dass diese sich permanent über den Sicherheitsstatus der Systeme und über neue Bedrohungen informieren (siehe M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*) und rechtzeitig Gegenmaßnahmen einleiten (siehe dazu M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*).

Aussonderung

Ein Server darf nicht einfach ohne Ankündigung abgeschaltet werden. Wenn ein Server außer Betrieb genommen werden soll, dann müssen die Anwender rechtzeitig informiert werden und es muss eine Reihe von Punkten beachtet werden, um Ausfallzeiten und Datenverluste zu verhindern. Diese Punkte sind in M 2.320 *Geregelte Außerbetriebnahme eines Servers* beschrieben. Sollen die Dienste des Servers auf einen anderen Rechner migriert werden, so ist M 2.319 *Migration eines Servers* zu berücksichtigen.

Bei der Aussonderung eines Servers ist außerdem darauf zu achten, dass keine schützenswerten Informationen mehr auf den Festplatten vorhanden sind. Dazu genügt es nicht, die Platten einfach neu zu formatieren, sondern sie müssen mindestens einmal vollständig überschrieben werden. Es ist zu beachten, dass ein reines logisches Löschen und auch nicht das Neuformatieren der Platten mit den Mitteln des installierten Betriebssystems die Daten nicht von den Festplatten entfernt, so dass sie mit geeigneter Software, oft sogar ohne großen Aufwand, wieder rekonstruiert werden können. Entsprechende Hinweise finden sich in M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*, die im Rahmen des übergeordneten Bausteins B 1.1 *Organisation* behandelt wird, und

in M 4.234 *Aussonderung von IT-Systemen* im übergeordneten Baustein B 1.9 *Hard- und Software-Management*.

Die Aussonderung des Servers muss dokumentiert werden. Bestandsverzeichnisse und Netzpläne müssen aktualisiert werden und sofern sich durch die Aussonderung strukturelle Veränderungen des IT-Verbundes ergeben, sollte auch das Sicherheitskonzept entsprechend angepasst werden.

Notfallvorsorge

Nur eine regelmäßige und umfassende Datensicherung gewährleistet zuverlässig, dass alle gespeicherten Daten auch im Falle von Störungen, Ausfällen der Hardware oder (absichtlichen oder unabsichtlichen) Löschungen weiter verfügbar gemacht werden können. Die notwendigen Maßnahmen sind im Baustein B 1.4 *Datensicherungskonzept* beschrieben.

Neben der Absicherung im laufenden Betrieb spielt jedoch auch die Notfallvorsorge eine wichtige Rolle, da nur so der Schaden im Notfall verringert werden kann. Hinweise zur Notfallvorsorge finden sich im Baustein B 1.3 *Notfallvorsorge-Konzept*. Hierzu gehört auch die Planung des Umgangs mit Sicherheitsvorfällen, die sich auf die Maßnahmen des Bausteins B 1.8 *Behandlung von Sicherheitsvorfällen* abstützen sollte. Einige Hinweise zu besonderen Aspekten, die bei der Notfallvorsorge für einen Server beachtet werden sollten, sind in M 6.96 *Notfallvorsorge für einen Server* beschrieben.

Maßnahmenempfehlung:

Es wird vorausgesetzt, dass der Server in einem Serverraum (siehe Baustein B 2.4 *Serverraum*), einem Serverschrank (siehe Baustein B 2.7 *Schutzschränke*) oder in einem Rechenzentrum (siehe Baustein B 2.9 *Rechenzentrum*) untergebracht ist. Die für die Serverbetriebssysteme umzusetzenden Maßnahmen sind den jeweiligen betriebssystemspezifischen Bausteinen zu entnehmen. Dies gilt analog auch für die angeschlossenen Clients. Die Maßnahmen des Bausteins B 1.9 *Hard- und Software-Management* bilden in jedem Fall den übergeordneten Rahmen für den Betrieb servergestützter Netze.

Darüber hinaus sind folgende weitere Maßnahmen umzusetzen:

Planung und Konzeption
- M 1.28 (B) Lokale unterbrechungsfreie Stromversorgung
- M 2.314 (Z) Verwendung von hochverfügbaren Architekturen für Server
- M 2.315 (A) Planung des Servereinsatzes
- M 2.316 (A) Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
- M 5.10 (A) Restriktive Rechtevergabe
- M 5.37 (B) Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
- M 5.138 (Z) Einsatz von RADIUS-Servern
- M 4.250 (Z) Auswahl eines zentralen, netzbasierten Authentisierungsdienstes

Beschaffung
- M 2.317 (C) Beschaffungskriterien für einen Server

Umsetzung
- M 2.32 (Z) Einrichtung einer eingeschränkten Benutzerumgebung
- M 2.138 (B) Strukturierte Datenhaltung
- M 2.318 (A) Sichere Installation eines Servers
- M 4.7 (A) Änderung voreingestellter Passwörter
- M 4.15 (A) Gesichertes Login
- M 4.16 (A) Zugangsbeschränkungen für Accounts und / oder Terminals
- M 4.17 (A) Sperren und Löschen nicht benötigter Accounts und Terminals
- M 4.40 (C) Verhinderung der unautorisierten Nutzung des Rechnermikrofons
- M 4.237 (A) Sichere Grundkonfiguration eines IT-Systems

Betrieb

- M 2.22 (A) Hinterlegen des Passwortes
- M 2.35 (B) Informationsbeschaffung über Sicherheitslücken des Systems
- M 2.204 (A) Verhinderung ungesicherter Netzzugänge
- M 2.273 (A) Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
- M 4.24 (A) Sicherstellung einer konsistenten Systemverwaltung
- M 4.93 (B) Regelmäßige Integritätsprüfung
- M 4.238 (A) Einsatz eines lokalen Paketfilters
- M 4.239 (A) Sicherer Betrieb eines Servers
- M 4.240 (Z) Einrichten einer Testumgebung für einen Server
- M 5.8 (B) Regelmäßiger Sicherheitscheck des Netzes
- M 5.9 (B) Protokollierung am Server

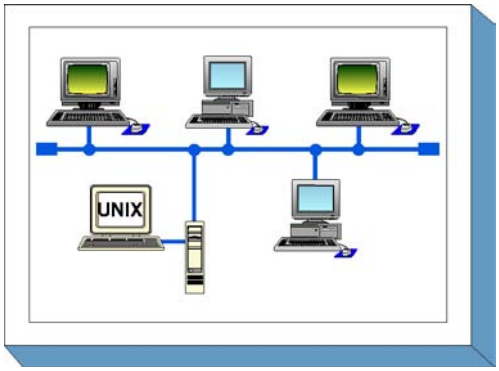
Aussonderung

- M 2.319 (C) Migration eines Servers
- M 2.320 (A) Geregelte Außerbetriebnahme eines Servers

Notfallvorsorge

- M 6.24 (A) Erstellen eines Notfall-Bootmediums
- M 6.96 (A) Notfallvorsorge für einen Server

B 3.102 Server unter Unix



Beschreibung

Unix-Server sind Rechner mit dem Betriebssystem Unix, die in einem Netz Dienste anbieten, die von anderen IT-Systemen in Anspruch genommen werden können.

In diesem Baustein werden ausschließlich die für einen Unix-Server spezifischen Gefährdungen und Maßnahmen beschrieben, daher sind zusätzlich noch diejenigen für allgemeine Server aus Baustein B 3.101 zu betrachten.

Gefährdungslage

Für den IT-Grundschutz eines Unix-Servers werden folgende typische Gefährdungen angenommen:

Organisatorische Mängel:
- G 2.15 Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System
- G 2.65 Komplexität der SAMBA-Konfiguration

Menschliche Fehlhandlungen:
- G 3.10 Falsches Exportieren von Dateisystemen unter Unix
- G 3.11 Fehlerhafte Konfiguration von sendmail

Technisches Versagen:
- G 4.11 Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client
- G 4.12 Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client

Vorsätzliche Handlungen:
- G 5.41 Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
- G 5.89 Hijacking von Netz-Verbindungen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den erfolgreichen Aufbau eines Servers unter Unix sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb dieses Servers. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Die nachfolgenden Maßnahmen beziehen sich auf die sichere Konfigurierung und den sicheren Betrieb eines Unix-Servers, der in einem Netz Dienste für Clients anbietet. Die generelle Planung der Netzarchitektur wird im Baustein B 3.101 *Allgemeiner Server* festgelegt, in denen insbesondere die generelle Netzarchitektur und netzweite Regelungen festgelegt werden. Die Vorgaben, die sich dort für die Server ergeben, sind zu beachten. Es ist sinnvoll, den Server in einem separaten Serverraum aufzustellen. Zu realisierende Maßnahmen sind im Baustein B 2.4 *Serverraum* beschrieben. Steht kein Serverraum zur Verfügung, sollte ein Serverschrank verwendet werden, vergleiche dazu den Baustein B 2.7 *Schutzschränke*.

Es ist ein Verfahren für die Vergabe von Benutzerkennungen festzulegen, durch das gewährleistet wird, dass privilegierte und unprivilegierte Benutzerkennungen klar getrennt sind. Weiterhin ist sicherzustellen, dass kein unkontrollierter Zugang zum Single-User-Modus möglich ist, da sonst alle für die Laufzeit des Systems festgelegten Sicherheitsmaßnahmen unterlaufen werden können.

Beschaffung

Die Anzahl der Server im Netz sowie deren Nutzung durch Clients sind ebenfalls im Baustein B 3.101 *Allgemeiner Server* festgelegt worden, ebenso wie die Anforderungen an die zu beschaffenden Produkte.

Umsetzung

Einige nachfolgend beschriebene Maßnahmen beziehen sich auf die Konfiguration der einzelnen Server, andere Maßnahmen müssen auf Servern und Clients eingesetzt werden, um wirksam zu werden. Für eventuell angeschlossene Clients sind die in den entsprechenden Bausteinen beschriebenen Maßnahmen zu realisieren.

Bei der Konfigurierung eines Unix-Servers ist nach der Installation mit der Maßnahme M 4.105 *Erste Maßnahmen nach einer Unix-Standardinstallation* zu beginnen. Hierbei sind, je nach Einsatzszenario (vergleiche B 3.101 *Allgemeiner Server*), Grundeinstellungen so vorzunehmen, dass nur benötigte Dienste aktiv sind bzw. die beschriebenen Vorkehrungen getroffen werden und die Systemprotokollierung aktiviert wird.

Ferner sind die Zugriffsrechte auf Benutzer- und Systemdateien und -verzeichnisse so nach einem übergreifenden Schema zu vergeben, dass nur diejenigen Benutzer und Prozesse Zugriff erhalten, die diesen wirklich benötigen, wobei insbesondere auf die durch setuid und setgid bestimmten Rechte zu achten ist (siehe dazu die Maßnahme M 4.19 *Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen*).

Betrieb

Um die Sicherheit eines Servers unter Unix im laufenden Betrieb zuverlässig aufrecht zu erhalten, ist es unabdingbar, durch regelmäßige Überprüfungen festzustellen, ob irgendwelche Lücken aufgetreten sind, und diese so schnell wie möglich zu schließen. Dabei sind auch die vom System erzeugten Protokolle auf eventuelle Unregelmäßigkeiten hin zu betrachten.

Notfallvorsorge

Da Unix-Systeme aufgrund ihrer Komplexität nach einem erfolgreichen Angriff oft auf schwer durchschaubare Weise kompromittiert sind, ist es wichtig, schon im Vorfeld Regeln festzulegen, nach denen bei einem echten oder vermuteten Verlust der Systemintegrität zu verfahren ist.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Server unter Unix" vorgestellt.

Planung und Konzeption

- M 2.33 (C) Aufteilung der Administrationstätigkeiten unter Unix
- M 4.13 (A) Sorgfältige Vergabe von IDs
- M 4.18 (A) Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus
- M 5.16 (B) Übersicht über Netzdienste
- M 5.34 (Z) Einsatz von Einmalpasswörtern
- M 5.36 (Z) Verschlüsselung unter Unix und Windows NT
- M 5.64 (Z) Secure Shell
- M 5.82 (A) Sicherer Einsatz von SAMBA
- M 5.83 (Z) Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN

Umsetzung

- M 4.9 (A) Einsatz der Sicherheitsmechanismen von X-Windows
- M 4.14 (A) Obligatorischer Passwortschutz unter Unix
- M 4.19 (A) Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
- M 4.20 (B) Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
- M 4.21 (A) Verhinderung des unautorisierten Erlangens von Administratorrechten
- M 4.22 (C) Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System
- M 4.23 (A) Sicherer Aufruf ausführbarer Dateien
- M 4.105 (A) Erste Maßnahmen nach einer Unix-Standardinstallation
- M 4.106 (A) Aktivieren der Systemprotokollierung
- M 5.17 (A) Einsatz der Sicherheitsmechanismen von NFS
- M 5.18 (A) Einsatz der Sicherheitsmechanismen von NIS
- M 5.19 (A) Einsatz der Sicherheitsmechanismen von sendmail
- M 5.20 (A) Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp
- M 5.21 (A) Sicherer Einsatz von telnet, ftp, tftp und rexec
- M 5.35 (A) Einsatz der Sicherheitsmechanismen von UUCP
- M 5.72 (A) Deaktivieren nicht benötigter Netzdienste

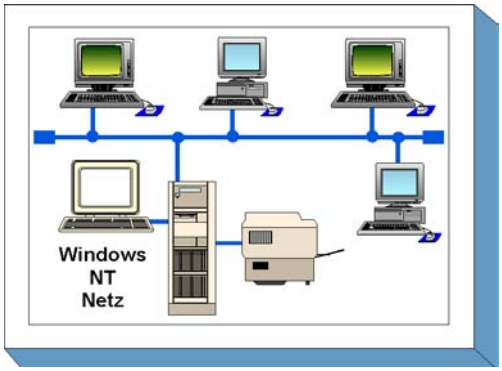
Betrieb

- M 4.25 (A) Einsatz der Protokollierung im Unix-System
- M 4.26 (B) Regelmäßiger Sicherheitscheck des Unix-Systems

Notfallvorsorge

- M 6.31 (A) Verhaltensregeln nach Verlust der Systemintegrität

B 3.103 Server unter Windows NT



Beschreibung

Betrachtet wird ein Server für ein Client-Server-System, der unter dem Betriebssystem Windows NT Version 3.51 oder 4.0 betrieben wird. Dieses Kapitel behandelt die Sicherheitsaspekte des Servers, die Client-spezifischen Maßnahmen sind den Bausteinen für die jeweiligen Client-Betriebssysteme zu entnehmen.

Auf sicherheitsspezifische Aspekte von Windows NT-Anwendungen, zum Beispiel bezüglich *Mail*, *Schedule+*, *Direct-Data-Exchange (DDE)* oder *Remote Access Service (RAS)*, wird nur am Rande eingegangen. Zusätzlich zu den hier angegebenen Gefährdungen und Schutzmaßnahmen gelten noch die im Baustein B 3.101 für einen allgemeinen Server genannten Maßnahmen. Falls im Windows NT Netz die Peer-to-Peer Funktionalität von Windows NT genutzt wird, ist außerdem der Inhalt des Bausteins B 5.1 zu berücksichtigen.

Gefährdungslage

Für den IT-Grundschutz eines servergestützten Netzes unter dem Betriebssystem Windows NT werden folgende typische Gefährdungen angenommen:

Organisatorische Mängel:

- G 2.25 Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten
- G 2.30 Unzureichende Domänenplanung
- G 2.31 Unzureichender Schutz des Windows NT Systems

Technisches Versagen:

- G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
- G 4.23 Automatische CD-ROM-Erkennung

Vorsätzliche Handlungen:

- G 5.23 Computer-Viren
- G 5.43 Makro-Viren
- G 5.52 Missbrauch von Administratorrechten im Windows NT/2000/XP System
- G 5.79 Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz

Bei der Bearbeitung der originären Windows NT Maßnahmen sollte zuerst anhand der Maßnahme M 2.91 *Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz* und zusätzlich, soweit Peer-to-Peer Funktionalität genutzt wird, auch der Maßnahme M 2.67 *Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste* eine Sicherheitsstrategie ausgearbeitet werden, da diese die Grundlage für die weiteren Maßnahmen ist.

Die eigentliche Planung des Windows NT Netzes sollte dann, wie in der Maßnahme M 2.93 *Planung des Windows NT Netzes* beschrieben, durchgeführt werden. Entsprechend den dabei erarbeiteten

Vorgaben sollte zunächst ein Server installiert und mit einer kleinen Anzahl von Clients ausgetestet werden, um die festgelegten Strukturen optimieren und anpassen zu können, ehe sie in der Breite eingesetzt werden.

Für die unter Windows NT vernetzten Systeme sind, neben den hier genannten Maßnahmen, die im Baustein B 3.101 beschriebenen Maßnahmen zu realisieren. Der Server sollte in einem separaten Serverraum aufgestellt werden. Zu realisierende Maßnahmen sind im Baustein B 2.4 beschrieben. Alternativ kann ein Serverschrank verwendet werden, vergleiche Baustein B 2.7.

Für angeschlossene Clients sind die in den entsprechenden Bausteinen beschriebenen Maßnahmen zu realisieren. Soweit auch die Peer-to-Peer Funktionalität von Windows NT genutzt wird, sind außerdem die im Baustein B 5.1 genannten Maßnahmen zu realisieren.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Windows NT Netz" vorgestellt:

Planung und Konzeption

- M 2.91 (A) Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz
- M 2.93 (A) Planung des Windows NT Netzes
- M 4.50 (Z) Strukturierte Systemverwaltung unter Windows NT
- M 4.51 (Z) Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT
- M 4.76 (B) Sichere Systemversion von Windows NT
- M 5.36 (Z) Verschlüsselung unter Unix und Windows NT
- M 5.41 (C) Sichere Konfiguration des Fernzugriffs unter Windows NT
- M 5.42 (C) Sichere Konfiguration der TCP/IP-Netzverwaltung unter Windows NT
- M 5.43 (B) Sichere Konfiguration der TCP/IP-Netzdienste unter Windows NT

Umsetzung

- M 2.94 (B) Freigabe von Verzeichnissen unter Windows NT
- M 4.48 (A) Passwortschutz unter Windows NT/2000/XP
- M 4.49 (A) Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
- M 4.52 (A) Geräteschutz unter Windows NT/2000/XP
- M 4.53 (A) Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT
- M 4.55 (A) Sichere Installation von Windows NT
- M 4.57 (A) Deaktivieren der automatischen CD-ROM-Erkennung
- M 4.75 (A) Schutz der Registrierung unter Windows NT/2000/XP
- M 4.77 (A) Schutz der Administratorkonten unter Windows NT

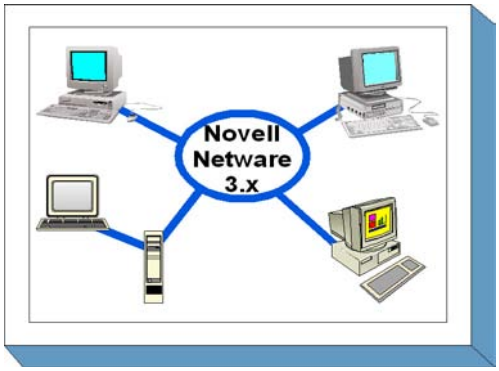
Betrieb

- M 2.92 (B) Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz
- M 4.54 (A) Protokollierung unter Windows NT
- M 4.56 (B) Sicheres Löschen unter Windows-Betriebssystemen

Notfallversorge

- M 6.42 (A) Erstellung von Rettungsdisketten für Windows NT
- M 6.43 (Z) Einsatz redundanter Windows NT/2000 Server
- M 6.44 (A) Datensicherung unter Windows NT

B 3.104 Server unter Novell Netware 3.x



Beschreibung

Betrachtet wird ein LAN mit PCs, die unter dem Netzbetriebssystem Novell Netware 3.x vernetzt sind. Die PCs können mit Festplatte, CD-ROM-Laufwerk, Diskettenlaufwerken und anderen Laufwerken für auswechselbare Datenträger sowie anderen Peripheriegeräten ausgestattet sein. An das Netz sind gegebenenfalls ein oder mehrere Netzdrucker als Warteschleifendrucker angeschlossen. Gegenstand dieses Kapitels ist das Novell 3.x Netz in einer Client-Server-Funktionalität. Damit ist dieser Baustein die betriebssystemspezifische Ergänzung des Bausteins B 3.101 *Allgemeiner Server*.

Die Funktionalitäten des sogenannten Accounting werden nicht betrachtet.

Bemerkung: Namen von Dateien und Programmen werden immer durch Großbuchstaben mit kursiver Schreibweise (z. B. *SYS:PUBLIC\SYSCON.EXE*) dargestellt.

Gefährdungen und die hieraus abgeleiteten Maßnahmen wurden anhand der Versionen Novell 3.11 und 3.12 erarbeitet. Aufgrund verschiedener Patchlevel im Netzbetriebssystem ist es möglich, dass nicht alle Gefährdungen auf jede Variante von Novell Netware 3.x zutreffen.

Gefährdungslage

Für den IT-Grundschutz werden die folgenden typischen Gefährdungen betrachtet:

Höhere Gewalt:
- G 1.2 Ausfall des IT-Systems

Organisatorische Mängel:
- G 2.33 Nicht gesicherter Aufstellungsort von Novell Netware Servern
- G 2.34 Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen

Technisches Versagen:
- G 4.1 Ausfall der Stromversorgung

Vorsätzliche Handlungen:
- G 5.23 Computer-Viren
- G 5.43 Makro-Viren
- G 5.54 Vorsätzliches Herbeiführen eines Abnormal End
- G 5.55 Login Bypass
- G 5.56 Temporär frei zugängliche Accounts
- G 5.57 Netzanalyse-Tools
- G 5.58 "Hacking Novell Netware"
- G 5.59 Missbrauch von Administrationsrechten unter Novell Netware 3.x

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für die Clients sind die in den Bausteinen zu den jeweiligen Betriebssystemen beschriebenen Maßnahmen zu realisieren. Zu beachten ist, dass das hier vorgestellte Maßnahmenbündel, das nur die Besonderheiten des Netzbetriebssystems Novell Netware 3.x berücksichtigt, um die allgemeinen Netzsicherheitsmaßnahmen des Bausteins B 3.101 *Allgemeiner Server* ergänzt werden muss.

Für Server unter Novell Netware 3.x sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption bis zum täglichen Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Die Vorkehrungen, die bei der Planung des Einsatzes von Servern unter Novell Netware 3.x zu treffen sind, werden in der Maßnahme M 2.99 *Sichere Einrichtung von Novell Netware Servern* aufgeführt.

Umsetzung

Die Maßnahme M 2.98 *Sichere Installation von Novell Netware Servern* nennt die wesentlichen Schritte, die bei der Installation des Servers zu beachten sind.

Betrieb

Die Maßnahme M 2.100 *Sicherer Betrieb von Novell Netware Servern* nennt die wesentlichen Schritte, die beim Betrieb des Servers zu beachten sind. Die erreichte Sicherheit kann durch Umsetzung der Maßnahme M 2.101 *Revision von Novell Netware Servern* nachgewiesen werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Server unter Novell Netware 3.x" vorgestellt.

Planung und Konzeption

- M 2.99 (A) Sichere Einrichtung von Novell Netware Servern

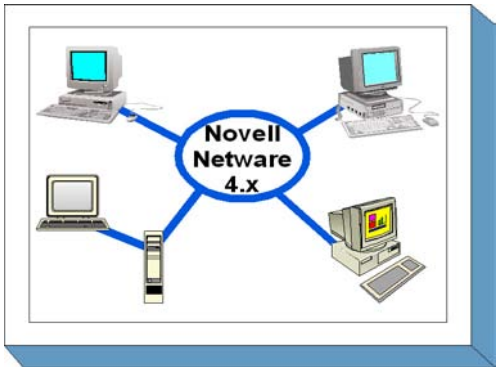
Umsetzung

- M 1.42 (A) Gesicherte Aufstellung von Novell Netware Servern
- M 2.98 (A) Sichere Installation von Novell Netware Servern
- M 2.102 (Z) Verzicht auf die Aktivierung der Remote Console

Betrieb

- M 2.100 (A) Sicherer Betrieb von Novell Netware Servern
- M 2.101 (B) Revision von Novell Netware Servern

B 3.105 Server unter Novell Netware Version 4.x



Beschreibung

Betrachtet wird das Netzbetriebssystem Novell Netware 4.x (mit dem Schwerpunkt auf Netware 4.11). Novell Netware wird auf PC-Servern betrieben und stellt im wesentlichen die Infrastrukturdienste Authentisierung, Verzeichnisdienst, Dateidienst, Druckdienst und Protokolldienst in einem Netz zur Verfügung. Gegenstand dieses Kapitels ist das Novell 4.x Netz in einer Client-Server-Funktionalität. Damit ist dieser Baustein eine betriebssystemspezifische Ergänzung des Bausteins B 3.101 *Allgemeiner Server*.

Zentraler Aspekt des Novell Netware 4.x-Betriebssystems ist die Verteilung der zentralen Datenbank des Verzeichnisdienstes NDS (Novell Directory Services) unabhängig von spezifischen Serversystemen über das LAN und der objektorientierte Ansatz zur Verwaltung aller Elemente im Betriebssystemumfeld in einer einheitlichen Umgebung.

Die Funktionalitäten der Zusatzprodukte von Novell Netware wie z. B. DHCP, WEB Server und WAN Connectivity sind ebenfalls Bestandteil dieser Betrachtung.

Bemerkungen:

- Namen von Dateien und Programmen werden immer durch Großbuchstaben mit kursiver Schreibweise (z. B. *SYS:PUBLIC\NWADMIN.EXE*) dargestellt.
- Gefährdungen und die hieraus abgeleiteten Maßnahmen wurden anhand der Version Novell 4.11 erarbeitet. Aufgrund verschiedener Patchlevel bzw. Entwicklungsunterschiede zwischen Netware 4.10 und Netware 4.11 im Netzbetriebssystem ist es möglich, dass nicht alle Gefährdungen auf jede Variante von Novell Netware 4.x zutreffen. Bei Bedarf wird darauf explizit hingewiesen bzw. im Text entsprechend unterschieden.

Gefährdungslage

Für den IT-Grundschutz von Novell Netware Version 4.x werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.2 Ausfall des IT-Systems

Organisatorische Mängel:
- G 2.33 Nicht gesicherter Aufstellungsort von Novell Netware Servern
- G 2.34 Fehlende oder unzureichende Aktivierung der Novell Netware Sicherheitsmechanismen
- G 2.42 Komplexität der NDS
- G 2.43 Migration von Novell Netware 3.x nach Novell Netware Version 4

Menschliche Fehlhandlungen:
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.25 Fahrlässiges Löschen von Objekten
- G 3.26 Ungewollte Freigabe des Dateisystems
- G 3.27 Fehlerhafte Zeitsynchronisation
- G 3.38 Konfigurations- und Bedienungsfehler

Vorsätzliche Handlungen:
- G 5.23 Computer-Viren
- G 5.43 Makro-Viren
- G 5.55 Login Bypass
- G 5.56 Temporär frei zugängliche Accounts
- G 5.57 Netzanalyse-Tools
- G 5.58 "Hacking Novell Netware"
- G 5.59 Missbrauch von Administrationsrechten im Novell Netware Netz

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für die Clients sind die in den Bausteinen zu den jeweiligen Betriebssystemen beschriebenen Maßnahmen zu realisieren. Zu beachten ist, dass das hier vorgestellte Maßnahmenbündel, das nur die Besonderheiten des Netzbetriebssystems Novell Netware 4.x berücksichtigt, um die allgemeinen Netzsicherheitsmaßnahmen des Bausteins B 3.101 ergänzt werden muss.

Für Server unter Novell Netware 4.x sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption bis zum täglichen Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Die Vorkehrungen, die bei der Planung des Einsatzes von Servern unter Novell Netware 4.x zu treffen sind, werden in der Maßnahme M 2.99 *Sichere Einrichtung von Novell Netware Servern* aufgeführt. Da sich diese Netze sehr stark auf das NDS-Verzeichnis abstützen, ist es wichtig, dessen Struktur schon in der Planungsphase festzulegen und genau zu dokumentieren.

Umsetzung

Mit Novell Netware 4.x lässt sich ein standardisiertes Sicherheitsniveau erreichen, indem die sogenannte C2-Sicherheit konfiguriert wird.

Betrieb

Die Maßnahme M 2.149 *Sicherer Betrieb von Novell Netware 4.x Netzen* nennt die wesentlichen Schritte, die beim Betrieb des Servers zu beachten sind. Die erreichte Sicherheit kann durch Umsetzung der Maßnahme M 2.150 *Revision von Novell Netware 4.x Netzen* nachgewiesen werden.

Darüber hinaus werden folgende weitere Maßnahmen vorgeschlagen:

Planung und Konzeption
- M 2.148 (A) Sichere Einrichtung von Novell Netware 4.x Netzen
- M 2.151 (A) Entwurf eines NDS-Konzeptes
- M 2.152 (B) Entwurf eines Zeitsynchronisations-Konzeptes
- M 2.153 (A) Dokumentation von Novell Netware 4.x Netzen

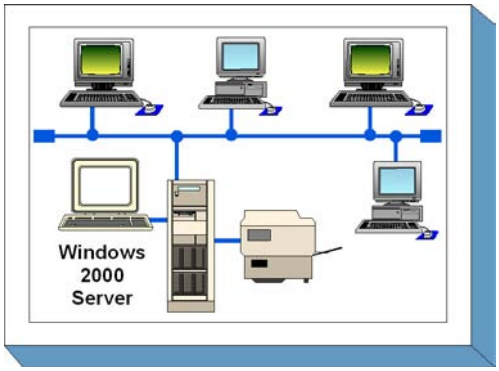
Umsetzung
- M 1.42 (A) Gesicherte Aufstellung von Novell Netware Servern
- M 2.102 (Z) Verzicht auf die Aktivierung der Remote Console
- M 2.147 (A) Sichere Migration von Novell Netware 3.x Servern in Novell Netware 4.x Netze
- M 4.102 (Z) C2-Sicherheit unter Novell 4.11

- M 4.103 (Z) DHCP-Server unter Novell Netware 4.x
- M 4.104 (Z) LDAP Services for NDS
- M 6.55 (C) Reduzierung der Wiederanlaufzeit für Novell Netware Server

Betrieb

- M 2.149 (A) Sicherer Betrieb von Novell Netware 4.x Netzen
- M 2.150 (B) Revision von Novell Netware 4.x Netzen
- M 4.108 (Z) Vereinfachtes und sicheres Netzmanagement mit DNS Services unter Novell NetWare 4.11

B 3.106 Windows 2000 Server



Beschreibung

Windows 2000 ist das Nachfolgeprodukt zum Betriebssystem Windows NT, das häufig eingesetzt wird, um kleine, mittlere und auch große Rechnernetze aufzubauen. Es ist zu erwarten, dass Windows 2000 in Zukunft die Rolle von Windows NT übernimmt, so dass mit einer entsprechend großen Verbreitung zu rechnen ist. Die Sicherheit eines solchen Betriebssystems spielt eine wichtige Rolle, da Schwachstellen auf der Betriebssystemebene die Sicherheit aller Anwendungen beeinträchtigen können. Der vorliegende Baustein beschreibt die aus Sicherheitssicht relevanten Gefährdungen und insbesondere auch Maßnahmen, die für einen Server mit Windows 2000 zutreffen.

Windows 2000 Produkte im Überblick

Die Windows 2000 Produktfamilie umfasst die Arbeitsplatz-Variante "Microsoft Windows 2000 Professional", die vergleichbar mit der Workstation Version von Microsoft Windows NT ist (siehe dazu Baustein B 3.209 *Client unter Windows XP*) und drei verschiedene Server-Versionen:

- Microsoft Windows 2000 Server,
- Microsoft Windows 2000 Advanced Server und
- Microsoft Windows 2000 Datacenter Server.

Die einzelnen Versionen des Microsoft Windows 2000 Server Betriebssystems unterscheiden sich dabei hauptsächlich in der Skalierbarkeit. Die unterstützte Hardware-Ausstattung liegt z. B.

- mit Microsoft Windows 2000 Server bei maximal 4 Prozessoren und 4 Gigabyte Hauptspeicher,
- mit Microsoft Windows 2000 Advanced Server bei maximal 8 Prozessoren und 8 Gigabyte Hauptspeicher sowie
- bei maximal 32 Prozessoren und 64 Gigabyte Hauptspeicher mit Microsoft Windows 2000 Datacenter Server.

Die zugrunde liegende Architektur der Software und die verfügbaren Dienste unterscheiden sich nur in wenigen Punkten. So unterstützen z. B. der Advanced Server und der Datacenter Server im Gegensatz zur Windows 2000 Server Software auch Clustering-Mechanismen, mit denen mehrere physikalische Rechner zu einem virtuellen Rechner mit erhöhter Ausfallsicherheit zusammengeschaltet werden können.

Hauptunterschiede zu Windows NT

Windows 2000 bietet im Vergleich zu Windows NT einige neue Sicherheitsmechanismen. Hauptsächlich ist hier das Kerberos-Protokoll zu nennen, das von Windows 2000 standardmäßig als Authentisierungsverfahren benutzt wird. Das NTLM-Verfahren von Windows NT kann ebenfalls zur Authentisierung benutzt werden, so dass ein gemeinsamer Betrieb von Windows NT und Windows 2000 Rechnern innerhalb einer Windows 2000 Domäne möglich ist.

Durch die Verwendung des Kerberos-Verfahrens wird es einfacher, die Authentisierung von Benutzern zu delegieren. Dies ist eine der Voraussetzungen für den Betrieb großer Windows 2000 Netze, in denen sich Benutzer auch über Domänengrenzen hinweg authentisieren können.

Eine der wichtigsten neuen Komponenten unter Windows 2000 ist das Active Directory. Dabei handelt es sich um eine verteilte Datenbank, die die Benutzer- und Konfigurationsdaten einer Domäne auf mehrere Domänen-Controller verteilt. Änderungen können an jedem Domänen-Controller vorgenommen werden. Die Domänen-Controller replizieren diese Änderungen untereinander. Durch die Verwendung des Active Directory werden größere Domänen möglich als bei Windows NT. Zum einen kann die Active Directory Datenbank wesentlich mehr Einträge fassen, als die SAM- Benutzerdatenbank eines Windows NT Domänen-Controllers. Zum anderen lässt sich aufgrund der verteilten Struktur des Active Directories die Last besser auf mehrere Domänen-Controller verteilen, als dies bei Windows NT der Fall ist.

Unter Sicherheitsaspekten spielt das Active Directory eine wichtige Rolle, da es

- viele sicherheitsrelevante Daten enthält,
- über eigene, dem Dateisystem sehr ähnliche Zugriffskontrollmechanismen verfügt, sowie
- die Basis für das wichtigste Konfigurationswerkzeug für Zugriffsrechte und Privilegien in Windows 2000 bildet: die Gruppenrichtlinien.

Weitere sicherheitsspezifische Neuerungen von Windows 2000 sind

- die Dateiverschlüsselung durch EFS (Encrypting File System),
- die Unterstützung von Chipkarten zur Anmeldung an Windows 2000 Benutzerkonten,
- die in Windows 2000 integrierte PKI-Funktionalität, die eine eigene Zertifikatsausgabestelle beinhaltet, sowie
- die Unterstützung von IPSec zur Netzverschlüsselung.

Ein weiterer Punkt, in dem sich Windows NT und Windows 2000 unterscheiden, ist die Voreinstellung der Zugriffsrechte auf das Dateisystem: Unter Windows 2000 lassen sich diese Zugriffsrechte restriktiver konfigurieren als unter Windows NT. Eine solche restriktive Konfiguration ist nicht zwingend erforderlich, unter Sicherheitsgesichtspunkten jedoch wünschenswert. Ihre Verwendung kann jedoch zu Problemen mit Windows NT Applikationen führen, die für eine solche Rechtekonfiguration nicht ausgelegt sind.

Gefährdungslage

Wie jedes IT-System ist auch ein Netz von Microsoft Windows 2000 Rechnern vielfältigen Gefahren ausgesetzt. Dabei sind neben Angriffen von außen auch Angriffe von innen möglich. Oft nutzen erfolgreiche Angriffe Fehlkonfigurationen einzelner oder mehrerer Systemkomponenten. Daher kommt der korrekten Konfiguration des Systems und seiner Komponenten eine wichtige Rolle zu. Generell gilt, dass die Gefährdungslage einzelner Rechner immer auch vom Einsatzszenario abhängt und diese Einzelgefährdungen auch in die Gefährdung des Gesamtsystems eingehen.

Für den IT-Grundschutz eines servergestützten Netzes unter dem Betriebssystem Microsoft Windows 2000 werden die folgenden typischen Gefährdungen angenommen:

Höhere Gewalt

- G 1.2 Ausfall des IT-Systems

Organisatorische Mängel:

- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.18 Ungeordnete Zustellung der Datenträger

- G 2.68 Fehlende oder unzureichende Planung des Active Directory

Menschliche Fehlhandlungen:
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.48 Fehlkonfiguration von Windows 2000/XP Rechnern
- G 3.49 Fehlkonfiguration des Active Directory

Technisches Versagen:
- G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
- G 4.23 Automatische CD-ROM-Erkennung
- G 4.35 Unsichere kryptographische Algorithmen

Vorsätzliche Handlungen:
- G 5.7 Abhören von Leitungen
- G 5.23 Computer-Viren
- G 5.52 Missbrauch von Administratorrechten im Windows NT/2000/XP System
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.79 Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
- G 5.83 Kompromittierung kryptographischer Schlüssel
- G 5.84 Gefälschte Zertifikate
- G 5.85 Integritätsverlust schützenswerter Informationen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den erfolgreichen Aufbau eines Windows 2000 Systems sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Installation bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

1. Nach der Entscheidung, Windows 2000 als internes Betriebssystem einzusetzen, muss die Beschaffung der Software und eventuell zusätzlich benötigter Hardware erfolgen. Folgende Maßnahmen sind durchzuführen:

   - Zunächst muss der Aufbau bzw. die Migration eines Windows 2000 Systems geplant werden (siehe Maßnahme M 2.227 *Planung des Windows 2000 Einsatzes*).

   - Parallel dazu ist eine Sicherheitsrichtlinie zu erarbeiten (siehe Maßnahme M 2.228 *Festlegen einer Windows 2000 Sicherheitsrichtlinie*), die einerseits die bereits bestehenden Sicherheitsrichtlinien im Windows 2000-Kontext umsetzt und andererseits die für Windows 2000 spezifischen Erweiterungen definiert.

   - Die Benutzer bzw. die Administratoren haben einen wesentlichen Einfluss auf die Windows 2000 Sicherheit. Vor der tatsächlichen Einführung von Windows 2000 müssen die Benutzer und Administratoren daher für den Umgang mit Windows 2000 und dessen Komponenten geschult werden. Insbesondere für Administratoren empfiehlt sich aufgrund der Komplexität in der Planung und in der Verwaltung eines Windows 2000-Systems eine intensive Schulung. Die Administratoren sollen dabei detaillierte Systemkenntnisse erwerben (siehe M 3.27 *Schulung zur Active Directory-Verwaltung* so dass eine konsistente und korrekte Systemverwaltung gewährleistet ist. Benutzern sollte insbesondere die Nutzung der Windows 2000 Sicherheitsmechanismen vermittelt werden (siehe M 3.28 *Schulung zu Windows 2000 Sicherheitsmechanismen für Benutzer*). Hier spielt als neuer Dateisystemmechanismus EFS - das verschlüsselnde Dateisystem - eine Rolle, da die

Sicherheit von EFS von der korrekten Konfiguration und Nutzung abhängt. Hinweise dazu finden sich unter M 4.147 *Sichere Nutzung von EFS unter Windows 2000/XP*.

2. Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt wurden, kann die Installation des Windows 2000-Systems erfolgen. Dabei sind die folgenden Maßnahmen zu beachten:
   - Schon die Installation muss mit besonderer Sorgfalt durchgeführt werden, da insbesondere die Sicherheitskonfiguration während der Installation noch nicht erfolgt ist. In M 4.136 *Sichere Installation von Windows 2000* sind die relevanten Empfehlungen zusammengefasst.
   - Nach der reinen Installation muss ein Windows 2000 System konfiguriert werden. Die dabei zu beachtenden Aspekte finden sich in M 4.137 *Sichere Konfiguration von Windows 2000*. Dabei kommt unter anderem auch zum tragen, für welchen Einsatzzweck ein Windows 2000 Rechner geplant ist, auf die jeweils relevanten Maßnahmen wird dort entsprechend verwiesen.
   - Die sichere Konfiguration eines Windows 2000 Systems hängt nicht nur von der sicheren Konfiguration des Betriebssystems ab, die Windows 2000 Sicherheit hängt auch wesentlich von systemnahen Diensten ab. Die relevanten Dienste sowie Verweise auf dienstespezifische Maßnahmen finden sich in M 4.140 *Sichere Konfiguration wichtiger Windows 2000 Dienste*.
3. Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:
   - Ein Windows 2000 System ändert sich in der Regel täglich. Dabei muss bei jeder Änderung sichergestellt werden, dass die Sicherheit auch nach der Änderung nicht beeinträchtigt wird. Die dabei zu beachtenden Aspekte sind in M 4.146 *Sicherer Betrieb von Windows 2000/XP* zusammengefasst.
   - Ein Mittel im Rahmen der Aufrechterhaltung der Sicherheit eines Windows 2000 Netzes ist die Überwachung des Systems bzw. seiner Einzelkomponenten. Die hier relevanten Maßnahmen finden sich in M 4.148 *Überwachung eines Windows 2000/XP Systems*. Dabei spielen auch insbesondere Datenschutzaspekte eine Rolle.
   - Neben der Absicherung im laufenden Betrieb spielt jedoch auch die Notfallvorsorge eine wichtige Rolle, da nur so der Schaden im Notfall verringert werden kann. Hinweise zur Notfallvorsorge finden sich in M 6.76 *Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes*.

Nachfolgend wird nun das Maßnahmenbündel für den Baustein "Windows 2000" vorgestellt.

Planung und Organisation

- M 2.227 (A) Planung des Windows 2000 Einsatzes
- M 2.228 (A) Festlegen einer Windows 2000 Sicherheitsrichtlinie
- M 2.229 (A) Planung des Active Directory
- M 2.230 (A) Planung der Active Directory-Administration
- M 2.231 (A) Planung der Gruppenrichtlinien unter Windows 2000
- M 2.232 (B) Planung der Windows 2000 CA-Struktur
- M 2.233 (B) Planung der Migration von Windows NT auf Windows 2000
- M 4.147 (Z) Sichere Nutzung von EFS unter Windows 2000/XP

- M 3.27 (A) Schulung zur Active Directory-Verwaltung
- M 4.48 (A) Passwortschutz unter Windows NT/2000/XP
- M 4.75 (A) Schutz der Registrierung unter Windows NT/2000/XP
- M 4.136 (A) Sichere Installation von Windows 2000
- M 4.137 (A) Sichere Konfiguration von Windows 2000
- M 4.138 (A) Konfiguration von Windows 2000 als Domänen-Controller
- M 4.139 (A) Konfiguration von Windows 2000 als Server
- M 4.140 (A) Sichere Konfiguration wichtiger Windows 2000 Dienste
- M 4.141 (A) Sichere Konfiguration des DDNS unter Windows 2000
- M 4.142 (B) Sichere Konfiguration des WINS unter Windows 2000
- M 4.143 (B) Sichere Konfiguration des DHCP unter Windows 2000
- M 4.144 (B) Nutzung der Windows 2000 CA
- M 4.145 (A) Sichere Konfiguration von RRAS unter Windows 2000
- M 4.149 (A) Datei- und Freigabeberechtigungen unter Windows 2000/XP
- M 5.89 (A) Konfiguration des sicheren Kanals unter Windows 2000/XP
- M 5.90 (Z) Einsatz von IPSec unter Windows 2000/XP

Betrieb

- M 4.56 (C) Sicheres Löschen unter Windows-Betriebssystemen
- M 4.146 (A) Sicherer Betrieb von Windows 2000/XP
- M 4.148 (B) Überwachung eines Windows 2000/XP Systems

Notfallvorsorge

- M 6.43 (Z) Einsatz redundanter Windows NT/2000 Server
- M 6.76 (C) Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes
- M 6.77 (A) Erstellung von Rettungsdisketten für Windows 2000
- M 6.78 (A) Datensicherung unter Windows 2000/XP

B 3.107 S/390- und zSeries-Mainframe

Beschreibung

Die IBM S/390- und zSeries-Systeme gehören zu den Server-Systemen, die allgemein als Mainframes ("Großrechner") bezeichnet werden. Mainframes haben sich von klassischen Einzelsystemen mit Stapelverarbeitung hin zu modernen Client-/Server-Systemen entwickelt. Sie bilden heute das obere Ende der Palette der angebotenen Server-Systeme.

In diesem Baustein werden nur Mainframes des Typs IBM zSeries bzw. IBM S/390 betrachtet. zSeries-Systeme, mit dem Betriebssystem z/OS, stellen eine logische Weiterentwicklung der OS/390-Architektur dar. Mit zSeries kommt z. B. die zusätzliche 64 Bit-Unterstützung hinzu. Beide Systemtypen existieren nebeneinander, wobei OS/390 als ein "auslaufendes" Betriebssystem betrachtet werden kann, da IBM den Service im Herbst 2004 eingestellt hat. Aus Gründen der Übersichtlichkeit wird in diesem Zusammenhang nur der Begriff "zSeries" für die Hardware und "z/OS" für das Betriebssystem verwendet.

Historie

Die im Jahr 1964 eingeführte S/360-Architektur stellt die Basis für alle folgenden Weiterentwicklungen dar und findet sich noch heute in ihren wesentlichen Teilen auf den aktuellen zSeries-Systemen wieder. Der Namenswechsel, von "S/360" über "S/370" und "S/390" bis zur heutigen "zSeries", reflektiert die fortwährende Entwicklung der zugrundeliegenden Architektur. Aufgrund ihrer Abwärtskompatibilität unterstützt die Architektur neben neueren 64-Bit-Applikationen auch Programme im älteren 24- oder 31-Bit-Modus.

Trotz steigender Leistungsfähigkeit haben sich die physischen Abmessungen von Mainframe-Systemen stark verringert. Mainframe-Systeme haben heute ähnliche Abmessungen wie andere Systeme, die typischerweise in Rechenzentren betrieben werden.

Überblick

Für zSeries-Systeme stehen Mechanismen zur Verfügung, mit denen eine hohe Verfügbarkeit und Skalierbarkeit erreicht werden kann. Die hohe Verfügbarkeit wird dabei durch redundante Auslegung der Komponenten erzielt. Zur Steigerung der Leistung und Verfügbarkeit können derzeit in einem zSeries-System bis zu 16 Prozessoren parallel betrieben und bis zu 32 zSeries-Systeme zu einem Cluster zusammengestellt werden. Dies wird als Parallel-Sysplex-Cluster bezeichnet.

Für die zSeries-Hardware sind verschiedene Betriebssysteme verfügbar (z. B. z/OS, VSE, z/VM oder TPF). Die Auswahl erfolgt in der Regel anhand der Parameter Rechnergröße und Einsatzzweck. Am häufigsten kommt jedoch das z/OS-Betriebssystem zum Einsatz. Um den Rahmen dieses Bausteins nicht zu sprengen, beschränken sich die Empfehlungen in diesem Baustein im Wesentlichen auf das Betriebssystem z/OS.

Durch die Erweiterung des früher auch als "MVS" bezeichneten z/OS-Betriebssystems um das Subsystem *Unix System Services* ist es möglich, parallel zu den klassischen Mainframe-Anwendungen auch Unix-basierte Anwendungen zu betreiben. Daneben ist für die zSeries-Hardware auch ein Linux-Betriebssystem verfügbar.

Einsatzbereiche für heutige z/OS-Systeme sind:

- klassische Stapelverarbeitung für große "Batch-Ketten",
- Stapelverarbeitung einschließlich der transaktionsorientierten Verarbeitung (z. B. IMS oder CICS),
- Datenbank-Server (z. B. DB2, IMS DB oder Oracle) oder
- Webserver und deren Anwendungen

Die in diesem Baustein beschriebenen Software-Komponenten beziehen sich hauptsächlich auf Produkte des Herstellers IBM. Es gibt darüber hinaus viele Produkte von Drittherstellern, die häufig in Großrechner-Umgebungen zum Einsatz kommen. Auf diese Produkte kann leider nur in Ausnahmefällen eingegangen werden, da sonst der Rahmen des Bausteins gesprengt würde.

Das z/OS-Betriebssystem besteht aus dem eigentlichen Betriebssystem (Kernel) mit Schnittstellen zu den Benutzerprozessen. Verschiedene Subsysteme steuern und unterstützen die Kommunikation. Die wichtigsten Subsysteme sind

- das *Job Entry Subsystem* (JES) für den Hintergrundbetrieb (Stapelverarbeitung oder Batch genannt),
- die *Time Sharing Option* (TSO) für den Vordergrundbetrieb (interaktiv) und
- die *Unix System Services* (Posix-kompatibles Unix-Subsystem).

Weitere Subsysteme sind z. B.

- der Transaktionsmanager IMS und die zugehörige Datenbank für die transaktionsorientierte Datenverarbeitung,
- der Transaktionsmanager CICS für die transaktionsorientierte Datenverarbeitung,
- die Datenbank DB2 für relationale Datenbanken und
- der *Communications Server* (SNA, TCP/IP) für Netzanbindungen.

Die Sicherheitsschnittstelle *System Authorization Facility* (SAF) ermöglicht es, das System und die Dateien vor unbefugten Zugriffen zu schützen. Die eigentlichen Sicherheitsfunktionen werden dabei von der Sicherheitssoftware RACF bereitgestellt. Als alternative Produkte sind an dieser Stelle auch *Top Secret* und *ACF2* zu nennen.

Die folgende Abbildung stellt die Zusammenhänge des Betriebssystemaufbaus stark vereinfacht dar:

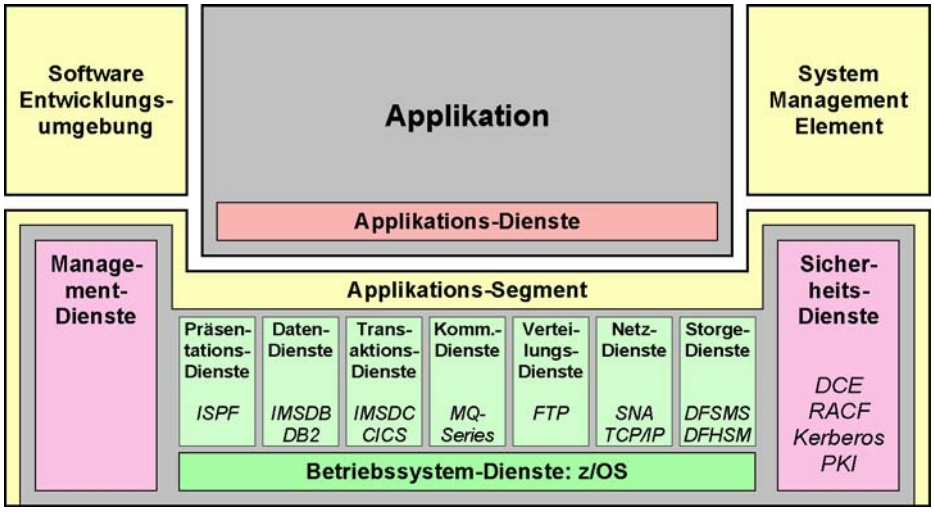


Abbildung: Prinzipieller Aufbau des z/OS-Betriebssystems

Eine Übersicht über die zSeries- und z/OS-Architektur und Erklärungen zu der Terminologie finden sich in den folgenden Maßnahmen:
- M 3.39 Einführung in die zSeries-Plattform
- M 3.40 Einführung in das z/OS-Betriebssystem
- M 3.41 Einführung in Linux und z/VM für zSeries-Systeme

Gefährdungslage

Generell hängt die Gefährdungslage vom Einsatzszenario ab. Ein z/OS-System mit SNA-Anschluss an einem isolierten behörden- oder firmeninternen Netz ist z. B. in der Regel weniger gefährdet als ein z/OS-System, das an das Internet angeschlossen ist und dort Web-Services anbietet. Darüber hinaus spielt es eine Rolle, ob auf Daten nur lesend zugegriffen werden soll (z. B. bei einem Auskunftssystem) oder ob die Daten bearbeitet werden können. Gerade durch den Einsatz von Web-Servern oder Web-Applikationen mit Internet-Anbindung hat sich die Gefährdungslage der früher als "sehr sicher" geltenden Mainframe-Systeme stark erhöht.

Aufgrund der öffentlichen Netzanbindung von Mainframe-Systemen ergeben sich wesentlich stärkere Gefährdungen durch unsachgemäße oder fehlerhafte Konfiguration der Systeme oder durch fehlende oder unvollständig etablierte Prozesse, als es früher der Fall war.

Dies gilt sowohl für externe Anbindungen und darüber mögliche Angriffe, als auch für den internen Bereich. Mainframe-Systeme sind heute ähnlichen Gefährdungen ausgesetzt wie Unix- oder Windows-Systeme.

Organisatorische Mängel:
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.27 Fehlende oder unzureichende Dokumentation
- G 2.54 Vertraulichkeitsverlust durch Restinformationen
- G 2.99 Unzureichende oder fehlerhafte Konfiguration der zSeries-Systemumgebung

Menschliche Fehlhandlungen:
- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.38 Konfigurations- und Bedienungsfehler
- G 3.66 Fehlerhafte Zeichensatzkonvertierung beim Einsatz von z/OS
- G 3.67 Unzureichende oder fehlerhafte Konfiguration des z/OS-Betriebssystems
- G 3.68 Unzureichende oder fehlerhafte Konfiguration des z/OS-Webservers
- G 3.69 Fehlerhafte Konfiguration der Unix System Services unter z/OS
- G 3.70 Unzureichender Dateischutz des z/OS-Systems
- G 3.71 Fehlerhafte Systemzeit bei z/OS-Systemen
- G 3.72 Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF
- G 3.73 Fehlbedienung der z/OS-Systemfunktionen
- G 3.74 Unzureichender Schutz der z/OS-Systemeinstellungen vor dynamischen Änderungen
- G 3.75 Mangelhafte Kontrolle der Batch-Jobs bei z/OS

Technisches Versagen:
- G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
- G 4.22 Software-Schwachstellen oder -Fehler
- G 4.50 Überlastung des z/OS-Betriebssystems

Vorsätzliche Handlungen:

- G 5.2 Manipulation an Daten oder Software
- G 5.10 Missbrauch von Fernwartungszugängen
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.19 Missbrauch von Benutzerrechten
- G 5.21 Trojanische Pferde
- G 5.28 Verhinderung von Diensten
- G 5.57 Netzanalyse-Tools
- G 5.116 Manipulation der z/OS-Systemsteuerung
- G 5.117 Verschleiern von Manipulationen unter z/OS
- G 5.118 Unbefugtes Erlangen höherer Rechte im RACF
- G 5.119 Benutzung fremder Kennungen unter z/OS-Systemen
- G 5.120 Manipulation der Linux/zSeries Systemsteuerung
- G 5.121 Angriffe über TCP/IP auf z/OS-Systeme
- G 5.122 Missbrauch von RACF-Attributen unter z/OS

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den erfolgreichen Aufbau eines z/OS-Mainframe-Systems sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der strategischen Entscheidung, über Konzeption und Installation bis zum Betrieb. Nicht vergessen werden darf dabei die ordnungsgemäße Aussonderung eines Systems, wenn das Ende der Betriebsphase erreicht wird.

Parallel zur Betriebsphase muss die Notfallvorsorge sicherstellen, dass der Betrieb auch im Notfall aufrecht erhalten werden kann. IT-Sicherheitsmanagement und Revision stellen sicher, dass das Regelwerk auch eingehalten wird.

Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Phasen beachtet werden sollten, sind im Folgenden aufgeführt:

Strategie

Vor Beginn einer jeden Planung findet eine Phase der strategischen Orientierung statt, die weitgehend auf den Anforderungen der Anwendungseigner basiert. Hier ist zu prüfen, ob die z/OS-Plattform für die Lösung der jeweiligen Aufgabenstellung geeignet ist.

Darüber hinaus kommt es auf die generelle Ausrichtung der IT-Landschaft des Rechenzentrums an. Gibt es noch keine z/OS-Plattform im Betrieb, muss der Aufbau des notwendigen Wissens des Betriebspersonals entsprechend vorbereitet werden. Als Hilfestellung für die strategische Planung dienen die Maßnahmen

- M 3.39 *Einführung in die zSeries-Plattform*,
- M 3.40 *Einführung in das z/OS-Betriebssystem* und
- M 3.41 *Einführung in Linux und z/VM für zSeries-Systeme*.

Sie geben einen Überblick über die einzelnen Funktionen von Hard- und Software und unterstützen damit das Verständnis für die z/OS-Plattform.

Konzeption

Sollte die strategische Entscheidung für den Einsatz eines z/OS-Mainframe-Systems gefallen sein, muss sich eine detaillierte Planung für den Einsatz dieses Systems anschließen. Die folgenden Maßnahmen sind dabei zu berücksichtigen:

- Vor der Anschaffung und Inbetriebnahme von zSeries-Systemen müssen verschiedene planerische Tätigkeiten durchgeführt werden (siehe M 2.286 *Planung und Einsatz von zSeries-Systeme*).
- Bei höheren Ansprüchen an die Verfügbarkeit oder die Skalierbarkeit empfiehlt sich der Einsatz eines Parallel-Sysplex-Clusters (siehe M 4.221 *Parallel-Sysplex unter z/OS*).
- Es müssen Sicherheitsrichtlinien für das z/OS-System und besonders auch für das Sicherheitssystem RACF (*Resource Access Control Facility*) geplant und festgelegt werden (siehe M 2.288 *Erstellung von Sicherheitsrichtlinien für z/OS-Systeme*).
- Es müssen Standards für die z/OS-Systemdefinitionen festgelegt werden (siehe M 2.285 *Festlegung von Standards für z/OS-Systemdefinitionen*).
- Es sollte ein Rollenkonzept für die Systemverwaltung von z/OS-Systemen eingeführt werden (siehe M 2.295 *Systemverwaltung von z/OS-Systemen*).

Umsetzung

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt worden sind, kann die Installation der zSeries-Hardware und des z/OS-Betriebssystems erfolgen. Dabei sind die folgenden Maßnahmen zu beachten:

- Es ist eine sichere Grundkonfiguration der Autorisierungsmechanismen des z/OS-Betriebssystems erforderlich (siehe M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen*).
- Wesentlich für die Absicherung der z/OS-Umgebung ist die entsprechende Konfiguration des Sicherheitssystems (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).
- Für die Umsetzung der z/OS-Steuerung einschließlich der Fernsteuerungskonsole RSF (*Remote Support Facility*) sind die Empfehlungen in Maßnahme M 4.207 *Einsatz und Sicherung systemnaher z/OS-Terminals* zu beachten.

Betrieb

Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:

- Die Bereitstellung der Funktionalitäten des z/OS-Betriebssystems setzt einen sicheren Betrieb des z/OS-Betriebssystems voraus (siehe M 4.210 *Sicherer Betrieb des z/OS-Betriebssystems*).
- Es müssen die Dienstprogramme abgesichert werden, die zur Unterstützung von betrieblichen Funktionen des z/OS-Betriebssystems dienen und eine hohe Autorisierung benötigen (siehe M 4.215 *Absicherung sicherheitskritischer z/OS-Dienstprogramme*).
- Die erforderlichen Wartungsaktivitäten eines z/OS-Systems sind in der Maßnahme M 2.293 *Wartung von zSeries-Systemen* beschrieben.
- z/OS-Systeme oder Parallel-Sysplex-Cluster müssen im laufenden Betrieb überwacht werden (siehe M 2.292 *Überwachung von z/OS-Systemen*).

Aussonderung

Empfehlungen zur Deinstallation von z/OS-Systemen, etwa nach Abschluss des Regelbetriebs, finden sich in der Maßnahme M 2.297 *Deinstallation von z/OS-Systemen*.

Notfallvorsorge

Empfehlungen zur Notfallvorsorge finden sich in der Maßnahme M 6.93 *Notfallvorsorge für z/OS-Systeme*.

IT-Sicherheitsmanagement und Revision

Das IT-Sicherheitsmanagement sollte den kompletten Lebenszyklus eines z/OS-Systems begleiten. Die folgenden Punkte sollten besonders beachtet werden:

- Bei der Vergabe und der Revision von Autorisierungen ist zu prüfen, ob die entsprechenden Mitarbeiter diese für ihre Tätigkeit benötigen. Dies gilt besonders für hohe Autorisierungen (siehe Maßnahme M 2.289 *Einsatz restriktiver z/OS-Kennungen*).
- Beim Betrieb eines z/OS-Systems ist regelmäßig zu kontrollieren, ob die Sicherheitsvorgaben eingehalten werden (siehe Maßnahme M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS*).

Nachfolgend wird das Maßnahmenbündel für den Baustein "S/390- und zSeries-Mainframe" vorgestellt.

Planung und Konzeption

- M 2.285 (Z) Festlegung von Standards für z/OS-Systemdefinitionen
- M 2.286 (Z) Planung und Einsatz von zSeries-Systemen
- M 2.287 (Z) Batch-Job-Planung für z/OS-Systeme
- M 2.288 (B) Erstellung von Sicherheitsrichtlinien für z/OS-Systeme
- M 2.295 (A) Systemverwaltung von z/OS-Systemen
- M 2.296 (Z) Grundsätzliche Überlegungen zu z/OS-Transaktionsmonitoren
- M 3.39 (A) Einführung in die zSeries-Plattform
- M 3.40 (A) Einführung in das z/OS-Betriebssystem
- M 3.41 (A) Einführung in Linux und z/VM für zSeries-Systeme
- M 4.221 (C) Parallel-Sysplex unter z/OS

Umsetzung

- M 2.289 (A) Einsatz restriktiver z/OS-Kennungen
- M 2.290 (Z) Einsatz von RACF-Exits
- M 3.42 (A) Schulung des z/OS-Bedienungspersonals
- M 4.207 (A) Einsatz und Sicherung systemnaher z/OS-Terminals
- M 4.208 (B) Absichern des Start-Vorgangs von z/OS-Systemen
- M 4.209 (A) Sichere Grundkonfiguration von z/OS-Systemen
- M 4.211 (A) Einsatz des z/OS-Sicherheitssystems RACF
- M 4.212 (Z) Absicherung von Linux für zSeries
- M 4.213 (A) Absichern des Login-Vorgangs unter z/OS
- M 4.216 (C) Festlegung der Systemgrenzen von z/OS
- M 4.217 (C) Workload Management für z/OS-Systeme
- M 4.219 (C) Lizenzschlüssel-Management für z/OS-Software
- M 4.220 (B) Absicherung von Unix System Services bei z/OS-Systemen
- M 5.113 (Z) Einsatz des VTAM Session Management Exit unter z/OS)
- M 5.114 (B) Absicherung der z/OS-Tracefunktionen

Betrieb

- M 2.291 (C) Sicherheits-Berichtswesen und -Audits unter z/OS
- M 2.292 (B) Überwachung von z/OS-Systemen
- M 2.293 (C) Wartung von zSeries-Systemen
- M 2.294 (Z) Synchronisierung von z/OS-Passwörtern und RACF-Kommandos
- M 4.210 (B) Sicherer Betrieb des z/OS-Betriebssystems
- M 4.214 (B) Datenträgerverwaltung unter z/OS-Systemen
- M 4.215 (B) Absicherung sicherheitskritischer z/OS-Dienstprogramme
- M 4.218 (Z) Hinweise zur Zeichensatzkonvertierung bei z/OS-Systemen

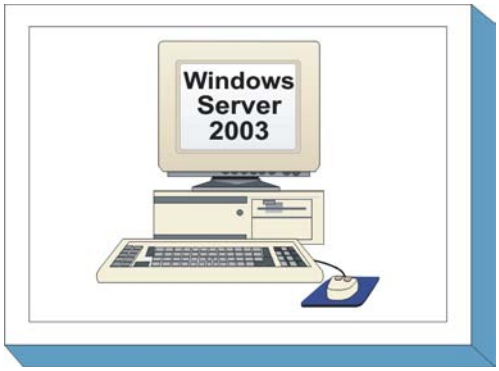
Aussonderung

- M 2.297 (B) Deinstallation von z/OS-Systemen

Notfallvorsorge

- M 6.67 (A) Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle
- M 6.93 (A) Notfallvorsorge für z/OS-Systeme

B 3.108 Windows Server 2003



Beschreibung

Das Software-Paket Windows Server 2003 ist das Nachfolgeprodukt zum Betriebssystem Windows 2000 Server. Windows Server 2003 ist in den Varianten *Standard Edition, Enterprise Edition*, *Web Edition* und *Datacenter Edition* erhältlich. Besonders weit verbreitet ist hierbei die Standard-Edition. Die Web-Edition bildet eine Teilmenge der Standard-Edition, die Enterprise-Edition enthält zusätzliche Funktionen, die nur in großen Umgebungen oder bei speziellen Anforderungen zum Einsatz kommen. Dazu gehören unter anderem die Funktionen *Fail-over-Cluster*, vollständige Terminalserver, netzgestützte UDDI-Datenbanken, unbegrenzte VPN- und RADIUS-Verbindungen, neue Zertifikatsdienste und der *Windows System Resource Manager* (WSRM). Jede dieser Editionen ist auch in einer 64-Bit-Version verfügbar, die sich in ihrem Funktionsumfang nicht signifikant von den 32-Bit-Versionen unterscheidet.

Abgrenzung des Bausteins

Der Baustein *Windows Server 2003* bezieht sich in der Regel auf die Funktionen der Standard-Edition inklusive Service Pack 1. Er kann jedoch auch problemlos auf die Varianten Web-Edition und Enterprise-Edition angewendet werden. Andere Editionen wie z. B. die Datacenter-Edition und Windows Small Business Server 2003 enthalten zusätzliche, anwendungsspezifische Funktionalitäten, die hier nicht betrachtet werden.

Die vielfältigen Einsatzmöglichkeiten erfordern eine differenzierte Betrachtung und damit eine inhaltliche Abgrenzung dieses Bausteins. Windows Server 2003 kann einerseits als reine Plattform für zusätzlich erhältliche Serverapplikationen dienen und andererseits mit den vielen im Lieferumfang von Windows Server 2003 enthaltenen Applikationen für bestimmte Bereiche ein vollständiges Gesamtsystem bilden.

Die Aktivierung einiger Funktionen ist nur bei bestimmten Anwendungsszenarien eines Windows-Server 2003 Systems notwendig. Für solche Anwendungsszenarien werden in diesem Baustein übergreifende Rahmenaspekte erläutert. Betroffen sind u. a. die Funktionen *Network Load Balancing* (NLB), Hochverfügbarkeitscluster, *Active Directory*, *Application Server*, *Role Based Access Control* (RBAC), *Zertifikatdienste* (PKI) sowie *Routing und RAS*.

Nicht näher betrachtet werden kostenlos von Microsoft erhältliche Zusatzpakete, die nicht im Standard-Lieferumfang enthalten sind. Hierzu zählen beispielsweise *Windows Sharepoint Services* (WSS), *Windows Software Update Service* (WSUS), *Rights Management Service* (RMS) oder *Microsoft Shared Computer Toolkit*.

Die folgenden mitgelieferten Komponenten werden ebenfalls nicht betrachtet, da ihr Einsatz die Berücksichtigung vieler nicht allgemeingültiger Aspekte erfordert:

- Windows Media Services

- Terminal-Server

Gefährdungslage

Für den IT-Grundschutz eines servergestützten Netzes unter dem Betriebssystem Windows Server 2003 werden die folgenden typischen Gefährdungen angenommen:

Organisatorische Mängel:
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.19 Unzureichendes Schlüsselmanagement bei Verschlüsselung
- G 2.111 Kompromittierung von Anmeldedaten bei Dienstleisterwechsel
- G 2.114 Uneinheitliche Windows-Server-2003-Sicherheitseinstellungen bei SMB, RPC und LDAP
- G 2.115 Ungeeigneter Umgang mit den Standard-Sicherheitsgruppen von Windows Server 2003
- G 2.116 Datenverlust beim Kopieren oder Verschieben von Daten unter Windows Server 2003

Menschliche Fehlhandlungen:
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.38 Konfigurations- und Bedienungsfehler
- G 3.48 Fehlerhafte Konfiguration von Windows 2000/XP/Server 2003 basierten IT-Systemen
- G 3.49 Fehlerhafte Konfiguration des Active Directory
- G 3.56 Fehlerhafte Einbindung des IIS in die Systemumgebung
- G 3.81 Unsachgemäßer Einsatz von Sicherheitsvorlagen für Windows Server 2003

Technisches Versagen:
- G 4.22 Software-Schwachstellen oder -Fehler
- G 4.54 Verlust des Schutzes durch verschlüsselnde Dateisystem EFS
- G 4.55 Datenverlust beim Zurücksetzen des Kennworts in Windows Server 2003/XP

Vorsätzliche Handlungen:
- G 5.52 Missbrauch von Administratorrechten im Windows NT/2000/XP/Server 2003 System
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.79 Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP/Server 2003 Systemen
- G 5.132 Kompromittierung einer RPD-Benutzersitzung unter Windows Server 2003
- G 5.133 Unautorisierte Benutzung web-basierter Administrationswerkzeuge

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Alle Überlegungen zu einem Windows Server 2003 sollten auf den im Baustein B 3.101 *Allgemeiner Server* enthaltenen Maßnahmen basieren. Die dort beschriebenen allgemeinen Maßnahmen werden im vorliegenden Baustein konkretisiert und ergänzt.

Server und Clients bilden eine Funktionseinheit. Daher muss auch der Baustein B 3.201 *Allgemeiner Client* und die darauf aufbauenden Betriebssystem-spezifischen Bausteine im Zusammenhang mit diesem Baustein beachtet werden.

Planung und Konzeption

Ist die allgemeine Planung des Servereinsatzes abgeschlossen und die Wahl des Betriebssystems auf Windows Server 2003 gefallen, müssen Teilkonzepte für den Servereinsatz unter Berücksichtigung aller geltenden übergeordneten Konzepte und Richtlinien erstellt werden. Die generelle Vorgehensweise bei der Planung wird in M 2.315 *Planung des Servereinsatzes* erläutert.

Für die darin genannten Themengebiete sind die spezifischen Empfehlungen aus den Maßnahmen M 4.276 *Planung des Einsatzes von Windows Server 2003* und M 2.364 *Planung der Administration für Windows Server 2003* zu entnehmen.

Während der Planung müssen wichtige Entscheidungen über grundlegende Infrastrukturdienste gefällt werden. Maßgeblich ist M 5.37 *Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz*. In die Entscheidungen hinsichtlich der Konzeption der Infrastrukturdienste fließen die geplanten Rollen und die Hinweise aus den Hilfsmitteln zum IT-Grundschutz (siehe *DNS/WINS/DHCP als Infrastrukturdienste unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*) ein.

Zu planen sind weiterhin die Kommunikationsprotokolle des Servers (M 4.277 Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows Server 2003, M 5.131 Absicherung von IP-Protokollen unter Windows Server 2003).

Weitere übergreifende Funktionen können die Sicherheit des Servers erhöhen, z. B. WebDAV und *Encrypting File System* (EFS) (siehe M 5.132 *Sicherer Einsatz von WebDAV unter Windows Server 2003*, M 4.278 *Sichere Nutzung von EFS unter Windows Server 2003*), Netzwerklastenausgleich (*Network Load Balancing*, NLB), IPSec, Benutzerauthentisierung mittels Smart Card und andere. Hierbei sollten auch M 6.99 *Regelmäßige Sicherung wichtiger Systemkomponenten für Windows Server 2003*, M 4.279 *Erweiterte Sicherheitsaspekte für Windows Server 2003* beachtet werden.

Bei allen bisher genannten Schritten sind die Grundsätze aus M 5.10 *Restriktive Rechtevergabe* und M 5.9 *Protokollierung am Server* zu berücksichtigen. Spezifische Hilfestellungen geben M 2.370 *Administration der Berechtigungen unter Windows Server 2003* und M 2.365 *Planung der Systemüberwachung unter Windows Server 2003*. Die dort genannten Empfehlungen für den Betrieb des Servers sollten auch schon bei der Planung von Berechtigungskonzepten berücksichtigt werden.

Im Rahmen der Planung des Servers sollte eine Sicherheitsrichtlinie erstellt und/oder bestehende Richtlinien ergänzt werden. Bei allen bisher genannten Schritten ergeben sich in Abhängigkeit von Einsatzzweck und Nutzdaten kritische Aspekte sowie individuelle Lösungen und Verfahrensweisen. Diese werden gesammelt. Dann wird anhand der individuellen Situation und Organisationsstruktur des Unternehmens oder der Behörde überlegt, welche Aspekte den Sicherheitsrichtlinien hinzugefügt werden sollen. Die Maßnahme M 2.316 *Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server* schildert eine geeignete Herangehensweise.

Beschaffung

Nach Abschluss der konzeptionellen Planungsarbeiten und der Definition der Beschaffungskriterien für einen Server (siehe M 2.317 *Beschaffungskriterien für einen Server*) sollte in Abhängigkeit der Anzahl der zu beschaffenden Server ein geeignetes Lizenzmodell ausgewählt werden. Die Hilfsmittel zum IT-Grundschutz bieten hierbei Hilfestellung (siehe *Auswahl geeigneter Lizenzierungsmethoden für Windows XP/Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Umsetzung

Nach der Planung von sicherheitsrelevanten Maßnahmen für Windows Server 2003 müssen diese im Rahmen der Umsetzung bzw. Installation und Konfiguration des Windows Server 2003 Systems realisiert werden.

Zur Gewährleistung eines angemessenen Sicherheitsniveaus sollten bei der Umsetzung (und später auch im Betrieb) eines Windows-Server-2003-Systems die folgenden Prämissen beachtet werden:

- Die Funktionalität ist auf die geplante und unbedingt benötigte zu reduzieren (auch im Hinblick auf Clients, die auf den Server zugreifen), um die Angriffsfläche zu minimieren und die Zahl von (potenziellen) Schwachstellen zu verringern (M 4.285 *Deinstallation nicht benötigter Client-Funktionen von Windows Server 2003* sowie M 4.286 *Verwendung der Softwareeinschränkungsrichtlinie unter Windows Server 2003* und M 4.284 *Umgang mit Diensten unter Windows Server 2003*).
- Die Konfiguration ist im Hinblick auf Sicherheit und Erfüllung der Aufgabe des Servers zu optimieren (Härten des Servers), so dass nur die tatsächlich notwendige Abwärtskompatibilität und Offenheit des Systems gegeben ist (M 4.282 *Sichere Konfiguration der IIS-Basis-Komponente unter Windows Server 2003* sowie M 4.283 *Sichere Migration von Windows NT 4 Server und Windows 2000 Server auf Windows Server 2003* und M 4.48 *Passwortschutz unter Windows NT/2000/XP).*
- Es muss eine aktuelle und angemessene Dokumentation erstellt werden, die den IT-Sicherheitsprozess bestmöglich unterstützt.

Die Maßnahme M 4.237 *Sichere Grundkonfiguration eines IT-Systems* wird durch M 4.280 *Sichere Basiskonfiguration von Windows Server 2003* konkretisiert. Hier sind eine Reihe von kleineren Funktionen sowie grundsätzliche Vorgehensweisen bei der Umsetzung erläutert, mit denen die oben genannten Prämissen erfüllt werden können.

Zur Installation und Konfiguration sollten Hilfsprogramme, sogenannte Assistenten, bevorzugt werden. Manuelle Einstellungen sollten nur wenn unbedingt notwendig vorgenommen werden. So wird einerseits Fehlkonfigurationen vorgebeugt und andererseits die Dokumentation vereinfacht (z. B.: "Assistent mit Standardeinstellungen sowie folgenden drei abweichenden Einstellungen konfiguriert..."). Administrative Hilfsmittel wie Vorlagen und Skripte (M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003* und M 2.367 *Einsatz von Kommandos und Skripten unter Windows Server 2003*) unterstützen die Standardisierung und Dokumentation.

Sofern der Server neu aufgesetzt wird, fließen alle bisher genannten Schritte bei der Installation und Bereitstellung des Servers zusammen. Um hierfür einen sicheren und zuverlässigen Prozess zu etablieren, sollte M 4.281 *Sichere Installation und Bereitstellung von Windows Server 2003* umgesetzt werden.

Betrieb

Im Regelbetrieb ist neben der Gewährleistung einer aktuellen Dokumentation insbesondere der Umgang mit administrativen Vorlagen und die Administration der Berechtigungen von Bedeutung (M 2.368 *Umgang mit administrativen Vorlagen unter Windows Server 2003* und M 2.370 *Administration der Berechtigungen unter Windows Server 2003*).

Die Aufrechterhaltung der Sicherheit wird neben den im Baustein B 3.101 *Allgemeiner Server*, genannten Maßnahmen M 4.93 *Regelmäßige Integritätsprüfung* und M 5.8 *Regelmäßiger Sicherheitscheck des Netzes* für einen Windows Server 2003 durch die Maßnahme M 2.369 *Regelmäßige sicherheitsrelevante Wartungsmaßnahmen eines Windows Server* ergänzt bzw. konkretisiert.

Aussonderung

Zur geregelten Aussonderung eines Windows Servers 2003 sollten generell die im Baustein B 3.101 *Allgemeiner Server* beschriebenen Maßnahmenempfehlungen berücksichtigt werden. Zusätzlich ist in Bezug auf die Deaktivierung bzw. Löschung von einzelnen Konten die Maßnahme M 2.371 *Geregelte Deaktivierung und Löschung ungenutzter Konten* zu beachten.

Notfallvorsorge

Aspekte der Notfallplanung für einen Windows Server 2003 werden in den Maßnahmen M 6.99 *Regelmäßige Sicherung wichtiger Systemkomponenten für Windows Server 2003* und M 6.76 *Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes* thematisiert.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Windows Server 2003" vorgestellt.

Planung und Konzeption

- M 2.232 (C) Planung der Windows 2000/2003 CA-Struktur
- M 2.364 (A) Planung der Administration für Windows Server 2003
- M 2.365 (A) Planung der Systemüberwachung unter Windows Server 2003
- M 4.276 (A) Planung des Einsatzes von Windows Server 2003
- M 4.277 (C) Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows Server 2003
- M 4.278 (Z) Sichere Nutzung von EFS unter Windows Server 2003
- M 4.279 (Z) Erweiterte Sicherheitsaspekte für Windows Server 2003
- M 5.131 (A) Absicherung von IP-Protokollen unter Windows Server 2003
- M 5.132 (B) Sicherer Einsatz von WebDAV unter Windows Server 2003

Umsetzung

- M 2.366 (B) Nutzung von Sicherheitsvorlagen unter Windows Server 2003
- M 2.367 (C) Einsatz von Kommandos und Skripten unter Windows Server 2003
- M 4.48 (A) Passwortschutz unter NT-basierten Windows-Systemen
- M 4.52 (A) Geräteschutz unter NT-basierten Windows-Systemen
- M 4.280 (A) Sichere Basiskonfiguration von Windows Server 2003
- M 4.281 (A) Sichere Installation und Bereitstellung von Windows Server 2003
- M 4.282 (B) Sichere Konfiguration der IIS-Basis-Komponente unter Windows Server 2003
- M 4.283 (B) Sichere Migration von Windows NT 4 Server und Windows 2000 Server auf Windows Server 2003
- M 4.284 (B) Umgang mit Diensten unter Windows Server 2003
- M 4.285 (A) Deinstallation nicht benötigter Client-Funktionen von Windows Server 2003
- M 4.286 (A) Verwendung der Softwareeinschränkungsrichtlinie unter Windows Server 2003

Betrieb

- M 2.368 (C) Umgang mit administrativen Vorlagen unter Windows Server 2003
- M 2.369 (A) Regelmäßige sicherheitsrelevante Wartungsmaßnahmen eines Windows Server 2003
- M 2.370 (A) Administration der Berechtigungen unter Windows Server 2003
- M 4.56 (C) Sicheres Löschen unter Windows-Betriebssystemen

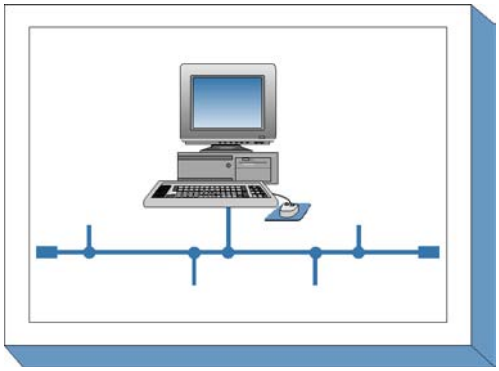
Aussonderung

- M 2.371 (A) Geregelte Deaktivierung und Löschung ungenutzter Konten

Notfallvorsorge

- M 6.76 (A) Erstellen eines Notfallplans für den Ausfall von Windows 2000/XP/2003-Systemen
- M 6.99 (A) Regelmäßige Sicherung wichtiger Systemkomponenten für Windows Server 2003

B 3.201 Allgemeiner Client



Beschreibung

Betrachtet wird ein IT-System mit einem beliebigen Betriebssystem, das die Trennung von Benutzern zulässt (es sollte mindestens eine Administrator- und eine Benutzer-Umgebung eingerichtet werden können). Typischerweise ist ein solches IT-System vernetzt und wird als Client in einem Client-Server-Netz betrieben.

Das IT-System kann auf einer beliebigen Plattform betrieben werden, es kann sich dabei um einen PC mit oder ohne Festplatte, aber auch um eine Unix-Workstation oder einen Apple Macintosh handeln. Das IT-System kann über Disketten-, CD-ROM-, DVD- oder andere Laufwerke für auswechselbare Datenträger sowie andere Peripheriegeräte verfügen. Falls der Client weitere Schnittstellen zum Datenaustausch hat, wie z. B. USB, Bluetooth, WLAN, müssen diese entsprechend den Sicherheitsvorgaben der Institution abgesichert werden, wie dies in den entsprechenden Bausteinen beschrieben ist.

Dieser Baustein bietet einen Überblick über Gefährdungen und IT-Sicherheitsmaßnahmen, die für alle Clients unabhängig von der verwendeten Plattform und vom eingesetzten Betriebssystem zutreffen. Je nach dem eingesetzten Betriebssystem sind zusätzlich die weiterführenden Bausteine der IT-Grundschutz-Kataloge (zum Beispiel B 3.206 *Unix-System*) zu beachten.

Gefährdungslage

Für den IT-Grundschutz eines allgemeinen Clients werden folgende Gefährdungen angenommen:

Höhere Gewalt:
- G 1.1 Personalausfall

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.21 Mangelhafte Organisation des Wechsels zwischen den Benutzern
- G 2.24 Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
- G 2.25 Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten
- G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindungen

Menschliche Fehlhandlungen:
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.17 Kein ordnungsgemäßer PC-Benutzerwechsel

Technisches Versagen:
- G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
- G 4.13 Verlust gespeicherter Daten
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör

Vorsätzliche Handlungen:

- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.7 Abhören von Leitungen
- G 5.9 Unberechtigte IT-Nutzung
- G 5.20 Missbrauch von Administratorrechten
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.40 Abhören von Räumen mittels Rechner mit Mikrofon
- G 5.43 Makro-Viren
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.85 Integritätsverlust schützenswerter Informationen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den Einsatz von Arbeitsplatzrechnern sollten im Hinblick auf die IT-Sicherheit von Clients folgende Schritte durchlaufen werden:

Planung des Einsatzes von Clients

Für die sichere Nutzung von IT-Systemen müssen vorab die Rahmenbedingungen festgelegt werden. Dabei müssen die Sicherheitsanforderungen für die bereits vorhandenen IT-Systeme sowie die geplanten Einsatzszenarien von Anfang an mit einbezogen werden (siehe M 2.321 *Planung des Einsatzes von Client-Server-Netzen*). Schon vor der Beschaffung der Rechner und Software sollte eine Sicherheitsrichtlinie für die Clients erstellt werden (siehe M 2.322 *Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz*).

Übergreifende Fragen der sicheren Nutzung von IT-Systemen werden im Baustein B 1.9 *Hard- und Software-Management* betrachtet.

Beschaffung

Für die Beschaffung von Clients, die typischerweise in größeren Mengen erfolgt, müssen ausgehend von den Einsatzszenarien Kriterien für die Auswahl geeigneter Produkte formuliert werden (siehe hierzu B 1.10 *Standardsoftware*). Auch bei der Beschaffung von Einzelsystemen ist es wichtig, dass das System zur vorhandenen Struktur passt, damit nicht für ein einzelnes System wegen dessen Besonderheiten ein unangemessen hoher Aufwand bei Integration und Betrieb entsteht.

Falls Hard- oder Software nicht die festgelegten Sicherheitsanforderungen erfüllen, sind weitere Maßnahmen erforderlich. Diese können organisatorischer Art sein (beispielsweise durch Regelungen, dass der Client ausschließlich hinter verschlossener Bürotür betrieben werden darf) oder es können Zusatzkomponenten beschafft werden, um die identifizierten Mankos auszugleichen (siehe hierzu M 4.41 *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*).

Bei besonders hohen Anforderungen an die Verfügbarkeit der Clients ist für diese der Einsatz einer Unterbrechungsfreien Stromversorgung (USV) empfehlenswert. Dabei kann es sich beispielsweise um eine "Einzelplatz-USV" handeln, falls die hohen Anforderungen nur für einzelne Clients gelten, oder aber um einen eigenen entsprechend abgesicherten Stromkreis ("rote Steckdose"). Weitere Informationen finden sich in M 1.28 *Lokale unterbrechungsfreie Stromversorgung*.

Umsetzung

Um Risiken durch Fehlbedienung oder absichtlichen Missbrauch der IT-Systeme auszuschließen, sind eine sorgfältige Auswahl der Betriebssystem- und Softwarekomponenten, eine sichere Installation und sorgfältige Konfiguration wichtig. Die dabei zu treffenden Maßnahmen sind in hohem Grade abhängig von dem eingesetzten Betriebssystem. Näheres dazu findet sich deswegen in spezifischen Bausteinen, beispielsweise in B 3.204 *Client unter Unix* oder B 3.205 *Client unter Windows NT.*

- Sichere Installation

  Der Grundstein für die Sicherheit wird bereits bei der Vorbereitung der Installation gelegt. Vor der Installation sollte festgelegt werden, welche Komponenten des Betriebssystems und welche Anwendungsprogramme und Tools installiert werden sollen. Die getroffenen Entscheidungen müssen so dokumentiert werden, dass gegebenenfalls nachvollzogen werden kann, welche Konfiguration und Softwareausstattung für das System gewählt wurde (siehe M 4.237 *Sichere Grundkonfiguration eines IT-Systems*).

  Für die Installation sollten nur Installationsmedien benutzt werden, die aus einer sicheren Quelle stammen (beispielsweise direkt vom Hersteller oder Distributor des Betriebssystems oder Programms). Die Installation des Betriebssystems sollte wenn möglich durchgeführt werden, ohne dass das System an das Netz angeschlossen ist (Offline-Installation). Falls bei der Installation Teile der Pakete über das Netz geladen werden sollen, sollte für die Installation ein eigenes Netz (Testnetz) genutzt werden, das vom übrigen Netz getrennt ist. Von einem Nachladen von Paketen über das Internet wird dringend abgeraten. Falls es in Ausnahmefällen erforderlich ist, ein System direkt im Produktionsnetz zu installieren, so muss durch geeignete zusätzliche Maßnahmen sichergestellt werden, dass auf das System während der Installation nicht von außen zugegriffen werden kann.

  Bereits im Verlauf der Installation werden meist einige Grundeinstellungen zur Systemkonfiguration (unterschiedlich je nach Betriebssystem) vorgenommen.

- Sichere Konfiguration

  An die eigentliche Installation schließt sich die Grundkonfiguration eines Clients an. In dieser Phase wird die vorläufige Konfiguration, wie sie im Verlauf der Installation vom Installationsprogramm eingerichtet wurde, an die tatsächlichen Gegebenheiten und Anforderungen des IT-Verbunds angepasst, in dem der Client eingesetzt werden soll. Oft werden dabei weitere Programme installiert oder es werden Programme aus einer Standardkonfiguration entfernt, die Einstellungen für den Zugriff auf das Netz werden festgelegt und der Client wird für den Zugriff auf Verzeichnisdienste oder ähnliches konfiguriert. Außerdem werden nicht benötigte Benutzer-Kennungen gelöscht oder deaktiviert, und die Benutzer-Kennungen für die eigentlichen Benutzer werden angelegt.

  In dieser Phase werden auch die benötigten Anwendungsprogramme installiert und konfiguriert. Für die Installation und Konfiguration der Anwendungsprogramme sind analoge Sicherheitsaspekte wie für die Installation des Betriebssystems selbst zu beachten.

  Falls eine größere Anzahl ähnlich konfigurierter Clients installiert und konfiguriert werden soll, so bietet es sich an, dies nicht für jeden Client einzeln durchzuführen, sondern eine "generische" Installation zu erstellen, die anschließend auf die einzelnen Clients übertragen wird, und an der nur noch minimale Änderungen vor der Inbetriebnahme erforderlich sind. Eine solche generische Konfiguration kann erheblich zur Effizienz beitragen und das Risiko von Fehlern verringern helfen. Andererseits ist bei der Erstellung der Referenzinstallation besondere Sorgfalt erforderlich. Die vorgenommenen Einstellungen müssen nachvollziehbar dokumentiert sein.

Ein wichtiger Grundsatz bei der Konfiguration von Clients ist, dass normale Bedienungsfehler der Anwender zu keinen gravierenden Schäden am System und an Daten anderer Benutzer führen sollten, und dass Anwender nicht durch einfache Neugierde Zugriff auf Informationen erlangen dürfen, die nicht für sie bestimmt sind. Mehr dazu findet sich in M 4.237 *Sichere Grundkonfiguration eines IT-Systems*.

Nachdem der Client fertig konfiguriert ist, kann der Rechner an die Anwender übergeben werden. Falls die Anwender keine ausreichenden Kenntnisse des eingesetzten Betriebssystems, einzelner Anwendungsprogramme oder Tools besitzen, so müssen sie vorab geschult werden. Allgemeine Aspekte hierzu finden sich im Baustein B 1.13 *IT-Sicherheitssensibilisierung und -schulung*.

Betrieb

Eine der wichtigsten IT-Sicherheitsmaßnahmen beim Betrieb heutiger Client-Systeme ist es, die Systeme durch zeitnahes Einspielen von Sicherheitspatches stets auf einem aktuellen Stand zu halten (siehe M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*) sowie die Installation und permanente Aktualisierung eines Virenscanners (siehe dazu auch B 1.6 *Computer-Virenschutzkonzept*). Daneben ist eine regelmäßige Datensicherung (siehe auch B 1.4 *Datensicherungskonzept*) eine grundlegende Voraussetzung dafür, dass Hardwaredefekte und Programm- oder Benutzerfehler nicht zu gravierenden Datenverlusten führen.

Ein Mittel zur Erkennung von Angriffen oder missbräuchlicher Nutzung ist die Überwachung des Systems. Dafür relevante Maßnahmen finden sich in M 4.93 *Regelmäßige Integritätsprüfung* und M 5.8 *Regelmäßiger Sicherheitscheck des Netzes* sowie im Baustein B 1.9 *Hard- und Software-Management*.

Auch bei Clients ist es wichtig, dass die Administration auf sicheren Wegen erfolgt und dass die Arbeit der Administratoren nachvollziehbar ist. Die entsprechenden Aspekte sind in M 4.234 *Aussonderung von IT-Systemen* beschrieben.

Aussonderung

Bei der Aussonderung eines Clients muss zunächst sichergestellt werden, dass alle Benutzerdaten gesichert oder auf ein Ersatzsystem übertragen werden. Anschließend muss dafür gesorgt werden, dass keine sensitiven Daten auf den Festplatten des Rechners zurück bleiben. Dazu genügt es nicht, die Platten einfach neu zu formatieren, sondern sie müssen mindestens einmal vollständig überschrieben werden. Es ist zu beachten, dass weder ein reines logisches Löschen noch das Neuformatieren der Platten mit den Mitteln des installierten Betriebssystems die Daten wirklich von den Festplatten entfernt. Mit geeigneter Software können Daten, die auf diese Weise gelöscht wurden wieder rekonstruiert werden, oft sogar ohne großen Aufwand. Hinweise zum sicheren Löschen finden sich in M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* und in M 2.309 *Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung*. Nach der Aussonderung eines Clients müssen Bestandsverzeichnisse und Netzpläne aktualisiert werden.

Notfallvorsorge

Das notwendige Maß an Notfallvorsorge für einen allgemeinen Client ist stark vom individuellen Einsatzszenario abhängig. Oft wird als Notfallvorsorge für einen Client eine regelmäßige Datensicherung (siehe M 6.32 *Regelmäßige Datensicherung*) und das Erstellen eines bootfähigen Datenträgers für Notfälle (siehe M 6.24 *Erstellen eines Notfall-Bootmediums*) ausreichend sein. Für Clients mit besonderen Anforderungen an die Verfügbarkeit kann es sinnvoll sein, weitere Maßnahmen zu ergreifen, beispielsweise ein Austauschsystem bereit zu halten.

Abhängig vom eingesetzten Betriebssystem sind bei der Anwendung dieses Bausteins gegebenenfalls weitere Maßnahmen erforderlich. Diese finden sich in den jeweiligen Bausteinen.

Für den allgemeinen Client sind folgende Maßnahmen umzusetzen:

Planung und Konzeption
- M 2.23 (Z) Herausgabe einer PC-Richtlinie
- M 2.321 (A) Planung des Einsatzes von Client-Server-Netzen
- M 2.322 (A) Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
- M 5.37 (B) Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz

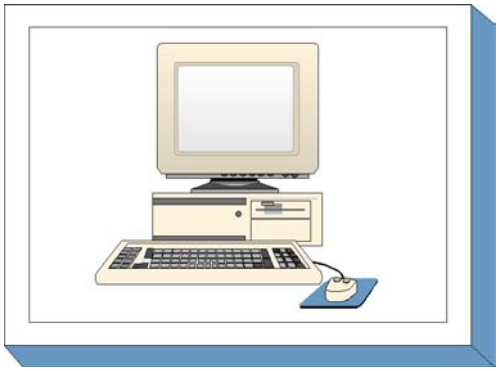
Umsetzung
- M 2.25 (A) Dokumentation der Systemkonfiguration
- M 4.237 (A) Sichere Grundkonfiguration eines IT-Systems

Betrieb
- M 2.273 (A) Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
- M 3.18 (A) Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
- M 4.2 (A) Bildschirmsperre
- M 4.3 (A) Regelmäßiger Einsatz eines Anti-Viren-Programms
- M 4.4 (C) Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
- M 4.40 (A) Verhinderung der unautorisierten Nutzung des Rechnermikrofons
- M 4.41 (C) Einsatz angemessener Sicherheitsprodukte für IT-Systeme
- M 4.93 (B) Regelmäßige Integritätsprüfung
- M 4.200 (Z) Umgang mit USB-Speichermedien
- M 4.238 (A) Einsatz eines lokalen Paketfilters
- M 4.241 (A) Sicherer Betrieb von Clients
- M 4.242 (Z) Einrichten einer Referenzinstallation für Clients
- M 5.45 (B) Sicherheit von WWW-Browsern

Aussonderung
- M 2.323 (A) Geregelte Außerbetriebnahme eines Clients

Notfallvorsorge
- M 6.24 (A) Erstellen eines Notfall-Bootmediums
- M 6.32 (A) Regelmäßige Datensicherung

B 3.202 Allgemeines nicht vernetztes IT-System



Beschreibung

Betrachtet wird ein IT-System, das mit keinem anderen IT-System vernetzt ist. Es kann mit einem beliebigen Betriebssystem ausgestattet sein. Das IT-System kann auf einer beliebigen Plattform betrieben werden, es kann sich dabei um einen PC mit oder ohne Festplatte, aber auch um eine Unix-Workstation oder einen Apple Macintosh handeln. Das IT-System kann beispielsweise über Disketten-, CD-ROM-, DVD- oder andere Laufwerke für auswechselbare Datenträger sowie andere Peripheriegeräte verfügen. Falls der Client weitere Schnittstellen zum Datenaustausch hat, wie z. B. USB, Bluetooth, WLAN, müssen diese entsprechend den Sicherheitsvorgaben der Institution abgesichert werden, wie dies in den entsprechenden Bausteinen beschrieben ist. Ein eventuell vorhandener Drucker wird direkt am IT-System angeschlossen.

Dieses Kapitel bietet einen Überblick über Gefährdungen und IT-Sicherheitsmaßnahmen, die für nicht vernetzte IT-Systeme typisch sind. Dieser Überblick ist unabhängig vom eingesetzten Betriebssystem. Dafür sind die weiterführenden Bausteine der IT-Grundschutz-Kataloge (zum Beispiel B 3.206 *Unix-System*) zu beachten.

Gefährdungslage

Für den IT-Grundschutz eines allgemeinen nicht vernetzten IT-Systems werden folgende Gefährdungen angenommen:

Höhere Gewalt:
- G 1.1 Personalausfall
- G 1.2 Ausfall des IT-Systems
- G 1.4 Feuer
- G 1.5 Wasser
- G 1.8 Staub, Verschmutzung

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.21 Mangelhafte Organisation des Wechsels zwischen den Benutzern

Menschliche Fehlhandlungen:
- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten
- G 3.17 Kein ordnungsgemäßer PC-Benutzerwechsel

Technisches Versagen:
- G 4.1 Ausfall der Stromversorgung
- G 4.7 Defekte Datenträger

Vorsätzliche Handlungen:

- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.9 Unberechtigte IT-Nutzung
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.19 Missbrauch von Benutzerrechten
- G 5.20 Missbrauch von Administratorrechten
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.40 Abhören von Räumen mittels Rechner mit Mikrofon
- G 5.43 Makro-Viren

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Allgemeines nicht vernetztes IT-System" vorgestellt. Ein Teil der hier genannten Maßnahmen ist in jedem Fall umzusetzen, auch wenn nur eine einzige Person dieses IT-System nutzt. Sollen an dem IT-System mehrere Benutzer arbeiten, so ist zusätzlich eine Administration des Rechners und eine Benutzertrennung unumgänglich. In diesem Fall sind auch die Maßnahmen und Gefährdungen zu betrachten, die für den Mehrbenutzerbetrieb relevant sind.

Abhängig vom eingesetzten Betriebssystem sind neben der Anwendung dieses Bausteins gegebenenfalls weitere Maßnahmen erforderlich, die in anderen Bausteinen beschrieben sind.

Für den Einsatz von nicht vernetzten Arbeitsplatzrechnern sollten im Hinblick auf die IT-Sicherheit folgende Schritte durchlaufen werden:

1. Richtlinien für die Nutzung von nicht vernetzten IT-Systemen

   Für die sichere Nutzung von IT-Systemen müssen verbindliche Richtlinien festgelegt werden. Dies umfasst beispielsweise, wer das System wann und wofür nutzen darf und auf welche Daten der Zugriff in welcher Weise gestattet wird. Diese Arbeiten werden im Rahmen der Umsetzung der Maßnahmen des Bausteins B 1.9 *Hard- und Software-Management* durchgeführt.

2. Sichere Installation von nicht vernetzten IT-Systemen

   Eine sorgfältige Auswahl der Betriebssystem- und Software-Komponenten sowie deren sichere Installation ist notwendig, um Risiken durch Fehlbedienung oder absichtlichen Missbrauch der IT-Systeme auszuschließen. Die hier zu treffenden Maßnahmen sind in hohem Grade abhängig von dem eingesetzten Betriebssystem und sind daher im Rahmen der Umsetzung der entsprechenden Bausteine, beispielsweise B 3.204 *Client unter Unix* oder B 3.209 *Client unter Windows XP*, zu realisieren. Dabei ist die Maßnahme M 4.15 *Gesichertes Login* von besonderer Bedeutung, da der technische Schutz nicht vernetzter Systeme zu einem großen Teil auf einer geeigneten Zugangskontrolle beruht. Zusätzliche Maßnahmen sind vor allem dann erforderlich, wenn mehrere Benutzer mit unterschiedlichen Berechtigungen auf dasselbe IT-System zugreifen sollen:
   - M 2.63 *Einrichten der Zugriffsrechte*
   - M 3.18 *Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung*
   - M 4.41 *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*

3. Sichere Konfiguration der installierten Komponenten

   Je nach Sicherheitsanforderungen müssen die beteiligten Software-Komponenten unterschiedlich konfiguriert werden. Die hier zu treffenden Maßnahmen sind ebenfalls abhängig von dem eingesetzten Betriebssystem und sind daher im Rahmen der Umsetzung der entsprechenden Bausteine zu realisieren. Auch hier sind zusätzliche Maßnahmen erforderlich, wenn eine Trennung der Rechte mehrerer Benutzer erforderlich ist. Zu beachten ist auch die Maßnahme M 4.7 *Änderung voreingestellter Passwörter*, weil nur zu häufig jede Zugangskontrolle dadurch illusorisch ist, dass die verwendeten Passwörter allgemein bekannt sind.

4. Sicherer Betrieb von nicht vernetzten IT-Systemen

   Eine der wichtigsten IT-Sicherheitsmaßnahmen beim Betrieb heutiger Client-Systeme ist die Installation und permanente Aktualisierung eines Virenscanners. Um Angriffsversuche und missbräuchliche Nutzung erkennen zu können, sind bei nicht vernetzten IT-Systemen vor allem organisatorische Maßnahmen notwendig. Die notwendigen Maßnahmen werden im Rahmen der Umsetzung der Bausteine B 1.6 *Computer-Virenschutzkonzept* und B 1.9 *Hard- und Software-Management* realisiert und brauchen daher hier nicht weiter betrachtet zu werden. Spezifische Maßnahmen für Einzelsysteme sind dabei vor allem M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern* und M 4.30 *Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen*.

5. Datensicherung der nicht vernetzten IT-Systeme (siehe M 6.32)

   Die Vorgehensweise und der erforderliche Umfang der Datensicherung richtet sich nach dem Einsatzszenario des IT-Systems (siehe Maßnahme M 6.32 *Regelmäßige Datensicherung*).

Für das allgemeine nicht vernetzte IT-System sind folgende Maßnahmen umzusetzen:

Planung und Konzeption
- M 2.23 (Z) Herausgabe einer PC-Richtlinie
- M 2.63 (A) Einrichten der Zugriffsrechte
- M 4.41 (Z) Einsatz angemessener Sicherheitsprodukte für IT-Systeme

Umsetzung
- M 4.2 (A) Bildschirmsperre
- M 4.7 (A) Änderung voreingestellter Passwörter
- M 4.15 (A) Gesichertes Login
- M 4.40 (C) Verhinderung der unautorisierten Nutzung des Rechnermikrofons

Betrieb
- M 2.22 (Z) Hinterlegen des Passwortes
- M 3.18 (A) Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
- M 4.4 (Z) Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern
- M 4.30 (A) Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen

Notfallvorsorge
- M 6.20 (A) Geeignete Aufbewahrung der Backup-Datenträger
- M 6.22 (A) Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
- M 6.32 (A) Regelmäßige Datensicherung

B 3.203 Laptop

Beschreibung

Unter einem Laptop oder Notebook wird ein PC verstanden, der aufgrund seiner Bauart transportfreundlich ist und mobil genutzt werden kann. Ein Laptop hat eine kompaktere Bauform als Arbeitsplatzrechner und kann über Akkus zeitweise unabhängig von externer Stromversorgung betrieben werden. Er verfügt über eine Festplatte und meist auch über weitere Speichergeräte wie ein Disketten-, CD-ROM- oder DVD-Laufwerke sowie über Schnittstellen zur Kommunikation über verschiedene Medien (beispielsweise Modem, ISDN, LAN, USB, Firewire, WLAN). Laptops können mit allen üblichen Betriebssystemen wie Windows oder Linux betrieben werden. Daher ist zusätzlich der betriebssystemspezifische Client-Baustein zu betrachten.

Typischerweise wird ein Laptop zeitweise allein, ohne Anschluss an ein Rechnernetz betrieben, und von Zeit zu Zeit wird er zum Abgleich der Daten sowie zur Datensicherung mit dem Behörden- oder Unternehmensnetz verbunden. Häufig wird er auch während der mobilen Nutzung über Modem direkt mit externen Netzen, insbesondere mit dem Internet, verbunden, so dass er indirekt als Brücke zwischen dem LAN und dem Internet wirken kann.

Die Einrichtungen zur Datenfernübertragung (über Modem, ISDN-Karte, etc.) werden hier nicht behandelt (siehe Baustein B 4.3). Für den Laptop wird vorausgesetzt, dass er innerhalb eines bestimmten Zeitraums nur von einem Benutzer gebraucht wird. Ein anschließender Benutzerwechsel wird berücksichtigt.

Gefährdungslage

Für den IT-Grundschutz eines Laptops werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.2 Ausfall des IT-Systems
- G 1.15 Beeinträchtigung durch wechselnde Einsatzumgebung

Organisatorische Mängel:
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.8 Unkontrollierter Einsatz von Betriebsmitteln
- G 2.16 Ungeordneter Benutzerwechsel bei tragbaren PCs

Menschliche Fehlhandlungen:
- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.38 Konfigurations- und Bedienungsfehler
- G 3.76 Fehler bei der Synchronisation mobiler Endgeräte

Technisches Versagen:
- G 4.9 Ausfall der internen Stromversorgung
- G 4.13 Verlust gespeicherter Daten
- G 4.22 Software-Schwachstellen oder -Fehler
- G 4.19 Informationsverlust bei erschöpftem Speichermedium

- G 4.52 Datenverlust bei mobilem Einsatz

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.9 Unberechtigte IT-Nutzung
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.21 Trojanische Pferde
- G 5.22 Diebstahl bei mobiler Nutzung des IT-Systems
- G 5.23 Computer-Viren
- G 5.43 Makro-Viren
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.123 Abhören von Raumgesprächen über mobile Endgeräte
- G 5.124 Missbrauch der Informationen von mobilen Endgeräten
- G 5.125 Unberechtigte Datenweitergabe über mobile Endgeräte
- G 5.126 Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Im Rahmen des Einsatzes von Laptops sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

1. Richtlinien für die Nutzung von Laptops

   Um Laptops sicher und effektiv in Behörden oder Unternehmen einsetzen zu können, sollte ein Konzept erstellt werden, das auf den Sicherheitsanforderungen für die bereits vorhandenen IT-Systeme sowie den Anforderungen aus den geplanten Einsatzszenarien beruht (siehe M 2.36 *Geregelte Übergabe und Rücknahme eines tragbaren PC* sowie Baustein B 3.201 *Allgemeiner Client*).

   Darauf aufbauend ist die Laptop-Nutzung zu regeln und Sicherheitsrichtlinien dafür zu erarbeiten (siehe M 2.309 *Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung*). Dies umfasst beispielsweise, wer das System wann und wofür nutzen darf und ob und in welcher Weise ein Anschluss an das Unternehmens- bzw. Behördennetz gestattet wird. Ebenso ist zu regeln, ob und in welcher Form bei mobiler Nutzung eine direkte Verbindung des Laptops mit dem Internet zulässig ist.

2. Beschaffung von Laptops

   Für die Beschaffung von Laptops müssen die aus dem Konzept resultierenden Anforderungen an die jeweiligen Produkte formuliert und basierend darauf die Auswahl der geeigneten Produkte getroffen werden (siehe M 2.310 *Geeignete Auswahl von Laptops*).

3. Sichere Installation von Laptops

   Eine sorgfältige Auswahl der Betriebssystem- und Software-Komponenten sowie deren sichere Installation ist notwendig, um Risiken durch Fehlbedienung oder absichtlichen Missbrauch der Laptops auszuschließen. Die hier zu treffenden Maßnahmen sind in hohem Grade abhängig von dem eingesetzten Betriebssystem und sind daher im Rahmen der Umsetzung der entsprechenden Bausteine, beispielsweise B 3.206 *Unix-System* oder B 3.209 *Client unter Windows XP*, zu realisieren.

Dabei ist die Maßnahme M 4.29 *Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme* von besonderer Bedeutung, da bei Laptops ein relativ hohes Diebstahlsrisiko besteht und die normalen Funktionen der Zugangs- und Zugriffskontrolle ihre Wirksamkeit verlieren, wenn der Laptop unter der Kontrolle des Diebes steht.

4. Sichere Konfiguration der installierten Komponenten

   Je nach Sicherheitsanforderungen müssen die beteiligten Software-Komponenten unterschiedlich konfiguriert werden. Die hier zu treffenden Maßnahmen sind ebenfalls abhängig vom eingesetzten Betriebssystem und sind daher im Rahmen der Umsetzung der entsprechenden Bausteine zu realisieren. Auch hier sind zusätzliche Maßnahmen erforderlich, wenn eine Trennung der Rechte mehrerer Benutzer erforderlich ist. Zu beachten ist auch die Maßnahme M 4.7 *Änderung voreingestellter Passwörter*, weil nur zu häufig jede Zugangskontrolle dadurch illusorisch ist, dass die verwendeten Passwörter allgemein bekannt sind.

5. Sicherer Betrieb von Laptops

   Eine der wichtigsten IT-Sicherheitsmaßnahmen beim Betrieb heutiger Laptops ist die Installation und permanente Aktualisierung eines Virenschutzprogramms. Laptops werden häufig über längere Zeit losgelöst vom Firmen- oder Behördennetz oder auch mit temporären Verbindungen zum Internet betrieben. Somit sind unter Umständen einerseits ihre Virendefinitionsdateien veraltet und sie sind andererseits einem hohen Infektionsrisiko ausgesetzt. Die im Baustein B 1.6 *Computer-Virenschutzkonzept* vorgesehenen Maßnahmen, vor allem die Maßnahme M 2.159 *Aktualisierung der eingesetzten Computer-Viren-Suchprogramme*, sind daher für Laptops ganz besonders wichtig. Diese Geräte können sonst bei Anschluss an ein Firmen- oder Behördennetz Infektionsquellen ersten Grades darstellen.

   Sofern Laptops bei mobiler Nutzung direkt an das Internet angeschlossen werden, ist es unabdingbar, sie durch eine restriktiv konfigurierte Personal Firewall gegen Angriffe aus dem Netz zu schützen. Der Virenschutz reicht alleine nicht aus, um alle zu erwartenden Angriffe abzuwehren. Ebenso ist es unbedingt erforderlich, die Software des Laptops auf aktuellem Stand zu halten und notwendige Sicherheitspatches zeitnah einzuspielen. Soll ein Laptop, der direkt am Internet betrieben wurde, wieder an das Unternehmens- bzw. Behördennetz angeschlossen werden, so ist zunächst durch eine gründliche Überprüfung mit aktuellen Virensignaturen sicherzustellen, dass dieser Laptop nicht infiziert ist. Erst wenn dies sichergestellt ist, darf der Anschluss an das lokale Netz erfolgen (siehe M 5.122 *Sicherer Anschluss von Laptops an lokale Netze*). Dies gilt auch für den Fall, dass der Anschluss an das Unternehmens- bzw. Behördennetz über ein Virtual Private Network (VPN) erfolgt, da Viren auch über verschlüsselte Kommunikationsverbindungen weiter verbreitet werden können.

   Bei einem Wechsel zwischen netzgebundenem und mobilem Betrieb müssen die Datenbestände zwischen dem Server und dem Laptop synchronisiert werden. Es muss dabei gewährleistet werden, dass jederzeit erkennbar ist, ob sich die aktuellste Version der bearbeiteten Daten auf dem Laptop oder im Netz befindet (siehe M 4.235 *Abgleich der Datenbestände von Laptops*).

   Um Angriffsversuche und missbräuchliche Nutzung erkennen zu können, sind bei Laptops vor allem organisatorische Maßnahmen notwendig. Die notwendigen Maßnahmen werden im Rahmen der Umsetzung des Bausteins B 1.9 *Hard- und Software-Management* realisiert und brauchen daher hier nicht weiter betrachtet zu werden. Um einen Überblick über die aktuell in das lokale Netz eingebundenen Laptops zu behalten und die Konfiguration aller Laptops jederzeit nachvollziehen zu können, ist eine zentrale Verwaltung dieser Geräte wichtig (siehe M 4.236 *Zentrale Administration von Laptops*).

Weitere spezifische Maßnahmen für Einzelsysteme sind vor allem M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern* und M 4.30 *Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen.*

Je nach der in einem Gebäude oder Büroraum gegebenen physischen Sicherheit kann es auch sinnvoll oder sogar notwendig sein, die Maßnahme M 1.46 *Einsatz von Diebstahl-Sicherungen* umzusetzen. Bei mobiler Nutzung ist in jedem Fall die Maßnahme M 1.33 *Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz* anzuwenden, um den Laptop vor Diebstahl zu schützen.

6. Aussonderung

   Bei Übergabe von Laptops an andere Benutzer, sei es im Rahmen des normalen Betriebs oder auch bei ihrer Aussonderung, ist darauf zu achten, dass keine schützenswerten Informationen mehr auf der Festplatte vorhanden sind. Hier sind vor allem die Maßnahmen M 2.36 *Geregelte Übergabe und Rücknahme eines tragbaren PC* sowie gegebenenfalls auch M 4.28 *Software-Reinstallation bei Benutzerwechsel eines Laptops* zu beachten.

7. Datensicherung von Laptops

   Die Vorgehensweise und der erforderliche Umfang der Datensicherung richten sich nach dem Einsatzszenario des Laptops (siehe Maßnahme M 6.71 *Datensicherung bei mobiler Nutzung des IT-Systems*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "Laptop" vorgestellt.

Planung und Konzeption
- M 2.36 (B) Geregelte Übergabe und Rücknahme eines tragbaren PC
- M 2.218 (C) Regelung der Mitnahme von Datenträgern und IT-Komponenten
- M 2.309 (A) Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung
- M 4.29 (Z) Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme

Beschaffung
- M 2.310 (A) Geeignete Auswahl von Laptops

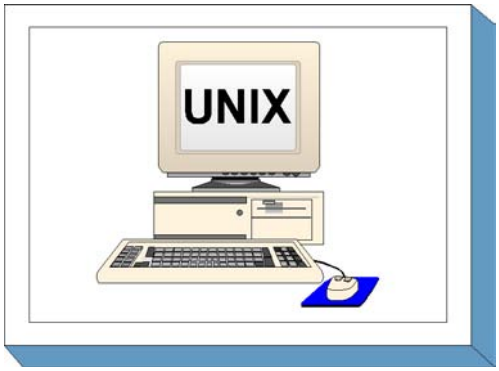
Umsetzung
- M 4.40 (A) Verhinderung der unautorisierten Nutzung des Rechnermikrofons

Betrieb
- M 1.33 (A) Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
- M 1.34 (A) Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz
- M 1.35 (Z) Sammelaufbewahrung tragbarer IT-Systeme
- M 1.46 (Z) Einsatz von Diebstahl-Sicherungen
- M 4.3 (A) Regelmäßiger Einsatz eines Anti-Viren-Programms
- M 4.27 (A) Zugriffsschutz am Laptop
- M 4.28 (Z) Software-Reinstallation bei Benutzerwechsel eines Laptops
- M 4.31 (A) Sicherstellung der Energieversorgung im mobilen Einsatz
- M 4.235 (B) Abgleich der Datenbestände von Laptops
- M 4.236 (Z) Zentrale Administration von Laptops
- M 4.255 (A) Nutzung von IrDA-Schnittstellen
- M 5.91 (A) Einsatz von Personal Firewalls für Internet-PCs
- M 5.121 (A) Sichere Kommunikation von unterwegs
- M 5.122 (A) Sicherer Anschluss von Laptops an lokale Netze

Aussonderung
- M 2.306 (B) Verlustmeldung

Notfallvorsorge
- M 6.71 (A) Datensicherung bei mobiler Nutzung des IT-Systems

B 3.204 Client unter Unix



Beschreibung

Betrachtet wird ein Unix-System, das entweder im Stand-alone-Betrieb oder als Client in einem Netz genutzt wird. Es können Terminals, Laufwerke, Drucker und andere Geräte angeschlossen sein. Weiterhin kann eine graphische Benutzeroberfläche wie X-Windows eingesetzt sein. Entsprechend können dann auch X-Terminals und graphische Eingabegeräte angeschlossen sein. Bei den weiteren Betrachtungen wird davon ausgegangen, dass ein Unix-System üblicherweise von mehreren Personen benutzt wird.

Gefährdungslage

Für den IT-Grundschutz eines Unix-Systems werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.1 Personalausfall
- G 1.2 Ausfall des IT-Systems
- G 1.8 Staub, Verschmutzung

Organisatorische Mängel:
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- G 2.15 Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System

Menschliche Fehlhandlungen:
- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.9 Fehlerhafte Administration des IT-Systems

Technisches Versagen:
- G 4.8 Bekanntwerden von Softwareschwachstellen
- G 4.11 Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client
- G 4.12 Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.7 Abhören von Leitungen
- G 5.8 Manipulation an Leitungen
- G 5.9 Unberechtigte IT-Nutzung
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.19 Missbrauch von Benutzerrechten
- G 5.20 Missbrauch von Administratorrechten
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.41 Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp
- G 5.89 Hijacking von Netz-Verbindungen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Clients unter Unix sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung des Einsatzes über den Betrieb bis zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Schon vor dem erstmaligen Einsatz eines Unix-Systems, gleichgültig ob es als Client, als Terminal- oder Anwendungsserver oder als Einzelplatz-System eingesetzt werden soll, sind eine Reihe von Festlegungen zu treffen, die die Grundlage eines geordneten, sicheren Betriebs bilden. Werden hier Fehler gemacht, so lassen sich diese im Nachhinein oft nur mit sehr hohem Aufwand korrigieren.

Es ist ein Verfahren für die Vergabe von User-IDs festzulegen, durch das gewährleistet wird, dass privilegierte und unprivilegierte Benutzerkennungen klar getrennt sind. Weiterhin ist sicherzustellen, dass kein unkontrollierter Zugang zum Single-User-Modus möglich ist, da sonst alle für die Laufzeit des Systems festgelegten Sicherheitsmaßnahmen unterlaufen werden können.

Umsetzung

Bei der Einrichtung eines Unix-Systems sind eine Reihe von Maßnahmen (siehe vor allem dazu die Maßnahme, M 4.105 *Erste Maßnahmen nach einer Unix-Standardinstallation* zu treffen, die die Sicherheit dieses Systems "härten", also Lücken schließen, die nach einer Standardinstallation in der Regel vorhanden sind. Dazu gehört auch, dass nur die wirklich benötigten Netzdienste aktiviert werden (siehe Maßnahme M 5.72 *Deaktivieren nicht benötigter Netzdienste*) und dass die Systemprotokollierung aktiviert wird.

Ferner sind die Zugriffsrechte auf Benutzer- und Systemdateien und -verzeichnisse so nach einem übergreifenden Schema zu vergeben, dass nur diejenigen Benutzer und Prozesse Zugriff erhalten, die diesen wirklich benötigen, wobei insbesondere auf die durch setuid und setgid bestimmten Rechte zu achten ist (siehe dazu die Maßnahme M 4.19 *Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen*).

Betrieb

Um den Überblick über die Sicherheit eines Unix-Systems zu behalten, ist es unabdingbar, die vorhandenen Benutzerprofile und ihre Rechte zeitnah zu dokumentieren, diese Dokumentation immer auf dem aktuellen Stand zu halten und durch regelmäßige Überprüfungen mit der Realität abzugleichen. Die Sicherheit des Systems ist regelmäßig zu überprüfen, wobei auch die vom System erzeugten Protokolle auf eventuelle Unregelmäßigkeiten hin zu betrachten sind.

Notfallvorsorge

Da Unix-Systeme aufgrund ihrer Komplexität nach einem erfolgreichen Angriff oft auf schwer durchschaubare Weise kompromittiert sind, ist es wichtig, schon im Vorfeld Regeln festzulegen, nach denen bei einem echten oder vermuteten Verlust der Systemintegrität zu verfahren ist.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Client unter Unix " vorgestellt.

Für eventuell angeschlossene Rechner (z. B. Clients unter Windows NT oder Windows 95) sind die in den entsprechenden Bausteinen beschriebenen Maßnahmen zu realisieren.

Darüber hinaus sind folgende weitere Maßnahmen umzusetzen:

Planung und Konzeption

- M 2.33 (Z) Aufteilung der Administrationstätigkeiten unter Unix
- M 4.13 (A) Sorgfältige Vergabe von IDs
- M 4.18 (A) Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus
- M 5.34 (Z) Einsatz von Einmalpasswörtern
- M 5.36 (Z) Verschlüsselung unter Unix und Windows NT
- M 5.64 (Z) Secure Shell

Umsetzung

- M 2.32 (Z) Einrichtung einer eingeschränkten Benutzerumgebung
- M 4.9 (A) Einsatz der Sicherheitsmechanismen von X-Windows
- M 4.14 (A) Obligatorischer Passwortschutz unter Unix
- M 4.16 (C) Zugangsbeschränkungen für Accounts und / oder Terminals
- M 4.17 (A) Sperren und Löschen nicht benötigter Accounts und Terminals
- M 4.19 (A) Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen
- M 4.20 (B) Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen
- M 4.21 (A) Verhinderung des unautorisierten Erlangens von Administratorrechten
- M 4.22 (Z) Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System
- M 4.23 (B) Sicherer Aufruf ausführbarer Dateien
- M 4.105 (A) Erste Maßnahmen nach einer Unix-Standardinstallation
- M 4.106 (B) Aktivieren der Systemprotokollierung
- M 5.17 (A) Einsatz der Sicherheitsmechanismen von NFS
- M 5.18 (A) Einsatz der Sicherheitsmechanismen von NIS
- M 5.19 (A) Einsatz der Sicherheitsmechanismen von sendmail
- M 5.20 (A) Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp
- M 5.21 (A) Sicherer Einsatz von telnet, ftp, tftp und rexec
- M 5.35 (A) Einsatz der Sicherheitsmechanismen von UUCP
- M 5.72 (A) Deaktivieren nicht benötigter Netzdienste

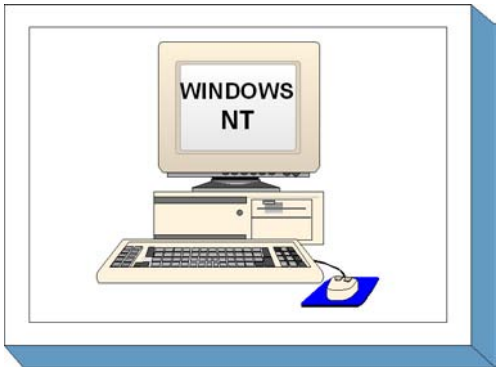
Betrieb

- M 4.25 (A) Einsatz der Protokollierung im Unix-System
- M 4.26 (C) Regelmäßiger Sicherheitscheck des Unix-Systems

Notfallvorsorge

- M 6.31 (A) Verhaltensregeln nach Verlust der Systemintegrität

B 3.205 Client unter Windows NT



Beschreibung

In diesem Baustein werden Clients betrachtet, die unter dem Betriebssystem Windows NT (Version 3.51 oder 4.0) betrieben werden. Das IT-System kann über Disketten-, CD-ROM-, DVD- oder andere Laufwerke für auswechselbare Datenträger sowie andere Peripheriegeräte verfügen. Falls der Client weitere Schnittstellen zum Datenaustausch hat, wie z. B. USB, Bluetooth, WLAN, müssen diese entsprechend den Sicherheitsvorgaben der Institution abgesichert werden, wie dies in den entsprechenden Bausteinen beschrieben ist. Auf sicherheitsspezifische Aspekte von einzelnen Windows NT-Anwendungen wird nur am Rande eingegangen.

Zusätzlich sind als Grundlage für die hier beschriebenen Empfehlungen die Bausteine B 3.201 *Allgemeiner Client* bzw. B 3.202 *Allgemeines nicht vernetztes IT-System*) zu beachten.

Gefährdungslage

Für den IT-Grundschutz einzelner PCs unter dem Betriebssystem Windows NT werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.2 Ausfall des IT-Systems

Organisatorische Mängel:
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- G 2.31 Unzureichender Schutz des Windows NT Systems

Menschliche Fehlhandlungen:
- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.9 Fehlerhafte Administration des IT-Systems

Technisches Versagen:
- G 4.1 Ausfall der Stromversorgung
- G 4.7 Defekte Datenträger
- G 4.23 Automatische CD-ROM-Erkennung

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.9 Unberechtigte IT-Nutzung
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.43 Makro-Viren

- G 5.52 Missbrauch von Administratorrechten im Windows NT/2000/XP/Server 2003 System
- G 5.79 Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP/Server 2003 Systemen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Die in den folgenden Listen als zusätzlich (Z) gekennzeichneten Maßnahmen gehen zumindest teilweise über den Grundschutz hinaus, oder sie beziehen sich auf spezielle Einsatzumgebungen. Sie sind dann zu realisieren, wenn die betreffenden Einsatzbedingungen gegeben sind, insbesondere dann, wenn mehrere Benutzer mit demselben System arbeiten und gegeneinander geschützt werden sollen bzw. wenn die Kontrolle sicherheitskritischer Funktionen nicht beim Benutzer selbst liegt, sondern zentral verwaltet werden soll.

Für Clients und Einzelplatz-Rechner unter dem Betriebssystem Windows NT sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption über den laufenden Betrieb bis hin zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Schon bei der Planung sollten entsprechende Vorgaben für die Installation und Konfiguration des Systems erarbeitet werden, durch die gewährleistet wird, dass sowohl der Systemstart als auch die Zugangs- und Zugriffsrechte sicher konfiguriert werden. Durch Verwendung von Zugriffsprofilen lässt sich darüber hinaus ein zusätzlicher, wenn auch nicht übermäßig starker, Schutz gegen Missbrauch durch den regulären Benutzer etablieren.

Umsetzung

Bei der Installation und Konfiguration eines Windows NT Systems sind eine Reihe von Maßnahmen zu treffen, die die Sicherheit dieses Systems "härten", also Lücken schließen, die nach einer Standardinstallation vorhanden sind. Dazu gehört, dass die Protokollierung aktiviert wird und sensible Bereiche, vor allem die Registrierung und die Administratorkonten, besonders geschützt werden.

Betrieb

Um den Überblick über die Sicherheit eines Windows NT Systems zu behalten, ist es unabdingbar, die vorhandenen Benutzerprofile und ihre Rechte zeitnah und genau zu dokumentieren.

Notfallvorsorge

Nur eine regelmäßige Datensicherung gewährleistet, dass auch im Fehlerfall und bei einem Angriff auf die Sicherheit wichtige Daten weiter verfügbar bleiben. Diese Sicherung wird bei einem Client unter Windows NT in der Regel darin bestehen, dass wichtige Dateien auf dem Server gehalten oder zumindest regelmäßig dorthin übertragen werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Client unter Windows NT" vorgestellt.

Planung und Konzeption

- M 4.48 (A) Passwortschutz unter NT-basierten Windows-Systemen
- M 4.49 (A) Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
- M 4.50 (Z) Strukturierte Systemverwaltung unter Windows NT
- M 4.51 (Z) Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT

- M 4.53 (A) Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT
- M 4.76 (C) Sichere Systemversion von Windows NT

Umsetzung

- M 2.32 (Z) Einrichtung einer eingeschränkten Benutzerumgebung
- M 4.17 (B) Sperren und Löschen nicht benötigter Accounts und Terminals
- M 4.52 (B) Geräteschutz unter NT-basierten Windows-Systemen
- M 4.54 (Z) Protokollierung unter Windows NT
- M 4.55 (B) Sichere Installation von Windows NT
- M 4.57 (A) Deaktivieren der automatischen CD-ROM-Erkennung
- M 4.75 (A) Schutz der Registrierung unter Windows NT/2000/XP
- M 4.77 (A) Schutz der Administratorkonten unter Windows NT

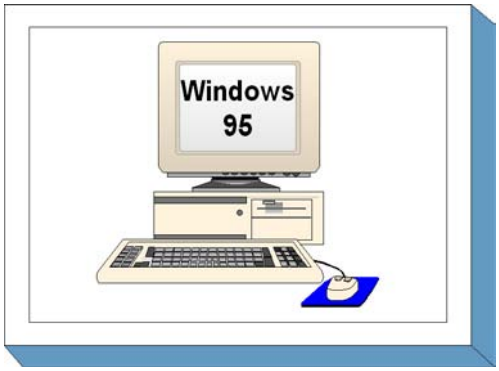
Betrieb

- M 4.56 (B) Sicheres Löschen unter Windows-Betriebssystemen

Notfallvorsorge

- M 6.42 (A) Erstellung von Rettungsdisketten für Windows NT
- M 6.44 (A) Datensicherung unter Windows NT

B 3.206 Client unter Windows 95



Beschreibung

Betrachtet wird ein handelsüblicher PC, der mit dem Betriebssystem Windows 95 oder einem der Nachfolgesysteme Windows 98, 98 SE oder ME betrieben wird. Die hier aufgeführten Maßnahmen gelten zunächst für Windows 95, sind jedoch weitgehend, eventuell mit leichten Anpassungen, auch auf die anderen hier genannten Systeme anwendbar. Der PC kann über Disketten-, CD-ROM-, DVD- oder andere Laufwerke für auswechselbare Datenträger sowie andere Peripheriegeräte verfügen. Falls der Client weitere Schnittstellen zum Datenaustausch hat, wie z. B. USB, Bluetooth, WLAN, müssen diese entsprechend den Sicherheitsvorgaben der Institution abgesichert werden, wie dies in den entsprechenden Bausteinen beschrieben ist.

Für die weiteren Betrachtungen wird zugrunde gelegt, dass dieser PC auch von mehreren Benutzern betrieben werden kann. Dabei gelten jedoch folgende grundlegende Überlegungen:

Wesentliche Sicherheitseigenschaften von Windows 95 lassen sich erst in einem servergestütztem Netz realisieren. Wird ein Windows 95-Rechner als Einzelplatzrechner betrieben, so sollte von einem Mehr-Benutzer-Betrieb abgesehen werden, solange nicht unter Zuhilfenahme eines PC-Sicherheitsproduktes wichtige Funktionen wie z. B. Rechtekontrolle und Protokollierung realisiert werden können. Selbst bei Nutzung des Rechners durch nur einen Benutzer gelten dieselben Überlegungen, wenn die Benutzerumgebung durch einen Administrator mittels Systemrichtlinien eingeschränkt werden soll, da faktisch damit wieder ein Mehr-Benutzer-Betrieb entsteht.

Fazit: Ein nicht vernetzter Windows 95-Rechner sollte nur von einem Benutzer und uneingeschränkt genutzt werden können. Eine Einschränkung des Benutzers ist nur dann sinnvoll, wenn damit das Navigieren im System erleichtert wird oder wenn Fehlbedienungen damit ausgeschlossen werden sollen. Wird dennoch ein Mehr-Benutzer-Betrieb realisiert, so ist dieser unter Sicherheitsgesichtspunkten nur in Kombination mit einem PC-Sicherheitsprodukt sinnvoll.

Gefährdungslage

Für den IT-Grundschutz eines PC mit Windows 95 werden folgende Gefährdungen angenommen:

Höhere Gewalt:
- G 1.2 Ausfall des IT-Systems
- G 1.4 Feuer
- G 1.5 Wasser
- G 1.8 Staub, Verschmutzung

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- G 2.21 Mangelhafte Organisation des Wechsels zwischen den Benutzern
- G 2.22 Fehlende Auswertung von Protokolldaten
- G 2.35 Fehlende Protokollierung unter Windows 95
- G 2.36 Ungeeignete Einschränkung der Benutzerumgebung

Menschliche Fehlhandlungen:
- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten
- G 3.17 Kein ordnungsgemäßer PC-Benutzerwechsel
- G 3.22 Fehlerhafte Änderung der Registrierung

Technisches Versagen:
- G 4.23 Automatische CD-ROM-Erkennung
- G 4.24 Dateinamenkonvertierung bei Datensicherungen unter Windows 95

Vorsätzliche Handlungen:
- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.9 Unberechtigte IT-Nutzung
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.43 Makro-Viren
- G 5.60 Umgehen der Systemrichtlinien

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Clients unter Windows 95 sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption über den Betrieb bis hin zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Zunächst muss festgelegt werden, unter welchen Bedingungen die Clients unter Windows 95 eingesetzt werden sollen. In Abhängigkeit davon sind zusätzliche Maßnahmen erforderlich.

Wenn mit einem Rechner unter Windows 95 mehrere Benutzer arbeiten sollen, so muss durch Einrichten von Zugriffsrechten dafür gesorgt werden, dass diese Benutzer gegeneinander geschützt sind. Bei Nutzung des Systems als Client lässt sich dieser Schutz durch die Zugangs- und Zugriffskontrolle des Servers für die dort gespeicherten Daten erreichen. Ein Schutz von lokal auf dem Windows 95 Rechner gespeicherten Daten kann dagegen nur durch Installation zusätzlicher Sicherheitssoftware erzielt werden, und auch dieser Schutz ist nur höchst mangelhaft, wenn auf eine Verschlüsselung verzichtet wird.

Sollen an dem Windows 95-Rechner mehrere Benutzer arbeiten, so ist eine Administration des Rechners und eine Benutzertrennung unumgänglich. In diesem Fall sind die folgenden Maßnahmen für den Mehrbenutzerbetrieb **zusätzlich** umzusetzen:
- M 2.63 *Einrichten der Zugriffsrechte*
- M 2.103 *Einrichten von Benutzerprofilen unter Windows 95*
- M 3.18 *Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung*

Soll die Benutzerumgebung benutzerspezifisch mit bestimmten Einschränkungen versehen werden, so sind weiterhin die folgenden Maßnahmen zu ergreifen (die Maßnahme M 2.65 wirkt nur in Verbindung mit M 4.41):

- M 2.65 *Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System*
- M 2.104 *Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95*
- M 4.41 *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*

Notfallvorsorge

Nur eine regelmäßige Datensicherung gewährleistet, dass auch im Fehlerfall und bei einem Angriff auf die Sicherheit wichtige Daten weiter verfügbar bleiben. Diese Sicherung wird bei einem Client unter Windows 95 in der Regel darin bestehen, dass wichtige Dateien auf dem Server gehalten oder zumindest regelmäßig dorthin übertragen werden. Zusätzlich bieten Rettungsdisketten bei einer Reihe lokaler Fehler eine Hilfe, den Rechner ohne Datenverlust wieder funktionsfähig zu machen.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Client unter Windows 95" vorgestellt.

Planung und Konzeption

- M 2.63 (A) Einrichten der Zugriffsrechte
- M 2.103 (A) Einrichten von Benutzerprofilen unter Windows 95
- M 2.104 (Z) Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
- M 4.41 (Z) Einsatz angemessener Sicherheitsprodukte für IT-Systeme
- M 4.74 (A) Vernetzte Windows 95 Rechner

Umsetzung

- M 4.57 (A) Deaktivieren der automatischen CD-ROM-Erkennung

Betrieb

- M 2.65 (Z) Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
- M 3.18 (A) Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
- M 4.56 (B) Sicheres Löschen unter Windows-Betriebssystemen

Notfallvorsorge

- M 6.45 (A) Datensicherung unter Windows 95
- M 6.46 (A) Erstellung von Rettungsdisketten für Windows 95

B 3.207 Client unter Windows 2000

Beschreibung

Betrachtet werden einzelne, als Client betriebene PCs mit Festplatte, die unter dem Betriebssystem Windows 2000 Professional ablaufen. Die PCs können miteinander, innerhalb eines LANs oder gar nicht vernetzt sein. Auf sicherheitsspezifische Aspekte von einzelnen Windows 2000-Anwendungen wird nur am Rande eingegangen. Die Server-spezifischen Sicherheitsmaßnahmen sind dem Baustein B 3.106 *Server unter Windows 2000* zu entnehmen.

Gefährdungslage

Für den IT-Grundschutz einzelner PCs unter dem Betriebssystem Windows 2000 werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.1 Personalausfall
- G 1.2 Ausfall des IT-Systems
- G 1.4 Feuer
- G 1.5 Wasser
- G 1.8 Staub, Verschmutzung

Organisatorische Mängel:
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz

Menschliche Fehlhandlungen:
- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.9 Fehlerhafte Administration des IT-Systems

Technisches Versagen:
- G 4.1 Ausfall der Stromversorgung
- G 4.7 Defekte Datenträger
- G 4.8 Bekanntwerden von Softwareschwachstellen
- G 4.23 Automatische CD-ROM-Erkennung

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.9 Unberechtigte IT-Nutzung
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.43 Makro-Viren
- G 5.52 Missbrauch von Administratorrechten im Windows NT/2000 System

- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.79 Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
- G 5.83 Kompromittierung kryptographischer Schlüssel

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Nach der Entscheidung, Windows 2000 als Client-Betriebssystem einzusetzen, sollte zunächst der Einsatz von Windows 2000 geplant werden (siehe Maßnahme M 2.227 *Planung des Windows 2000 Einsatzes*). Parallel dazu ist eine Sicherheitsrichtlinie zu erarbeiten (siehe Maßnahme M 2.228 *Festlegen einer Windows 2000 Sicherheitsrichtlinie*). Daher sollte mit der Umsetzung der Maßnahmen M 2.227 und M 2.228 begonnen werden.

Nachfolgend wird das Maßnahmenbündel für den Baustein "Windows 2000 Client" vorgestellt.

Planung und Konzeption

- M 2.227 (A) Planung des Windows 2000 Einsatzes
- M 2.228 (A) Festlegen einer Windows 2000 Sicherheitsrichtlinie
- M 2.231 (A) Planung der Gruppenrichtlinien unter Windows 2000

Umsetzung

- M 2.32 (Z) Einrichtung einer eingeschränkten Benutzerumgebung
- M 3.28 (A) Schulung zu Windows 2000 Sicherheitsmechanismen für Benutzer
- M 4.17 (A) Sperren und Löschen nicht benötigter Accounts und Terminals
- M 4.48 (A) Passwortschutz unter Windows NT/2000
- M 4.49 (A) Absicherung des Boot-Vorgangs für ein Windows NT/2000 System
- M 4.52 (A) Geräteschutz unter Windows NT/2000
- M 4.57 (A) Deaktivieren der automatischen CD-ROM-Erkennung
- M 4.75 (A) Schutz der Registrierung unter Windows NT/2000
- M 4.136 (A) Sichere Installation von Windows 2000
- M 4.149 (A) Datei- und Freigabeberechtigungen unter Windows 2000
- M 4.150 (A) Konfiguration von Windows 2000 als Workstation

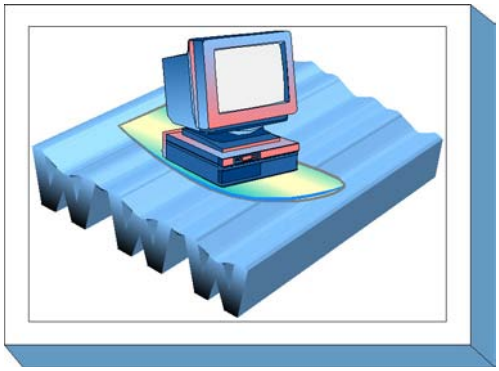
Betrieb

- M 4.147 (Z) Sichere Nutzung von EFS unter Windows 2000/XP
- M 4.148 (B) Überwachung eines Windows 2000 Systems

Notfallvorsorge

- M 6.77 (A) Erstellung von Rettungsdisketten für Windows 2000
- M 6.78 (A) Datensicherung unter Windows 2000

B 3.208 Internet-PC



Beschreibung

Die Nutzung des Internets zur Informationsbeschaffung und Kommunikation ist in weiten Bereichen der öffentlichen Verwaltung und Privatwirtschaft zur Selbstverständlichkeit geworden. Auch E-Commerce- und E-Government-Anwendungen gewinnen immer mehr an Bedeutung. Größtmöglichen Komfort bietet es dabei, den Mitarbeitern einer Institution einen Internet-Zugang direkt über den Arbeitsplatz-PC zur Verfügung zu stellen. Dieser ist jedoch meist in ein lokales Netz (LAN) eingebunden, so dass dadurch unter Umständen zusätzliche Bedrohungen für die Institution entstehen.

Um diese Probleme zu umgehen oder aus anderen anwendungsspezifischen Gründen stellen viele Behörden und Unternehmen eigenständige "Internet-PCs" zur Verfügung. Ein Internet-PC ist ein Computer, der über eine Internet-Anbindung verfügt, jedoch nicht mit dem internen Netz der Institution verbunden ist. Falls es sich um mehrere Internet-PCs handelt, können diese Computer auch untereinander vernetzt sein, beispielsweise um eine gemeinsame Internet-Anbindung zu nutzen. Internet-PCs dienen meist dazu, Mitarbeitern die Nutzung von Internet-Diensten zu ermöglichen und dabei zusätzliche Bedrohungen für das lokale Netz zu vermeiden.

Betrachtet wird ein Internet-PC auf der Basis eines Windows-Betriebssystems oder Linux. Für die Nutzung der Internet-Dienste kommen gängige Browser, wie z. B. Internet Explorer, Netscape Navigator oder Opera, sowie E-Mail-Clients, wie z. B. Microsoft Outlook, Outlook Express, Netscape Messenger oder KMail, zum Einsatz. Je nach Einsatzszenario können weitere Programme für die Nutzung anderer Internet-Dienste, beispielsweise News, Instant Messaging oder Internet-Banking, installiert sein.

Gefährdungslage

Für den IT-Grundschutz eines Internet-PCs werden die folgenden typischen Gefährdungen angenommen:

Höhere Gewalt:
- G 1.2 Ausfall des IT-Systems

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.21 Mangelhafte Organisation des Wechsels zwischen den Benutzern

Menschliche Fehlhandlungen:
- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.38 Konfigurations- und Bedienungsfehler

Technisches Versagen:
- G 4.22 Software-Schwachstellen oder -Fehler

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software

- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.43 Makro-Viren
- G 5.48 IP-Spoofing
- G 5.78 DNS-Spoofing
- G 5.87 Web-Spoofing
- G 5.88 Missbrauch aktiver Inhalte
- G 5.91 Abschalten von Sicherheitsmechanismen für den RAS-Zugang
- G 5.103 Missbrauch von Webmail

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Ist geplant, in einem Unternehmen bzw. in einer Behörde einen oder mehrere Internet-PCs zur Verfügung zu stellen, sollten im Hinblick auf die IT-Sicherheit folgende Schritte durchlaufen werden:

1. Konzeption von Internet-PCs (siehe M 2.234 *Konzeption von Internet-PCs*)

   Zu Anfang müssen grundsätzliche Fragen des Einsatzes festgelegt werden, beispielsweise welche Internet-Dienste genutzt werden sollen und wer für die Administration des Internet-PCs zuständig ist.

2. Richtlinien für die Nutzung von Internet-PCs (siehe M 2.235 *Richtlinien für die Nutzung von Internet-PCs*)

   Für die sichere Nutzung eines Internet-PCs müssen verbindliche Richtlinien festgelegt werden. Dies umfasst beispielsweise, wer den Internet-PC wann und wofür nutzen darf und ggf. wie Daten zwischen dem Internet-PC und dem Hausnetz transportiert werden.

3. Sichere Installation von Internet-PCs (siehe M 4.151 *Sichere Installation von Internet-PCs*)

   Durch die Verbindung zum Internet ergeben sich für die auf dem Internet-PC installierten Anwendungen und für die gespeicherten Daten zusätzliche Gefährdungen. Eine sorgfältige Auswahl der Betriebssystem- und Software-Komponenten sowie deren sichere Installation ist daher besonders wichtig.

4. Sichere Konfiguration der installierten Komponenten

   Je nach Sicherheitsanforderungen müssen die beteiligten Software-Komponenten unterschiedlich konfiguriert werden. Dies betrifft insbesondere den verwendeten Browser (siehe M 5.93 *Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs*) den E-Mail-Client (siehe M 5.94 *Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs*) und ggf. spezielle E-Business-Software.

5. Sicherer Betrieb von Internet-PCs (siehe M 4.152 *Sicherer Betrieb von Internet-PCs*)

   Eine der wichtigsten IT-Sicherheitsmaßnahmen beim Betrieb eines Internet-PCs ist das systematische und schnellstmögliche Einspielen sicherheitsrelevanter Patches und Updates. Um Angriffsversuche und missbräuchliche Nutzung erkennen zu können, sollte das System außerdem überwacht werden.

6. Datensicherung beim Einsatz von Internet-PCs (siehe M 6.79 *Datensicherung beim Einsatz von Internet-PCs*)

   Die Vorgehensweise und der erforderliche Umfang der Datensicherung richtet sich nach dem Einsatzszenario des Internet-PC.

Der vorliegende Baustein gibt Empfehlungen zur Konzeption, Konfiguration und Betrieb eines solchen Internet-PCs. Wichtig ist dabei, dass die hier aufgeführten Maßnahmen nicht ausreichend sind für einen Standard-Arbeitsplatz-PC, auf dem in der Regel mehrere unterschiedliche Anwendungen betrieben und mit dem schützenswerte Daten verarbeitet werden. Dieses Maßnahmenbündel richtet sich ausschließlich an das spezielle Einsatzszenario "Internet-PC". Geeignete IT-Sicherheitsempfehlungen für Standard-Arbeitsplatz-PCs sind in anderen Client-Bausteinen der Schicht 3 beschrieben.

Nachfolgend wird das Maßnahmenbündel für den Baustein "Internet-PC" vorgestellt.

Planung und Konzeption

- M 2.234 (A) Konzeption von Internet-PCs
- M 2.235 (A) Richtlinien für die Nutzung von Internet-PCs
- M 4.41 (Z) Einsatz angemessener Sicherheitsprodukte für IT-Systeme
- M 5.66 (B) Verwendung von SSL
- M 5.91 (Z) Einsatz von Personal Firewalls für Internet-PCs
- M 5.92 (B) Sichere Internet-Anbindung von Internet-PCs

Umsetzung

- M 4.151 (B) Sichere Installation von Internet-PCs
- M 5.59 (C) Schutz vor DNS-Spoofing
- M 5.98 (C) Schutz vor Missbrauch kostenpflichtiger Einwahlnummern

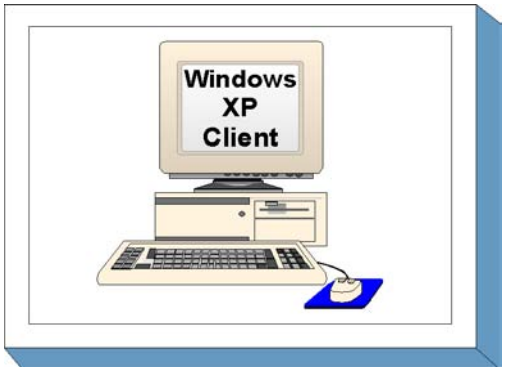
Betrieb

- M 2.313 (A) Sichere Anmeldung bei Internet-Diensten
- M 4.3 (A) Regelmäßiger Einsatz eines Viren-Schutzprogramms
- M 4.152 (B) Sicherer Betrieb von Internet-PCs
- M 5.93 (A) Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs
- M 5.94 (A) Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs
- M 5.95 (B) Sicherer E-Commerce bei der Nutzung von Internet-PCs
- M 5.96 (A) Sichere Nutzung von Webmail

Notfallvorsorge

- M 6.79 (A) Datensicherung beim Einsatz von Internet-PCs

B 3.209 Client unter Windows XP



Beschreibung

Betrachtet werden Arbeitsplatz-PCs (APCs) mit dem Betriebssystem Windows XP Professional. Windows XP ist das Nachfolgeprodukt von Windows 2000 Professional. Die Sicherheit eines solchen Betriebssystems spielt eine wichtige Rolle für die Sicherheit in einem IT-Verbund, da Schwachstellen auf der Betriebssystemebene die Sicherheit aller Anwendungen und des gesamten Netzes beeinträchtigen können. Der vorliegende Baustein beschreibt die Sicherheitsmaßnahmen, die für einen APC mit Windows XP umzusetzen sind. Die Maßnahmen beziehen sich insbesondere auf die Planung und den Betrieb eines Windows XP Clients in einer Domänenumgebung, auf Installationen von Windows XP auf Einzelplatzrechnern wird nur am Rande eingegangen. Die serverspezifischen Sicherheitsmaßnahmen, die beim Betrieb der Clients in einer Domänenumgebung relevant sind, sind in den Server-Bausteinen der Schicht 3 beschrieben (siehe z. B. Baustein B 3.106 *Server unter Windows 2000*).

Gefährdungslage

Wie jedes IT-System sind auch Clients unter Microsoft Windows XP vielfältigen Gefährdungen ausgesetzt. Oft nutzen erfolgreiche Angriffe Fehlkonfigurationen einzelner oder mehrerer Systemkomponenten aus. Daher kommt der korrekten Konfiguration des Systems und seiner Komponenten eine wichtige Rolle zu. Generell gilt, dass die Gefährdungslage einzelner Rechner immer auch vom Einsatzszenario abhängt und diese Einzelgefährdungen auch in die Gefährdung des Gesamtsystems eingehen. Es ist zu beachten, dass bei nicht vernetzten PCs alle Angriffe (siehe "Vorsätzliche Handlungen") den lokalen Zugang zum Gerät (Konsole) erfordern.

Für den IT-Grundschutz einzelner PCs unter dem Betriebssystem Windows XP werden folgende typische Gefährdungen angenommen.

Höhere Gewalt:
- G 1.1 Personalausfall
- G 1.2 Ausfall des IT-Systems
- G 1.4 Feuer
- G 1.5 Wasser
- G 1.8 Staub, Verschmutzung

Organisatorische Mängel:
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz

Menschliche Fehlhandlungen:
- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.22 Fehlerhafte Änderung der Registrierung
- G 3.48 Fehlkonfiguration von Windows 2000/XP Rechnern

Technisches Versagen:
- G 4.1 Ausfall der Stromversorgung

- G 4.7 Defekte Datenträger
- G 4.8 Bekanntwerden von Softwareschwachstellen
- G 4.23 Automatische CD-ROM-Erkennung

Vorsätzliche Handlungen:

- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.7 Abhören von Leitungen
- G 5.9 Unberechtigte IT-Nutzung
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.43 Makro-Viren
- G 5.52 Missbrauch von Administratorrechten im Windows NT/2000/XP System
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.79 Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP Systemen
- G 5.83 Kompromittierung kryptographischer Schlüssel
- G 5.85 Integritätsverlust schützenswerter Informationen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Aufgrund der oben aufgeführten besonderen Gefährdungen für vernetzte Geräte werden einige Maßnahmen ausdrücklich herausgestellt. Vor allem Maßnahmen zum Schutz gegen Angriffe aus dem Netz müssen hierbei sorgfältig durchgeführt werden. Eine effiziente, zentralisierte Verwaltung der Clients leistet einen wichtigen Beitrag zur Aufrechterhaltung eines hohen Sicherheitsstandards. Einheitliche Konfigurationsvorgaben erleichtern die Überwachung von ungewollten Änderungen der Konfiguration, Änderungen der Sicherheitsvorgaben können schneller auf allen Clients wirksam werden und Softwareaktualisierungen können schneller verteilt werden. Die Mehrzahl der empfohlenen Maßnahmen aus dem Bereich Hardware/Software lassen sich mit zentral vorgegebenen Gruppenrichtlinien umsetzen. Wenn in der Organisation der Einsatz von Microsoft Active Directory vorgesehen ist, muss dieser Einsatz gründlich geplant werden.

Einen Sonderfall stellt die Verwaltung von Windows XP Clients in Windows NT Domänenumgebungen dar. In diesem Fall stehen als Werkzeug zur zentralen Verwaltung nur die Windows NT Systemrichtlinien zur Verfügung. In der Maßnahme M 4.51 *Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT* werden die Möglichkeiten der Systemadministration mit Windows NT Systemrichtlinien erläutert. Aufgrund der technischen Beschränkungen dieser Lösung wird der Einsatz von Systemrichtlinien für Windows XP jedoch nicht empfohlen. Für die Verwaltung von Clients unter Windows XP sollte der Einsatz von Active Directory Gruppenrichtlinien erwogen werden.

Clients unter Windows XP können anstatt in Domänen auch in Arbeitsgruppen verwendet werden. Die Verwaltung sämtlicher Sicherheitsmerkmale erfolgt in diesem Fall lokal auf jedem einzelnen Client. Freigegebene Ressourcen auf einzelnen Rechnern lassen sich nur schwer zentral verwalten und überwachen. Ein Problem stellt auch die Datensicherung dar. Aufgrund der Vernetzung können jedoch einige netzbasierte Maßnahmen angewendet werden, z. B. die Verwendung von Sicherheitsvorlagen zur Konfiguration und die automatische Aktualisierung des Betriebssystems mithilfe des Software Update Service. Weitere Ausführungen zu diesem Einsatz-Szenario enthält der Baustein B 5.1 *Peer-to-Peer-Dienste*.

Für die erfolgreiche und sichere Konfiguration von Clients unter Windows XP sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Installation bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Nach der Entscheidung, Windows XP als Client-Betriebssystem einzusetzen, sollte zunächst der Einsatz geplant werden (siehe Maßnahme M 2.324 *Einführung von Windows XP planen*). Parallel dazu ist eine Sicherheitsrichtlinie zu erarbeiten (siehe Maßnahme M 2.325 *Planung der Windows XP Sicherheitsrichtlinie*), die einerseits die bereits bestehenden Sicherheitsrichtlinien im Windows XP-Kontext umsetzt und andererseits die für Windows XP spezifischen Erweiterungen definiert.

In einer vernetzten Umgebung wird der Einsatz eines zentralen Verwaltungssystems empfohlen. Hierfür kann z. B. Microsoft Active Directory zum Einsatz kommen. Insbesondere die Verwendung von Gruppenrichtlinien ermöglicht eine relativ einfache zentrale Umsetzung von Sicherheitsvorgaben. Beim Betrieb eines Windows XP Einzelsystems ist der Einsatz lokaler Gruppenrichtlinien empfehlenswert. Die Maßnahme M 2.326 *Planung der Windows XP Gruppenrichtlinien* enthält die entsprechenden Empfehlungen zum Einsatz von Gruppenrichtlinien zur Konfiguration und Verwaltung eines Windows XP Systems.

Weitere Aspekte müssen in der Planungsphase berücksichtigt werden. Diese betreffen vor allem die sichere Konfiguration eines Windows XP Systems. Folgende Maßnahmen sind hierfür relevant:

- M 4.244 *Sichere Windows XP Systemkonfiguration*
- M 4.245 *Basiseinstellungen für Windows XP GPOs*
- M 4.246 *Konfiguration der Systemdienste unter Windows XP*
- M 5.123 *Absicherung der Netzwerkkommunikation unter Windows XP*
- M 4.247 *Restriktive Berechtigungsvergabe unter Windows XP*

Wird in einem Unternehmen bzw. einer Behörde der Einsatz von Windows XP spezifischen Fernzugriffsmöglichkeiten beabsichtigt, so müssen in der Planungsphase die entsprechenden Technologien ausgewählt und damit verbundene Sicherheitsaspekte evaluiert werden (siehe dazu die Maßnahme M 2.327 *Sicherheit beim Fernzugriff unter Windows XP*).

Soll Windows XP zum Einsatz auf mobilen Rechnern kommen, so müssen bereits in der Planungsphase spezifische Sicherheitsaspekte berücksichtigt werden. Die Maßnahme M 2.328 *Einsatz von Windows XP auf mobilen Rechnern* fasst die für Windows XP spezifischen Aspekte zusammen.

Windows XP bietet einige Verwaltungswerkzeuge an, die bereits in der Planungs- bzw. Testphase helfen können, Konfigurationsfehler zu vermeiden, was zweifellos einen Sicherheitsgewinn bringt.

Die Maßnahme M 4.243 *Windows XP Verwaltungswerkzeuge* fasst die wichtigsten Werkzeuge zusammen.

Umsetzung

In der Umsetzungsphase werden alle Maßnahmen ergriffen, die den sicheren Betrieb vorbereiten und gewährleisten. Dazu zählen insbesondere Maßnahmen zur Sicherheit bei der Installation und Grundkonfiguration des Systems.

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt wurden, kann die Installation von Windows XP Systemen erfolgen. Die Installation muss mit besonderer Sorgfalt durchgeführt werden. In M 4.248 *Sichere Installation von Windows XP* sind die relevanten Empfehlungen zusammengefasst. Die für die Konfiguration eines Windows XP Systems zu beachtenden Aspekte müssen während der Planungsphase ermittelt worden sein.

Betrieb

Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:

- Ein Windows XP System ändert sich in der Regel täglich. Dabei muss bei jeder Änderung sichergestellt werden, dass die Sicherheit auch nach der Änderung nicht beeinträchtigt wird. Die dabei zu beachtenden Aspekte sind in M 4.146 *Sicherer Betrieb von Windows 2000/XP* zusammengefasst.
- Ein Mittel im Rahmen der Aufrechterhaltung der Sicherheit eines Windows XP Netzes ist die Überwachung des Systems bzw. seiner Einzelkomponenten. Die hier relevanten Maßnahmen finden sich in M 4.148 *Überwachung eines Windows 2000/XP Systems*. Dabei spielen auch insbesondere Datenschutzaspekte eine Rolle.
- Windows XP Systeme sind wie auch andere IT-Systeme den allgemeinen Sicherheitsrisiken ausgesetzt. Um die Wahrscheinlichkeit eines erfolgreichen Angriffs entschieden zu verringern, müssen Windows XP Systeme aktuell gehalten werden. Die entsprechenden Empfehlungen sind in M 4.249 *Windows XP Systeme aktuell halten* zu finden.
- Für die bereits im Betrieb befindlichen Windows XP Systeme müssen die aus dem Einspielen des Service Packs 2 resultierende Auswirkungen berücksichtigt werden (siehe dazu M 2.329 *Einführung von Windows XP SP2*).
- Eine regelmäßige Prüfung der geltenden Sicherheitseinstellungen und generell der existierenden Sicherheitsrichtlinien ist maßgebend für die Sicherheit der Windows XP Systeme im laufenden Betrieb. Die dabei zu beachtenden Aspekte sind in M 2.330 *Regelmäßige Prüfung der Windows XP Sicherheitsrichtlinien und ihrer Umsetzung* zusammengefasst.
- Windows XP bietet einige Verwaltungswerkzeuge an, deren Einsatz auch aus Sicherheitssicht empfehlenswert ist, da mit ihrer Hilfe unter anderem auch Konfigurationsfehler vermieden werden können. Im Weiteren sind diese Werkzeuge bei der Fehleranalyse bzw. bei der Revision nützlich (siehe dazu M 4.243 *Windows XP Verwaltungswerkzeuge*).

Aussonderung/Stilllegung

Wenn ein Windows XP APC stillgelegt wird, ist dafür Sorge zu tragen, dass die gespeicherten Daten nicht in falsche Hände geraten oder missbräuchlich verwendet werden können. Zu den gespeicherten Daten gehören auch Passwörter, Cookies, temporäre Internetdateien usw. Gleichzeitig ist zu beachten, dass bei Archivierung der Daten der Zugriff erhalten bleibt, auch wenn beispielsweise der bisherige Benutzer eines APCs die Organisation verlassen hat. Die gleichen Anforderungen gelten, wenn ein APC von einem Benutzer zu einem anderen Benutzer umgesetzt wird.

Notfallvorsorge

Neben der Absicherung im laufenden Betrieb spielt jedoch auch die Notfallvorsorge eine wichtige Rolle, da nur so der Schaden im Notfall verringert werden kann. Hinweise zur Notfallvorsorge finden sich in M 6.76 *Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes*. Hinweise zur Datensicherung sind in M 6.78 *Datensicherung unter Windows 2000/XP* enthalten.

Maßnahmenbündel

Nachfolgend wird das Maßnahmenbündel für den Baustein "Windows XP Client" vorgestellt.

Planung und Konzeption

- M 2.324 (A) Einführung von Windows XP planen
- M 2.325 (A) Planung der Windows XP Sicherheitsrichtlinie
- M 2.326 (A) Planung der Windows XP Gruppenrichtlinien
- M 2.327 (B) Sicherheit beim Fernzugriff unter Windows XP
- M 2.328 (B) Einsatz von Windows XP auf mobilen Rechnern
- M 3.28 (A) Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer
- M 4.48 (A) Passwortschutz unter Windows NT/2000/XP
- M 4.57 (A) Deaktivieren der automatischen CD-ROM-Erkennung
- M 4.75 (A) Schutz der Registrierung unter Windows NT/2000/XP
- M 4.147 (Z) Sichere Nutzung von EFS unter Windows 2000/XP
- M 4.149 (A) Datei- und Freigabeberechtigungen unter Windows 2000/XP
- M 4.243 (Z) Windows XP Verwaltungswerkzeuge
- M 4.244 (A) Sichere Windows XP Systemkonfiguration
- M 4.245 (A) Basiseinstellungen für Windows XP GPOs
- M 4.246 (A) Konfiguration der Systemdienste unter Windows XP
- M 4.247 (A) Restriktive Berechtigungsvergabe unter Windows XP
- M 5.37 (B) Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz
- M 5.123 (B) Absicherung der Netzwerkkommunikation unter Windows XP

Umsetzung

- M 2.32 (Z) Einrichtung einer eingeschränkten Benutzerumgebung
- M 4.248 (A) Sichere Installation von Windows XP
- M 5.89 (A) Konfiguration des sicheren Kanals unter Windows 2000/XP
- M 5.90 (Z) Einsatz von IPSec unter Windows 2000/XP

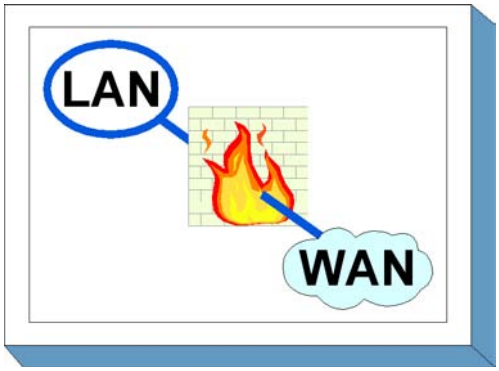
Betrieb

- M 2.329 (A) Einführung von Windows XP SP2
- M 2.330 (B) Regelmäßige Prüfung der Windows XP Sicherheitsrichtlinien und ihrer Umsetzung
- M 4.49 (A) Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System
- M 4.52 (A) Geräteschutz unter Windows NT/2000/XP
- M 4.56 (C) Sicheres Löschen unter Windows-Betriebssystemen
- M 4.146 (A) Sicherer Betrieb von Windows 2000/XP
- M 4.148 (B) Überwachung eines Windows 2000/XP Systems
- M 4.249 (A) Windows XP Systeme aktuell halten

Notfallvorsorge

- M 6.76 (C) Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes
- M 6.78 (A) Datensicherung unter Windows 2000/XP

B 3.301 Sicherheitsgateway (Firewall)



Beschreibung

Ein Sicherheitsgateway (oft auch Firewall genannt) ist ein System aus soft- und hardwaretechnischen Komponenten, um IP-Netze sicher zu koppeln. Dazu wird die technisch mögliche auf die in einer IT-Sicherheitsleitlinie ordnungsgemäß definierte Kommunikation eingeschränkt. Sicherheit bei der Netzkopplung bedeutet hierbei die ausschließliche Zulassung erwünschter Zugriffe oder Datenströme zwischen verschiedenen Netzen.

Sicherheitsgateways werden am zentralen Übergang zwischen zwei unterschiedlich vertrauenswürdigen Netzen eingesetzt. Unterschiedlich vertrauenswürdige Netze stellen dabei nicht unbedingt nur die Kombination Internet-Intranet dar. Vielmehr können auch zwei organisationsinterne Netze unterschiedlich hohen Schutzbedarf besitzen, z. B. bei der Trennung des Bürokommunikationsnetzes vom Netz der Personalabteilung, in dem besonders schutzwürdige, personenbezogene Daten übertragen werden.

Die Verwendung des Begriffs Sicherheitsgateway anstatt des üblicherweise verwendeten Begriffs "Firewall" soll verdeutlichen, dass zur Absicherung von Netzübergängen heute oft nicht mehr ein einzelnes Gerät verwendet wird, sondern eine ganze Reihe von IT-Systemen, die unterschiedliche Aufgaben übernehmen, z. B. Paketfilterung, Schutz vor Viren oder die Überwachung des Netzverkehrs ("Intrusion Detection").

In diesem Baustein werden ausschließlich die für ein Sicherheitsgateway spezifischen Gefährdungen und Maßnahmen beschrieben. Zusätzlich sind noch die Gefährdungen und Maßnahmen zu betrachten, die für das IT-System, mit dem das Sicherheitsgateway realisiert wird, spezifisch sind. Oftmals werden Komponenten von Sicherheitsgateways auf einem Unix-System implementiert, in diesem Fall sind zusätzlich zu den im Folgenden beschriebenen Gefährdungen und Maßnahmen die in Baustein B 3.102 *Server unter Unix* beschriebenen zu beachten.

Gefährdungslage

Für den IT-Grundschutz eines Sicherheitsgateways werden die folgenden typischen Gefährdungen angenommen:

Organisatorische Mängel:

- G 2.24 Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
- G 2.101 Unzureichende Notfallvorsorge bei einem Sicherheitsgateway

Menschliche Fehlhandlungen:

- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.38 Konfigurations- und Bedienungsfehler

Technisches Versagen:

- G 4.8 Bekanntwerden von Softwareschwachstellen
- G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
- G 4.11 Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client

- G 4.12 Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client
- G 4.20 Datenverlust bei erschöpftem Speichermedium
- G 4.22 Software-Schwachstellen oder -Fehler
- G 4.39 Software-Konzeptionsfehler

Vorsätzliche Handlungen:

- G 5.2 Manipulation an Daten oder Software
- G 5.9 Unberechtigte IT-Nutzung
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.24 Wiedereinspielen von Nachrichten
- G 5.25 Maskerade
- G 5.28 Verhinderung von Diensten
- G 5.39 Eindringen in Rechnersysteme über Kommunikationskarten
- G 5.48 IP-Spoofing
- G 5.49 Missbrauch des Source-Routing
- G 5.50 Missbrauch des ICMP-Protokolls
- G 5.51 Missbrauch der Routing-Protokolle
- G 5.78 DNS-Spoofing

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Ein Sicherheitsgateway schützt nicht vor Angriffen, die innerhalb des internen Netzes erfolgen. Um das interne Netz gegen Angriffe von Innentätern zu schützen, müssen auch beim Einsatz eines Sicherheitsgateways alle erforderlichen Sicherheitsmaßnahmen umgesetzt sein. Wenn es sich bei dem internen Netz beispielsweise um ein Unix- bzw. PC-Netz handelt, sind die in den jeweiligen Bausteinen beschriebenen Sicherheitsmaßnahmen umzusetzen.

Das Sicherheitsgateway sollte in einem separaten Serverraum aufgestellt werden. Hierbei zu realisierende Maßnahmen sind in Baustein B 2.4 *Serverraum* beschrieben. Wenn kein Serverraum zur Verfügung steht, kann das Sicherheitsgateway alternativ in einem Serverschrank aufgestellt werden (siehe Baustein B 2.7 *Schutzschränke*). Soll das Sicherheitsgateway nicht in Eigenregie, sondern von einem Dienstleister betrieben werden, so ist der Baustein B 1.11 *Outsourcing* anzuwenden. Insbesondere sollten die Empfehlungen in M 5.116 *Integration eines E-Mailservers in ein Sicherheitsgateway* beachtet werden.

Für den erfolgreichen Aufbau eines Sicherheitsgateway sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb der Komponenten. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

1. Konzept der Netzkopplung mit Hilfe eines Sicherheitsgateway (siehe M 2.70 *Entwicklung eines Konzepts für Sicherheitsgateways*):
   - Festlegung der Sicherheitsziele
   - Anpassung der Netzstruktur
   - grundlegende Voraussetzungen
2. Policy des Sicherheitsgateways (siehe M 2.71 *Festlegung einer Policy für ein Sicherheitsgateway*):
   - Auswahl der Kommunikationsanforderungen

- Auswahl der Dienste (Vor der Diensteauswahl sollten die Erläuterungen und Randbedingungen aus M 5.39 *Sicherer Einsatz der Protokolle und Dienste* gelesen werden.)
- Organisatorische Regelungen

3. Sicherheitsrichtlinie für das Sicherheitsgateway (siehe M 2.299 *Erstellung einer Sicherheitsleitlinie für ein Sicherheitsgateway*)
   - Regelungen und Hinweise zum sicheren Betrieb und zur sicheren Administration des Sicherheitsgateways bzw. seiner einzelnen Komponenten
4. Beschaffung der Komponenten des Sicherheitsgateways:
   - Auswahl des Grundaufbaus des Sicherheitsgateways (siehe M 2.73 *Auswahl geeigneter Grundstrukturen für Sicherheitsgateways)*
   - Beschaffungskriterien (siehe M 2.74 *Geeignete Auswahl eines Paketfilters* und M 2.75 *Geeignete Auswahl eines Application-Level-Gateways*)
5. Aufbau des Sicherheitsgateways:
   - Filterregeln aufstellen und implementieren (siehe M 2.76 *Auswahl und Einrichtung geeigneter Filterregeln*)
   - Umsetzung der IT-Grundschutz-Maßnahmen für die Komponenten des Sicherheitsgateways
   - Umsetzung der IT-Grundschutz-Maßnahmen, die IT-Systeme des internen Netzes überprüfen
   - Randbedingungen für sicheren Einsatz der einzelnen Protokolle und Dienste beachten (siehe M 5.39 *Sicherer Einsatz der Protokolle und Dienste*)
   - Einbindung weiterer Komponenten (siehe M 2.77 *Integration von Servern in das Sicherheitsgateway*)
6. Betrieb des Sicherheitsgateways: (siehe M 2.78 *Sicherer Betrieb eines Sicherheitsgateways*)
   - Regelmäßige Kontrolle
   - Anpassung an Änderungen und Tests
   - Protokollierung der Sicherheitsgateway-Aktivitäten (siehe M 4.47 *Protokollierung der Sicherheitsgateway-Aktivitäten*)
   - Notfallvorsorge für das Sicherheitsgateway (ergänzend siehe Baustein B 1.3 *Notfallvorsorge-Konzept*)
   - Datensicherung (siehe Baustein B 1.4 *Datensicherungskonzept*)
7. Betrieb der an das Sicherheitsgateway angeschlossenen Clients

   Auf Seite der Clients ist - neben den in den Client-Bausteinen beschriebenen Maßnahmen - zusätzlich die Maßnahme M 5.45 *Sicherheit von WWW-Browsern* zu beachten.

Es kann verschiedene Gründe geben, sich gegen den Einsatz eines Sicherheitsgateways zu entscheiden. Dies können die Anschaffungskosten oder der Administrationsaufwand sein, aber auch die Tatsache, dass die bestehenden Restrisiken nicht in Kauf genommen werden können. Falls trotzdem ein Anschluss an das Internet gewünscht ist, kann alternativ ein Stand-alone-System eingesetzt werden (siehe M 5.46 *Einsatz von Stand-alone-Systemen zur Nutzung des Internets*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "Sicherheitsgateway" vorgestellt.

Planung und Konzeption
- M 2.70 (A) Entwicklung eines Konzepts für Sicherheitsgateways
- M 2.71 (A) Festlegung einer Policy für ein Sicherheitsgateway
- M 2.301 (Z) Outsourcing des Sicherheitsgateway

Beschaffung
- M 2.73 (A) Auswahl geeigneter Grundstrukturen für Sicherheitsgateways
- M 2.74 (A) Geeignete Auswahl eines Paketfilters
- M 2.75 (A) Geeignete Auswahl eines Application-Level-Gateways
- M 2.299 (A) Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway

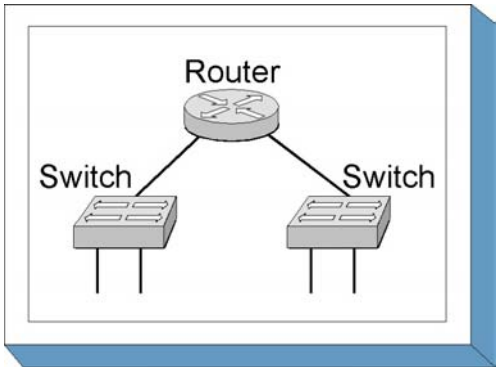
Umsetzung
- M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln
- M 2.77 (A) Integration von Servern in das Sicherheitsgateway
- M 3.43 (C) Schulung der Administratoren des Sicherheitsgateways

Betrieb
- M 2.78 (A) Sicherer Betrieb eines Sicherheitsgateways
- M 2.302 (Z) Sicherheitsgateways und Hochverfügbarkeit
- M 4.47 (A) Protokollierung der Sicherheitsgateway-Aktivitäten
- M 4.93 (B) Regelmäßige Integritätsprüfung
- M 4.100 (C) Sicherheitsgateways und aktive Inhalte
- M 4.101 (C) Sicherheitsgateways und Verschlüsselung
- M 4.222 (B) Festlegung geeigneter Einstellungen von Sicherheitsproxies
- M 4.223 (B) Integration von Proxy-Servern in das Sicherheitsgateway
- M 4.224 (Z) Integration von Virtual Private Networks in ein Sicherheitsgateway
- M 4.225 (Z) Einsatz eines Protokollierungsservers in einem Sicherheitsgateway
- M 4.226 (Z) Integration von Virenscannern in ein Sicherheitsgateway
- M 4.227 (C) Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation
- M 5.39 (A) Sicherer Einsatz der Protokolle und Dienste
- M 5.46 (A) Einsatz von Stand-alone-Systemen zur Nutzung des Internets
- M 5.59 (A) Schutz vor DNS-Spoofing
- M 5.70 (A) Adreßumsetzung - NAT (Network Address Translation)
- M 5.71 (Z) Intrusion Detection und Intrusion Response Systeme
- M 5.115 (Z) Integration eines Webservers in ein Sicherheitsgateway
- M 5.116 (Z) Integration eines E-Mailservers in ein Sicherheitsgateway
- M 5.117 (Z) Integration eines Datenbank-Servers in ein Sicherheitsgateway
- M 5.118 (Z) Integration eines DNS-Servers in ein Sicherheitsgateway
- M 5.119 (Z) Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway
- M 5.120 (A) Behandlung von ICMP am Sicherheitsgateway

Aussonderung
- M 2.300 (C) Sichere Außerbetriebnahme oder Ersatz von Komponenten eines Sicherheitsgateways

Notfallvorsorge
- M 6.94 (C) Notfallvorsorge bei Sicherheitsgateways

B 3.302 Router und Switches



Beschreibung

Netze spielen eine immer wichtigere Rolle als Teile der IT-Infrastruktur, weil Anwendungen heutzutage vermehrt über lokale Netze oder Weitverkehrsnetze betrieben werden. Die Verfügbarkeit, Integrität und Vertraulichkeit der Netze muss sichergestellt sein und mindestens den Anforderungen der Anwendungen an den Schutz dieser drei Grundwerte der IT-Sicherheit entsprechen.

Ein Netz besteht aus aktiver und passiver Netztechnik. Als passive Netztechnik wird in erster Linie die strukturierte Verkabelung verstanden. Hierzu gehören Patch-Felder (über Steckfelder konfigurierbare Kabelverteiler), Schutzschränke und Anschlussdosen am Arbeitsplatz. Zur aktiven Netztechnik gehören beispielsweise Hubs, Bridges, Switches und Router. In modernen Netzen ersetzen Switches heutzutage vielfach Hubs sowie Bridges. Ein Ausfall einer oder mehrerer Komponenten der aktiven Netztechnik (Router und Switches) kann zum kompletten Stillstand der gesamten IT-Infrastruktur führen. Da diese Komponenten die Basis und das Rückgrat der IT-Infrastruktur bilden, müssen Router und Switches vor unerlaubten Zugriffen und Manipulationen geschützt werden.

Die Funktionsweise von Routern ist in M 2.276 *Funktionsweise eines Routers* beschrieben. Die Maßnahme M 2.277 *Funktionsweise eines Switches* beschreibt die Funktionsweise eines Switches. Die wichtigsten funktionalen Unterschiede der in der folgenden Abbildung dargestellten aktiven Netzkomponenten werden kurz erklärt.

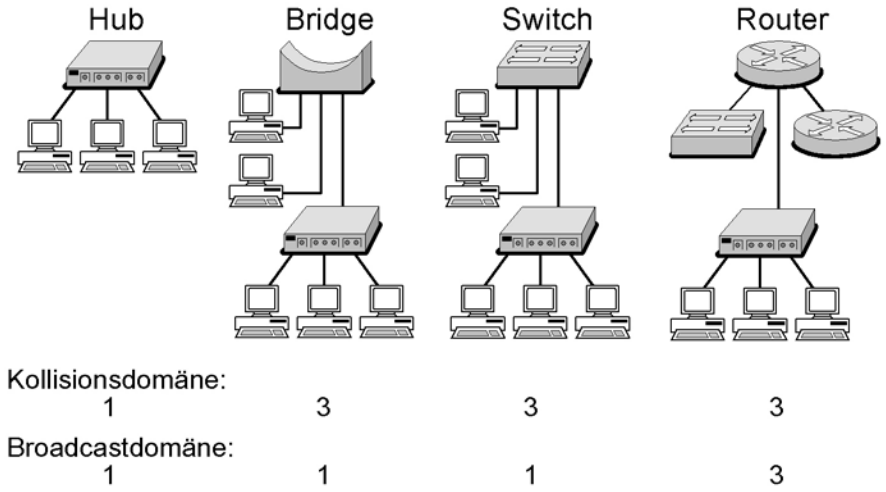


Abbildung: Hub, Bridge, Switch und Router

Kollisionsdomäne

Unter einer Kollisionsdomäne wird ein einzelnes Segment beim Netzzugangsverfahren CSMA/CD (Carrier Sense Multipe Access with Collision Detection) verstanden. Alle Geräte, die im selben Segment angeschlossen sind, sind Bestandteil dieser Kollisionsdomäne. Versuchen zwei Geräte, zum gleichen Zeitpunkt ein Paket ins Netz zu senden, so spricht man von einer Kollision. Beide Geräte warten dann einen bestimmten Zeitraum zufällig gewählter Länge und versuchen dann erneut, das Paket zu senden. Durch diese Wartezeit verringert sich die effektive Bandbreite, die den Geräten zur Verfügung steht.

Broadcast-Domäne

Broadcast-Informationen sind nicht an ein bestimmtes Endgerät gerichtet, sondern an alle "benachbarten" Endgeräte. Diejenigen Geräte in einem Netz, die die jeweiligen Broadcast-Informationen der anderen Geräte empfangen, bilden zusammen eine Broadcast-Domäne. Geräte, die in einer Broadcast-Domäne zusammen gefasst sind, müssen sich nicht in derselben Kollisionsdomäne befinden. Beim IP-Protokoll spricht man in diesem Fall auch von einem IP-Subnetz. Beispielsweise bilden die Stationen mit den IP-Adressen von 192.168.1.1 bis 192.168.1.254 in einem IP-Subnetz mit einer Subnetzmaske von 255.255.255.0 eine Broadcast-Domäne.

Hub

Hubs arbeiten auf der OSI Schicht 1 (Bitübertragungsschicht). Alle angeschlossenen Geräte befinden sich in derselben Kollisionsdomäne und damit auch in derselben Broadcast-Domäne. Hubs werden heutzutage durch Access-Switches (siehe M 2.277 *Funktionsweise eines Switches*) abgelöst.

Bridge

Bridges verbinden Netze auf der OSI Schicht 2 (Sicherungsschicht) und segmentieren Kollisionsdomänen. Jedes Segment bzw. Port an einer Bridge bildet eine eigene Kollisionsdomäne. Alle angeschlossenen Stationen sind im Normalfall Bestandteil einer Broadcast-Domäne. Bridges können auch dazu dienen, Netze mit unterschiedlichen Topographien (Ethernet, Token Ring, FDDI, etc.) auf der OSI Schicht 2 miteinander zu verbinden (transparent bridging, translational bridging). Hauptsächlich wurden Bridges zur Lastverteilung in Netzen eingesetzt. Die Entlastung wird dadurch erzielt, dass eine Bridge als zentraler Übergang zwischen zwei Netzsegmenten nicht mehr jedes Datenpaket weiterleitet. Eine Bridge hält eine interne MAC-Adresstabelle vor, aus der hervorgeht, in welchem angeschlossenen Segment entsprechende MAC-Adressen vorhanden sind. Wenn die Bridge beispielsweise aus dem Teilsegment A ein Datenpaket für eine Station im Teilsegment B erhält, wird das Datenpaket weitergeleitet. Falls die Bridge hingegen ein Datenpaket aus dem Teilsegment A für eine Station aus dem Teilsegment A empfängt, wird dieses Datenpaket nicht in das Teilsegment B übertragen. Dadurch wird eine Entlastung des Teilsegments B erreicht. Heutzutage werden Bridges durch Switches ersetzt.

Layer-2-Switch

Herkömmliche Layer-2-Switches verbinden Netze auf der OSI Schicht 2. Jeder Switch-Port bildet eine eigene Kollisionsdomäne. Normalerweise sind alle angeschlossenen Stationen Bestandteil einer Broadcast-Domäne. Das bedeutet, dass ein Layer-2-Switch die Ziel-MAC-Adresse im MAC-Header als Entscheidungskriterium dafür verwendet, auf welchen Port eingehende Datenpakete weitergeleitet werden. Trotz der vergleichbaren Funktionsweise gibt es zwei wesentliche Unterschiede zu Bridges:

- Ein Switch verbindet in der Regel wesentlich mehr Teilsegmente miteinander als eine Bridge.
- Der Aufbau eines Switches basiert auf sogenannten Application Specific Interface Circuits (ASICs). Dadurch ist ein Switch in der Lage, Datenpakete wesentlich schneller als eine Bridge von einem Segment in ein anderes zu transportieren. Unterschiedliche Switching-Technologien sind in M 2.277 *Funktionsweise eines Switches* beschrieben.

Gelegentlich werden Switches auch als *Multiport Bridges* bezeichnet.

Router

Router arbeiten auf der OSI Schicht 3 (Netzschicht) und vermitteln Datenpakete anhand der Ziel-IP-Adresse im IP-Header. Jedes Interface an einem Router stellt eine eigene Broadcast-Domäne und damit auch eine Kollisionsdomäne dar. Router sind in der Lage, Netze mit unterschiedlichen Topographien zu verbinden. Router werden verwendet, um lokale Netze zu segmentieren oder um

lokale Netze über Weitverkehrsnetze zu verbinden. Ein Router identifiziert eine geeignete Verbindung zwischen dem Quellsystem beziehungsweise Quellnetz und dem Zielsystem beziehungsweise Zielnetz. In den meisten Fällen geschieht dies durch die Weitergabe des Datenpaketes an den nächsten Router, den sogenannten Next Hop. Weitergehende Aspekte sind in M 2.276 *Funktionsweise eines Routers* beschrieben.

Router müssen jedes IP-Paket vor der Weiterleitung analysieren. Dies führt zu Verzögerungen und damit im Vergleich zu "klassischen" Switches zu einem geringeren Datendurchsatz.

Layer-3-Switch und Layer-4-Switch

Layer-3- und Layer-4-Switches sind Switches, die zusätzlich eine Routing-Funktionalität bieten. Layer-2-Switches verwenden die Ziel-MAC-Adresse im MAC-Header eines Paketes zur Entscheidung, zu welchem Port Datenpakete weitergeleitet werden. Ein Layer-3-Switch behandelt Datenpakete beim ersten Mal wie ein Router (Ziel-IP-Adresse im IP-Header). Alle nachfolgenden Datenpakete des Senders an diesen Empfänger werden daraufhin jedoch auf der OSI Schicht 2 (Ziel-MAC-Adresse im MAC-Header) weitergeleitet. Dadurch kann ein solcher Switch eine wesentlich höhere Durchsatzrate erzielen als ein herkömmlicher Router.

Ein weiteres Unterscheidungsmerkmal zwischen einem Router und einem Layer-3-Switch ist die Anzahl von Ports zum Anschluss von einzelnen Endgeräten. Ein Layer-3-Switch verfügt in der Regel über eine wesentlich größere Portdichte.

Durch die Routing-Funktion können Layer-3 oder Layer-4-Switches in lokalen Netzen herkömmliche LAN-to-LAN-Router ersetzen.

Abgrenzung

In diesem Baustein werden Gefährdungen und Maßnahmen beim Einsatz von Routern und Switches beschrieben. Die Abgrenzung zwischen Routern und Switches wird durch die Einführung der Bezeichnungen Layer-2-Switch, Layer-3-Switch oder Layer-4-Switch durch verschiedene Hersteller erschwert. Durch die Verschmelzung der Funktionen von Routern und Switches kann der Großteil der beschriebenen Maßnahmen sowohl auf Router als auch auf Switches angewendet werden.

Es ist eine große Auswahl von unterschiedlichen Routern und Switches von verschiedenen Herstellern am Markt verfügbar. Die Beschreibung der Maßnahmen und Gefährdungen in diesem Baustein ist so gehalten, dass sie so weit wie möglich herstellerunabhängig ist.

Neben den übergreifenden Aspekten und den infrastrukturellen Maßnahmen ist bei dem Einsatz von Routern und Switches der Baustein B 4.1 *Heterogene Netze* zu berücksichtigen. Speziell bei der Einbindung der aktiven Netzkomponenten in ein umfassendes Netz- und Systemmanagement ist der Baustein B 4.2 *Netz- und Systemmanagement* von Bedeutung. Bei der Verwendung eines Routers als Paketfilter oder als Einwahlmöglichkeit sind zusätzlich die Bausteine B 3.301 *Sicherheitsgateway (Firewall)* und B 4.4 *Remote Access* zu berücksichtigen.

Neben eigens dafür hergestellten Geräten bieten auch verschiedene Betriebssysteme (beispielsweise diverse Unix-Derivate, Windows 2000, etc.) Routing-Funktionalität. Das bedeutet, dass ein Router aus einem entsprechenden Rechner mit zwei oder mehr Netzwerkkarten und einem Standardbetriebssystem bestehen kann. In kleineren lokalen Netzen kann dies unter Umständen eine kostengünstige Alternative sein. Neben den in diesem Baustein beschriebenen Sicherheitsmaßnahmen sind beim Betrieb eines solchen Routers die Sicherheitsmaßnahmen des eingesetzten Betriebssystems (Unix, Windows 2000, etc.) zu berücksichtigen.

Gefährdungslage

Neben den Gefährdungen, die generell für den Großteil der IT-Systeme gelten, existieren für aktive Netzkomponenten eine Reihe spezieller Gefährdungen.

Diese Gefährdungen basieren oft auf bekannten Schwachstellen in den verwendeten Protokollen, wie TCP, UDP, IP oder ICMP. Durch Schwachstellen in dynamischen Routing-Protokollen können beispielsweise Routing-Tabellen auf Routern modifiziert werden. Die oft fehlende oder unzureichende Möglichkeit zur Authentisierung auf aktiven Netzkomponenten ist als weitere Gefährdung anzufügen.

Aktive Netzkomponenten werden oft mit einer unsicheren Default-Konfiguration ausgeliefert (siehe G 4.49), die bei der Inbetriebnahme der Geräte geprüft werden sollte. Für die sichere Trennung von Teilnetzen mit unterschiedlichem Schutzbedarf wird gelegentlich die Nutzung von virtuellen Netzen (VLANs) vorgeschlagen. Es sind jedoch einige Angriffsmethoden bekannt, die es ermöglichen, die Grenzen zwischen VLANs zu überwinden und unberechtigt auf andere VLANs zuzugreifen (siehe G 5.115).

Nachfolgend ist die Gefährdungslage beim Einsatz von Routern und Switches als Übersicht dargestellt:

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.3 Fehlende, ungeeignete, inkompatible Betriebsmittel
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.22 Fehlende Auswertung von Protokolldaten
- G 2.27 Fehlende oder unzureichende Dokumentation
- G 2.44 Inkompatible aktive und passive Netzkomponenten
- G 2.54 Vertraulichkeitsverlust durch Restinformationen
- G 2.98 Fehlerhafte Planung und Konzeption des Einsatzes von Routern und Switches

Menschliche Fehlhandlungen
- G 3.64 Fehlerhafte Konfiguration von Routern und Switchen
- G 3.65 Fehlerhafte Administration von Routern und Switchen

Technisches Versagen
- G 4.8 Bekanntwerden von Softwareschwachstellen
- G 4.49 Unsichere Default-Einstellungen auf Routern und Switchen

Vorsätzliche Handlungen
- G 5.4 Diebstahl
- G 5.51 Missbrauch der Routing-Protokolle
- G 5.66 Unberechtigter Anschluss von IT-Systemen an ein Netz
- G 5.112 Manipulation von ARP-Tabellen
- G 5.113 MAC-Spoofing
- G 5.114 Missbrauch von Spanning Tree
- G 5.115 Überwindung der Grenzen zwischen VLANs

Maßnahmenempfehlungen

Die diesem Baustein zugeordneten Sicherheitsmaßnahmen orientieren sich an dem Lebenszyklus der aktiven Netzkomponenten. Es werden Maßnahmen beschrieben, die in folgende Zyklen kategorisiert sind:

- Planung und Konzeption des Einsatzes von Routern und Switches

  Der Einsatz von Routern und Switches muss sorgfältig geplant werden. Die Funktionen von Routern und Switches sind in M 2.276 *Funktionsweise eines Routers* und M 2.277 *Funktionsweise eines Switches* beschrieben. Typische Einsatzszenarien von Routern und Switches, die bei der Planung und Konzeption hilfreich sein können, sind in M 2.278 *Typische Einsatzszenarien von Routern und Switches* zu finden.

- Festlegung einer Sicherheitsstrategie für Router und Switches

  Vor der Beschaffung aktiver Netzkomponenten (siehe M 2.280 *Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches*) ist eine Sicherheitsstrategie für den sicheren Betrieb der Geräte festzulegen und zu dokumentieren (siehe M 2.279 *Erstellung einer Sicherheitsrichtlinie für Router und Switches*). Anschließend können geeignete Netzkoppelelemente ausgewählt werden, die anschließend sicher in die bestehende Netzinfrastruktur zu integrieren sind. In dieser Phase ist es zudem wichtig, die Administratoren für die sichere Administration zu schulen (siehe M 3.38 *Administratorenschulung für Router und Switches*).

- Konfiguration und Inbetriebnahme von Routern und Switches

  Bei der Konfiguration und Inbetriebnahme von Routern und Switches ist eine Reihe von wichtigen Sicherheitsmaßnahmen zu berücksichtigen. Unsichere Default-Konfigurationen von Netzkomponenten stellen oft ein erhebliches Sicherheitsrisiko dar. Deswegen muss die Konfiguration bei der Inbetriebnahme überprüft und angepasst werden.

  Bei der Inbetriebnahme von Routern und Switches spielt die sichere Einrichtung der Systeme eine große Rolle (siehe M 4.201 *Sichere lokale Grundkonfiguration von Routern und Switches* und M 4.202 *Sichere Netz-Grundkonfiguration von Routern und Switches*). Beim Einsatz von Routern muss zudem darauf geachtet werden, dass die Routing-Protokolle sicher eingesetzt werden. Abhängig vom Einsatzzweck sollten auf Routern Access Control Lists (ACLs) konfiguriert werden (siehe M 5.111 *Einrichtung von Access Control Lists auf Routern*). Hierbei, aber auch im normalen Betrieb, muss die Systemkonfiguration sorgfältig dokumentiert werden (siehe M 2.281 *Dokumentation der Systemkonfiguration von Routern und Switches*).

  Router werden außerdem oft zur sicheren Einwahl und zur Etablierung von virtuellen privaten Netzen (VPNs) verwendet. Bei der Einrichtung von VLANs auf Switches sind einige Sicherheitsaspekte zu berücksichtigen. Zusammenfassend ist in M 4.203 *Konfigurations-Checkliste für Router und Switches* eine Checkliste zur sicheren Konfiguration von Routern und Switches dokumentiert.

- Sicherer Betrieb von Routern und Switches

  Hinweise zum sicheren Betrieb von Routern und Switches finden sich in M 2.282 Regelmäßige Kontrolle von Routern und Switches , M 2.283 Software-Pflege auf Routern und Switches und M 6.91 Datensicherung und Recovery bei Routern und Switches gegeben. Aspekte der Protokollierung auf Routern und Switches werden in M 4.205 Protokollierung bei Routern und Switches beschrieben. Sicherheitsaspekte, die im Fall einer Störung wichtig sind, werden in M 6.92 Notfallvorsorge bei Routern und Switches beschrieben.

- Sicherheitsaspekte bei der Außerbetriebnahme von Routern und Switches

  Gespeicherte Konfigurationsdateien und Log-Dateien auf Routern und Switches verraten Informationen über die Netzstruktur. Bei der Außerbetriebnahme aktiver Netzkomponenten sind die Hinweise aus M 2.284 *Sichere Außerbetriebnahme von Routern und Switches* zu berücksichtigen.

Nachfolgend sind die beim Einsatz von Routern und Switches zu berücksichtigenden Maßnahmen aufgelistet:

Planung und Konzeption:
- M 2.276 (Z) Funktionsweise eines Routers
- M 2.277 (Z) Funktionsweise eines Switches
- M 2.278 (Z) Typische Einsatzszenarien von Routern und Switches
- M 2.279 (A) Erstellung einer Sicherheitsrichtlinie für Router und Switches

Beschaffung:
- M 2.280 (C) Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches

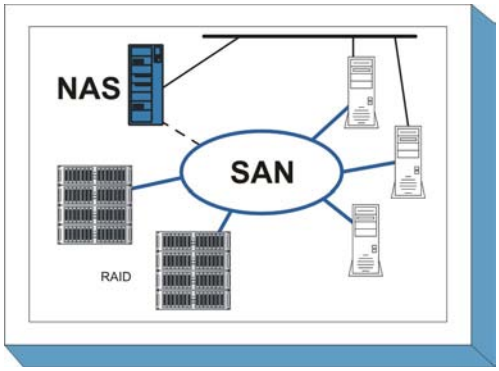
Umsetzung:
- M 1.43 (A) Gesicherte Aufstellung aktiver Netzkomponenten
- M 3.38 (B) Administratorenschulung für Router und Switches
- M 4.201 (A) Sichere lokale Grundkonfiguration von Routern und Switches
- M 4.202 (A) Sichere Netz-Grundkonfiguration von Routern und Switches
- M 4.203 (A) Konfigurations-Checkliste für Router und Switches
- M 5.111 (C) Einrichtung von Access Control Lists auf Routern

Betrieb:
- M 2.281 (A) Dokumentation der Systemkonfiguration von Routern und Switches
- M 2.282 (A) Regelmäßige Kontrolle von Routern und Switches
- M 2.283 (B) Software-Pflege auf Routern und Switches
- M 4.204 (C) Sichere Administration von Routern und Switches
- M 4.205 (C) Protokollierung bei Routern und Switches
- M 4.206 (C) Sicherung von Switch-Ports
- M 5.112 (C) Sicherheitsaspekte von Routing-Protokollen

Aussonderung:
- M 2.284 (C) Sichere Außerbetriebnahme von Routern und Switches

Notfallvorsorge:
- M 6.91 (C) Datensicherung und Recovery bei Routern und Switches
- M 6.92 (C) Notfallvorsorge bei Routern und Switches

B 3.303 Speichersysteme und Speichernetze



Beschreibung

Über ein Speichernetz können gleichzeitig mehrere Server oder gegebenenfalls auch direkt Endgeräte diesen Speicher nutzen. Vorteile sind geringere Verwaltungskosten und eine Vereinfachung der Datensicherung. Da Speichersysteme, die aus mehreren vernetzten Einheiten bestehen, üblicherweise ein dediziertes Speichernetz nutzen, werden diese Systeme oft in der Literatur als "Speichernetze" bezeichnet. Da nicht nur das Netz, sondern auch viele weitere Komponenten beim Speicherprozess zusammenwirken müssen, betrachtet dieser Baustein Speichersysteme und Speichernetze zusammen. Als Speichersystem wird also hier die zentrale Instanz bezeichnet, die für andere Systeme Speicherplatz zur Verfügung stellt. Die Datensicherungsgeräte, die an das Speichersystem angeschlossen sind, werden im Baustein B 1.12 *Archivierung* betrachtet. Konzeptionelle Aspekte der Datensicherung werden im Baustein B 1.4 *Datensicherungskonzept* erläutert.

Mit dem Einsatz von Speichersystemen wird die Speicherkonsolidierung in der Institution möglich. Konsolidierung bedeutet:

- Speicherkapazität wird aus den einzelnen Servern "abgezogen" und in zentralen Systemen zusammengefasst.
- Ein erhöhter Bedarf an Speicherplatz kann durch flexible Nutzung des zentral verfügbaren Speicherplatzes ohne Hardware-Umbau erfüllt werden.
- Anwendungen können den Speicherplatz und die darin enthaltenen Informationen gemeinsam nutzen.

Speichersysteme werden als Network-Attached-Storage-Systeme (NAS) oder als Storage-Area-Network (SAN) ausgeführt. Extrem vereinfacht dargestellt sind NAS-Systeme spezielle Server im Netz. Der Zugriff auf den Speicher erfolgt "File-basierend". SAN-Systeme dagegen sind eine spezielle, leistungsfähige aber auch technisch aufwändige Art, Plattenplatz an Servermaschinen anzuschließen. Der Zugriff auf diese System ist "block-basierend".

Network-Attached-Storage-Systeme verwenden das vorhandene Ethernet-Netzwerk mit einem TCP/IP Protokoll wie NFS (Network File System Protokoll) oder CIFS (Common Internet File System) für Zugriffe der angeschlossenen Rechner auf die Datenträger. Sie arbeiten oft als reine Fileserver. Viele Anbieter verwenden deshalb den Begriff "Filer" für solche Systeme. Für NAS-Systeme ist daher auch zusätzlich Baustein B 3.101 *Allgemeiner Server* anzuwenden.

Storage Area Networks werden in der Regel durch ein dediziertes Netz zwischen Speichersystemen und angeschlossenen Servern geschaffen. Ein SAN besteht aus einem oder mehreren Plattensystemen, aktiven Elementen im Speichernetz (SAN-Switches), weiteren Speichersystemen (z. B. Bandlaufwerken) und den angeschlossenen Servern. Für das dedizierte Speichernetz von SAN-Systemen oder von kombinierten Speichersystemen ist daher auch der Baustein B 4.1 *Heterogene Netze* anzuwenden.

Gefährdungslage

Für den IT-Grundschutz von Speichersystemen werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.2 Ausfall des IT-Systems

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.5 Fehlende oder unzureichende Wartung
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.27 Fehlende oder unzureichende Dokumentation
- G 2.54 Vertraulichkeitsverlust durch Restinformationen
- G 2.82 Fehlerhafte Planung des Aufstellungsortes von Speicher- und Archivsystemen
- G 2.109 Fehlende oder unzureichende Planung des Speichersystems

Menschliche Fehlhandlungen:
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.38 Konfigurations- und Bedienungsfehler
- G 3.79 Fehlerhafte Zuordnung von Ressourcen des SANs

Technisches Versagen:
- G 4.8 Bekanntwerden von Softwareschwachstellen
- G 4.13 Verlust gespeicherter Daten
- G 4.53 Unsichere Default-Einstellungen bei Speicherkomponenten

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.7 Abhören von Leitungen
- G 5.8 Manipulation an Leitungen
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.20 Missbrauch von Administratorrechten
- G 5.28 Verhinderung von Diensten
- G 5.57 Netzanalyse-Tools
- G 5.102 Sabotage
- G 5.129 Manipulation von Daten über das Speichersystem
- G 5.130 Manipulation der Konfiguration des Speichersystems

Maßnahmenempfehlungen

Um ein Speichersystem abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine gemäß den Ergebnissen der Modellierung nach IT-Grundschutz umgesetzt werden.

Für den erfolgreichen Aufbau und Betrieb eines Speichersystems sind eine Reihe von Maßnahmen umzusetzen. Es beginnt mit der strategischen Entscheidung, welche Art von System zu wählen ist. Die Konzeption führt über die Installation zum Betrieb. Wenn das Ende der Betriebsphase erreicht wird, sind Maßnahmen zur ordnungsgemäßen Aussonderung des Systems umzusetzen.

Parallel zur Betriebsphase muss durch eine geeignete Notfallvorsorgeplanung sichergestellt werden, dass der Betrieb auch im Notfall aufrecht erhalten werden kann. Begleitend stellen IT-Sicherheitsmanagement und Revision sicher, dass das Regelwerk auch eingehalten wird.

Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Phasen beachtet werden sollten, sind im Folgenden aufgeführt:

Planung und Konzeption

Um zu einer Entscheidung zu kommen, welche Art Speichersystem in der Institution eingesetzt werden kann, ist eine Anforderungsanalyse vorzunehmen und anschließend die Auswahl eines Speichersystems zu treffen. Zunächst zu klären, welche Technik angemessen ist (siehe dazu M 2.362 *Auswahl eines geeigneten Speichersystems* und M 2.351 *Planung von Speichersystemen*). Ausgangspunkt der Planung muss grundsätzlich die mit Speicher zu versorgende Anwendung sein. Nur hier lassen sich die Sicherheitsanforderungen an das Speichersystem und das Speichernetz sinnvoll definieren. Wichtige Parameter bei der Planung sind das erwartete spätere Wachstum der Anwendung sowie die erforderliche Performance und die Sicherheitsanforderungen. Dabei muss die Auslegung der NAS- oder SAN-Komponenten durch absehbare Entwicklungen und fundierte Wachstumsprognosen so definiert werden, dass diese zentralen IT-Komponenten auf Dauer den Anforderungen der Institution genügen können.

Neben der reinen Abschätzung und Planung der benötigten Speicherkapazität ist insbesondere frühzeitig zu prüfen, wo die NAS- oder SAN-Systeme aufgestellt werden sollen (siehe M 1.59 *Geeignete Aufstellung von Archivsystemen*). Dabei ist kritisch zu hinterfragen, ob die Serverräume oder das Rechenzentrum technisch und organisatorisch geeignet sind, um Speichersysteme dort unterzubringen.

Mit der Planung eines Speichersystems muss auch die Planung eines angemessenen Datensicherungskonzepts einhergehen. Dazu ist das Datensicherungskonzept (B 1.4 *Datensicherungskonzept*) der Institution organisatorisch und technisch an die Anforderungen anzupassen, die sich aus dem Einsatz eines Speichersystems ergeben.

Die Anforderungen an die Speichersysteme, die sich aus den Anforderungen der Institution herleiten, sind in einer Sicherheitsrichtlinie festzuschreiben (siehe M 2.352 *Erstellung einer Sicherheitsrichtlinie für NAS-Systeme* und M 2.353 *Erstellung einer Sicherheitsrichtlinie für SAN-Systeme*)

Bei höheren Ansprüchen an die Verfügbarkeit oder die Skalierbarkeit empfiehlt sich der Einsatz eines hochverfügbaren Speichersystems (siehe auch M 2.354 *Einsatz einer hochverfügbaren SAN-Konfiguration*).

Beschaffung

Wenn die Institution ihre grundsätzliche Anforderungen an die Speichersysteme definiert hat, müssen mögliche Anbieter und Lieferanten geprüft werden (M 2.355 *Auswahl von Lieferanten für ein Speichersystem*).

Mit dem Lieferanten der Hardware-Komponenten des Speichersystems sind Service Level Agreements zu treffen, in denen Reaktionszeiten vereinbart werden, die unter realistischer Betrachtung zu den in der Planung definierten Service Level Agreements und insgesamt zu den Anforderungen an die Verfügbarkeit des Systems passen (M 2.356 *Vertragsgestaltung mit SAN-Dienstleistern*).

Umsetzung

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt worden sind, kann die Installation eines NAS-Systems oder der Aufbau eines SAN-Systems mit den dedizierten Netz- und Speicherkomponenten erfolgen. Dabei sind die folgenden Maßnahmen zu beachten:

Es ist eine sichere Grundkonfiguration der Autorisierungsmechanismen des Speichersystems erforderlich (siehe M 4.274 *Sichere Grundkonfiguration von Speichersystemen*).

Das Speichersystem ist zur Administration möglichst innerhalb eines abgesicherten Netzes zu platzieren (M 2.357 *Aufbau eines Administrationsnetzes für Speichersysteme).*

In dieser Phase sind Sicherheitsvorgaben und die erkennbaren Anforderungen des Betriebs abzustimmen. Alle mit dem NAS- beziehungsweise SAN-System befassten Administratoren müssen auf die eingesetzte Lösung geschult werden (siehe M 3.54 *Schulung der Administratoren des Speichersystems)*.

Bei Aufbau eines SAN-Systems ist die logische Zuordnung zwischen Servern und Komponenten des Speichersystems nach den schriftlichen spezifizierten Anforderungen und Planungen vorzunehmen (siehe M 5.130 *Absicherung des SANs durch Segmentierung*).

Mit den Erkenntnissen der Testphase ist eine Systemdokumentation anzufertigen. Hier müssen die gesamte eingesetzte Hard- und Software, sowie alle Schritte zur Installation und der individuellen Konfiguration dokumentiert werden (siehe M 2.358 *Dokumentation der Systemeinstellungen von Speichersystemen*).

Betrieb

Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:

- Die Bereitstellung der Funktionalitäten des Speichersystems setzt einen sicheren Betrieb des Speichersystems voraus. Es müssen die Dienstprogramme abgesichert werden, die zur Unterstützung von betrieblichen Funktionen des Speichersystems dienen und eine hohe Autorisierung benötigen (siehe M 4.275 *Sicherer Betrieb eines Speichersystems*).
- Speichersysteme müssen im laufenden Betrieb überwacht und auch gewartet werden. Die erforderlichen Wartungsaktivitäten eines Speichersystems Systems sind in M 2.359 *Überwachung und Verwaltung von Speichersystemen* beschrieben.
- Neben der Überwachung und Wartung, die vor allem die technische Verfügbarkeit sicherstellen soll, müssen weitere sicherheitsrelevante Aspekte überwacht werden (M 2.360 *Sicherheits-Audits und Berichtswesen bei Speichersystemen*).

Aussonderung

Empfehlungen zur Deinstallation von Einzelkomponenten und von Komplettsystemen, etwa nach Abschluss des Regelbetriebs, finden sich in der Maßnahme M 2.361 *Deinstallation von Speichersystemen*.

Notfallvorsorge

Speichersysteme erfordern die Überarbeitung und Anpassung vorhandener IT-Notfallpläne. Empfehlungen zur Notfallvorsorge finden sich in der Maßnahme M 6.98 *Notfallvorsorge für Speichersysteme*.

Nachfolgend wird das Maßnahmenbündel für diesen Baustein vorgestellt.

Planung und Konzeption

- M 1.59 (A) Geeignete Aufstellung von Speicher- und Archivsystemen
- M 2.362 (A) Auswahl eines geeigneten Speichersystems
- M 2.351 (A) Planung von Speichersystemen
- M 2.352 (A) Erstellung einer Sicherheitsrichtlinie für NAS-Systeme
- M 2.353 (A) Erstellung einer Sicherheitsrichtlinie für SAN-Systeme
- M 2.354 (Z) Einsatz einer hochverfügbaren SAN-Konfiguration

Beschaffung

- M 2.355 (A) Auswahl von Lieferanten für ein Speichersystem
- M 2.356 (A) Vertragsgestaltung mit SAN-Dienstleistern

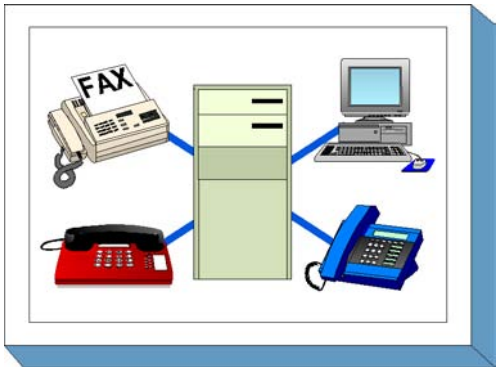
Umsetzung
- M 4.274 (A) Sichere Grundkonfiguration von Speichersystemen
- M 2.357 (B) Aufbau eines Administrationsnetzes für Speichersysteme
- M 3.54 (A) Schulung der Administratoren des Speichersystems
- M 2.358 (A) Dokumentation der Systemeinstellungen von Speichersystemen
- M 5.130 (B) Absicherung des SANs durch Segmentierung

Betrieb
- M 2.359 (B) Überwachung und Verwaltung von Speichersystemen
- M 4.275 (A) Sicherer Betrieb eines Speichersystems
- M 4.80 (B) Sichere Zugriffsmechanismen bei Fernadministration
- M 2.360 (B) Sicherheits-Audits und Berichtswesen bei Speichersystemen

Aussonderung
- M 2.361 (C) Deinstallation von Speichersystemen

Notfallvorsorge
- M 6.1 (A) Erstellung einer Übersicht über Verfügbarkeitsanforderungen
- M 6.20 (A) Geeignete Aufbewahrung der Backup-Datenträger
- M 6.22 (A) Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
- M 6.32 (A) Regelmäßige Datensicherung
- M 6.98 (A) Notfallvorsorge für Speichersysteme

B 3.401 TK-Anlage



Beschreibung

Die private, digitale ISDN-Telekommunikations-Anlage (TK-Anlage) stellt sowohl eine Kommunikationsbasis für den eigenen Bereich als auch die Schnittstelle zum öffentlichen Netz dar. Sie dient der Übertragung von Sprache und Bildern (Fax) und in zunehmendem Maß als LAN bzw. LAN-Koppler sowie als Übertragungsmedium für elektronische Mailsysteme. Bei der Nutzung als LAN ist der Baustein B 3.101 Allgemeiner Server zu beachten.

Es wird davon ausgegangen, dass ein Verantwortlicher für die TK-Anlage benannt ist, der die grundsätzlichen Sicherheitsentscheidungen fällen und Sicherheitsmaßnahmen initiieren kann.

Gefährdungslage

Für den IT-Grundschutz einer TK-Anlage werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.4 Feuer

Organisatorische Mängel:
- G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen

Menschliche Fehlhandlungen:
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.7 Ausfall der TK-Anlage durch Fehlbedienung

Technisches Versagen:
- G 4.6 Spannungsschwankungen/Überspannung/ Unterspannung

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.11 Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
- G 5.12 Abhören von Telefongesprächen und Datenübertragungen
- G 5.13 Abhören von Räumen
- G 5.14 Gebührenbetrug
- G 5.15 "Neugierige" Mitarbeiter
- G 5.16 Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal
- G 5.17 Gefährdung bei Wartungsarbeiten durch externes Personal
- G 5.44 Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlagen

Es werden hier solche Gefährdungen betrachtet, die die Funktionsfähigkeit einer Institution beeinträchtigen können. Datenschutzrechtliche Erwägungen stehen somit nicht im Vordergrund. Diesen wird bereits zu großen Teilen durch bestehende Betriebs- bzw. Dienstvereinbarungen Rechnung getragen. Gleichwohl trägt der IT-Grundschutz natürlich auch zum Schutz der personenbezogenen Daten bei.

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Die zentralen Einrichtungen einer TK-Anlage sollten in einem Raum aufgestellt werden, der den Anforderungen an einen Serverraum (Baustein B 2.4 *Serverraum*) oder einen Raum für technische Infrastruktur (Baustein B 2.6 *Raum für technische Infrastruktur*) genügt. Für die Verkabelung der TK-Anlage wird auf den Baustein B 2.2 *Verkabelung* hingewiesen.

Für die TK-Anlage sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über den Betrieb bis zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Schon bei der Planung der TK-Anlage ist dafür Sorge zu tragen, dass der Bedienplatz in einem geschützten Bereich aufgestellt wird, und der Installationsort sollte auch nicht durch eine explizite Beschilderung für Unbefugte erkennbar gemacht werden. Je nach den durch die Anlage abzudeckenden Verfügbarkeitsanforderungen ist die Installation einer unterbrechungsfreien Stromversorgung vorzusehen. Ein Überspannungsschutz ist in den meisten Fällen sinnvoll, da Fernübertragungsleitungen in der Regel sehr anfällig gegen Überspannungen durch Blitzschlag sind.

Beschaffung

Die Maßnahme M 2.105 *Beschaffung von TK-Anlagen* nennt die wesentlichen Kriterien, die bei der Auswahl einer TK-Anlage zu beachten sind.

Umsetzung

Bei der Installation sind unbedingt die vom Hersteller voreingestellten Passwörter zu ändern, da die Anlage sonst von beliebigen Angreifern manipuliert werden kann. Ebenso sind alle Schnittstellen und die internen und externen Remote-Zugänge abzusichern. Bei der Konfiguration ist nach der Grundregel zu verfahren, dass alle nicht benötigten Leistungsmerkmale abzuschalten sind, weil sie nur unnötige Risiken mit sich bringen.

Betrieb

Die Administrationsarbeiten an der TK-Anlage sollte nach Möglichkeit protokolliert werden, um nachvollziehbar zu machen, auf welche Weise sicherheitsrelevante Einstellungen verändert wurden. Bei hohen Sicherheitsanforderungen an den Betrieb der TK-Anlage ist eine regelmäßige Revision der Konfigurationseinstellungen erforderlich. Da die Sicherheit nur zu häufig durch ungeeignete Bedienung der Endgeräte durch die Benutzer unterlaufen wird, sollten die Mitarbeiter regelmäßig für mögliche Gefährdungen sensibilisiert werden.

Notfallvorsorge

Die TK-Anlage ist in den Notfall-Plan für DFÜ-Ausfall einzubeziehen und ihre Konfigurationsdaten sind regelmäßig zu sichern, um die Anlage nach einem eventuellen Ausfall schnell wieder hochfahren und korrekt konfigurieren zu können.

Nachfolgend wird das Maßnahmenbündel für den Bereich "TK-Anlage" vorgestellt:

Planung und Konzeption

- M 1.12 (B) Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile
- M 1.13 (Z) Anordnung schützenswerter Gebäudeteile
- M 1.25 (B) Überspannungsschutz
- M 1.28 (B) Lokale unterbrechungsfreie Stromversorgung
  M 2.27 (Z) Verzicht auf Fernwartung der TK-Anlage
- M 2.28 (Z) Bereitstellung externer TK-Beratungskapazität
- M 4.8 (A) Schutz des TK-Bedienplatzes
- M 4.62 (Z) Einsatz eines D-Kanal-Filters

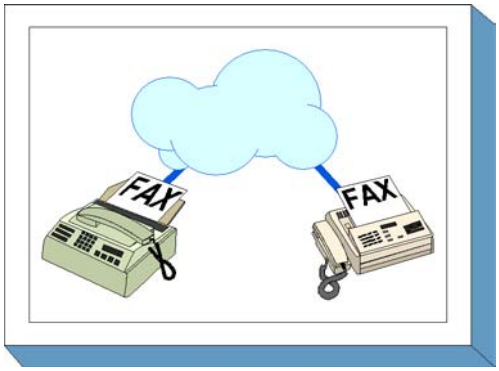
Beschaffung:
- M 2.105 (A) Beschaffung von TK-Anlagen

Umsetzung:
- M 1.30 (A) Absicherung der Datenträger mit TK-Gebührendaten
- M 2.29 (B) Bedienungsanleitung der TK-Anlage für die Benutzer
- M 4.7 (A) Änderung voreingestellter Passwörter
- M 4.10 (Z) Passwortschutz für TK-Endgeräte
- M 4.11 (B) Absicherung der TK-Anlagen-Schnittstellen
- M 4.12 (A) Sperren nicht benötigter TK-Leistungsmerkmale
- M 5.14 (A) Absicherung interner Remote-Zugänge
- M 5.15 (A) Absicherung externer Remote-Zugänge

Betrieb:
- M 3.12 (B) Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne
- M 3.13 (B) Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen
- M 4.5 (B) Protokollierung der TK-Administrationsarbeiten
- M 4.6 (C) Revision der TK-Anlagenkonfiguration

Notfallvorsorge:
- M 6.10 (B) Notfall-Plan für DFÜ-Ausfall
- M 6.26 (B) Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten
- M 6.28 (Z) Vereinbarung über Lieferzeiten "lebensnotwendiger" TK-Baugruppen
- M 6.29 (Z) TK-Basisanschluss für Notrufe
- M 6.30 (Z) Katastrophenschaltung

B 3.402 Faxgerät



Beschreibung

Betrachtet wird die Informationsübermittlung in Form eines Fax. Hierbei werden von einer Vorlage die darauf aufgezeichneten Inhalte vom Sendegerät Punkt für Punkt abgetastet und übertragen und von einem Empfangsgerät ebenso wieder aufgebaut. Für die Maßnahmenauswahl im Bereich IT-Grundschutz wurde nicht nach dem verwendeten Übertragungsstandard (z. B. CCITT Gruppe 3) unterschieden. In diesem Baustein werden als technische Basis des Faxversands ausschließlich marktübliche Stand-Alone-Faxgeräte betrachtet, nicht jedoch Fax-Einschubkarten oder Faxserver (siehe Baustein B 5.6 Faxserver).

Gefährdungslage

Für den IT-Grundschutz werden bei der Informationsübermittlung per Fax folgende typische Gefährdungen angenommen:

Organisatorische Mängel
- G 2.20 Unzureichende Versorgung mit Druck-Verbrauchsgütern für Faxfgeräte

Menschliche Fehlhandlungen:
- G 3.14 Fehleinschätzung der Rechtsverbindlichkeit eines Fax

Technisches Versagen:
- G 4.14 Verblassen spezieller Faxpapiere
- G 4.15 Fehlerhafte Faxübertragung

Vorsätzliche Handlungen:
- G 5.7 Abhören von Leitungen
- G 5.30 Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
- G 5.31 Unbefugtes Lesen von Faxsendungen
- G 5.32 Auswertung von Restinformationen in Faxgeräten und Faxservern
- G 5.33 Vortäuschen eines falschen Absenders bei Faxsendungen
- G 5.34 Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes
- G 5.35 Absichtliche Überlastung durch Faxsendungen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Faxgeräte sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Beschaffung über den Betrieb bis zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Beschaffung

Die Maßnahme M 2.49 *Beschaffung geeigneter Faxgeräte* nennt die wesentlichen Kriterien, die bei der Auswahl eines Faxgeräts zu beachten sind.

Umsetzung

Bei der Installation des Faxgeräts ist darauf zu achten, dass es unter den Gesichtpunkten der Nutzbarkeit, Bedienbarkeit und Verwendung zweckmäßig aufgestellt wird. Die Mitarbeiter, die das Gerät benutzen sollen, sind in seine Bedienung einzuweisen.

Betrieb

Im laufenden Betrieb ist darauf zu achten, dass notwendige Verbrauchsgüter geeignet bevorratet werden, damit keine Nachrichten nur deshalb verloren gehen, weil zu einem bestimmten Zeitpunkt kein Papier oder kein Toner vorhanden ist. In der Regel ist es zweckmäßig, alle Sendungen durch ein geeignetes Faxvorblatt zu kennzeichnen und leichter identifizierbar zu machen. Durch regelmäßige Kontrollen der Sende- und Empfangsprotokolle lässt sich ein eventueller Missbrauch des Faxgeräts leichter aufdecken, und eine gelegentliche Kontrolle programmierter Zieladressen hilft zu vermeiden, dass Sendungen versehentlich an den falschen Empfänger gehen.

Aussonderung

Bei der Entsorgung von Verbrauchsgütern und Ersatzteilen ist zu beachten, dass bei bestimmten Geräten Abbilder gesendeter oder empfangener Faxsendungen auf Zwischenträgerfolien, Belichtungstrommeln oder auch auf Papier vorhanden sind, so dass diese Materialien nicht so entsorgt werden dürfen, dass später Unbefugte darauf Zugriff erhalten.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Faxgerät" vorgestellt:

Beschaffung:
- M 2.49 (A) Beschaffung geeigneter Faxgeräte

Umsetzung:
- M 1.37 (A) Geeignete Aufstellung eines Faxgerätes
- M 2.47 (B) Ernennung eines Fax-Verantwortlichen
- M 3.15 (A) Informationen für alle Mitarbeiter über die Faxnutzung
- M 4.36 (Z) Sperren bestimmter Faxempfänger-Rufnummern
- M 4.37 (Z) Sperren bestimmter Absender-Faxnummern

Betrieb:
- M 2.48 (Z) Festlegung berechtigter Faxbediener
- M 2.51 (Z) Fertigung von Kopien eingehender Faxsendungen
- M 2.52 (C) Versorgung und Kontrolle der Verbrauchsgüter
- M 2.53 (Z) Abschalten des Faxgerätes außerhalb der Bürozeiten
- M 4.43 (Z) Faxgerät mit automatischer Eingangskuvertierung
- M 5.24 (Z) Nutzung eines geeigneten Faxvorblattes
- M 5.25 (A) Nutzung von Sende- und Empfangsprotokollen
- M 5.26 (Z) Telefonische Ankündigung einer Faxsendung
- M 5.27 (Z) Telefonische Rückversicherung über korrekten Faxempfang
- M 5.28 (Z) Telefonische Rückversicherung über korrekten Faxabsender
- M 5.29 (C) Gelegentliche Kontrolle programmierter Zieladressen und Protokolle

Aussonderung:
- M 2.50 (B) Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen

Notfallvorsorge:
- M 6.39 (C) Auflistung von Händleradressen zur Fax-Wiederbeschaffung

B 3.403 Anrufbeantworter

Beschreibung

Betrachtet werden Anrufbeantworter, die zusätzlich zum Telefon an das lokale Haus-Telefonnetz angeschlossen werden können. Sie dienen üblicherweise der Aufzeichnung eingehender Gespräche oder Nachrichten in gesprochener Form, wenn der Angerufene nicht erreichbar ist. Technisch unterscheiden sich diese Geräte durch unterschiedliche Aufzeichnungsweisen: vollständig analog aufzeichnende Geräte, vollständig digital aufzeichnende Geräte und Kombinationsformen. Insbesondere das heute verbreitete Leistungsmerkmal der Fernabfrage legt es nahe, Anrufbeantworter als IT-System aufzufassen, wobei gerade die Fernabfrage ein erhebliches Gefährdungspotential darstellen kann.

Gefährdungslage

Für den IT-Grundschutz eines Anrufbeantworters werden folgende typische Gefährdungen angenommen:

Organisatorische Mängel
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.5 Fehlende oder unzureichende Wartung

Menschliche Fehlhandlungen:
- G 3.15 Fehlbedienung eines Anrufbeantworters

Technisches Versagen:
- G 4.1 Ausfall der Stromversorgung
- G 4.18 Entladene oder überalterte Notstromversorgung im Anrufbeantworter
- G 4.19 Informationsverlust bei erschöpftem Speichermedium

Vorsätzliche Handlungen:
- G 5.36 Absichtliche Überlastung des Anrufbeantworters
- G 5.37 Ermitteln des Sicherungscodes
- G 5.38 Missbrauch der Fernabfrage

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den Einsatz eines Anrufbeantworters sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über den laufenden Betrieb bis zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Vor Einsatz eines Anrufbeantworters sollte festgelegt werden, welche Personen die Zugangscodes kennen, über die wichtige Funktionen des Geräts abgesichert sind, und wo diese Codes für den Notfall sicher gelagert werden.

Beschaffung

Die Maßnahme M 2.54 *Beschaffung geeigneter Anrufbeantworter* nennt die wesentlichen Kriterien, die bei der Auswahl eines Anrufbeantworters zu beachten sind.

Umsetzung

Die Mitarbeiter, die das Gerät benutzen sollen, sind in seine Bedienung einzuweisen.

Betrieb

Die aufgezeichneten Gespräche sollten regelmäßig abgehört und anschließend gelöscht werden, um ein Überlaufen des Aufzeichnungsspeichers und damit den Verlust von Informationen zu vermeiden.

Notfallvorsorge

Bei batteriebetriebenen Geräten sollten die Batterien regelmäßig überprüft und bei Bedarf gewechselt werden, um Ausfälle zu vermeiden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Anrufbeantworter" vorgestellt.

Planung und Konzeption:
- M 2.11 (A) Regelung des Passwortgebrauchs

Beschaffung:
- M 2.54 (A) Beschaffung geeigneter Anrufbeantworter

Umsetzung:
- M 2.55 (Z) Einsatz eines Sicherungscodes
- M 2.58 (Z) Begrenzung der Sprechdauer
- M 3.16 (A) Einweisung in die Bedienung des Anrufbeantworters
- M 4.38 (A) Abschalten nicht benötigter Leistungsmerkmale

Betrieb:
- M 2.56 (A) Vermeidung schutzbedürftiger Informationen auf dem Anrufbeantworter
- M 2.57 (A) Regelmäßiges Abhören und Löschen aufgezeichneter Gespräche
- M 4.39 (Z) Abschalten des Anrufbeantworters bei Anwesenheit

Notfallvorsorge:
- M 6.40 (A) Regelmäßige Batterieprüfung/-wechsel

B 3.404 Mobiltelefon

Beschreibung

Mobiltelefone sind inzwischen nicht mehr wegzudenkende Bestandteile der Kommunikationsinfrastruktur geworden. Damit stellt sich die Frage nach deren sicheren Nutzung.

In diesem Kapitel werden digitale Mobilfunksysteme nach dem GSM-Standard (D- und E-Netze) betrachtet. Um deren sicheren Einsatz zu gewährleisten, müssen verschiedene Komponenten und deren Zusammenspiel betrachtet werden (siehe Bild):

- Mobiltelefon
- Basisstation
- Festnetz

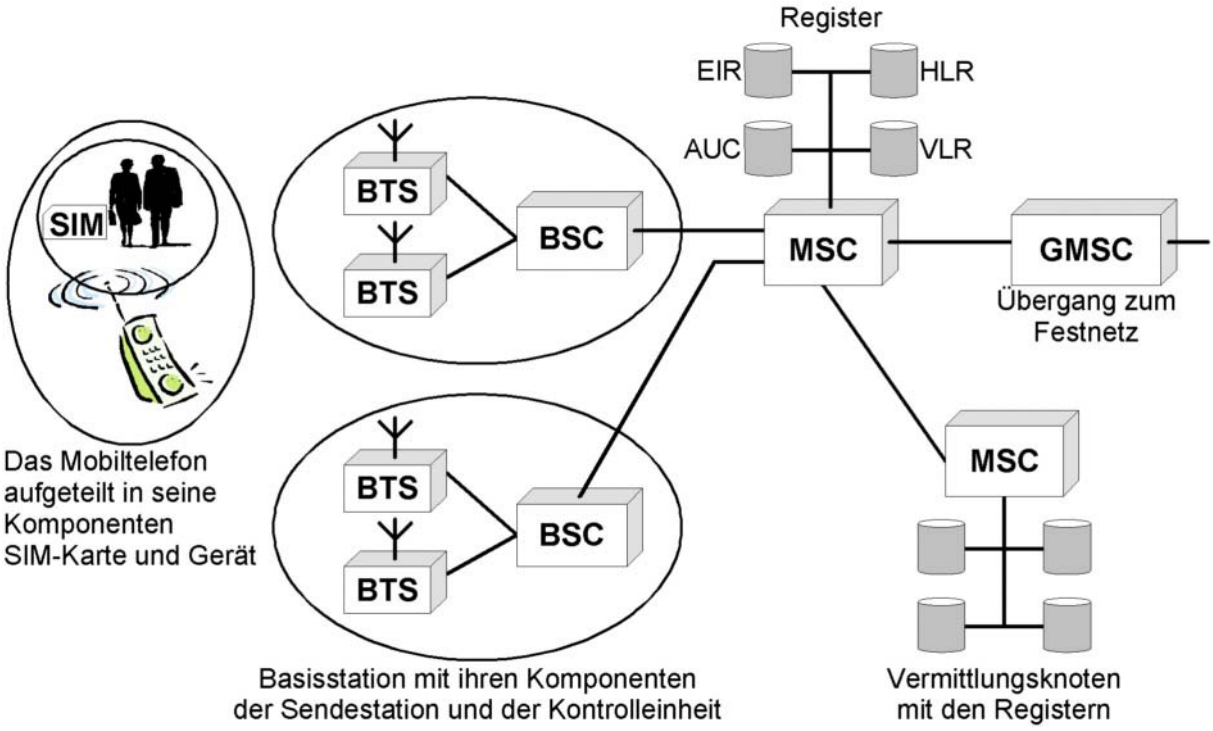


Abbildung: Verschiedene Komponenten für den sicheren Einsatz von Mobilfunksystemen

Mobiltelefon

Ein Mobiltelefon besteht aus zwei Komponenten: Dem Mobilfunkgerät selbst und dem Identifikationsmodul, der SIM-Karte (SIM - Subscriber Identity Module). Damit kann im GSM-Netz zwischen Benutzer und Gerät unterschieden werden.

Das Mobilfunkgerät ist gekennzeichnet durch seine international eindeutige Seriennummer (IMEI - International Mobile Equipment Identity). Der Benutzer wird durch seine auf der SIM-Karte gespeicherten Kundennummer (IMSI - International Mobile Subscriber Identity) identifiziert. Sie wird dem

Teilnehmer beim Vertragsabschluss vom Netzbetreiber zugeteilt. Sie ist zu unterscheiden von den ihm zugewiesenen Telefonnummern (MSISDN). Durch diese Trennung ist es möglich, dass ein Teilnehmer mit seiner SIM-Karte verschiedene Mobilfunkgeräte nutzen kann.

Auf der SIM-Karte wird u. a. die teilnehmerbezogene Rufnummer (MSISDN) gespeichert. Ebenso sind dort die kryptographischen Algorithmen für die Authentisierung und Nutzdatenverschlüsselung implementiert. Darüber hinaus können dort Kurznachrichten, Gebühreninformationen und ein persönliches Telefonbuch gespeichert werden.

SIM-Toolkit

Seit 1999 sind Mobiltelefone und SIM-Karten auf dem Markt, bei denen die Menüfunktionen der Mobiltelefone erweitert wurden. Dieser neue Standard "SIM-Toolkit" definiert neue Funktionen zwischen SIM-Karte und Mobilfunkgerät. Damit können im laufenden Betrieb neue Daten und Programme vom Netzbetreiber heruntergeladen werden. Mit SIM-Toolkit lassen sich so ganz neue Serviceangebote realisieren. Beispielsweise bietet es dem Kartenanbieter die Möglichkeit, die Menüstruktur des Mobiltelefons den Bedürfnissen der Kunden anzupassen. Möchte der Kunde über sein Mobiltelefon eine Hotelreservierung vornehmen oder eine Reise buchen, wird die Menüstruktur des Mobiltelefons vom Serviceanbieter entsprechend angepasst. Dafür müssen allerdings sowohl Karte als auch Gerät den Standard "SIM-Toolkit" unterstützen.

Basisstation

Jeder Netzbetreiber unterhält eine Vielzahl von Sendestationen (BTS - Base Station Transceiver System). Jede dieser Stationen kann ein Gebiet mit einem Radius von ca. 250 m bis 35 km versorgen, je nach Sendeleistung und Geländebeschaffenheit. Das Versorgungsgebiet einer Sendestation wird als Funkzelle bezeichnet. Mehrere Funkzellen werden von einer Kontrollstation (BSC - Base Station Controller) gesteuert. Der Verbund von Sendestationen und Kontrollstation heißt wiederum Base Station Subsystem (BSS) oder kurz Basisstation.

Die Basisstation stellt also die Schnittstelle zwischen dem Netz und dem Mobiltelefon dar. Hier werden die Kanäle für die Signalisierung und den Nutzverkehr bereitgestellt. Die Basisstation wird über den Vermittlungsknoten (MSC) gesteuert. Dieser Vermittlungsknoten übernimmt alle technischen Funktionen eines Festnetz-Vermittlungsknotens, wie z. B. Wegsuche, Signalwegschaltung und Dienstmerkmalsbearbeitung. Falls Verbindungswünsche zu einem Teilnehmer im Festnetz bestehen, werden sie vom Vermittlungsknoten über einen Koppelpfad (GMSC) ins Festnetz weitergeleitet.

Als Besonderheit im GSM-Netz gegenüber dem Festnetz kann die Verschlüsselung der Daten auf der Luftschnittstelle, d. h. zwischen Mobiltelefon und Basisstation, angesehen werden. Dies soll den Teilnehmer gegen unbefugtes Mithören schützen.

Register

Damit der Netzbetreiber in die Lage versetzt wird, auch alle gewünschten Dienste zu erbringen, muss er verschiedene Daten speichern. Er muss z. B. wissen, welche Teilnehmer sein Netz nutzen und welche Dienste sie in Anspruch nehmen wollen. Diese Daten, wie Teilnehmer, Kundennummer und beanspruchte Dienste, werden im Heimatregister (HLR - Home Location Register) abgelegt. Soll eine Verbindung, z. B. von einem Festnetzanschluss zu einem Mobiltelefon, hergestellt werden, muss der Netzbetreiber wissen, wo sich der Teilnehmer befindet und ob er sein Mobiltelefon eingeschaltet hat. Diese Informationen werden im Besucher- (VLR) und im Heimatregister (HLR) abgelegt. Um zu prüfen, ob der Teilnehmer überhaupt berechtigt ist, das Mobilfunknetz zu nutzen (also einen Kartenvertrag besitzt), führt der Netzbetreiber das Identifikationsregister (AUC). Hier werden der Sicherheitscode der SIM-Karte sowie die vom Teilnehmer festgelegten PINs abgelegt.

Außerdem kann der Netzbetreiber noch ein Geräteregister, das EIR, führen. Hier sind alle im Netz zugelassenen Mobilfunkgeräte registriert, aufgeteilt in drei Gruppen, den so genannten weißen, grauen und schwarzen Listen. In der weißen Liste sind alle unbedenklichen Geräte registriert, die graue Liste enthält alle Geräte, die möglicherweise fehlerhaft sind und in der schwarzen Liste stehen all jene, die defekt oder als gestohlen gemeldet sind. Allerdings führen nicht alle Netzbetreiber ein Geräteregister.

Damit der Netzbetreiber eine detaillierte Abrechnung der durch den Kunden in Anspruch genommenen Dienste erstellen kann, müssen die Verbindungsdaten gespeichert werden. Hierzu gehören z. B. Angaben über Kommunikationspartner (z. B. Rufnummern des Angerufenen), Zeitpunkt und Dauer der Verbindung und die Standortkennungen der mobilen Endgeräte.

Verbindungsaufbau

Sobald der Besitzer sein Mobiltelefon einschaltet, meldet es sich über die nächstgelegene Basisstation beim Netzbetreiber an. Mit seiner SIM-Karte und den darauf befindlichen kryptographischen Algorithmen identifiziert sich der Teilnehmer gegenüber dem Netzbetreiber. Die Authentikation erfolgt mit Hilfe eines Schlüssels, der nur dem Netzbetreiber und dem Teilnehmer bekannt ist. Beim Netzbetreiber werden Daten zur Identität des Nutzers, die Seriennummer des Mobiltelefons und die Kennung der Basisstation, über die seine Anmeldung erfolgt ist, protokolliert und gespeichert. Dies erfolgt auch dann, wenn kein Gespräch geführt wird. Weiterhin wird jeder Verbindungsversuch gespeichert, unabhängig vom Zustandekommen der Verbindung. Damit ist dem Netz bekannt, welcher Teilnehmer sich im Netz befindet, und es können nun Verbindungen von und zum Teilnehmer aufgebaut werden.

Festnetz

Als Festnetz wird das herkömmliche öffentliche Telefonnetz mit seinen Verbindungswegen bezeichnet.

Da bei jeder Mobilfunkverbindung auch Festnetze benutzt werden, treten eine Reihe von Festnetz-Gefährdungen auch bei der Nutzung von Mobilfunknetzen auf. Der leitungsgebundene Teil eines GSM-Netzes ist ein Spezialfall eines ISDN-Netzes. Daher sind auch die Gefährdungen und Maßnahmen, die für ISDN gelten, größtenteils für GSM relevant. Für den Bereich des Datenaustausches über GSM ist der Baustein B 4.5 LAN-Anbindung eines IT-Systems über ISDN zu betrachten.

In diesem Kapitel werden diejenigen IT-Sicherheitseigenschaften von Mobiltelefonen betrachtet, die für die Anwender bei deren Nutzung relevant sind. Es soll ein systematischer Weg aufgezeigt werden, wie ein Konzept zum Einsatz von Mobiltelefonen innerhalb einer Organisation erstellt und wie dessen Umsetzung und Einbettung sichergestellt werden kann.

Gefährdungslage

Für den IT-Grundschutz werden im Rahmen der Nutzung von Mobiltelefonen folgende typische Gefährdungen angenommen:

Organisatorische Mängel:
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.7 Unerlaubte Ausübung von Rechten

Menschliche Fehlhandlungen:
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.43 Ungeeigneter Umgang mit Passwörtern
- G 3.44 Sorglosigkeit im Umgang mit Informationen
- G 3.45 Unzureichende Identifikationsprüfung von Kommunikationspartnern

Technisches Versagen:
- G 4.41 Nicht-Verfügbarkeit des Mobilfunknetzes
- G 4.42 Ausfall des Mobiltelefons

Vorsätzliche Handlungen:
- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.80 Hoax
- G 5.94 Kartenmissbrauch
- G 5.95 Abhören von Raumgesprächen über Mobiltelefone
- G 5.96 Manipulation von Mobiltelefonen
- G 5.97 Unberechtigte Datenweitergabe über Mobiltelefone
- G 5.98 Abhören von Mobiltelefonaten
- G 5.99 Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen
- G 5.126 Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Mobiltelefone sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Nutzung bis zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Damit die Möglichkeiten, Mobiltelefone sicher einzusetzen, in der Praxis auch tatsächlich genutzt werden, sollte eine Sicherheitsrichtlinie erstellt werden, die die umzusetzenden Maßnahmen beschreibt.

Beschaffung

Bei häufiger und wechselnder dienstlicher Nutzung von Mobiltelefonen, die vom Unternehmen oder der Behörde zur Verfügung gestellt werden, kann es sinnvoll sein, diese Telefone in einer Sammelaufbewahrung zu halten.

Umsetzung

Die Maßnahme M 4.114 *Nutzung der Sicherheitsmechanismen von Mobiltelefonen* gibt einen Überblick über die wichtigsten Sicherheitsfunktionen dieser Geräte.

Betrieb

Eine geordnete und zuverlässige Nutzung von Mobiltelefonen erfordert die Umsetzung einiger Maßnahmen, zu denen die Sicherstellung der Energieversorgung und bei Bedarf auch der Schutz vor Rufnummernermittlung gehören. Falls das Gerät zur Datenübertragung eingesetzt wird, sind ebenfalls einige spezifische Maßnahmen zu beachten, um einerseits eine zuverlässige Funktionsweise zu gewährleisten und andererseits gegen Missbrauch geschützt zu sein. Bei einem eventuellen Verlust des Telefons sollte die SIM-Karte dieses Telefons unverzüglich gesperrt werden, um Missbrauch und unnötige Kosten zu verhindern.

Notfallvorsorge

In der Maßnahme M 6.72 *Ausfallvorsorge bei Mobiltelefonen* werden wichtige Vorkehrungen beschrieben, durch die sich der Benutzer vor Ausfall und bei Verlust eines Mobiltelefons schützen kann.

Nachfolgend wird das Maßnahmenbündel für den Einsatz von Mobiltelefonen vorgestellt.

Planung und Konzeption:
- M 2.188 (A) Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
- M 2.190 (Z) Einrichtung eines Mobiltelefon-Pools

Umsetzung:
- M 4.114 (A) Nutzung der Sicherheitsmechanismen von Mobiltelefonen

Betrieb:
- M 2.189 (A) Sperrung des Mobiltelefons bei Verlust
- M 4.115 (B) Sicherstellung der Energieversorgung von Mobiltelefonen
- M 4.255 (A) Nutzung von IrDA-Schnittstellen
- M 5.78 (Z) Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung
- M 5.79 (Z) Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung
- M 5.80 (Z) Schutz vor Abhören der Raumgespräche über Mobiltelefone
- M 5.81 (B) Sichere Datenübertragung über Mobiltelefone

Notfallvorsorge:
- M 6.72 (C) Ausfallvorsorge bei Mobiltelefonen

B 3.405 PDA

Beschreibung

Dieser Baustein beschäftigt sich mit handtellergroßen, mobilen Endgeräten zur Datenerfassung, -bearbeitung und -kommunikation, die im folgenden der einfacheren Lesbarkeit halber alle als PDAs (Personal Digital Assistant) bezeichnet werden. Diese gibt es in verschiedenen Geräteklassen, die sich nach Abmessungen und Leistungsmerkmalen unterscheiden, dazu gehören unter anderem:

- Organizer, um Adressen und Termine zu verwalten.
- PDAs ohne eigene Tastatur, bei denen die Dateneingabe über das Display erfolgt (mittels Stift). Der primäre Einsatzzweck ist das Erfassen und Verwalten von Terminen, Adressen und kleinen Notizen.
- PDAs, bei denen die Dateneingabe über eine eingebaute Tastatur und/oder einen Touchscreen erfolgt. Diese sollen neben dem Erfassen und Verwalten von Terminen, Adressen und kleinen Notizen auch die Bearbeitung von E-Mail ermöglichen.
- PDAs mit integriertem Mobiltelefon, sogenannte Smartphones, die damit eine eingebaute Schnittstelle zur Datenübertragung besitzen. Beim Einsatz von Smartphones ist zusätzlich Baustein 3.404 *Mobiltelefon* umzusetzen.
- Den Übergang zu "echten" Notebooks stellen sogenannte Sub-Notebooks dar, die wesentlich kleiner als normale Notebooks sind und daher beispielsweise weniger Peripheriegeräte und Anschlussmöglichkeiten bieten, die aber unter anderem für die Vorführung von Präsentationen geeignet sind. Beim Einsatz von Sub-Notebooks ist der Baustein B 3.203 *Laptop* umzusetzen.

Die Übergänge zwischen den verschiedenen Gerätetypen sind fließend und außerdem dem ständigen Wandel der Technik unterworfen. PDA- und Mobiltelefon-Funktionalitäten werden in zunehmendem Maß kombiniert.

Eine typische Anforderung an PDAs ist die Nutzung von Standard-Office-Anwendungen auch unterwegs. Zum Teil werden hierfür angepasste Varianten von Textverarbeitungs-, Tabellenkalkulations-, E-Mail- bzw. Kalenderprogrammen angeboten. PDAs werden aber auch zunehmend für sicherheitskritische Applikationen eingesetzt, wie beispielsweise die Nutzung als Authentisierungstoken für Zugriffe auf Unternehmensnetze (z. B. Generierung von Einmalpasswörtern), Speicherung von Patientendaten oder die Führung von Kundenkarteien.

In diesem Kapitel werden diejenigen IT-Sicherheitseigenschaften von PDAs betrachtet, die für die Anwender bei deren Nutzung relevant sind. Es soll ein systematischer Weg aufgezeigt werden, wie ein Konzept zum Einsatz von PDAs innerhalb einer Organisation erstellt und wie dessen Umsetzung und Einbettung sichergestellt werden kann.

Gefährdungslage

Für den IT-Grundschutz werden im Rahmen der Nutzung von PDAs folgende typische Gefährdungen angenommen:

Höhere Gewalt:

- G 1.15 Beeinträchtigung durch wechselnde Einsatzumgebung

Organisatorische Mängel:
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.7 Unerlaubte Ausübung von Rechten

Menschliche Fehlhandlungen:
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.43 Ungeeigneter Umgang mit Passwörtern
- G 3.44 Sorglosigkeit im Umgang mit Informationen
- G 3.45 Unzureichende Identifikationsprüfung von Kommunikationspartnern
- G 3.76 Fehler bei der Synchronisation mobiler Endgeräte

Technisches Versagen:
- G 4.42 Ausfall des Mobiltelefons oder des PDAs
- G 4.51 Unzureichende Sicherheitsmechanismen bei PDAs
- G 4.52 Datenverlust bei mobilem Einsatz

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.9 Unberechtigte IT-Nutzung
- G 5.22 Diebstahl bei mobiler Nutzung des IT-Systems
- G 5.23 Computer-Viren
- G 5.123 Abhören von Raumgesprächen über mobile Endgeräte
- G 5.124 Missbrauch der Informationen von mobilen Endgeräten
- G 5.125 Unberechtigte Datenweitergabe über mobile Endgeräte
- G 5.126 Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Im Rahmen des PDA-Einsatzes sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

1. Um PDAs sicher und effektiv in Behörden oder Unternehmen einsetzen zu können, sollte ein Konzept erstellt werden, das auf den Sicherheitsanforderungen für die bereits vorhandenen IT-Systeme sowie den Anforderungen aus den geplanten Einsatzszenarien beruht. Darauf aufbauend ist die PDA-Nutzung zu regeln und Sicherheitsrichtlinien dafür zu erarbeiten (siehe M 2.304 *Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung*).

2. Für die Beschaffung von PDAs müssen die aus dem Konzept resultierenden Anforderungen an die jeweiligen Produkte formuliert und basierend darauf die Auswahl der geeigneten Produkte getroffen werden (siehe M 2.305 *Geeignete Auswahl von PDAs*).

3. Je nach Sicherheitsanforderungen müssen die beteiligten Software-Komponenten (PDA, Synchronisationssoftware, Software zum zentralen PDA-Management) unterschiedlich konfiguriert werden. Dies betrifft vor allem die PDAs selber (siehe M 4.228 *Nutzung der Sicherheitsmechanismen von PDAs*), die Synchronisationsumgebung (siehe M 4.229 *Sicherer Betrieb von PDAs*) und gegebenenfalls spezielle Software zum zentralen PDA-Management.

Damit PDAs sicher eingesetzt werden können, müssen auch damit gekoppelte Arbeitsplatz-Rechner und hier vor allem die Synchronisationsschnittstelle sicher konfiguriert sein. Geeignete IT-Sicherheits-

empfehlungen für Standard-Arbeitsplatz-PCs sind in den Client-Bausteinen der Schicht 3 beschrieben.

Nachfolgend wird das Maßnahmenbündel für den Einsatz von PDAs vorgestellt.

Planung und Konzeption:
- M 2.218 (C) Regelung der Mitnahme von Datenträgern und IT-Komponenten
- M 2.303 (A) Festlegung einer Strategie für den Einsatz von PDAs
- M 2.304 (A) Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung

Beschaffung:
- M 2.305 (B) Geeignete Auswahl von PDAs
- M 4.231 (Z) Einsatz zusätzlicher Sicherheitswerkzeuge für PDAs

Umsetzung:
- M 5.121 (B) Sichere Kommunikation von unterwegs

Betrieb:
- M 1.33 (A) Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
- M 4.3 (A) Regelmäßiger Einsatz eines Anti-Viren-Programms
- M 4.31 (A) Sicherstellung der Energieversorgung im mobilen Einsatz
- M 4.228 (A) Nutzung der Sicherheitsmechanismen von PDAs
- M 4.229 (C) Sicherer Betrieb von PDAs
- M 4.230 (Z) Zentrale Administration von PDAs
- M 4.232 (Z) Sichere Nutzung von Zusatzspeicherkarten
- M 4.255 (A) Nutzung von IrDA-Schnittstellen

Aussonderung:
- M 2.306 (A) Verlustmeldung

Notfallvorsorge:
- M 6.95 (C) Ausfallvorsorge und Datensicherung bei PDAs

4 Netze

In der Schicht Netze sind folgende Bausteine enthalten:

B 4.1 Heterogene Netze

B 4.2 Netz- und Systemmanagement

B 4.3 Modem

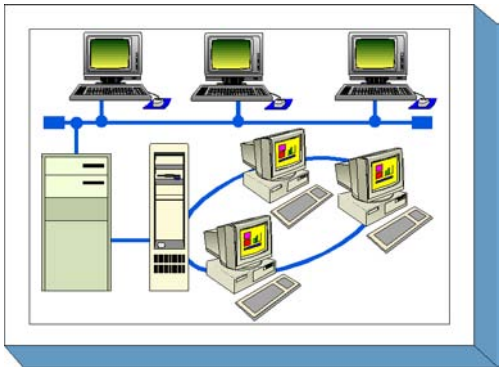
B 4.4 Remote Access

B 4.5 LAN-Anbindung eines IT-Systems über ISDN

B 4.6 WLAN

B 4.7 VoIP

B 4.1 Heterogene Netze



Beschreibung

Ein lokales Netz setzt sich aus der Verkabelung (d. h. den passiven Netzkomponenten Kabel und den Verbindungselementen) sowie den aktiven Netzkomponenten zur Netzkopplung zusammen. Generell können dabei unterschiedliche Verkabelungstypen wie auch unterschiedliche aktive Netzkomponenten in ein LAN integriert werden. Als aktive Netzkomponenten werden alle Netzkomponenten bezeichnet, die eine eigene (Netz-)Stromversorgung benötigen. Dazu gehören unter anderem Repeater, Brücken, Switches, Router, Gateways. Als passive Netzkomponenten werden alle Netzkomponenten betrachtet, die keine eigene Netzstrom-Versorgung benötigen. Dazu gehören z. B. Kabel, Verteilerschränke, Patchfelder, Steckverbinder.

Die Verkabelung wird bereits detailliert im Baustein B 2.2 Verkabelung, die anwendungsbezogene Peripherie in den Bausteinen der Schicht 3 behandelt, so dass im vorliegenden Baustein primär die aktiven Netzkomponenten, die ihnen zugrunde liegende Topologie, ihre Konfiguration, Kriterien zur Auswahl geeigneter Komponenten, die Auswahl von Übertragungsprotokollen sowie das zugehörige Netzmanagement betrachtet werden.

Es werden nur LAN-Technologien betrachtet, z. B. die Netzprotokolle Ethernet, Token Ring oder FDDI bzw. die zugehörigen Netzkomponenten wie Bridges, Switches oder Router. Diese Technologien können unter Umständen auch in einem MAN zum Einsatz kommen. Fragestellungen im Zusammenhang mit einer WAN-Anbindung werden dagegen nicht behandelt. Hier sei unter anderem auf den Baustein B 3.301 Sicherheitsgateway (Firewall) verwiesen.

Soll ein LAN hinreichend im Sinne des IT-Grundschutzes geschützt werden, so genügt es nicht, nur den vorliegenden Baustein zu bearbeiten. Neben den aktiven Netzkomponenten und der eingesetzten Software zum Netzmanagement müssen auch die physikalische Verkabelung und die im Netz zur Verfügung stehenden Serversysteme beachtet werden. Deshalb ist es unumgänglich, auch die oben genannten Bausteine durchzuarbeiten.

Dieser Baustein beschreibt einen Leitfaden, wie ein heterogenes Netz analysiert und darauf aufbauend unter Sicherheitsaspekten konzipiert und betrieben werden kann. Damit richtet sich dieser Baustein an die Stelle einer Organisation, die für den Netzbetrieb verantwortlich ist und das entsprechende fachliche Wissen besitzt.

Gefährdungslage

Für den IT-Grundschutz eines heterogenen Netzes werden pauschal die folgenden Gefährdungen angenommen:

Höhere Gewalt:

- G 1.2 Ausfall des IT-Systems
- G 1.3 Blitz
- G 1.4 Feuer
- G 1.5 Wasser
- G 1.7 Unzulässige Temperatur und Luftfeuchte
- G 1.8 Staub, Verschmutzung

Organisatorische Mängel:

- G 2.7 Unerlaubte Ausübung von Rechten

- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- G 2.22 Fehlende Auswertung von Protokolldaten
- G 2.27 Fehlende oder unzureichende Dokumentation
- G 2.32 Unzureichende Leitungskapazitäten
- G 2.44 Inkompatible aktive und passive Netzkomponenten
- G 2.45 Konzeptionelle Schwächen des Netzes
- G 2.46 Überschreiten der zulässigen Kabel- oder Buslänge bzw. der Ringgröße

Menschliche Fehlhandlungen:
- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.5 Unbeabsichtigte Leitungsbeschädigung
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.28 Ungeeignete Konfiguration der aktiven Netzkomponenten
- G 3.29 Fehlende oder ungeeignete Segmentierung

Technisches Versagen:
- G 4.1 Ausfall der Stromversorgung
- G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
- G 4.31 Ausfall oder Störung von Netzkomponenten

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.5 Vandalismus
- G 5.6 Anschlag
- G 5.7 Abhören von Leitungen
- G 5.8 Manipulation an Leitungen
- G 5.9 Unberechtigte IT-Nutzung
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.20 Missbrauch von Administratorrechten
- G 5.28 Verhinderung von Diensten
- G 5.66 Unberechtigter Anschluss von IT-Systemen an ein Netz
- G 5.67 Unberechtigte Ausführung von Netzmanagement-Funktionen
- G 5.68 Unberechtigter Zugang zu den aktiven Netzkomponenten

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

An dieser Stelle sei nochmals darauf hingewiesen, dass ein ausreichender Schutz für ein LAN im Sinne der IT-Grundschutz-Kataloge nur dann gewährleistet werden kann, wenn zusätzlich die Maßnahmenbündel aus den Bausteinen B 2.2 Verkabelung, B 3.101 Allgemeiner Server und gegebenenfalls die betriebssystem-spezifischen Ergänzungen und B 4.2 Netz- und Systemmanagement umgesetzt werden.

Weiterhin sollten die aktiven Netzkomponenten in Räumen für technische Infrastruktur (z. B. Verteilerräume) untergebracht werden, so dass auch die Maßnahmen aus dem Baustein B 2.6 Raum für technische Infrastruktur realisiert werden müssen.

Der Arbeitsplatz des Netzadministrators sollte ebenfalls besonders geschützt werden. Neben den Maßnahmen aus dem Baustein B 2.3 *Büroraum* sind hier die Regelungen für das eingesetzte Betriebssystem zu nennen (siehe die entsprechenden Bausteine der Schicht 3).

Für den sicheren Einsatz eines heterogenen Netzes sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Analyse der aktuellen Netzsituation über die Entwicklung eines Netzmanagement-Konzeptes bis zum Betrieb eines heterogenen Netzes. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

1. Analyse der aktuellen Netzsituation (siehe M 2.139 *Ist-Aufnahme der aktuellen Netzsituation* und M 2.140 *Analyse der aktuellen Netzsituation*)
   - Erhebung von Lastfaktoren und Verkehrsflussanalyse
   - Feststellung von Netzengpässen
   - Identifikation kritischer Bereiche
2. Konzeption
   - Konzeption eines Netzes (siehe M 2.141 *Entwicklung eines Netzkonzeptes* und M 2.142 *Entwicklung eines Netz-Realisierungsplans* und M 5.60 *Auswahl einer geeigneten Backbone-Technologie*)
   - Konzeption Netzmanagement (siehe M 2.143 *Entwicklung eines Netzmanagementkonzeptes* und M 2.144 *Geeignete Auswahl eines Netzmanagement-Protokolls*)
3. Sicherer Betrieb des Netzes
   - Segmentierung des Netzes (siehe M 5.61 *Geeignete physikalische Segmentierung* und M 5.62 *Geeignete logische Segmentierung*)
   - Einsatz einer Netzmanagement-Software (siehe M 2.145 *Anforderungen an ein Netzmanagement-Tool* und M 2.146 *Sicherer Betrieb eines Netzmanagementsystems*)
   - Audit und Revision des Netzes (siehe M 4.81 *Audit und Protokollierung der Aktivitäten im Netz* und M 2.64 *Kontrolle der Protokolldateien*)
4. Notfallvorsorge
   - Redundante Auslegung der Netzkomponenten (siehe M 6.53 *Redundante Auslegung der Netzkomponenten*)
   - Sicherung der Konfigurationsdaten (siehe M 6.52 *Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten* und M 6.22 *Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen*)

Nachfolgend wird das komplette Maßnahmenbündel für den Bereich Heterogene Netze vorgestellt, in dem auch Maßnahmen von eher grundsätzlicher Art enthalten sind, die zusätzlich zu den oben aufgeführten Schritten beachtet werden müssen.

Planung und Konzeption

- M 2.139 (A) Ist-Aufnahme der aktuellen Netzsituation
- M 2.140 (Z) Analyse der aktuellen Netzsituation
- M 2.141 (B) Entwicklung eines Netzkonzeptes
- M 2.142 (B) Entwicklung eines Netz-Realisierungsplans
- M 4.79 (A) Sichere Zugriffsmechanismen bei lokaler Administration

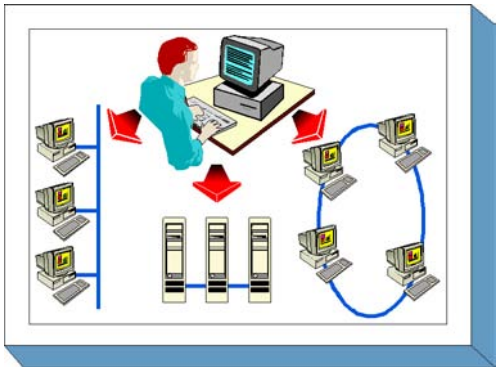
- M 4.80 (B) Sichere Zugriffsmechanismen bei Fernadministration
- M 5.2 (A) Auswahl einer geeigneten Netz-Topographie
- M 5.13 (A) Geeigneter Einsatz von Elementen zur Netzkopplung
- M 5.60 (A) Auswahl einer geeigneten Backbone-Technologie
- M 5.61 (A) Geeignete physikalische Segmentierung
- M 5.62 (Z) Geeignete logische Segmentierung
- M 5.77 (Z) Bildung von Teilnetzen

Umsetzung:
- M 4.7 (A) Änderung voreingestellter Passwörter
- M 4.82 (A) Sichere Konfiguration der aktiven Netzkomponenten
- M 5.7 (A) Netzverwaltung

Betrieb:
- M 4.81 (B) Audit und Protokollierung der Aktivitäten im Netz
- M 4.83 (C) Update/Upgrade von Soft- und Hardware im Netzbereich

Notfallvorsorge:
- M 6.52 (A) Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten
- M 6.53 (Z) Redundante Auslegung der Netzkomponenten
- M 6.54 (B) Verhaltensregeln nach Verlust der Netzintegrität

B 4.2 Netz- und Systemmanagement



Beschreibung

Ein Managementsystem für ein im Allgemeinen lokales Rechnernetz (LAN, VLAN) dient dazu, möglichst alle im lokale Netz angesiedelten Hard- und Software-Komponenten zentral zu verwalten. Ein solches System soll den Systemverwalter maximal in seiner täglichen Arbeit unterstützen. Grundsätzlich kann zwischen Netzmanagement und Systemmanagement unterschieden werden. Die Unterschiede ergeben sich durch die jeweils verwalteten Komponenten.

Netzmanagement umfasst die Gesamtheit der Vorkehrungen und Aktivitäten zur Sicherstellung des effektiven Einsatzes eines Netzes. Hierzu gehört beispielsweise die Überwachung der Netzkomponenten auf ihre korrekte Funktion, das Monitoring der Netzperformance und die zentrale Konfiguration der Netzkomponenten. Netzmanagement ist in erster Linie eine organisatorische Problemstellung, deren Lösung lediglich mit technischen Mitteln, einem Netzmanagementsystem, unterstützt werden kann.

Systemmanagement befasst sich in erster Linie mit dem Management verteilter IT-Systeme. Hierzu gehören beispielsweise eine zentrale Verwaltung der Benutzer, Softwareverteilung, Management der Anwendungen usw. In einigen Bereichen, wie z. B. dem Konfigurationsmanagement (dem Überwachen und Konsolidieren von Konfigurationen eines Systems oder einer Netzkomponente), sind Netz- und Systemmanagement nicht klar zu trennen.

Im folgenden wird das (Software-) System, das zum Verwalten eines Netzes und dessen Komponenten dient, immer als "Managementsystem" bezeichnet, die damit verwalteten Komponenten werden als "verwaltetes System" bezeichnet. Im Englischen werden hier die Begriffe "management system" und "managed system" verwendet, dies gilt insbesondere für den Bereich Netzmanagement.

In der ISO/IEC-Norm 7498-4 bzw. als X.700 der ITU-T ist ein Netz- und Systemmanagement-Framework definiert. Zu den Aufgaben eines Managementsystems gehören demnach:

1. Konfigurationsmanagement,
2. Performancemanagement,
3. Fehlermanagement,
4. Abrechnungsmanagement,
5. Sicherheitsmanagement.

Dabei muss ein konkretes Systemmanagement-Produkt nicht für jeden der Bereiche Unterstützung anbieten. Die Hersteller bieten i.d.R Produktpaletten an, die so konzipiert sind, dass spezielle Funktionalitäten als Modul oder als kooperierendes Einzelprodukt erhältlich sind.

Netzmanagement ist die ältere und ausgereiftere Managementdisziplin. Systemmanagement ist im Gegensatz dazu eine noch junge Disziplin, wird aber durch die stark gewachsene Vernetzung in Unternehmen bzw. Behörden und die damit zunehmende Heterogenität und Komplexität immer mehr gefordert. Ziel muss es hier sein, beide Disziplinen zu integrieren. Die zurzeit erhältlichen Managementprodukte sind so angelegt, dass sie primär entweder zum Netzmanagement oder zum Systemmanagement konzipiert sind. Produkte, die beide Funktionalitäten vereinen, sind in der Entwicklung. In der Regel erlauben Produkte, die für das Systemmanagement ausgelegt sind, auch den Zugriff auf Informationen des Netzmanagements.

Aufgrund der Heterogenität von Hard- und Software heutiger Netze ist Systemmanagement eine sehr komplexe Aufgabe. Erschwert wird Systemmanagement zusätzlich dadurch, dass die Managementsoftware und die Software, die verwaltet werden soll, sehr eng zusammenarbeiten müssen. In der Regel ist heute erhältliche Software jedoch nicht darauf eingerichtet, mit einem Managementsystem zusammenzuarbeiten. Dies liegt zum einen an fehlenden Standards, die z. B. ausreichende Sicherheit garantieren, zum anderen daran, dass größere Softwarepakete mit eigenem, proprietärem Management ausgestattet sind, da Interna über die Software, die zum Verwalten dieser nötig sind, nicht offengelegt werden sollen. Beispielsweise existiert für den Microsoft Internet Explorer eine Managementsoftware, das "Internet Explorer Administration Kit (IEAK)", welches z. B. die Vorgabe von Sicherheitseinstellungen durch den Administrator erlaubt, die vom Benutzer nachträglich nicht mehr oder nur im Rahmen vorgegebener Werte verändert werden können. Die Funktionsweise dieses Tools ist proprietär und unterliegt keinem Standard.

Prinzipiell ist die Architektur von Managementsoftware zentralistisch aufgebaut: es gibt eine zentrale Managementstation oder -konsole, von der aus der Systemadministrator das ihm anvertraute Netz mit den darin befindlichen Hard- und Software-Komponenten verwalten kann. Insbesondere die Systeme zum Netzmanagement bauen darauf auf. Durch die fehlenden Standards im Bereich Systemmanagement findet man hier in den erhältlichen Produkten in vielen Fällen zwar die zentralistische Architektur, die jedoch im Detail proprietär realisiert ist, so dass hier keine weitere generelle Architekturaussage gemacht werden kann.

Einem *Netzmanagementsystem* liegt in der Regel ein Modell zugrunde, das zwischen "Manager", "Agent" (auch "Managementagent") und "verwalteten Objekten" (auch "managed objects") unterscheidet. Die weiteren Bestandteile sind das zur Kommunikation verwendete Protokoll zwischen Manager und den Agenten, sowie eine Informationsdatenbank, die so genannte "MIB" (Management Information Base). Die MIB muss sowohl dem Manager als auch jedem Managementagenten zur Verfügung stehen. Konzeptionell werden Managementagenten und deren MIB als Teil des verwalteten Systems angesehen.

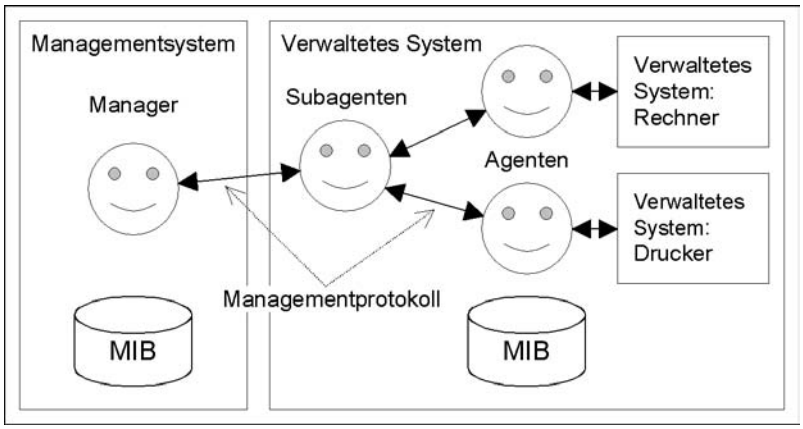


Abbildung: Netzmanagementsystem

Ein Agent ist für ein oder mehrere zu verwaltende Objekte zuständig. Es ist möglich, die Agenten hierarchisch zu organisieren: Ein Agent ist dann für die ihm zugeordneten Unteragenten zuständig. Am Ende einer jeden auf diese Art entstehenden Befehlskette steht immer ein zu verwaltendes Objekt. Ein zu verwaltendes Objekt ist entweder ein physikalisch vorhandenes Objekt (Gerät), wie ein Rechner, ein Drucker oder ein Router, oder ein Softwareobjekt, wie z. B. ein Hintergrundprozeß zur

Verwaltung von Druckaufträgen. Bei Geräten, die über ein Managementsystem verwaltet werden können, ist der Managementagent in der Regel schon vom Hersteller in das Gerät "fest" eingebaut. Versteht dieser das vom Manager verwendete Kommunikationsprotokoll nicht, ist z. B. ein Software-Managementagent nötig, der die Protokollumsetzung beherrscht. In ähnlicher Weise können Software-Komponenten den Managementagenten schon enthalten, oder es wird ein spezieller Managementagent benötigt, der für die Verwaltung dieser Software-Komponente konzipiert ist.

Um die einzelnen Komponenten des zu verwaltenden Systems anzusprechen, tauschen der Manager und die jeweiligen Agenten Informationen aus. Die Art des zur Kommunikation verwendeten Protokolls bestimmt maßgeblich die Mächtigkeit und insbesondere die Sicherheit des Managementsystems.

Prinzipiell können Managementsysteme bezüglich des verwendeten Kommunikationsprotokolls in drei Kategorien unterteilt werden (siehe auch M 2.144 *Geeignete Auswahl eines Netzmanagement-Protokolls*):

1. Es wird SNMP (Simple Network Management Protocol) benutzt, das weit verbreitete Standardprotokoll des TCP/IP-basierten Systemmanagements.
2. Es wird CMIP (Common Management Information Protocol) benutzt, das seltener benutzte Standardprotokoll des ISO/OSI-basierten Systemmanagements.
3. Es wird ein herstellerspezifisches Protokoll benutzt. Es existiert meist die Möglichkeit, so genannte Adapter zum Einbinden der Standardprotokolle zu verwenden, wobei in der Regel lediglich eine SNMP-Anbindung existiert.

Das am häufigsten benutzte Protokoll ist SNMP. SNMP ist ein sehr einfaches Protokoll, das nur fünf Nachrichtentypen kennt und daher auch einfach zu implementieren ist. CMIP wird hauptsächlich zum Management von Telekommunikationsnetzen verwandt, und hat im Inter- und Intranet-basierten Management keine Bedeutung, da es den OSI-Protokollstack verwendet und nicht den TCP/IP-Stack.

Systemmanagementsysteme sind zwar in der Regel auch zentralistisch ausgelegt, um das Verwalten des Systems von einer Managementstation aus zu erlauben, die konkrete Architektur hängt jedoch davon ab, wie groß die Systeme, die verwaltet werden können, sein dürfen und welcher Funktionsumfang angeboten wird. Hier reicht die Palette von einfachen Sammlungen von Management-Tools, die ohne Integration nebeneinander in kleinen Netzen eingesetzt werden, bis hin zu Managementplattformen, die ein weltumspannendes Firmennetz mit mehreren Tausend Rechnern verwalten können.

Bestimmte Managementplattformen benutzen proprietäre Protokolle zur Kommunikation zwischen den Komponenten. Diese Systeme weisen in der Regel ein wesentlich höheres Leistungsspektrum auf und dienen nicht nur dem Netz- und Systemmanagement, sondern bieten unternehmens- bzw. behördenweites Ressourcenmanagement an. Durch die unzureichend spezifizierten Sicherheitsmechanismen in den wenigen existierenden Standards, erlauben proprietäre Lösungen zudem die (zwar nicht standardisierte) Verfügbarkeit sicherheitsrelevanter Mechanismen, wie z. B. Verschlüsselungsverfahren.

Gefährdungslage

Für den IT-Grundschutz eines Managementsystems werden die folgenden typischen Gefährdungen angenommen:

Höhere Gewalt

- G 1.1 Personalausfall
- G 1.2 Ausfall des IT-Systems

Organisatorische Mängel:
- G 2.27 Fehlende oder unzureichende Dokumentation
- G 2.32 Unzureichende Leitungskapazitäten
- G 2.59 Betreiben von nicht angemeldeten Komponenten
- G 2.60 Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement
- G 2.61 Unberechtigte Sammlung personenbezogener Daten

Menschliche Fehlhandlungen:
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.28 Ungeeignete Konfiguration der aktiven Netzkomponenten
- G 3.34 Ungeeignete Konfiguration des Managementsystems
- G 3.35 Server im laufenden Betrieb ausschalten
- G 3.36 Fehlinterpretation von Ereignissen

Technisches Versagen:
- G 4.31 Ausfall oder Störung von Netzkomponenten
- G 4.38 Ausfall von Komponenten eines Netz- und Systemmanagementsystems

Vorsätzliche Handlungen:
- G 5.2 Manipulation an Daten oder Software
- G 5.8 Manipulation an Leitungen
- G 5.9 Unberechtigte IT-Nutzung
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.28 Verhinderung von Diensten
- G 5.66 Unberechtigter Anschluss von IT-Systemen an ein Netz
- G 5.67 Unberechtigte Ausführung von Netzmanagement-Funktionen
- G 5.86 Manipulation von Managementparametern

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Das zu verwaltende System besteht aus einzelnen Rechnern, Netzkoppelelementen und dem physikalischen Netz. Jede dieser Komponenten ist ein potentielles Sicherheitsrisiko für das Gesamtsystem. Diese Risiken können im allgemeinen alleine durch die Einführung von Managementsoftware nicht vollständig beseitigt werden. Dies gilt schon deshalb, weil in der Regel nicht alle Systeme in gleichem Maße durch ein Managementsystem erfasst werden. Grundvoraussetzung für die Systemsicherheit ist hier einerseits die Definition und andererseits die Realisierung einer organisationsweiten Sicherheitsrichtlinie, die sich im betrachteten Fall insbesondere in der Konfiguration von Hard- und Software niederschlagen muss. Aus diesem Grund sollten insbesondere die Maßnahmen der Bausteine der Schicht 3 betrachtet werden. Als Ausgangsbaustein kann der Baustein B 4.1 *Heterogene Netze* dienen.

Da Managementsysteme von einem zentralistischen Ansatz ausgehen, kommt der zentralen Managementstation eine besondere Bedeutung unter Sicherheitsgesichtspunkten zu und ist daher besonders zu schützen. Zentrale Komponenten eines Managementsystems sollten daher in Räumen aufgestellt werden, die den Anforderungen an einen Serverraum (vergleiche Baustein B 2.4 *Serverraum*) entsprechen. Wenn kein Serverraum zur Verfügung steht, können sie alternativ in einem Serverschrank aufgestellt werden (vergleiche Baustein B 2.7 *Schutzschränke*).

Für den erfolgreichen Aufbau eines Netz- und Systemmanagementsystems sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die

Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

1. Erstellen eines Managementkonzeptes, das auf den Anforderungen beruht, die sich aus den Gegebenheiten des in der Regel bereits vorhandenen IT-Systems ergeben
   - Anforderungsanalyse (siehe M 2.168 *IT-System-Analyse vor Einführung eines Systemmanagementsystems*)
   - Definition des Konzeptes (siehe M 2.169 *Entwickeln einer Systemmanagementstrategie*)
2. Die Beschaffung des Managementsystems erfordert zunächst, die aus dem Managementkonzept resultierenden
   - Anforderungen an das Managementprodukt zu formulieren (siehe M 2.170 *Anforderungen an ein Systemmanagementsystem*) und basierend darauf
   - die Auswahl eines geeigneten Managementproduktes zu treffen (siehe M 2.171 *Geeignete Auswahl eines Systemmanagement-Produktes*).
3. Die sicherheitsrelevanten Maßnahmen für den Betrieb des Managementsystems untergliedern sich in die Bereiche:
   - Installation, mit der Umsetzung des Managementkonzeptes (siehe M 4.91 *Sichere Installation eines Systemmanagementsystems*) und
   - den laufenden Betrieb des Managementsystems (siehe M 4.92 *Sicherer Betrieb eines Systemmanagementsystems*).
   - Daneben sind natürlich die bisherigen Maßnahmen für den laufenden Betrieb des verwalteten Systems zu beachten (siehe relevante Bausteine der Schicht 3).

Nachfolgend wird das Maßnahmenbündel für den Baustein *Netz- und Systemmanagement* vorgestellt.

Planung und Konzeption
- M 2.143 (A) Entwicklung eines Netzmanagementkonzeptes
- M 2.144 (A) Geeignete Auswahl eines Netzmanagement-Protokolls
- M 2.168 (A) IT-System-Analyse vor Einführung eines Systemmanagementsystems
- M 2.169 (A) Entwickeln einer Systemmanagementstrategie

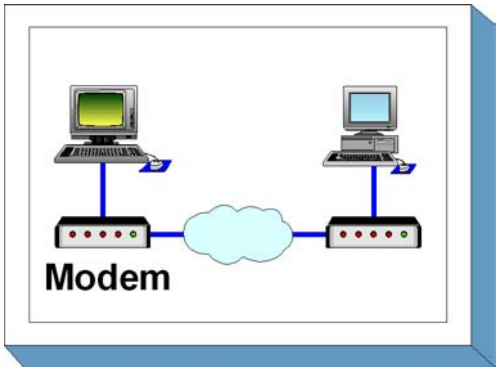
Beschaffung
- M 2.145 (B) Anforderungen an ein Netzmanagement-Tool
- M 2.170 (A) Anforderungen an ein Systemmanagementsystem
- M 2.171 (A) Geeignete Auswahl eines Systemmanagement-Produktes

Umsetzung
- M 4.91 (A) Sichere Installation eines Systemmanagementsystems

Betrieb
- M 2.146 (A) Sicherer Betrieb eines Netzmanagementsystems
- M 4.92 (A) Sicherer Betrieb eines Systemmanagementsystems

Notfallvorsorge
- M 6.57 (C) Erstellen eines Notfallplans für den Ausfall des Managementsystems

B 4.3 Modem



Beschreibung

Über ein Modem wird eine Datenendeinrichtung, z. B. ein PC, über das öffentliche Telefonnetz mit anderen Datenendeinrichtungen verbunden, um Informationen austauschen zu können. Ein Modem wandelt die digitalen Signale aus der Datenendeinrichtung in analoge elektrische Signale um, die über das Telefonnetz übertragen werden können. Damit zwei IT-Systeme über Modem kommunizieren können, muss auf den IT-Systemen die entsprechende Kommunikationssoftware installiert sein.

Unterschieden werden externe, interne und PCMCIA-Modems. Ein externes Modem ist ein eigenständiges Gerät mit eigener Stromversorgung, das üblicherweise über eine serielle Schnittstelle mit dem IT-System verbunden wird. Als internes Modem werden Steckkarten mit Modem-Funktionalität, die über keine eigene Stromversorgung verfügen, bezeichnet. Ein PCMCIA-Modem ist eine scheckkartengroße Einsteckkarte, die über eine PCMCIA-Schnittstelle üblicherweise in Laptops eingesetzt wird.

In diesem Baustein wird Datenübertragung über ISDN nicht betrachtet, dazu siehe die Bausteine B 3.401 *TK-Anlage* und B 4.5 *LAN-Anbindung eines IT-Systems über ISDN*.

Gefährdungslage

In diesem Kapitel werden für den IT-Grundschutz beim Einsatz eines Modems folgende Gefährdungen angenommen:

Höhere Gewalt:
- G 1.2 Ausfall des IT-Systems

Menschliche Fehlhandlungen:
- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.5 Unbeabsichtigte Leitungsbeschädigung

Technisches Versagen:
- G 4.6 Spannungsschwankungen/Überspannung/Unterspannung

Vorsätzliche Handlungen:
- G 5.2 Manipulation an Daten oder Software
- G 5.7 Abhören von Leitungen
- G 5.8 Manipulation an Leitungen
- G 5.9 Unberechtigte IT-Nutzung
- G 5.10 Missbrauch von Fernwartungszugängen
- G 5.12 Abhören von Telefongesprächen und Datenübertragungen
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.23 Computer-Viren
- G 5.25 Maskerade
- G 5.39 Eindringen in Rechnersysteme über Kommunikationskarten

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den Einsatz eines Modems sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Beschaffung bis zum Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Schon vor dem Einsatz eines Modems sollte geprüft werden, ob die lokalen Gegebenheiten die Installation eines Überspannungsschutzes erforderlich machen. Auch sollte festgelegt werden, wer unter welchen Umständen das Modem benutzen darf.

Beschaffung

Die Maßnahme M 2.59 *Auswahl eines geeigneten Modems in der Beschaffung* nennt die wesentlichen Kriterien, die bei der Auswahl eines Modems zu beachten sind.

Umsetzung

Vor der Inbetriebnahme ist das Modem geeignet zu konfigurieren, wobei unbedingt darauf zu achten ist, dass eventuell vorhandene, vom Hersteller vorgegebene Passwörter geändert werden. Die Installation eines Modems darf nicht dazu führen, dass hierdurch ein zusätzlicher, ungesicherter Zugang zu einem Rechnernetz, beispielsweise an einer Firewall vorbei, entsteht.

Betrieb

Damit nicht durch die Nutzung eines Modems ein zusätzliches Sicherheitsrisiko entsteht, muss für eine sichere Administration und Nutzung gesorgt werden. Dies lässt sich nur dann erreichen, wenn das Personal in diesem Bereich entsprechend geschult wird. Dazu gehört auch, dass sich die Mitarbeiter bewusst sind, dass über eine Modem-Verbindung Viren eingeschleppt werden können und dass sie daher besonders dafür Sorge zu tragen haben, dass alle übertragenen Daten auf Viren geprüft werden.

Um externe Angriffe über die Modem-Verbindung zu erschweren, sollte überlegt werden, ob das Modem so konfiguriert werden kann, dass alle Verbindungen von innen nach außen aufgebaut werden müssen und eingehende Verbindungen über ein Callback-Verfahren durchgeschaltet werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Modem" vorgestellt.

Planung und Konzeption

- M 1.25 (Z) Überspannungsschutz
- M 2.42 (B) Festlegung der möglichen Kommunikationspartner
- M 2.46 (Z) Geeignetes Schlüsselmanagement
- M 2.61 (A) Regelung des Modem-Einsatzes
- M 4.34 (Z) Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
- M 5.32 (A) Sicherer Einsatz von Kommunikationssoftware

Beschaffung

- M 2.59 (A) Auswahl eines geeigneten Modems in der Beschaffung

Umsetzung

- M 1.38 (A) Geeignete Aufstellung eines Modems
- M 2.204 (A) Verhinderung ungesicherter Netzzugänge
- M 4.7 (A) Änderung voreingestellter Passwörter
- M 5.30 (Z) Aktivierung einer vorhandenen Callback-Option

- M 5.31 (A) Geeignete Modem-Konfiguration

Betrieb

- M 2.60 (A) Sichere Administration eines Modems
- M 3.17 (A) Einweisung des Personals in die Modem-Benutzung
- M 4.33 (A) Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
- M 5.33 (A) Absicherung der per Modem durchgeführten Fernwartung
- M 5.44 (Z) Einseitiger Verbindungsaufbau

B 4.4 Remote Access Dienste

Beschreibung

Durch entfernte Zugriffe (Remote Access) wird es einem Benutzer ermöglicht, sich mit einem lokalen Rechner an ein entferntes Rechnernetz zu verbinden und dessen Ressourcen zu nutzen, als ob eine direkte LAN-Koppelung bestehen würde. Die dafür benutzten Dienste werden Remote Access Service (RAS) genannt. Durch RAS wird entfernten Benutzern der Zugriff auf die Ressourcen des Netzes gewährt.

Generell lassen sich für den Einsatz von RAS im Wesentlichen folgende Szenarien unterscheiden:

- das Anbinden einzelner stationärer Arbeitsplatzrechner (z. B. für Telearbeit einzelner Mitarbeiter),
- das Anbinden mobiler Rechner (z. B. zur Unterstützung von Mitarbeitern im Außendienst oder auf Dienstreise),
- das Anbinden von ganzen LANs (z. B. zur Anbindung von lokalen Netzen von Außenstellen oder Filialen),
- der Managementzugriff auf entfernte Rechner (z. B. zur Fernwartung).

Für diese Szenarien bietet RAS eine einfache Lösung: der entfernte Benutzer verbindet sich z. B. über das Telefonnetz mit Hilfe eines Modems mit dem Firmennetz. Diese Direktverbindung kann solange wie nötig bestehen bleiben und als Standleitung angesehen werden, die nur bei Bedarf geschaltet wird.

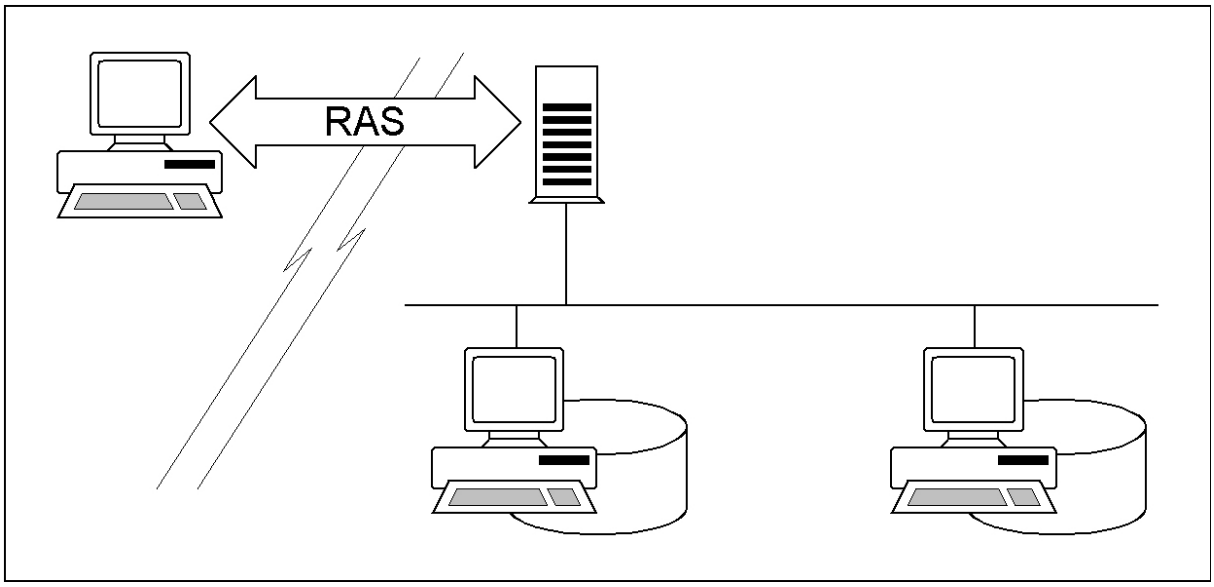


Abbildung: Entfernter Zugriff auf Ressourcen

Damit eine RAS-Verbindung aufgebaut werden kann, werden in der Regel drei Komponenten benötigt:

1. ein Rechner mit RAS-Software im Firmennetz, der bereit ist, RAS-Verbindungen entgegenzunehmen - der so genannte RAS-Server oder Zugangsserver (engl. Access-Server),
2. ein entfernter Rechner mit RAS-Software, der die RAS-Verbindung initiiert - der so genannte RAS-Client - und
3. das Kommunikationsmedium, über das die RAS-Verbindung aufgebaut wird. In den meisten Szenarien nutzt der RAS-Client ein Telekommunikationsnetz zur Verbindungsaufnahme. Es wirddaher mindestens ein Telefonanschluss und ein entsprechendes Modem benötigt. Je nach RAS-Architektur kommen serverseitig unterschiedliche Anbindungstechniken zum Einsatz.

Der RAS-Dienst ist als Client-Server-Architektur realisiert: Der RAS-Client kann so konfiguriert werden, dass er die RAS-Verbindung automatisch aufbaut, wenn Ressourcen des Firmennetzes benötigt werden. Dies geschieht dadurch, dass er die Telefonnummer des Rechners anwählt, auf dem die RAS-Server-Software installiert ist. Alternativ kann die RAS-Verbindung auch "von Hand" vom Benutzer initiiert werden. Einige Betriebssysteme erlauben auch das Aktivieren des RAS-Dienstes schon bei der Systemanmeldung, beispielsweise Windows NT.

Für die Verbindungsaufnahme zum entfernten LAN kommen im Wesentlichen zwei Verfahren zum Einsatz (siehe Maßnahme M 2.185 *Auswahl einer geeigneten RAS-Systemarchitektur*):

- das direkte Anwählen des Zugangsservers, der in diesem Fall Teil des entfernten LANs ist,
- das Anwählen eines Zugangsservers eines Internetdienstanbieters (Internet Service Provider - ISP) und Zugang zum entfernten LAN über das Internet.

Unter dem Gesichtspunkt der Sicherheit sind für RAS-Zugänge folgende Sicherheitsziele zu unterscheiden:

1. Zugangssicherheit: Der entfernte Benutzer muss durch das RAS-System eindeutig zu identifizieren sein. Die Identität des Benutzers muss durch einen Authentisierungsmechanismus bei jedem Verbindungsaufbau zum lokalen Netz sichergestellt werden. Im Rahmen des Systemzugangs müssen weitere Kontrollmechanismen angewandt werden, um den Systemzugang für entfernte Benutzer reglementieren zu können (z. B. zeitliche Beschränkungen oder Einschränkung auf erlaubte entfernte Verbindungspunkte).
2. Zugriffskontrolle: Ist der entfernte Benutzer authentisiert, so muss das System in der Lage sein, die entfernten Zugriffe des Benutzers auch zu kontrollieren. Dazu müssen die Berechtigungen und Einschränkungen, die für lokale Netzressourcen durch befugte Administratoren festgelegt wurden, auch für den entfernten Benutzer durchgesetzt werden.
3. Kommunikationssicherheit: Bei einem entfernten Zugriff auf lokale Ressourcen sollen im Allgemeinen auch über die aufgebaute RAS-Verbindung Nutzdaten übertragen werden. Generell sollen auch für Daten, die über RAS-Verbindungen übertragen werden, die im lokalen Netz geltenden Sicherheitsanforderungen bezüglich Kommunikationsabsicherung (Vertraulichkeit, Integrität, Authentizität) durchsetzbar sein. Der Absicherung der RAS-Kommunikation kommt jedoch eine besondere Bedeutung zu, da zur Abwicklung der Kommunikation verschiedene Kommunikationsmedien in Frage kommen, die in der Regel nicht dem Hoheitsbereich des Betreibers des lokalen Netzes zuzurechnen sind.
4. Verfügbarkeit: Wird der RAS-Zugang im produktiven Betrieb genutzt, so ist die Verfügbarkeit des RAS-Zugangs von besonderer Bedeutung. Der reibungslose Ablauf von Geschäftsprozessen kann bei Totalausfall des RAS-Zugangs oder bei Verbindungen mit nicht ausreichender Bandbreite unter Umständen beeinträchtigt werden. Durch die Nutzung von alternativen oder redundanten RAS-

Zugängen kann diese Gefahr bis zu einem gewissen Grad verringert werden. Dies gilt insbesondere für RAS-Zugänge, die das Internet als Kommunikationsmedium nutzen, da hier in der Regel keine Verbindungs- oder Bandbreitengarantien gegeben werden.

Gefährdungslage

Durch die Client-Server-Architektur von RAS-Systemen ergeben sich für RAS-Client und RAS-Server jeweils spezifische Gefahren durch die Art des Einsatzumfeldes und die Nutzungsweise.

- RAS-Clients können stationär (heimischer PC), aber auch mobil (Laptop) verwendet werden. In der Regel unterliegt der Client-Standort jedoch nicht der Kontrolle des LAN-Betreibers, so dass insbesondere für den mobilen Einsatz von einem unsicheren Umfeld mit spezifischen Gefährdungen ausgegangen werden muss. Hier müssen insbesondere auch physische Gefahren (Diebstahl, Beschädigung, usw.) in Betracht gezogen werden. Hierzu können auch die Bausteine B 2.8 *Häuslicher Arbeitsplatz*, B 3.203 *Laptop* und B 5.8 *Telearbeit* betrachtet werden.

  RAS-Server sind in der Regel Teil des LANs, mit dem sich entfernte Benutzer verbinden wollen. Sie sind im Hoheits- und Kontrollbereich des LAN-Betreibers angesiedelt und können damit durch die lokal geltenden Sicherheitsvorschriften erfasst werden. Da die Hauptaufgabe des RAS-Servers darin besteht, nur berechtigten Benutzern den Zugriff auf das angeschlossene LAN zu gewähren, sind die Gefahren für RAS-Server eher im Bereich von Angriffen zu sehen, die den unberechtigten Zugang zum LAN zum Ziel haben.

Von einer vollständig getrennten Betrachtung der Client- und Server-seitigen Gefährdungen soll an dieser Stelle abgesehen werden, da sich z. B. durch die Gefahr der Kompromittierung eines RAS-Clients automatisch eine Gefährdung für den RAS-Server ergibt. Ferner ist zu bedenken, dass sich z. B. im Windows-Umfeld jeder RAS-Client auch als RAS-Server betreiben lässt, so dass sich hier die Gefährdungen kumulieren.

Für den IT-Grundschutz eines RAS-Systems werden die folgenden typischen Gefährdungen angenommen:

Höhere Gewalt
- G 1.2 Ausfall des IT-Systems

Organisatorische Mängel:
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.16 Ungeordneter Benutzerwechsel bei tragbaren PCs
- G 2.19 Unzureichendes Schlüsselmanagement bei Verschlüsselung
- G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindungen
- G 2.44 Inkompatible aktive und passive Netzkomponenten
- G 2.64 Fehlende Regelungen für das RAS-System

Menschliche Fehlhandlungen:
- G 3.39 Fehlerhafte Administration des RAS-Systems
- G 3.40 Ungeeignete Nutzung von Authentisierungsdiensten bei Remote Access
- G 3.41 Fehlverhalten bei der Nutzung von RAS-Diensten
- G 3.42 Unsichere Konfiguration der RAS-Clients
- G 3.43 Ungeeigneter Umgang mit Passwörtern
- G 3.44 Sorglosigkeit im Umgang mit Informationen

Technisches Versagen:
- G 4.35 Unsichere kryptographische Algorithmen
- G 4.40 Ungeeignete Ausrüstung der Betriebsumgebung des RAS-Clients

Vorsätzliche Handlungen:

- G 5.7 Abhören von Leitungen
- G 5.8 Manipulation an Leitungen
- G 5.22 Diebstahl bei mobiler Nutzung des IT-Systems
- G 5.39 Eindringen in Rechnersysteme über Kommunikationskarten
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.83 Kompromittierung kryptographischer Schlüssel
- G 5.91 Abschalten von Sicherheitsmechanismen für den RAS-Zugang
- G 5.92 Nutzung des RAS-Clients als RAS-Server
- G 5.93 Erlauben von Fremdnutzung von RAS-Komponenten

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Ein RAS-System besteht aus mehreren Komponenten, die zunächst als Einzelkomponenten abgesichert werden sollten. Jenseits der RAS-Funktionalität sind diese als normale IT-Systeme oder Netzkoppelelemente anzusehen und sollten gemäß der Maßnahmenvorschläge aus den entsprechenden Bausteinen abgesichert werden. RAS-Server sind Rechner, die sich üblicherweise im Hoheitsgebiet eines Unternehmens oder einer Behörde befinden, und nehmen die wichtige Aufgabe wahr, den Zugriff auf das interne Netz zu kontrollieren. Die RAS-Funktionalität ist in der Regel auf einem Betriebssystem aufgesetzt, das in den meisten Fällen weitere Dienste anbietet. Daher hängt die Sicherheit des RAS-Zuganges auch davon ab, dass auch auf Betriebssystem- und Dienstebene keine Sicherheitslücken existieren.

Zusätzlich zu der Absicherung der RAS-Systemkomponenten muss jedoch auch ein RAS-Sicherheitskonzept erstellt werden, das sich in das bestehende Sicherheitskonzept eingliedert: das RAS-System muss einerseits bestehende Sicherheitsforderungen umsetzen und erfordert andererseits das Aufstellen neuer, RAS-spezifischer Sicherheitsregeln.

Ein RAS-System wird in der Regel im Umfeld anderer Systeme eingesetzt, die dazu dienen, den Zugriff auf das interne Netz von außen zu kontrollieren. Hier sind z. B. Firewall-Systeme oder Systeme zur Fernwartung zu nennen, mit denen ein RAS-System im Verbund zusammenarbeiten muss. Aus diesem Grund sind bei der Durchführung der RAS-spezifischen Maßnahmen auch die Maßnahmen aus den jeweiligen Bausteinen der betroffenen Systeme zu berücksichtigen. Zu nennen sind u. a. die Bausteine:

- B 2.8 *Häuslicher Arbeitsplatz*
- B 3.301 *Sicherheitsgateway (Firewall)*
- B 3.401 *TK-Anlage*
- B 5.8 *Telearbeit*

Für den sicheren Aufbau eines RAS-Zuganges sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

1. Begonnen wird mit dem Erstellen eines RAS-Konzeptes, das auf den Sicherheitsanforderungen für die bereits vorhandenen IT-Systeme sowie den Anforderungen aus den geplanten Einsatzszenarien für Remote Access beruht.

1.1 Um das Konzept individuell zuschneiden zu können, müssen zunächst die Anforderungen festgestellt werden. Dazu ist eine Anforderungsanalyse (siehe M 2.183 *Durchführung einer RAS-Anforderungsanalyse*) durchzuführen.

1.2 Aufgrund der festgestellten Anforderungen kann dann die Definition eines RAS-Konzeptes (siehe M 2.184 *Entwicklung eines RAS-Konzeptes*) erfolgen.

1.3 Zur Umsetzung des Konzeptes ist eine RAS-Systemarchitektur zu definieren (siehe M 2.185 *Auswahl einer geeigneten RAS-Systemarchitektur*), die auf die Anforderungen des RAS-Einsatzes und das umzusetzende Konzept abgestimmt ist.

2. Die Beschaffung des RAS-Systems erfordert, die aus dem RAS-Konzept resultierenden Anforderungen an das RAS-Produkt zu formulieren und basierend darauf die Auswahl eines geeigneten RAS-Produktes zu treffen (siehe M 2.186 *Geeignete Auswahl eines RAS-Produktes*).

3. Die sicherheitsrelevanten Maßnahmen für die Umsetzung des RAS-Konzepts untergliedern sich in die Bereiche:

3.1 Definition der Sicherheitsrichtlinie für den RAS-Einsatz (siehe M 2.187 *Festlegen einer RAS-Sicherheitsrichtlinie*),

3.2 Installation und erste Konfiguration (siehe M 4.110 *Sichere Installation des RAS-Systems* und M 4.111 *Sichere Konfiguration des RAS-Systems*) und

3.3 den laufenden Betrieb des RAS-Systems (siehe M 4.112 *Sicherer Betrieb des RAS-Systems*).
Typischerweise muss für RAS-Systeme immer eine Betrachtung von RAS-Servern und RAS-Clients erfolgen. Da die Benutzer eines RAS-Systems wesentlich zu dessen sicheren Betrieb beitragen, müssen sie auf die Nutzung des RAS-Zugangs vorbereitet werden und den Umgang mit der RAS-Software erlernen. Hier muss insbesondere auf die Gefahren aufmerksam gemacht werden, die sich bei der Nutzung des RAS-Zugangs von zu Hause oder von unterwegs ergeben (siehe M 3.4 *Schulung vor Programmnutzung* und M 3.5 *Schulung zu IT-Sicherheitsmaßnahmen*).
Zur Absicherung von RAS-Verbindungen werden in vielen Fällen so genannte Tunnel-Protokolle eingesetzt. Diese erlauben es, aufbauend auf einer bestehenden Verbindung einen durch Zugriffskontrolle und Verschlüsselung abgeschotteten Kommunikationskanal zwischen IT-Systemen oder Netzen herzustellen. Aufgrund dieser Abschottung gegen die Außenwelt wird hier auch häufig von Virtuellen Privaten Netzen (VPN) gesprochen (siehe M 5.76 *Einsatz geeigneter Tunnel-Protokolle für die RAS-Kommunikation*).

Nachfolgend wird das Maßnahmenbündel für den Baustein "Remote Access" vorgestellt.

Planung und Konzeption

- M 2.183 (A) Durchführung einer RAS-Anforderungsanalyse
- M 2.184 (A) Entwicklung eines RAS-Konzeptes
- M 2.185 (A) Auswahl einer geeigneten RAS-Systemarchitektur
- M 2.187 (A) Festlegen einer RAS-Sicherheitsrichtlinie
- M 2.205 (A) Übertragung und Abruf personenbezogener Daten
- M 4.113 (Z) Nutzung eines Authentisierungsservers beim RAS-Einsatz
- M 5.76 (Z) Einsatz geeigneter Tunnel-Protokolle für die RAS-Kommunikation

Beschaffung

- M 2.186 (A) Geeignete Auswahl eines RAS-Produktes

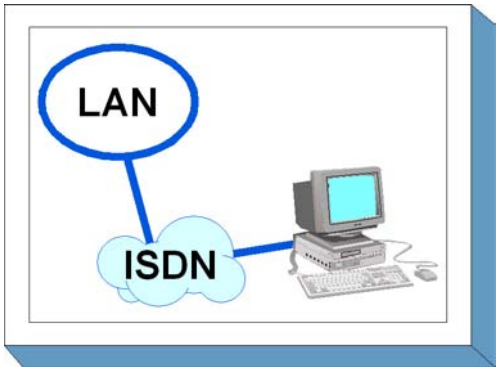
Umsetzung
- M 4.110 (A) Sichere Installation des RAS-Systems
- M 4.111 (A) Sichere Konfiguration des RAS-Systems

Betrieb
- M 4.112 (A) Sicherer Betrieb des RAS-Systems

Aussonderung
- M 4.233 (B) Sperrung nicht mehr benötigter RAS-Zugänge

Notfallvorsorge
- M 6.70 (B) Erstellen eines Notfallplans für den Ausfall des RAS-Systems
- M 6.71 (B) Datensicherung bei mobiler Nutzung des IT-Systems

B 4.5 LAN-Anbindung eines IT-Systems über ISDN



Beschreibung

ISDN (Integrated Services Digital Network) ist ein digitales Telekommunikationsnetz, über das verschiedene Dienste, wie Telefon und Telefax, genutzt sowie Daten und Bilder übertragen werden können.

In diesem Kapitel wird die Anbindung eines abgesetzten IT-Systems an ein lokales Netz über ein öffentliches ISDN-Netz betrachtet. Hierbei erfolgt die Anbindung auf Seiten des abgesetzten IT-Systems mittels einer ISDN-Adapterkarte mit S0-Schnittstelle. Die Anbindung des LAN wird über einen Router hergestellt, der über eine S2M-Schnittstelle mit einem öffentlichen ISDN-Netz verbunden ist.

Diese Form der Anbindung eines entfernt stehenden IT-Systems kommt typischerweise für die Anbindung von Telearbeitsplätzen in Betracht.

Gefährdungslage

Für den Grundschutz werden die folgenden Gefährdungen als typisch für die LAN-Anbindung eines IT-Systems über ISDN angenommen:

Höhere Gewalt:
- G 1.2 Ausfall des IT-Systems

Organisatorische Mängel:
- G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- G 2.19 Unzureichendes Schlüsselmanagement bei Verschlüsselung
- G 2.22 Fehlende Auswertung von Protokolldaten
- G 2.24 Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
- G 2.32 Unzureichende Leitungskapazitäten
- G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindungen

Menschliche Fehlhandlungen:
- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.13 Übertragung falscher oder nicht gewünschter Datensätze
- G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten

Technisches Versagen:
- G 4.6 Spannungsschwankungen/Überspannung/Unterspannung
- G 4.25 Nicht getrennte Verbindungen

Vorsätzliche Handlungen:
- G 5.2 Manipulation an Daten oder Software
- G 5.7 Abhören von Leitungen
- G 5.8 Manipulation an Leitungen
- G 5.9 Unberechtigte IT-Nutzung
- G 5.10 Missbrauch von Fernwartungszugängen
- G 5.14 Gebührenbetrug

- G 5.16 Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal
- G 5.17 Gefährdung bei Wartungsarbeiten durch externes Personal
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.25 Maskerade
- G 5.39 Eindringen in Rechnersysteme über Kommunikationskarten
- G 5.48 IP-Spoofing
- G 5.61 Missbrauch von Remote-Zugängen für Managementfunktionen von Routern
- G 5.62 Missbrauch von Ressourcen über abgesetzte IT-Systeme
- G 5.63 Manipulationen über den ISDN-D-Kanal

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

In diesem Kapitel steht die Gewährleistung einer sicheren Kommunikation im Vordergrund. Die für die kommunizierenden IT-Systeme weiterhin erforderlichen Maßnahmen sind den jeweiligen Bausteinen zu entnehmen.

Für die LAN-Anbindung eines IT-Systems über ISDN sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption über die Beschaffung bis hin zum laufenden Betrieb. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Die sichere Nutzung von Fernzugriff auf IT-Systeme erfordert die Beachtung einer Reihe von Maßnahmen zum Schutz der Kommunikation (siehe Maßnahme M 5.32 *Sicherer Einsatz von Kommunikationssoftware*).

Beschaffung

Die Maßnahme M 2.106 *Auswahl geeigneter ISDN-Karten in der Beschaffung* nennt eine Reihe wichtiger Kriterien, die bei der Auswahl von ISDN-Karten zu beachten sind.

Umsetzung

Bei der Installation des ISDN-Zugangs ist nach der Grundregel zu verfahren, dass alle nicht benötigten Dienste und Funktionalitäten abzuschalten sind, weil sie nur unnötige Risiken mit sich bringen. Die tatsächlich genutzten Funktionen sind durch geeignete Konfiguration so gut wie möglich abzusichern, wozu unbedingt auch die sofortige Änderung eventueller vom Hersteller vorgegebener Passwörter gehört. Die vorgesehene Konfiguration ist zu dokumentieren, und diese Dokumentation ist bei Änderungen zu aktualisieren.

Ein wesentlicher Aspekt bei der Installation eines ISDN-Zugangs ist noch, dass hierdurch die vorhandene Sicherheit eines Rechnernetzes nicht unterlaufen werden darf. Insbesondere darf hierdurch auf keinen Fall eine Verbindung mit externen Netzen entstehen, die ein vorhandenes Firewall-System überbrückt und damit weitestgehend unwirksam macht.

Betrieb

Durch regelmäßige Kontrollen der erzeugten Protokolldateien lässt sich ein eventueller Missbrauch der ISDN-Verbindung leichter aufdecken. Eine gelegentliche Kontrolle programmierter Zieladressen und Protokolle hilft zu vermeiden, dass versehentlich Verbindungen mit einem falschen Kommunikationspartner aufgebaut werden.

Nachfolgend wird das Maßnahmenbündel für den Bereich LAN-Anbindung eines IT-Systems über ISDN vorgestellt.

Planung und Konzeption

- M 1.25 (B) Überspannungsschutz
- M 2.42 (A) Festlegung der möglichen Kommunikationspartner
- M 2.46 (Z) Geeignetes Schlüsselmanagement
- M 2.108 (Z) Verzicht auf Fernwartung der ISDN-Netzkoppelelemente
- M 4.34 (Z) Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
- M 4.62 (Z) Einsatz eines D-Kanal-Filters
- M 5.32 (A) Sicherer Einsatz von Kommunikationssoftware
- M 5.47 (Z) Einrichten einer Closed User Group

Beschaffung

- M 2.106 (A) Auswahl geeigneter ISDN-Karten in der Beschaffung

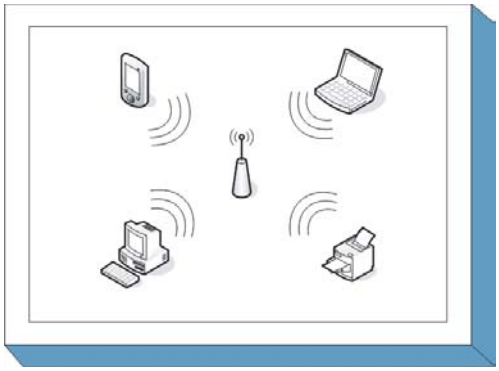
Umsetzung

- M 1.43 (A) Gesicherte Aufstellung aktiver Netzkomponenten
- M 2.107 (A) Dokumentation der ISDN-Karten-Konfiguration
- M 2.109 (A) Rechtevergabe für den Fernzugriff
- M 2.204 (A) Verhinderung ungesicherter Netzzugänge
- M 4.7 (A) Änderung voreingestellter Passwörter
- M 4.59 (A) Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten
- M 4.60 (A) Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten
- M 4.61 (A) Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten
- M 5.48 (A) Authentisierung mittels CLIP/COLP
- M 5.49 (A) Callback basierend auf CLIP/COLP
- M 5.50 (A) Authentisierung mittels PAP/CHAP

Betrieb

- M 2.64 (A) Kontrolle der Protokolldateien
- M 5.29 (C) Gelegentliche Kontrolle programmierter Zieladressen und Protokolle

B 4.6 WLAN



Beschreibung

Wireless LANs (WLANs) bieten die Möglichkeit, mit geringem Aufwand drahtlose lokale Netze aufzubauen oder bestehende drahtgebundene Netze zu erweitern. Mit WLAN werden hier drahtlose Netze bezeichnet, die auf der als IEEE 802.11 bezeichneten Gruppe von Standards basieren, die vom Institute of Electrical and Electronics Engineers (IEEE) spezifiziert wurden.

Aufgrund der einfachen Installation werden WLANs auch für temporär zu installierende Netze, wie z. B. auf Messen oder kleineren Veranstaltungen, verwendet. Darüber hinaus besteht die Möglichkeit, an öffentlichen Plätzen wie Flughäfen oder Bahnhöfen Netzzugänge über so genannte Hotspots anzubieten. Dadurch wird den mobilen Benutzern Verbindungen in das Internet oder in ihr Firmennetz ermöglicht. Die Kommunikation findet dann generell zwischen einem zentralen Zugangspunkt, dem Access Point, und der WLAN-Komponente des mobilen Endgeräts (z. B. über einen WLAN-USB-Stick oder entsprechende WLAN Netzkarte) statt.

Die Mehrzahl der derzeit am Markt verfügbaren WLAN Komponenten basieren auf der 2003 vom IEEE verabschiedeten Erweiterung 802.11g, die eine Übertragungsgeschwindigkeit von bis zu 54 Mbit/s definiert. Darüber hinaus gibt es einige Systeme, die nur die 1999 veröffentlichte Erweiterung IEEE 802.11b unterstützen, mit der bis zu 11 Mbit/s erreicht werden können. Beide Erweiterungen funken dabei im lizenzfreien 2,4 GHz Frequenzbereich.

Die Sicherheitsmechanismen sind im Standard IEEE 802.11 und in der Erweiterung IEEE 802.11i definiert. Im ursprünglichen Standard 802.11 ist Wired Equivalent Privacy (WEP) als Sicherheitsmechanismus definiert, WEP kann jedoch aufgrund mehrerer Schwachstellen nicht mehr als ausreichend sicher eingestufet werden. Aus diesem Grund entwickelte die Hersteller-Vereinigung WiFi-Alliance den Sicherheitsmechanismus Wi-Fi Protected Access (WPA). Hierbei wird neben einer Erweiterung der statischen Schlüssel, den sogenannten Pre-Shared Keys, auch eine dynamische Schlüsselverwaltung mittels TKIP eingeführt. Diese Mechanismen wurden in großen Teilen in die 2004 veröffentlichte offizielle Erweiterung IEEE 802.11i integriert, wobei dort, wie auch bei WPA2, der Advanced Encryption Standard (AES) zur Verschlüsselung verwendet wird, anstelle von RC4 bei WEP und WPA. Weiterhin ist in IEEE 802.11i das Counter Mode with CBC-MAC Protocol (CCMP) als Implementierungsmethode für AES zur Verschlüsselung und Integritätsprüfung definiert. Dieses Verfahren ist langfristig tragbar, erfordert aber im Gegensatz zu der TKIP-Variante neue Hardware. Als Authentisierungsmethode definiert die Erweiterung 802.11i das Extensible Authentication Protocol (EAP) gemäß dem Standard IEEE 802.1X. Weitere technische Hinweise zum sicheren Einsatz von WLAN ist beispielsweise in der Technischen Richtlinie *Sicheres WLAN* des BSI nachzulesen.

In diesem Baustein soll ein systematischer Weg aufgezeigt werden, wie ein Konzept zum Einsatz von WLANs innerhalb einer Institution erstellt und wie deren Umsetzung und Einbettung sichergestellt werden kann.

Gefährdungslage

Für den IT-Grundschutz werden im Rahmen der Nutzung von WLANs folgende typische Gefährdungen angenommen:

Höhere Gewalt:

- G 1.17 Ausfall oder Störung eines Funknetzes

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.117 Fehlende oder unzureichende Planung des WLAN-Einsatzes
- G 2.118 Unzureichende Regelungen zum WLAN-Einsatz
- G 2.119 Ungeeignete Auswahl von WLAN-Authentikationsverfahren
- G 2.120 Ungeeignete Aufstellung von sicherheitsrelevanten IT-Systemen
- G 2.121 Unzureichende Kontrolle von WLANs

Menschliche Fehlhandlungen:
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.38 Konfigurations- und Bedienungsfehler
- G 3.43 Ungeeigneter Umgang mit Passwörtern
- G 3.84 Fehlerhafte Konfiguration der WLAN-Infrastruktur

Technisches Versagen:
- G 4.60 Unkontrollierte Ausbreitung der Funkwellen
- G 4.61 Unzuverlässige oder fehlende WLAN-Sicherheitsmechanismen

Vorsätzliche Handlungen:
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.137 Auswertung von Verbindungsdaten bei der drahtlosen Kommunikation
- G 5.138 Angriffe auf WLAN-Komponenten
- G 5.139 Abhören der WLAN-Kommunikation

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz

Im Rahmen des WLAN-Einsatzes sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Beschaffung bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Planung und Konzeption

Die Absicherung eines WLANs beginnt bereits in der Planungsphase. Nur durch eine durchdachte Strategie (siehe M 2.381 *Festlegung einer Strategie für die WLAN-Nutzung*) und die Auswahl des richtigen WLAN-Standards und den damit verbundenen Kryptoverfahren (siehe M 2.383 *Auswahl eines geeigneten WLAN-Standards* und M 2.384 *Auswahl geeigneter Kryptoverfahren für WLAN*) ist bereits der Grundstein für ein sicheres WLAN gelegt. Die Maßnahme M 3.58 *Einführung in WLAN-Grundbegriffe* hilft dabei, sich in der Begriffswelt für die Absicherung eines WLANs zurechtzufinden.

Alle getroffenen Entscheidungen über Sicherheitseinstellungen, ausgewählten WLAN-Standards, sowie die Regelungen für die Nutzung und Administration des WLANs, sind in einer WLAN-Sicherheitsrichtlinie niederzuschreiben (siehe M 2.382 *Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung*).

Beschaffung

Bei der Auswahl der WLAN-Komponenten ist die Maßnahme M 2.385 *Geeignete Auswahl von WLAN-Komponenten* anzuwenden. WLANs unterliegen einem schnellen Wandel bei Standards, Protokollen und Sicherheitsmechanismen. Daher befinden sich WLANs häufig in der Migration.

Für solche Migrationsphasen einzelner WLAN-Komponenten oder ganzer WLAN-Bereiche ist die Maßnahme M 2.386 *Sorgfältige Planung notwendiger WLAN-Migrationsschritte* zu beachten.

Umsetzung

Sind alle Komponenten beschafft und geht es um die Einrichtung des WLANs, so ist es nicht unerheblich, an welcher Stelle die Access Points positioniert werden (siehe M 1.63 *Geeignete Aufstellung von Access Points*) oder wie das WLAN mit der eventuell bereits vorhandenen kabelgebundenen Infrastruktur verbunden wird (siehe M 5.139 *Sichere Anbindung eines WLANs an ein LAN*). Aber auch die Konfiguration der unterschiedlichen WLAN-Komponenten, wie Access Points (siehe M 4.294 *Sichere Konfiguration der Access Points*) oder WLAN-Clients (siehe M 4.295 *Sichere Konfiguration der WLAN-Clients*), ist während der Installation stets gemäß der Sicherheitsrichtlinie und der festgelegten Strategie zu erfolgen.

In jedem Fall sind die Benutzer und Administratoren des WLANs ausreichend zu schulen, um Sicherheitsvorfälle zu minimieren und auf mögliche Gefahren bei einer unsachgemäßen Verwendung des WLANs hinzuweisen und zu sensibilisieren (siehe M 3.59 *Schulung zum sicheren WLAN-Einsatz*).

Sollte das WLAN durch einen externen Dienstleister installiert, konfiguriert bzw. betreut werden, so ist auf jeden Fall die Maßnahme M 2.387 *Installation, Konfiguration und Betreuung eines WLANs durch Dritte* anzuwenden.

Betrieb

Ist das WLAN in Betrieb genommen und wurden alle WLAN-Anwender ausreichend geschult, so ist zum einen durch regelmäßige Audits (siehe M 4.298 *Regelmäßige Audits der WLAN-Komponenten*) sicherzustellen, dass alle getroffenen Sicherheitseinstellungen noch aktuell sind und durch regelmäßig Sicherheitschecks (siehe M 5.141 *Regelmäßige Sicherheitschecks in WLANs*), ob diese Einstellungen auch greifen. Darüber hinaus ist stets ein sicherer Betrieb aller WLAN-Komponenten zu gewährleisten (siehe M 4.297 *Sicherer Betrieb der WLAN-Komponenten*).

Unumgänglich ist ein Schlüsselmanagement für die im WLAN benutzten kryptographischen Schlüssel zur Absicherung der Kommunikation (siehe M 2.388 *Geeignetes WLAN-Schlüsselmanagement*). Eine WLAN-Management-Lösung kann die Verwaltung der Schlüssel erleichtern und das WLAN kann zentral administriert werden (siehe M 4.296 *Einsatz einer geeigneten WLAN-Management-Lösung*).

Aussonderung

Werden WLAN-Komponenten außer Betrieb genommen, so sind entsprechende Konfigurationseinstellungen, wie z. B. Netzname oder SSID, wieder auf Standard-Werte zurückzusetzen und eventuell auf der WLAN-Komponente gespeicherte Informationen zur Absicherung des Netzverkehrs über das WLAN oder Zugangsinformationen zu löschen (siehe M 2.390 *Außerbetriebnahme von WLAN-Komponenten*).

Notfallvorsorge

Wurden Angriffe auf ein WLAN erkannt, so müssen sowohl die Benutzer, als auch die Administratoren des WLANs wissen, wie sie sich zu verhalten haben (siehe M 6.102 *Verhaltensregeln bei WLAN-Sicherheitsvorfällen*). Hieraus ergibt sich ein Notfallplan, welche Schritte notwendig und welche Personen zu informieren sind, wenn ein Sicherheitsvorfall eintritt. Darüber hinaus kann es notwendig sein, ein redundantes WLAN aufzubauen, um schnell einen Ersatz für wichtige Kommunikationsverbindungen zu schaffen. Dabei ist stets darauf zu achten, dass das redundante WLAN denselben Sicherheitsanforderungen wie das normale WLANs entspricht. Für das redundante WLAN sind daher ebenfalls alle Maßnahmen dieses Bausteins anzuwenden, da es als eigenes WLAN zu betrachten ist. Allgemeine Hinweise zu redundanten Kommunikationsverbindungen stehen in der Maßnahme M 6.75 *Redundante Kommunikationsverbindungen*.

Damit WLANs sicher eingesetzt werden können, müssen auch damit gekoppelte Clients sicher konfiguriert sein und regelmäßig gewartet und administriert werden. Geeignete IT-Sicherheitsempfehlungen für Clients sind in den entsprechenden Bausteinen der IT-Grundschutz-Kataloge beschrieben.

Nachfolgend wird das Maßnahmenbündel für den Einsatz von WLANs vorgestellt.

Planung und Konzeption
- M 2.381 (A) Festlegung einer Strategie für die WLAN-Nutzung
- M 2.382 (A) Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung
- M 2.383 (A) Auswahl eines geeigneten WLAN-Standards
- M 2.384 (A) Auswahl geeigneter Kryptoverfahren für WLAN
- M 3.58 (A) Einführung in WLAN-Grundbegriffe
- M 4.293 (Z) Sicherer Betrieb von Hotspots
- M 5.138 (Z) Einsatz von RADIUS-Servern

Beschaffung
- M 2.385 (A) Geeignete Auswahl von WLAN-Komponenten
- M 2.386 (Z) Sorgfältige Planung notwendiger WLAN-Migrationsschritte

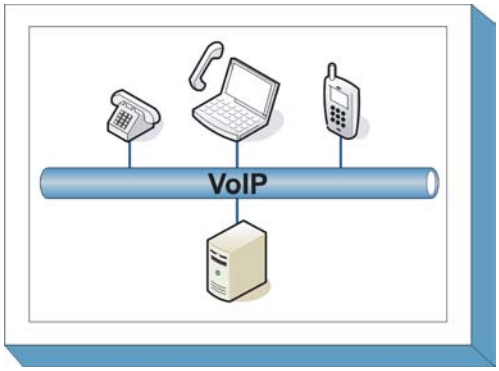
Umsetzung
- M 1.63 (B) Geeignete Aufstellung von Access Points
- M 2.387 (Z) Installation, Konfiguration und Betreuung eines WLANs durch Dritte
- M 3.59 (C) Schulung zum sicheren WLAN-Einsatz
- M 4.294 (A) Sichere Konfiguration der Access Points
- M 4.295 (A) Sichere Konfiguration der WLAN-Clients
- M 5.139 (A) Sichere Anbindung eines WLANs an ein LAN
- M 5.140 (C) Aufbau eines Distribution Systems

Betrieb
- M 2.388 (B) Geeignetes WLAN-Schlüsselmanagement
- M 2.389 (Z) Sichere Nutzung von Hotspots
- M 4.296 (C) Einsatz einer geeigneten WLAN-Management-Lösung
- M 4.297 (A) Sicherer Betrieb der WLAN-Komponenten
- M 4.298 (B) Regelmäßige Audits der WLAN-Komponenten
- M 5.141 (B) Regelmäßige Sicherheitschecks in WLANs

Aussonderung
- M 2.390 (C) Außerbetriebnahme von WLAN-Komponenten

Notfallvorsorge
- M 6.75 (Z) Redundante Kommunikationsverbindungen
- M 6.102 (A) Verhaltensregeln bei WLAN-Sicherheitsvorfällen

B 4.7 VoIP



Für die Übertragung der Signalisierungsinformationen, zum Beispiel bei einem Anruf, werden spezielle Signalisierungsprotokolle eingesetzt. Die eigentlichen Nutzdaten, wie Sprache oder Video, werden mit Hilfe eines Medientransportprotokolls übermittelt. Beide Protokolle werden jeweils für den Aufbau und die Aufrechterhaltung einer Multimediaverbindung benötigt. Bei einigen Technologien wird nur ein Protokoll sowohl für die Signalisierung als auch den Medientransport benötigt.

Dieser Baustein betrachtet die Sicherheitsaspekte der Endgeräte und Vermittlungseinheiten (Middleware). Die hier beschriebenen Komponenten gleichen hinsichtlich ihrer Funktionalität den im Baustein B 3.401 *TK-Anlage* beschriebenen Telekommunikationsanlagen.

Gefährdungslage

Auch beim Einsatz von VoIP sind eine Reihe von Gefährdungen zu berücksichtigen. Viele davon lassen sich auf die Datennetze zurückführen, die für VoIP genutzt werden. Hierzu gehören zahlreiche Angriffe auf die Vertraulichkeit, wie beispielsweise Sniffen, und auf die Verfügbarkeit.

Generell gilt, dass die Gefährdungslage der einzelnen Komponenten immer auch vom Einsatzszenario, beispielsweise der Nutzung als Endgerät oder Middleware, abhängt und diese Einzelgefährdungen auch in die Gefährdung des Gesamtsystems eingehen.

Für den IT-Grundschutz beim Einsatz von VoIP werden folgende Gefährdungen angenommen:

Organisatorische Mängel:
- G 2.112 Unzureichende Planung von VoIP
- G 2.113 Unzureichende Planung der Netzkapazität beim Einsatz von VoIP

Menschliche Fehlhandlungen:
- G 3.7 Ausfall der TK-Anlage durch Fehlbedienung
- G 3.82 Fehlerhafte Konfiguration der VoIP-Middleware
- G 3.83 Fehlerhafte Konfiguration von VoIP-Komponenten

Technisches Versagen:
- G 4.56 Ausfall der VoIP-Architektur
- G 4.57 Störungen beim Einsatz von VoIP über VPNs
- G 4.58 Schwachstellen beim Einsatz von VoIP-Endgeräten
- G 4.59 Nicht-Erreichbarkeit bei VoIP durch NAT

Vorsätzliche Handlungen:
- G 5.11 Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten
- G 5.12 Abhören von Telefongesprächen und Datenübertragungen
- G 5.13 Abhören von Räumen
- G 5.14 Gebührenbetrug
- G 5.15 "Neugierige" Mitarbeiter
- G 5.134 Fehlende Identifizierung zwischen Gesprächsteilnehmern
- G 5.135 SPIT und Vishing
- G 5.136 Missbrauch frei zugänglicher Telefonanschlüsse

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Da VoIP über Datennetze betrieben wird, muss der Baustein B 4.1 *Heterogene Netze* für eine Sicherheitsbetrachtung hinzugezogen werden. Weiterhin sind die im Datennetz befindlichen aktiven Netzkomponenten zu berücksichtigen. Diese werden im Baustein B 3.302 *Router und Switches* betrachtet.

Statt auf Spezialgeräten, sogenannten Appliances, wird VoIP sehr oft auf gewöhnlichen IT-Systemen betrieben. Für den Betrieb einer Middleware-Komponente wird auf dem IT-System ein entsprechender Netzdienst benötigt. Daher ist in diesem Fall der Baustein B 3.101 *Allgemeiner Server* zu berücksichtigten.

Als *Softphone* wird eine client-seitige Software bezeichnet, die es erlaubt, einen Multimedia-PC mit Mikrofon als Telefonie-Endgerät zu nutzen. Wird ein Softphone verwendet, ist auf den beteiligten Client der Baustein B 3.201 *Allgemeiner Client* anzuwenden. Weiterhin muss sowohl bei der Middleware als auch beim Softphone der Baustein für das Betriebssystem, das auf dem jeweiligen IT-System genutzt wird, berücksichtigt werden, beispielsweise B 3.102 *Server unter Unix* beziehungsweise B 3.209 *Client unter Windows XP*.

Für den Einsatz von VoIP sollten im Hinblick auf die IT-Sicherheit folgende Schritte bezüglich der Endgeräte und der Middleware durchlaufen werden:

Planung des Einsatzes von VoIP

Der Einsatz von VoIP muss sorgfältig geplant werden (siehe M 2.372 *Planung des VoIP-Einsatzes*). In der Maßnahme M 3.57 *Szenarien für den Einsatz von VoIP* werden mögliche Einsatzbereiche von VoIP vorgestellt. Die Auswahl eines Signalisierungsprotokolls spielt eine wichtige Rolle, weil die verschiedenen Hersteller von VoIP-Geräten oft nur ein Protokoll unterstützen. Da die Signalisierungsprotokolle untereinander nicht kompatibel sind, beeinflusst die Entscheidung für ein Signalisierungsprotokoll die Auswahl der VoIP-Komponenten. In der Maßnahme M 5.133 *Auswahl eines VoIP-Signalisierungsprotokolls* werden die verbreitesten Protokolle skizziert.

Beim Telefonieren über VoIP können die gleichen Probleme wie bei jeder anderen Kommunikation über IP auftreten. Viele der von IP-Datennetzen bekannten Angriffe auf die Vertraulichkeit und Integrität können direkt für VoIP übernommen werden. Schutz hiergegen bietet unter anderem eine Verschlüsselung der Signalisierungs- oder Medientransportinformationen. Welche Inhalte in welchen Netzen geschützt werden sollten, verdeutlicht die Maßnahme M 2.374 *Umfang der Verschlüsselung von VoIP*. Die Maßnahmen M 5.134 *Sichere Signalisierung bei VoIP* und M 5.135 *Sicherer Medientransport mit SRTP* vertiefen die Funktionsweise der Verschlüsselung für Signalisierungs- und Medientransportinformationen.

Parallel dazu ist die allgemeine Sicherheitsrichtlinie um eine detaillierte Richtlinie für den Einsatz von VoIP zu ergänzen (siehe M 2.373 *Erstellung einer Sicherheitsrichtlinie für VoIP*).

Beschaffung

Im nächsten Schritt sollte die Beschaffung der Endgeräte und der VoIP-Middleware erfolgen. Dabei können Softwarelösungen oder Appliances eingesetzt werden. Aufbauend auf die Einsatzszenarien sind die Anforderungen an die zu beschaffenden Produkte zu formulieren und basierend darauf die Auswahl der geeigneten Produkte zu treffen. In der Maßnahme M 2.375 *Geeignete Auswahl von VoIP-Systemen* sind Empfehlungen für die Auswahl zu finden.

Umsetzung

Um auf die Einführung oder den Umstieg auf VoIP vorbereitet zu sein, sollten die Administratoren ausreichend geschult werden (siehe M 3.56 *Schulung der Administratoren für die Nutzung von VoIP*).

Neben VoIP-spezifischen Änderungen muss oft das bestehende IP-Datennetz angepasst werden. In einigen Fällen bietet es sich an, zwei Datennetze parallel zu betreiben. Die nicht immer unproblematisch Trennung des VoIP-Sprachnetzes vom restlichen Datennetz, die in M 2.376 *Trennung des Daten- und VoIP-Netzes* beschrieben wird, kann durch logische oder physikalische Segmentierung erfolgen. Daneben sollte auch der Zugriff auf die VoIP-Komponenten abgesichert werden (siehe Maßnahme M 4.289 *Einschränkung der Erreichbarkeit über VoIP*). Falls keine physische Trennung erfolgt, sollten Regelungen für die priorisierte Weiterleitung von VoIP-Paketen getroffen werden, um einer Netzüberlastung vorzubeugen. Diese werden unter anderem in der Maßnahme M 5.136 *Dienstgüte und Netzmanagement bei VoIP* vorgestellt.

Besonders für die Erreichbarkeit aus einem öffentlichen Netz müssen Vorkehrungen getroffen werden. Diese betrifft unter anderem die Anpassung des Übergangs zwischen dem öffentlichen und privaten Netz. Beispielsweise kann die Übersetzung von privaten IP-Adressen in öffentliche IP-Adressen über Network Adress Translation (NAT) sehr aufwendig sein (siehe Maßnahme M 5.137 *Einsatz von NAT für VoIP*). Aber auch für den Sicherheitsgateway gelten besondere Voraussetzungen, die in Maßnahme M 4.290 *Anforderungen an ein Sicherheitsgateway für den Einsatz von VoIP* beschrieben sind.

Betrieb

Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen, siehe die Maßnahmen M 4.287 *Sichere Administration der VoIP-Middleware* und M 4.288 *Sichere Administration von VoIP-Endgeräten*. Um auf Probleme reagieren zu können, müssen wichtige Ereignisse protokolliert und ausgewertet werden. Empfehlungen hierfür sind in Maßnahme M 4.292 *Protokollierung bei VoIP* zu finden.

Eine Benutzer-Schulung über die Benutzung eines Telefons ist oft nicht wirtschaftlich und sinnvoll, auch wenn typische Büro-Endgeräte heutzutage hochkomplex sind. Dennoch sollten die Anwender über grundlegende Gefährdungen informiert werden, siehe hierzu die Maßnahmen M 3.12 *Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne* und M 3.13 *Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen*.

Aussonderung

Sehr oft sind im Speicher der VoIP-Komponenten schutzbedürftige Informationen abgelegt. Bei der Entsorgung der Komponenten sollte die Maßnahme M 2.377 *Sichere Außerbetriebnahme von VoIP-Komponenten* berücksichtigt werden.

Notfallvorsorge

Nur eine regelmäßige und umfassende Datensicherung gewährleistet zuverlässig, dass alle gespeicherten Daten auch im Falle von Störungen, Ausfällen der Hardware oder (absichtlichen oder unabsichtlichen) Löschungen wieder verfügbar gemacht werden können. Die notwendigen Maßnahmen sind im Baustein B 1.4 *Datensicherungskonzept* beschrieben. Darüber hinaus sollte das Datensicherungskonzept um die Datensicherung der VoIP-Komponeten, wie sie in Maßnahme M 6.101 *Datensicherung bei VoIP* beschrieben ist, erweitert werden.

Einige Hinweise zu besonderen Aspekten, die bei der Notfallvorsorge für einen VoIP-Server beachtet werden sollten, sind in Maßnahme M 6.100 *Erstellung eines Notfallplans für den Ausfall von VoIP* beschrieben.

Für den Einsatz von VoIP sind folgende Maßnahmen umzusetzen:

Planung und Konzeption
- M 2.28 (Z) Bereitstellung externer TK-Beratungskapazität
- M 2.372 (A) Planung des VoIP-Einsatzes
- M 2.373 (A) Erstellung einer Sicherheitsrichtlinie für VoIP
- M 2.374 (C) Umfang der Verschlüsselung von VoIP
- M 3.57 (Z) Szenarien für den Einsatz von VoIP
- M 5.133 (A) Auswahl eines VoIP-Signalisierungsprotokolls
- M 5.134 (C) Sichere Signalisierung bei VoIP
- M 5.135 (C) Sicherer Medientransport mit SRTP

Beschaffung
- M 2.375 (A) Geeignete Auswahl von VoIP-Systemen

Umsetzung
- M 1.30 (A) Absicherung der Datenträger mit TK-Gebührendaten
- M 2.29 (B) Bedienungsanleitung der TK-Anlage für die Benutzer
- M 2.376 (C) Trennung des Daten- und VoIP-Netzes
- M 3.56 (A) Schulung der Administratoren für die Nutzung von VoIP
- M 4.287 (A) Sichere Administration der VoIP-Middleware
- M 4.288 (A) Sichere Administration von VoIP-Endgeräten
- M 4.289 (A) Einschränkung der Erreichbarkeit über VoIP
- M 4.290 (C) Anforderungen an ein Sicherheitsgateway für den Einsatz von VoIP
- M 5.136 (B) Dienstgüte und Netzmanagement bei VoIP
- M 5.137 (C) Einsatz von NAT für VoIP

Betrieb
- M 3.12 (B) Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne
- M 3.13 (B) Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen
- M 4.5 (B) Protokollierung der TK-Administrationsarbeiten
- M 4.6 (C) Revision der TK-Anlagenkonfiguration
- M 4.7 (A) Änderung voreingestellter Passwörter
- M 4.10 (Z) Passwortschutz für TK-Endgeräte
- M 4.291 (A) Sichere Konfiguration der VoIP-Middleware
- M 4.292 (A) Protokollierung bei VoIP

Aussonderung
- M 2.377 (B) Sichere Außerbetriebnahme von VoIP-Komponenten

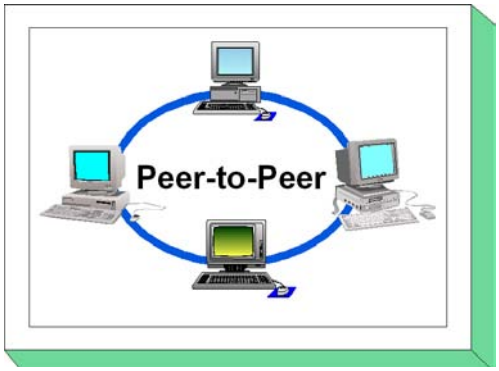
Notfallvorsorge:
- M 6.29 (Z) TK-Basisanschluss für Notrufe
- M 6.100 (A) Erstellung eines Notfallplans für den Ausfall von VoIP
- M 6.101 (A) Datensicherung bei VoIP

5 IT-Anwendungen

In der Schicht IT-Anwendungen sind folgende Bausteine enthalten:

B 5.1 Peer-to-Peer-Dienste
B 5.2 Datenträgeraustausch
B 5.3 E-Mail
B 5.4 Webserver
B 5.5 Lotus Notes
B 5.6 Faxserver
B 5.7 Datenbanken
B 5.8 Telearbeit
B 5.9 Novell eDirectory
B 5.10 Internet Information Server
B 5.11 Apache Webserver
B 5.12 Exchange 2000 / Outlook 2000
B 5.13 SAP System

B 5.1 Peer-to-Peer-Dienste



Beschreibung

Peer-to-Peer-Dienste sind Funktionen auf Arbeitsplatz-Computern, die anderen IT-Systemen im lokalen Netz Ressourcen zur Verfügung stellen, beispielsweise gemeinsamen Zugriff auf die Festplatte oder auf Drucker. Solche Dienste werden von den gängigen Betriebssystemen unterstützt. In diesem Baustein werden die Betriebssysteme Windows für Workgroups (WfW), Windows 95/NT/2000 und Unix betrachtet, berücksichtigt wird hier aber nur die reine Peer-to-Peer-Funktionalität dieser Betriebssysteme. Auf sicherheitsspezifische Aspekte einzelner Anwendungen bei der Benutzung von Peer-to-Peer-Funktionalitäten, zum Beispiel bezüglich *Mail*, *Exchange*, *Schedule+*, *Direct-Data-Exchange (DDE)* oder *Remote Access Service (RAS)*, wird nur am Rande eingegangen. Weiterhin werden in diesem Kapitel ausschließlich die für Peer-to-Peer-Dienste spezifischen Gefährdungen und Maßnahmen beschrieben, daher sind zusätzlich noch die betriebssystemspezifischen Bausteine zu betrachten. Peer-to-Peer-Kommunikation über das Internet ist nicht Gegenstand dieses Bausteins.

Da Peer-to-Peer-Dienste wesentlich geringere Sicherheitsfunktionalitäten bieten als durch dedizierte Server bereitgestellte Dienste, sollten Peer-to-Peer-Dienste innerhalb servergestützter Netze nicht verwendet werden.

Gefährdungslage

Für den IT-Grundschutz von Peer-to-Peer-Diensten werden folgende typische Gefährdungen angenommen:

Organisatorische Mängel:

- G 2.25 Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten
- G 2.65 Komplexität der SAMBA-Konfiguration

Menschliche Fehlhandlungen:

- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.18 Freigabe von Verzeichnissen, Druckern oder der Ablagemappe
- G 3.19 Speichern von Passwörtern unter WfW und Windows 95
- G 3.20 Ungewollte Freigabe des Leserechtes bei Schedule+

Vorsätzliche Handlungen:

- G 5.45 Ausprobieren von Passwörtern unter WfW und Windows 95
- G 5.46 Maskerade unter WfW
- G 5.47 Löschen des Post-Office unter WfW

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Bei der Bearbeitung der originären Peer-to-Peer-Maßnahmen sollte zuerst anhand von Maßnahme M 2.67 *Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste* eine Sicherheitsstrategie ausgearbeitet werden, da diese die Grundlage für die weiteren Maßnahmen ist.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Peer-to-Peer-Dienste" vorgestellt:

Planung und Konzeption

- M 2.67 (A) Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste
- M 5.37 (B) Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz

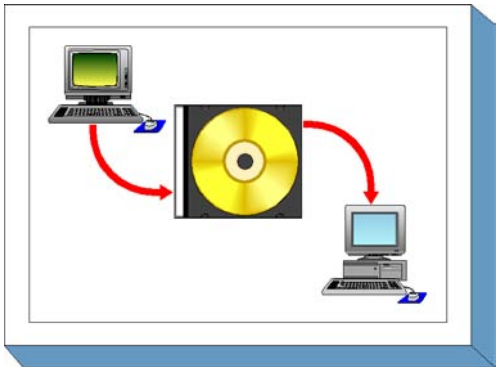
Umsetzung

- M 2.94 (B) Freigabe von Verzeichnissen unter Windows NT
- M 3.19 (A) Einweisung in den richtigen Einsatz der Sicherheitsfunktionen von Peer-to-Peer-Diensten
- M 4.45 (A) Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW
- M 4.149 (A) Datei- und Freigabeberechtigungen unter Windows 2000/XP

Betrieb

- M 2.68 (B) Sicherheitskontrollen durch die Benutzer beim Einsatz von Peer-to-Peer-Diensten
- M 4.46 (A) Nutzung des Anmeldepasswortes unter WfW und Windows 95
- M 4.58 (B) Freigabe von Verzeichnissen unter Windows 95
- M 5.82 (A) Sicherer Einsatz von SAMBA

B 5.2 Datenträgeraustausch



Beschreibung

Betrachtet wird in diesem Baustein der Austausch von Datenträgern zur Datenübertragung zwischen IT-Systemen. Der Austausch von Datenträgern, um Informationen zwischen IT-Systemen zu übertragen, kann aus verschiedenen Gründen sinnvoll oder notwendig sein. Ein Grund kann sein, dass es keine oder keine hinreichend vertrauenswürdige Vernetzung zwischen den betroffenen IT-Systemen gibt. Typischerweise verwendete Datenträger sind Disketten, Wechselplatten (magnetisch, magneto-optisch), CD-ROMs, DVDs, Magnetbänder, Kassetten und auch Flash-Speicher wie USB-Sticks und USB-Festplatten. Daneben wird auch die Speicherung der Daten auf dem Sender- und Empfänger-System, soweit es in direktem Zusammenhang mit dem Datenträgeraustausch steht, sowie der Umgang mit den Datenträgern vor bzw. nach dem Versand berücksichtigt.

Gefährdungslage

Für den IT-Grundschutz im Rahmen des Austausches von Datenträgern werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.7 Unzulässige Temperatur und Luftfeuchte
- G 1.8 Staub, Verschmutzung
- G 1.9 Datenverlust durch starke Magnetfelder beim Transport

Organisatorische Mängel:
- G 2.3 Fehlende, ungeeignete, inkompatible Betriebsmittel
- G 2.10 Nicht fristgerecht verfügbare Datenträger
- G 2.17 Mangelhafte Kennzeichnung der Datenträger
- G 2.18 Ungeordnete Zustellung der Datenträger
- G 2.19 Unzureichendes Schlüsselmanagement bei Verschlüsselung

Menschliche Fehlhandlungen:
- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.12 Verlust der Datenträger beim Versand
- G 3.13 Übertragung falscher oder nicht gewünschter Datensätze

Technisches Versagen:
- G 4.7 Defekte Datenträger

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten und Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.9 Unberechtigte IT-Nutzung
- G 5.23 Computer-Viren
- G 5.29 Unberechtigtes Kopieren der Datenträger
- G 5.43 Makro-Viren

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den Datenträgeraustausch sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption über den täglichen Betrieb bis hin zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Im Vorfeld des Datenträgeraustausches ist zu klären und verbindlich festzulegen, mit welchen Kommunikationspartnern dieser Austausch stattfinden soll, und in der Datenträgerverwaltung sind die Datenträger festzulegen und zu kennzeichnen, die für den Austausch mit externen Stellen vorzusehen sind.

Beschaffung

Die Auswahl geeigneter Datenträger ist mit den Kommunikationspartner abzustimmen. Bei der Entscheidung, welche Arten von Datenträgern geeignet sind, kann M 4.169 *Verwendung geeigneter Archivmedien* hilfreich sein.

Umsetzung

Um eventuelle Schäden durch unsachgemäße Behandlung der Datenträger beim Transport so gering wie möglich zu halten, sollte eine geeignete Versandart festgelegt werden, die, je nach verwendetem Datenträger (z. B. CD-ROM, Magnetband) durchaus unterschiedlich sein kann.

Betrieb

Bei der Durchführung des Datenträgeraustauschs sind eine Reihe von Maßnahmen zu beachten, die mögliche Schäden vermeiden bzw. in ihren Auswirkungen minimieren. Dazu gehören die sichere Aufbewahrung und Verpackung der Datenträger sowie eine eindeutige Kennzeichnung, die die Gefahr der Verwechslung verringert. Zur allgemeinen Hygiene gehört eine Überprüfung auf Viren vor dem Versenden und nach dem Empfang.

Aussonderung

Wenn magnetische Datenträger mit unterschiedlichen Kommunikationspartnern ausgetauscht werden, sollten diese Datenträger vor ihrer erneuten Verwendung physikalisch gelöscht werden, um die Übermittlung von Informationsresten an den falschen Empfänger zu vermeiden.

Notfallvorsorge

Da es nie auszuschließen ist, dass Datenträger beim Transport verloren gehen, sollten die übermittelten Daten zumindest so lange noch lokal in einer Kopie vorgehalten werden, bis der Empfang des Datenträgers bestätigt wurde. Je nach Art und Zweck des Datenträgeraustausches kann auch eine längere Speicherung als Beweismittel für spätere Konflikte erforderlich sein.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Datenträgeraustausch" vorgestellt.

Planung und Konzeption

- M 2.3 (B) Datenträgerverwaltung
- M 2.42 (B) Festlegung der möglichen Kommunikationspartner
- M 2.45 (A) Regelung des Datenträgeraustausches
- M 2.46 (Z) Geeignetes Schlüsselmanagement
- M 4.34 (Z) Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen

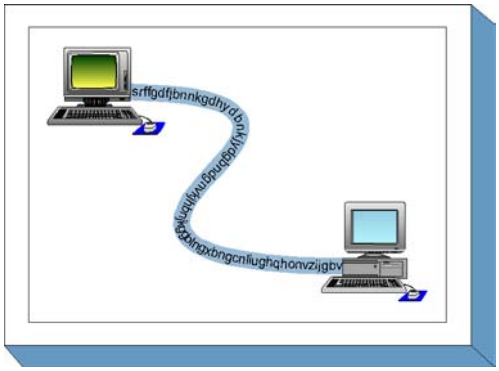
Umsetzung
- M 5.22 (B) Kompatibilitätsprüfung des Sender- und Empfängersystems
- M 5.23 (A) Auswahl einer geeigneten Versandart für den Datenträger

Betrieb
- M 1.36 (A) Sichere Aufbewahrung der Datenträger vor und nach Versand
- M 2.43 (A) Ausreichende Kennzeichnung der Datenträger beim Versand
- M 2.44 (A) Sichere Verpackung der Datenträger
- M 3.14 (B) Einweisung des Personals in den geregelten Ablauf eines Datenträgeraustausches
- M 4.33 (A) Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
- M 4.35 (Z) Verifizieren der zu übertragenden Daten vor Versand

Aussonderung
- M 4.32 (B) Physikalisches Löschen der Datenträger vor und nach Verwendung

Notfallvorsorge
- M 6.38 (A) Sicherungskopie der übermittelten Daten

B 5.3 E-Mail



Beschreibung

Der Dienst "Electronic Mail", kurz E-Mail, erlaubt es, elektronische Nachrichten innerhalb kürzester Zeit weltweit zu versenden und zu empfangen. Eine E-Mail hat im Allgemeinen neben den Adressangaben (From/To) eine Titel- oder Betreffzeile (Subject), einen Textkörper und eventuell ein oder mehrere Anhänge (Attachments). Mittels E-Mail können nicht nur kurze Informationen schnell, bequem und informell weitergegeben werden, sondern es können auch Geschäftsvorfälle zur Weiterbearbeitung an andere Bearbeiter weitergeleitet werden. Abhängig davon, für welchen Einsatzzweck E-Mail eingesetzt wird, unterscheiden sich auch die Ansprüche an Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit der zu übertragenden Daten sowie des eingesetzten E-Mail-Programms.

Gefährdungslage

Für den IT-Grundschutz im Rahmen des elektronischen Dateiaustausches über E-Mail werden folgende typische Gefährdungen angenommen:

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- G 2.19 Unzureichendes Schlüsselmanagement bei Verschlüsselung
- G 2.54 Vertraulichkeitsverlust durch Restinformationen
- G 2.55 Ungeordnete E-Mail-Nutzung
- G 2.56 Mangelhafte Beschreibung von Dateien

Menschliche Fehlhandlungen:
- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.13 Übertragung falscher oder nicht gewünschter Datensätze

Technisches Versagen:
- G 4.13 Verlust gespeicherter Daten
- G 4.20 Datenverlust bei erschöpftem Speichermedium
- G 4.32 Nichtzustellung einer Nachricht
- G 4.37 Mangelnde Authentizität und Vertraulichkeit von E-Mail

Vorsätzliche Handlungen:
- G 5.2 Manipulation an Daten oder Software
- G 5.7 Abhören von Leitungen
- G 5.9 Unberechtigte IT-Nutzung
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.24 Wiedereinspielen von Nachrichten
- G 5.25 Maskerade
- G 5.26 Analyse des Nachrichtenflusses
- G 5.27 Nichtanerkennung einer Nachricht

- G 5.28 Verhinderung von Diensten
- G 5.43 Makro-Viren
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.72 Mißbräuchliche E-Mail-Nutzung
- G 5.73 Vortäuschen eines falschen Absenders
- G 5.74 Manipulation von Alias-Dateien oder Verteilerlisten
- G 5.75 Überlastung durch eingehende E-Mails
- G 5.76 Mailbomben
- G 5.77 Mitlesen von E-Mails
- G 5.85 Integritätsverlust schützenswerter Informationen
- G 5.110 Web-Bugs
- G 5.111 Missbrauch aktiver Inhalte in E-Mails

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Bei der Betrachtung von E-Mailsystemen sind im Wesentlichen die folgenden Komponenten zu untersuchen:

- Die Benutzer setzen für den Versand, den Empfang und die Bearbeitung von E-Mails Mailprogramme ein.
- Die Benutzer-Mailprogramme übergeben und erhalten die E-Mail an bzw. von einem Mailserver. Zu diesem Zweck führt der Mailserver für jeden Benutzer eine Mailbox. Für den weiteren Nachrichtentransport kommuniziert der Mailserver mit Gateways, die die Nachrichten an andere Mailsysteme senden.

Dies erfordert bei der Umsetzung von Sicherheitsmaßnahmen für den Informationsaustausch per E-Mail, dass zunächst eine übergreifende Sicherheitsrichtlinie erarbeitet wird (siehe M 2.118 *Konzeption der sicheren E-Mail-Nutzung*).

Der Betrieb von E-Mailsystemen erfordert neben der Umsetzung von Sicherheitsmaßnahmen am Mailserver auch Sicherheitsmaßnahmen an den eingesetzten Clients. Von besonderer Bedeutung sind jedoch die von den Benutzern einzuhaltenden Sicherheitsvorkehrungen und Anweisungen.

Werden als E-Mail-Programme Lotus Notes oder Microsoft Exchange eingesetzt, so sind zusätzlich zu den hier beschriebenen Maßnahmen die in den Bausteinen B 5.5 *Lotus Notes* und B 5.12 *Exchange 2000 / Outlook 2000* vorgestellten systemspezifischen Maßnahmen umzusetzen. Für andere E-Mail-Programme sind analoge Sicherheitsmaßnahmen zu ergreifen.

Nachfolgend wird das Maßnahmenbündel für den Bereich "E-Mail" vorgestellt.

Planung und Konzeption

- M 2.30 (A) Regelung für die Einrichtung von Benutzern / Benutzergruppen
- M 2.42 (B) Festlegung der möglichen Kommunikationspartner
- M 2.46 (Z) Geeignetes Schlüsselmanagement
- M 2.118 (A) Konzeption der sicheren E-Mail-Nutzung
- M 2.119 (A) Regelung für den Einsatz von E-Mail
- M 2.122 (B) Einheitliche E-Mail-Adressen
- M 2.274 (A) Vertretungsregelungen bei E-Mail-Nutzung
- M 5.63 (Z) Einsatz von GnuPG oder PGP
- M 5.67 (Z) Verwendung eines Zeitstempel-Dienstes
- M 5.108 (Z) Kryptographische Absicherung von E-Mail
- M 5.110 (Z) Absicherung von E-Mail mit SPHINX (S/MIME)

Beschaffung
- M 2.123 (B) Auswahl eines Mailproviders

Umsetzung
- M 2.120 (A) Einrichtung einer Poststelle
- M 2.275 (Z) Einrichtung funktionsbezogener E-Mailadressen
- M 5.22 (B) Kompatibilitätsprüfung des Sender- und Empfängersystems
- M 5.32 (A) Sicherer Einsatz von Kommunikationssoftware
- M 5.57 (A) Sichere Konfiguration der Mail-Clients

Betrieb
- M 2.121 (B) Regelmäßiges Löschen von E-Mails
- M 4.33 (A) Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
- M 4.34 (Z) Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
- M 4.64 (C) Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen
- M 4.199 (B) Vermeidung gefährlicher Dateiformate
- M 5.53 (B) Schutz vor Mailbomben
- M 5.54 (B) Schutz vor Mailüberlastung und Spam
- M 5.55 (B) Kontrolle von Alias-Dateien und Verteilerlisten
- M 5.56 (A) Sicherer Betrieb eines Mailservers
- M 5.109 (Z) Einsatz eines E-Mail-Scanners auf dem Mailserver

Notfallvorsorge
- M 6.38 (A) Sicherungskopie der übermittelten Daten
- M 6.90 (C) Datensicherung und Archivierung von E-Mails

B 5.4 Webserver

Beschreibung

Das World Wide Web (WWW) ist eines der zentralen Medien der heutigen Informationsgesellschaft. Die Informationsangebote im WWW werden von Servern bereitgestellt, die Daten, meist Dokumente in Form von HTML-Seiten, an entsprechende Clientprogramme ausliefern. Dies erfolgt typischerweise über die Protokolle HTTP (*Hypertext Transfer Protocol*) oder HTTPS (*HTTP über SSL* bzw. *TLS*, d. h. HTTP geschützt durch eine verschlüsselte Verbindung). Neben dem Einsatz im Internet werden Webserver auch in zunehmendem Maße für interne Informationen und Anwendungen in Firmennetzen (Intranet) eingesetzt. Ein Grund dafür ist, dass sie eine einfache und standardisierte Schnittstelle zwischen Server-Anwendungen und Benutzern bieten und entsprechende Client-Software (Webbrowser) für praktisch jede Betriebssystemumgebung kostenlos verfügbar ist.

Die Bezeichnung *Webserver* (oder auch *WWW-Server*) wird meist sowohl für das *Programm* benutzt, welches die HTTP-Anfragen beantwortet, als auch für den *Rechner*, auf dem dieses Programm läuft. Bei Webservern sind verschiedene Sicherheitsaspekte zu beachten.

Da ein Webserver ein öffentlich zugängliches System darstellt, sind eine sorgfältige Planung vor dem Aufbau eines Webservers und die sichere Installation und Konfiguration des Systems und seiner Netzumgebung von großer Bedeutung. Das Thema Sicherheit umfasst bei Webservern auch deswegen eine relativ große Anzahl von Gebieten, weil auf einem Webserver meist neben der reinen Webserver-Anwendung noch weitere Serveranwendungen vorhanden sind, die zum Betrieb des Webservers erforderlich sind und deren sicherer Betrieb ebenfalls gewährleistet sein muss. Beispielsweise werden die Daten meist über das Netz (etwa per *ftp* oder *scp*) auf den Server übertragen oder es wird Zugriff auf eine Datenbank benötigt.

Einige der relevanten Aspekte sollen an dieser Stelle kurz erläutert werden.

Planung des Webauftritts

Ein wichtiger Aspekt der Sicherheit eines Webservers ist bereits relevant, bevor dieser überhaupt existiert: Planung und Organisation des Webangebots. Nur dann, wenn geklärt ist, welche Ziele mit dem Webangebot erreicht werden sollen (handelt es sich um ein reines Informationsangebot, um ein E-Commerce- oder ein E-Government-Angebot?) und welche Inhalte oder Anwendungen zu diesem Zweck angeboten werden, kann durch entsprechende Maßnahmen dafür gesorgt werden, dass Sicherheitsprobleme so weit wie möglich vermieden werden.

Der Aspekt der Sicherheit muss bereits sehr früh in der Planungsphase berücksichtigt werden, um die entstehende Architektur entsprechend sicher auslegen zu können.

Organisation

Bei der Betreuung eines Webangebots sind oft mehrere Organisationseinheiten beteiligt, häufig werden die technische und die inhaltliche Betreuung von verschiedenen Stellen übernommen. Manchmal wird der Server gar nicht mehr in der Organisation selbst betrieben, sondern bei einem externen Dienstleister untergebracht. Für das möglichst reibungslose Funktionieren des Webangebots müssen daher entsprechende organisatorische Rahmenbedingungen geschaffen werden. Idealerweise sollte eine Redaktion für das Webangebot eingerichtet werden (siehe M 2.272 *Einrichtung eines WWW-Redaktionsteams*).

Auch bei der Festlegung der organisatorischen Rahmenbedingungen eines Webangebots sollte das Thema Sicherheit eine Rolle spielen. Davon hängt insbesondere eine schnelle und effektive Reaktion auf Probleme ab.

Sicherheit von Datenübertragung und Authentisierungsmechanismen

Generell wird ein Webserver von außen über die HTTP-Schnittstelle angesprochen. Abhängig davon, welches Ziel das Webangebot hat und welche Inhalte und Anwendungen angeboten werden, sind die folgenden Fragen von Bedeutung:

- Muss die Integrität der Daten bei der Übertragung vom Webserver zum Client geschützt werden?
- Muss die Vertraulichkeit der Daten bei der Übertragung vom Webserver zum Client gewährleistet werden?
- Ist eine Authentisierung des Webservers dem Client gegenüber erforderlich?
- Ist eine Authentisierung der Clients gegenüber dem Webserver erforderlich?

Bei einem reinen Informationsangebot, das öffentlich zugänglich sein soll, werden alle diese Fragen normalerweise verneint werden können. Handelt es sich jedoch um ein E-Commerce- oder E-Government-Angebot, so werden sicherlich mehrere Fragen bejaht.

Im Wesentlichen betreffen diese Fragen nur Eigenschaften der verwendeten Übertragungsprotokolle HTTP oder HTTPS. Spezifisch für den einzelnen Webserver ist dabei nur, inwieweit der Webserver diese Protokolle unterstützt. Diese Punkte können daher als Kriterien für die Auswahl eines Webserver-Produktes herangezogen werden.

Sicherheit der Inhalte und Anwendungen auf dem Webserver

Um die Inhalte und Anwendungen auf dem Server vor unbefugtem Zugriff oder Veränderung zu schützen, ist es wichtig, die Rechte der verschiedenen beteiligten Benutzer klar festzulegen. Die organisatorische und technische Realisierung der Trennung zwischen verschiedenen Benutzern, die eventuell Inhalte auf dem Server einstellen bzw. pflegen dürfen, oder gar zwischen verschiedenen Webangeboten, die gemeinsam auf einem Server beheimatet sind, ist ein wichtiger Aspekt der Sicherheit eines Webangebots.

Technische Sicherheit des Servers

Die Kompromittierung eines Webservers kann erhebliche finanzielle Verluste oder Imageschäden nach sich ziehen. Da es in der Regel keine oder nur wenige (vertrauenswürdige) Anwender auf einem Web-Server gibt, werden die meisten Angriffe nicht lokal, sondern über das Netz ausgeführt. Daher spielt der Schutz des Webservers gegen Angriffe über das Netz (also z. B. über das Internet, aber auch aus dem Intranet heraus) eine sehr wichtige Rolle. Neben Angriffen auf die Webserver-Anwendung sind auch Angriffe auf Schwachstellen des verwendeten Betriebssystems oder anderer Programme möglich, beispielsweise auf eine nicht ausreichend gesicherte Datenbankanbindung, auf einen eventuell vorhandenen ftp-Zugang oder auf per NFS oder SMB freigegebene Verzeichnisse. Oft wird zur Realisierung eines Webangebots auch der Zugriff auf weitere IT-Systeme, etwa einen Datenbankserver, benötigt. Da immer mehr Webangebote nicht mehr ausschließlich aus statischen HTML-Seiten bestehen, sondern beispielsweise über entsprechende Anwendungen Zugriff auf Datenbanken bieten, spielt außerdem die Sicherheit dieser Programme eine zunehmende Rolle.

Gefährdungslage

Für den IT-Grundschutz werden pauschal die folgenden Gefährdungen als typisch im Zusammenhang mit einem Webserver und der Nutzung des WWW angenommen:

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- G 2.28 Verstöße gegen das Urheberrecht
- G 2.32 Unzureichende Leitungskapazitäten
- G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindungen
- G 2.96 Veraltete oder falsche Informationen in einem Webangebot
- G 2.100 Fehler bei der Beantragung und Verwaltung von Internet-Domainnamen

Menschliche Fehlhandlungen:
- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- G 3.37 Unproduktive Suchzeiten
- G 3.38 Konfigurations- und Bedienungsfehler

Technisches Versagen:
- G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
- G 4.22 Software-Schwachstellen oder -Fehler
- G 4.39 Software-Konzeptionsfehler

Vorsätzliche Handlungen:
- G 5.2 Manipulation an Daten oder Software
- G 5.19 Missbrauch von Benutzerrechten
- G 5.20 Missbrauch von Administratorrechten
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.28 Verhinderung von Diensten
- G 5.43 Makro-Viren
- G 5.48 IP-Spoofing
- G 5.78 DNS-Spoofing
- G 5.87 Web-Spoofing
- G 5.88 Missbrauch aktiver Inhalte

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

In diesem Baustein werden die für einen Webserver spezifischen Gefährdungen und Maßnahmen beschrieben. Darüber hinaus muss für die Sicherheit des organisationseigenen Netzes Baustein B 3.101 *Servergestütztes Netz* umgesetzt werden, sowie je nach dem eingesetzten Betriebssystem beispielsweise die Bausteine B 3.102 *Unix-Server* oder B 3.106 *Windows 2000 Server*. Falls das Webangebot Inhalte enthält, die von einer Webanwendung dynamisch aus einer Datenbank erzeugt werden, ist auch der Baustein B 5.7 *Datenbanken* zu berücksichtigen. Insbesondere dann, wenn der Webserver aus dem Internet heraus angesprochen werden kann, sollte auch Baustein B 1.8 *Behandlung von Sicherheitsvorfällen* beachtet werden.

Für die sichere Anbindung eines Webservers an öffentliche Netze (z. B. das Internet) ist Baustein B 3.301 *Sicherheitsgateway (Firewall)* zu betrachten, ebenso wie für den Zusammenschluss mehrerer Intranets zu einem übergreifenden Intranet. Die kontrollierte Anbindung externer Anschlusspunkte (z. B. von Telearbeitsplätzen via ISDN) wird im Baustein B 5.8 *Telearbeit* behandelt.

Ein Webserver sollte in einem separaten Serverraum aufgestellt werden. Hierbei zu realisierende Maßnahmen sind in Baustein B 2.4 *Serverraum* beschrieben. Wenn kein Serverraum zur Verfügung steht, kann der Webserver alternativ in einem Serverschrank aufgestellt werden (siehe Baustein B 2.7 *Schutzschränke*). Wird der Webserver nicht bei der Organisation selbst, sondern bei einem externen Dienstleister betrieben, so muss Baustein B 1.11 *Outsourcing* betrachtet werden.

Für den erfolgreichen und sicheren Aufbau eines Webservers sind eine Reihe von Maßnahmen umzusetzen. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

1. Planung des Einsatzes (siehe M 2.172 *Entwicklung eines Konzeptes für die WWW-Nutzung*) und Festlegung einer WWW-Sicherheitsstrategie (siehe M 2.173 *Festlegung einer WWW-Sicherheitsstrategie*):
   - Festlegung des Einsatzzwecks des Webservers
   - Festlegung der Sicherheitsziele
   - Gegebenenfalls Auswahl geeigneter Authentisierungsmechanismen
   - Anpassung der Netzstruktur
   - Organisatorische Regelungen
2. Einrichtung des Webservers (siehe M 2.175 *Aufbau eines Webservers*):
   - Umsetzung der IT-Grundschutz-Maßnahmen für den Serverrechner (siehe z. B. Baustein B 3.102 *Server unter Unix*) oder Umsetzung der Maßnahmen des Bausteins B 1.11 *Outsourcing*, falls der Betrieb des Webservers von einem externen Dienstleister übernommen wird.
   - Gegebenenfalls Nutzung sicherer Kommunikationsverbindungen (siehe M 5.66 *Verwendung von SSL* beziehungsweise M 5.64 *Secure Shell*)
   - Vermeidung von Java, ActiveX und anderen aktiven Inhalten im eigenen Webangebot (siehe auch M 5.69 *Schutz vor aktiven Inhalten*)
3. Betrieb des Webservers (siehe M 2.174 *Sicherer Betrieb eines Webservers*):
   - regelmäßige Kontrolle
   - Anpassung an Änderungen und Tests
   - Zugriffsschutz auf WWW-Dateien (M 4.94 *Schutz der Webserver-Dateien*)
   - Protokollierung am Webserver
   - Notfallvorsorge für den Webserver (siehe M 6.88 *Erstellen eines Notfallplans für den Webserver* und ergänzend auch Baustein B 1.3 *Notfallvorsorge-Konzept*)
   - Datensicherung (siehe Baustein B 1.4 *Datensicherungskonzept*)
4. Sicherer Betrieb von WWW-Clients

   Obwohl der sichere Betrieb von WWW-Clients (Arbeitsplatzrechner) nicht direkt zum Thema Webserver gehört, sollen an dieser Stelle einige Hinweise zur Sicherheit von Webbrowsern gegeben werden. Für jeden (Client-) Rechner, der mit dem Internet verbunden wird, müssen die entsprechenden Maßnahmen aus dem hier anzuwendenden Baustein B 3.201 *Allgemeiner Client* umgesetzt werden. Für den sicheren Zugriff auf das WWW sind außerdem folgende Maßnahmen zu beachten:

   - Sichere Konfiguration und Nutzung der WWW-Client Software (Webbrowser) (siehe M 5.45 *Sicherheit von WWW-Browsern*)
   - Schutz vor Viren, Makro-Viren, aktiven Inhalten (siehe M 4.33 *Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung*, M 5.69 *Schutz vor aktiven Inhalten*)

- Soweit möglich, sollten sichere Kommunikationsverbindungen genutzt werden (siehe M 5.66 *Verwendung von SSL*).

Nachfolgend wird das Maßnahmenbündel für den Bereich "*Webserver*" vorgestellt. Auf eine Wiederholung von Maßnahmen anderer Bausteine wird hier aus Redundanzgründen verzichtet.

Planung und Konzeption

- M 2.172 (A) Entwicklung eines Konzeptes für die WWW-Nutzung
- M 2.173 (A) Festlegung einer WWW-Sicherheitsstrategie
- M 2.175 (A) Aufbau eines WWW-Servers
- M 2.271 (A) Festlegung einer Sicherheitsstrategie für den WWW-Zugang
- M 2.272 (A) Einrichtung eines WWW-Redaktionsteams
- M 2.298 (Z) Verwaltung von Internet-Domainnamen
- M 4.176 (B) Auswahl einer Authentisierungsmethode für Webangebote
- M 5.64 (Z) Secure Shell
- M 5.66 (Z) Verwendung von SSL
- M 5.69 (A) Schutz vor aktiven Inhalten

Beschaffung

- M 2.176 (B) Geeignete Auswahl eines Internet Service Providers

Umsetzung

- M 4.94 (A) Schutz der WWW-Dateien
- M 4.95 (A) Minimales Betriebssystem
- M 4.96 (Z) Abschaltung von DNS
- M 4.97 (Z) Ein Dienst pro Server
- M 4.98 (A) Kommunikation durch Paketfilter auf Minimum beschränken
- M 4.99 (C) Schutz gegen nachträgliche Veränderungen von Informationen

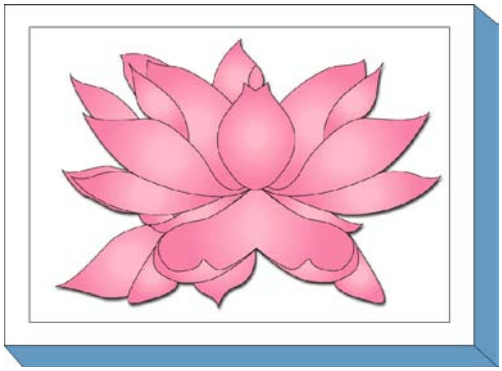
Betrieb

- M 2.174 (A) Sicherer Betrieb eines WWW-Servers
- M 2.273 (A) Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
- M 4.33 (A) Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
- M 4.34 (Z) Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen
- M 4.64 (C) Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen
- M 4.78 (A) Sorgfältige Durchführung von Konfigurationsänderungen
- M 4.93 (B) Regelmäßige Integritätsprüfung
- M 4.177 (B) Sicherstellung der Integrität und Authentizität von Softwarepaketen
- M 5.59 (A) Schutz vor DNS-Spoofing

Notfallvorsorge

- M 6.88 (B) Erstellen eines Notfallplans für den Webserver

B 5.5 Lotus Notes



Beschreibung

Lotus Notes ist ein Produkt im Bereich der Workgroup-Unterstützung. Es bietet die Möglichkeit, die in einem Unternehmen anfallenden Büroarbeitsabläufe zu unterstützen und zu organisieren. Die gesamte dazu nötige Kommunikation, Datenübertragung und Datenhaltung kann über Lotus Notes abgewickelt werden. Dem Notes Konzept liegt eine Client-Server-Architektur zugrunde: Benutzer verwenden den Notes-Client oder einen Browser, um sich mit dem Domino Server zu verbinden und zu arbeiten.

Unter dem Gesichtspunkt der Sicherheit sind für Lotus Notes Aspekte aus den folgenden Kategorien zu unterscheiden:

1. Zugangssicherheit: Die auf einem Notes-Server gehaltenen Daten dürfen nur berechtigten Benutzern zugänglich gemacht werden. Dazu wird vom Notes-Server eine Zugangskontrolle zum Server selbst bereitgestellt. Dadurch kann gesteuert werden, welche Benutzer prinzipiell auf welchen Notes-Server zugreifen dürfen.
2. Zugriffskontrolle: Neben der Kontrolle des Serverzugriffs stellt die Zugriffskontrolle auf Datenbankebene einen wichtigen Sicherheitsmechanismus zur Verfügung. Durch die von Lotus Notes bereitgestellten Methoden ist eine detaillierte Kontrolle möglich, welche Benutzer (oder welche Benutzergruppen) welche Aktionen auf einer bestimmten Datenbank ausführen dürfen.
3. Kommunikationssicherheit: Wenn ein Client auf eine Datenbank auf einem Server zugreift, werden die abgerufenen Daten über eine Netzverbindung übertragen. Um die Vertraulichkeit und Integrität der Daten zu sichern, stellt Lotus Notes Verschlüsselungsverfahren zur Verfügung.
4. Verfügbarkeit: Wird ein Notes-System für Unternehmensbereiche als Bürokommunikationsmedium eingesetzt, so müssen auch Anforderungen an die Verfügbarkeit gestellt werden. Dies betrifft zum einen die Schadensminderung bei Ausfall durch redundante Datenhaltung oder physikalische Redundanz von Rechnern und zum anderen das Erstellen eines Notfallvorsorgeplanes, der bei einem Ausfall Anleitungen und Hinweise für eine schnelle Wiederherstellung des Systems gibt.

Gefährdungslage

Für den IT-Grundschutz eines Notes-Systems werden die folgenden typischen Gefährdungen angenommen:

Höhere Gewalt:
- G 1.1 Personalausfall
- G 1.2 Ausfall des IT-Systems

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.16 Ungeordneter Benutzerwechsel bei tragbaren PCs
- G 2.18 Ungeordnete Zustellung der Datenträger
- G 2.19 Unzureichendes Schlüsselmanagement bei Verschlüsselung
- G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindungen

- G 2.40 Mangelhafte Konzeption des Datenbankzugriffs
- G 2.49 Fehlende oder unzureichende Schulung der Telearbeiter

Menschliche Fehlhandlungen:
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.43 Ungeeigneter Umgang mit Passwörtern
- G 3.44 Sorglosigkeit im Umgang mit Informationen
- G 3.46 Fehlkonfiguration eines Lotus Notes Servers
- G 3.47 Fehlkonfiguration des Browser-Zugriffs auf Lotus Notes

Technisches Versagen:
- G 4.26 Ausfall einer Datenbank
- G 4.28 Verlust von Daten einer Datenbank
- G 4.35 Unsichere kryptographische Algorithmen

Vorsätzliche Handlungen:
- G 5.7 Abhören von Leitungen
- G 5.8 Manipulation an Leitungen
- G 5.22 Diebstahl bei mobiler Nutzung des IT-Systems
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.77 Mitlesen von E-Mails
- G 5.83 Kompromittierung kryptographischer Schlüssel
- G 5.84 Gefälschte Zertifikate
- G 5.85 Integritätsverlust schützenswerter Informationen
- G 5.100 Missbrauch aktiver Inhalte beim Zugriff auf Lotus Notes
- G 5.101 "Hacking Lotus Notes"

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Zusätzlich zu der Absicherung der Lotus Notes-Komponenten muss jedoch auch ein spezifisches Sicherheitskonzept erstellt werden, das sich in das bestehende Sicherheitskonzept eingliedert: das Notes-System muss einerseits bestehende Sicherheitsanforderungen umsetzen und erfordert andererseits das Aufstellen neuer, Notes-spezifischer Sicherheitsregeln.

Ein Notes-System wird in der Regel im Umfeld anderer Systeme eingesetzt, die dazu dienen, den Zugriff auf das interne Netz von außen zu kontrollieren. Hier sind z. B. Firewall-Systeme oder Systeme zur Fernwartung zu nennen, mit denen ein Notes-System im Verbund zusammenarbeiten muss. Aus diesem Grund sind bei der Durchführung der Notes-spezifischen Maßnahmen auch die Maßnahmen aus den jeweiligen Bausteinen der betroffenen Systeme zu berücksichtigen. Neben den entsprechenden Bausteinen der Schicht 3 sind u. a. auch die folgenden Bausteine zu nennen:

- B 3.301 *Sicherheitsgateway (Firewall)*, wenn Notes-Systeme in einer Firewall-Umgebung eingesetzt werden (siehe auch M 2.211 *Planung des Einsatzes von Lotus Notes in einer DMZ*).
- B 4.4 *Remote Access*, wenn der Zugriff auf das Notes-System über Einwahl-Leitungen erfolgt.

Die im Baustein B 5.7 *Datenbanken* aufgeführten Maßnahmen sind im Kontext von Lotus Notes nur bedingt anwendbar, da Notes ein proprietäres Datenbanksystem darstellt.

Für den erfolgreichen Aufbau eines Notes-Systems sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Installation bis zum Betrieb. Die Schritte, die dabei zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

1. Nach der Entscheidung, Lotus Notes als internes Kommunikationssystem einzusetzen, muss die Beschaffung der Software und eventuell zusätzlich benötigter Hardware erfolgen. Da Lotus Notes in verschiedenen Konfigurationsvarianten angeboten wird (siehe oben), hängt die zu beschaffende Software auch von den geplanten Einsatzszenarien ab. Daher sind folgende Maßnahmen durchzuführen:
   - Zunächst muss der Einsatz für das Notes System geplant werden (siehe Maßnahme M 2.206 *Planung des Einsatzes von Lotus Notes*).
   - Parallel dazu ist eine Sicherheitsrichtlinie zu erarbeiten (siehe Maßnahme M 2.207 *Festlegen einer Sicherheitsrichtlinie für Lotus Notes*), die einerseits die bereits bestehenden Sicherheitsrichtlinien im Kontext von Lotus Notes umsetzt und andererseits Notes-spezifische Erweiterungen definiert.
   - Vor der tatsächlichen Einführung des Notes-Systems müssen die Benutzer und Administratoren auf den Umgang mit Lotus Notes durch eine Schulung vorbereitet werden. Insbesondere für Administratoren empfiehlt sich aufgrund der Komplexität der Verwaltung eines Notes-Systems eine intensive Schulung. Die Administratoren sollen dabei detaillierte Systemkenntnisse erwerben (siehe M 3.24 *Schulung zur Lotus Notes Systemarchitektur für Administratoren*), so dass eine konsistente und korrekte Systemverwaltung gewährleistet ist. Benutzern sollte die Nutzung der Sicherheitsmechanismen von Lotus Notes vermittelt werden (siehe M 3.25 *Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer*).
2. Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt wurden, kann die Installation des Notes-Systems erfolgen. Dabei sind folgenden Maßnahmen zu beachten:
   - Die Installation kann erst dann als abgeschlossen betrachtet werden, wenn die Lotus Notes Systeme in einen sicheren Zustand gebracht wurden (siehe M 4.116 *Sichere Installation von Lotus Notes*). Dadurch wird sichergestellt, dass in der folgenden Konfigurationsphase nur berechtigte Administratoren auf das Notes System zugreifen können.
   - Nach der "Rohinstallation" erfolgt eine erstmalige Konfiguration des Notes-Systems, das aus den Servern (siehe M 4.117 *Sichere Konfiguration eines Lotus Notes Servers*) und den Clients (siehe M 4.126 *Sichere Konfiguration eines Lotus Notes Clients* und M 4.127 *Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes*) besteht.
3. Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:
   - Ein Notes-System ist in der Regel ständigen Veränderungen unterworfen. Daher müssen sicherheitsrelevante Konfigurationsparameter kontinuierlich angepasst werden. Daneben hängt die Sicherheit in einem Client-Server-basierten System auch von der Sicherheit aller Teilsysteme - hier auch insbesondere der Clients - ab. Die für den sicheren Betrieb relevanten Maßnahmen sind in M 4.128 *Sicherer Betrieb von Lotus Notes* und den Maßnahmen zur Kommunikationsabsicherung (siehe M 5.84 *Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation*, M 5.85 *Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail und* M 5.86 *Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes*) zusammengefasst.
   - Neben der Absicherung im laufenden Betrieb spielt jedoch auch die Notfallvorsorge eine wichtige Rolle, da nur so der Schaden im Notfall verringert werden kann. Hinweise zur Notfallvorsorge finden sich in M 6.73 *Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems*.

Nachfolgend wird nun das Maßnahmenbündel für den Baustein "Lotus Notes" vorgestellt.

Planung und Konzeption

- M 2.206 (A) Planung des Einsatzes von Lotus Notes
- M 2.207 (A) Festlegen einer Sicherheitsrichtlinie für Lotus Notes
- M 2.208 (A) Planung der Domänen und der Zertifikatshierarchie von Lotus Notes
- M 2.209 (B) Planung des Einsatzes von Lotus Notes im Intranet
- M 2.210 (B) Planung des Einsatzes von Lotus Notes im Intranet mit Browser-Zugriff
- M 2.211 (A) Planung des Einsatzes von Lotus Notes in einer DMZ
- M 4.131 (Z) Verschlüsselung von Lotus Notes Datenbanken

Umsetzung

- M 3.24 (A) Schulung zur Lotus Notes Systemarchitektur für Administratoren
- M 3.25 (A) Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer
- M 4.116 (A) Sichere Installation von Lotus Notes
- M 4.117 (A) Sichere Konfiguration eines Lotus Notes Servers
- M 4.118 (A) Konfiguration als Lotus Notes Server
- M 4.119 (A) Einrichten von Zugangsbeschränkungen auf Lotus Notes Server
- M 4.120 (A) Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken
- M 4.121 (A) Konfiguration der Zugriffsrechte auf das Namens- und Adressbuch von Lotus Notes
- M 4.122 (B) Konfiguration für den Browser-Zugriff auf Lotus Notes
- M 4.123 (B) Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes
- M 4.124 (A) Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes
- M 4.125 (A) Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken
- M 4.126 (A) Sichere Konfiguration eines Lotus Notes Clients
- M 4.127 (A) Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes

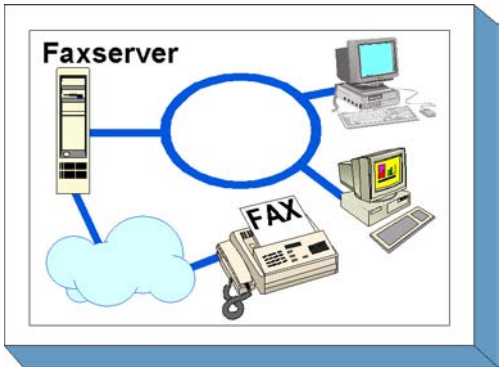
Betrieb

- M 4.128 (A) Sicherer Betrieb von Lotus Notes
- M 4.129 (A) Sicherer Umgang mit Notes-ID-Dateien
- M 4.130 (A) Sicherheitsmaßnahmen nach dem Anlegen neuer Lotus Notes Datenbanken
- M 4.132 (C) Überwachen eines Lotus Notes-Systems
- M 5.84 (Z) Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation
- M 5.85 (Z) Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail
- M 5.86 (C) Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes

Notfallvorsorge

- M 6.49 (A) Datensicherung einer Datenbank
- M 6.73 (B) Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems

B 5.6 Faxserver



Beschreibung

Betrachtet wird die Informationsübermittlung in Form eines Fax. Für die Maßnahmenauswahl im Bereich IT-Grundschutz wird nicht nach dem verwendeten Übertragungsstandard (z. B. CCITT Gruppe 3) unterschieden. In diesem Baustein werden als technische Basis des Fax-Verkehrs ausschließlich Faxserver betrachtet. Ein Faxserver in diesem Sinne ist eine Applikation, die auf einem IT-System installiert ist und in einem Netz für andere IT-Systeme die Dienste Faxversand und/oder Faxempfang zur Verfügung stellt.

Faxserver werden in der Regel in bereits bestehende E-Mailsysteme integriert. So ist es u. a. möglich, dass eingehende Fax-Dokumente durch den Faxserver per E-Mail an den Benutzer zugestellt werden. Abzusendende Dokumente werden entweder über eine Druckerwarteschlange oder per E-Mail an den Faxserver übergeben. Durch die Integration des Faxservers in ein E-Mail-System ist es auch möglich, "Serienbriefe" wahlweise per Fax und per E-Mail zu versenden. Sofern ein Adressat über einen E-Mail-Zugang verfügt, erhält er die Nachricht kostengünstig per E-Mail, ansonsten per Fax. Das von einem Faxserver gesendete oder empfangene Dokument ist eine Grafik-Datei, die nicht unmittelbar in Textverarbeitungssystemen weiterverarbeitet werden kann. Möglich ist aber auf jeden Fall die Archivierung. Dies kann durch die Faxserver-Software oder auch in Dokumentenmanagementsystemen erfolgen.

Faxserver gibt es für eine Reihe von Betriebssystemen wie z. B. für verschiedene Unix-Derivate, Microsoft Windows und Novell Netware. Überlegungen zu Gefährdungen und Maßnahmen, die durch das jeweils verwendete Betriebssystem bedingt werden, sind nicht Gegenstand dieses Bausteins. Vielmehr sind hierzu der Baustein B 3.101 *Allgemeiner Server* und der jeweilige betriebssystemspezifische Baustein zu bearbeiten.

Faxserver verfügen häufig zusätzlich über den Binary-Transfer-Mode. Hiermit werden beliebige Daten, die nicht im Fax-Format vorliegen, übertragen. Es handelt sich dabei nicht um Faxübertragungen. Daher werden spezielle Gefährdungen und Maßnahmen, die diesen Dienst betreffen, nicht in diesem Baustein betrachtet. Wird der Binary-Transfer-Mode zugelassen, so ist zusätzlich der Baustein B 4.3 *Modem* zu bearbeiten.

Gefährdungslage

Für den IT-Grundschutz werden bei der Informationsübermittlung per Fax mittels eines Faxservers folgende typische Gefährdungen angenommen:

Organisatorische Mängel

- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- G 2.22 Fehlende Auswertung von Protokolldaten
- G 2.63 Ungeordnete Faxnutzung

Menschliche Fehlhandlungen:

- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.14 Fehleinschätzung der Rechtsverbindlichkeit eines Fax

Technisches Versagen:
- G 4.15 Fehlerhafte Faxübertragung
- G 4.20 Datenverlust bei erschöpftem Speichermedium

Vorsätzliche Handlungen:
- G 5.2 Manipulation an Daten oder Software
- G 5.7 Abhören von Leitungen
- G 5.9 Unberechtigte IT-Nutzung
- G 5.24 Wiedereinspielen von Nachrichten
- G 5.25 Maskerade
- G 5.27 Nichtanerkennung einer Nachricht
- G 5.30 Unbefugte Nutzung eines Faxgerätes oder eines Faxservers
- G 5.31 Unbefugtes Lesen von Faxsendungen
- G 5.32 Auswertung von Restinformationen in Faxgeräten und Faxservern
- G 5.33 Vortäuschen eines falschen Absenders bei Faxsendungen
- G 5.35 Überlastung durch Faxsendungen
- G 5.39 Eindringen in Rechnersysteme über Kommunikationskarten
- G 5.90 Manipulation von Adressbüchern und Verteillisten

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Zunächst sollte eine übergreifende Sicherheitsleitlinie für den Faxserver erarbeitet werden (siehe M 2.178 *Erstellung einer Sicherheitsleitlinie für die Faxnutzung*) und ein geeigneter Faxserver beschafft werden (siehe M 2.181 *Auswahl eines geeigneten Faxservers*). Hieraus müssen Regelungen abgeleitet werden. Schließlich sind Verantwortliche für den Einsatz des Faxservers zu benennen (siehe M 3.10 *Auswahl eines vertrauenswürdigen Administrators und Vertreters* und M 2.180 *Einrichten einer Fax-Poststelle*). Sowohl die Sicherheitsleitlinie als auch die daraus folgenden Regelungen und die Benennung von Verantwortlichen sollte schriftlich erfolgen. Die dort erarbeiteten Festlegungen sollten sodann in konkrete Sicherheitsmaßnahmen umgesetzt werden. Neben dem sicheren Betrieb des Faxservers ist von besonderer Bedeutung, dass von den Benutzern die entsprechenden Sicherheitsvorkehrungen und Anweisungen eingehalten werden.

Nachfolgend wird das Maßnahmenbündel für die Applikation "Faxserver" vorgestellt:

Planung und Konzeption
- M 2.178 (A) Erstellung einer Sicherheitsleitlinie für die Faxnutzung
- M 2.179 (A) Regelungen für den Faxserver-Einsatz

Beschaffung
- M 2.181 (A) Auswahl eines geeigneten Faxservers

Umsetzung
- M 2.180 (A) Einrichten einer Fax-Poststelle
- M 4.36 (Z) Sperren bestimmter Faxempfänger-Rufnummern
- M 4.37 (Z) Sperren bestimmter Absender-Faxnummern

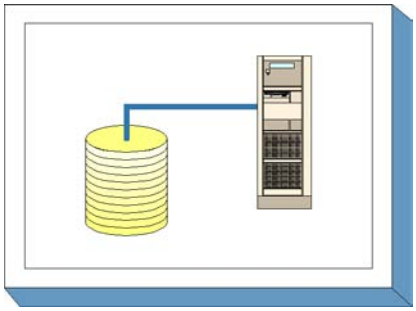
Betrieb
- M 3.15 (A) Informationen für alle Mitarbeiter über die Faxnutzung
- M 5.24 (Z) Nutzung eines geeigneten Faxvorblattes
- M 5.25 (A) Nutzung von Sende- und Empfangsprotokollen

- M 5.26 (Z) Telefonische Ankündigung einer Faxsendung
- M 5.27 (Z) Telefonische Rückversicherung über korrekten Faxempfang
- M 5.28 (Z) Telefonische Rückversicherung über korrekten Faxabsender
- M 5.73 (A) Sicherer Betrieb eines Faxservers
- M 5.74 (A) Pflege der Faxserver-Adressbücher und der Verteillisten
- M 5.75 (Z) Schutz vor Überlastung des Faxservers

Notfallvorsorge

- M 6.69 (B) Notfallvorsorge und Ausfallsicherheit bei Faxservern

B 5.7 Datenbanken



Beschreibung

Datenbanksysteme sind ein weithin genutztes Hilfsmittel zur rechnergestützten Organisation, Erzeugung, Veränderung und Verwaltung großer Datensammlungen und stellen in vielen Unternehmen und Organisationen die zentrale Informationsbasis zu ihrer Aufgabenerfüllung bereit. Ein DBS besteht aus dem so genannten Datenbankmanagement-System (DBMS) und einer oder mehrerer Datenbanken.

Eine Datenbank ist eine Zusammenstellung von Daten samt ihrer Beschreibung (Metadaten), die persistent im DBS abgelegt werden.

Das DBMS bildet die Schnittstelle zwischen den Datenbanken und dient den Benutzern zur Daten-Verwaltung und Veränderung. Die zentralen Aufgaben eines DBMS sind im Wesentlichen die Bereitstellung verschiedener Sichten auf die Daten (Views), die Konsistenzprüfung der Daten (Integritätssicherung), die Autorisationsprüfung, die Behandlung gleichzeitiger Zugriffe verschiedener Benutzer (Synchronisation) und das Bereitstellen einer Datensicherungsmöglichkeit, um im Falle eines Systemausfalls zeitnah Daten wiederherstellen zu können.

Moderne Datenbanksysteme sind überwiegend Bestandteil einer 3-Tier-Architektur. Als Erweiterung der 2-Tier-Architektur (Client-/Server-Architektur) wird hier zwischen Client und Server als dritte Ebene ein Applikationsserver zur Bereitstellung der Datenbank-Anwendungen eingeführt. Durch diese Architektur kann eine Kosteneinsparung aufgrund einer verringerten Client-Ausstattung und einer vereinfachten Datenbankadministration insbesondere bei der Software-Verteilung erreicht werden. Den Anwendern können auf diese Art mit geringem Aufwand neue Software-Versionen zur Verfügung gestellt werden, die durch den Anwender automatisch vom Datenbanksystem über den Applikations-Server bezogen werden.

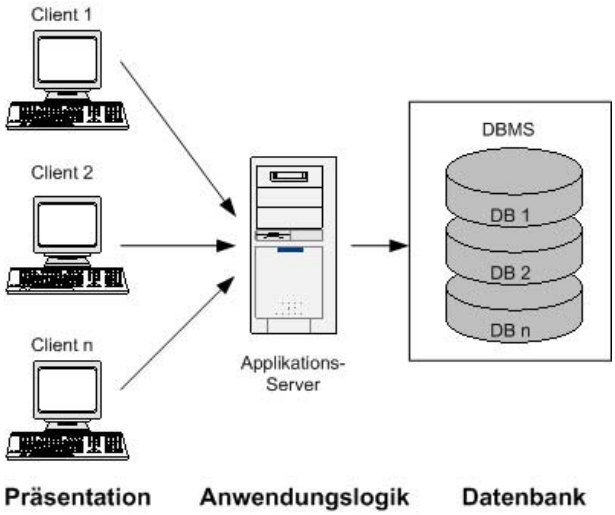


Abbildung: 3-Tier-Architektur eines DBMS

Ein Datenbanksystem muss die parallele Verarbeitung verschiedener Benutzeraufträge (so genannte Transaktionen) ermöglichen. Wesentlich dafür ist die Einhaltung der folgenden vier Eigenschaften, die unter dem ACID-Prinzip bekannt sind:

- Atomarität (Atomicity)

  Eine Transaktion ist die kleinste, nicht mehr zerlegbare Einheit von Verarbeitungsschritten und wird nur vollständig oder gar nicht ausgeführt. Sollte es bei der Ausführung zu einem Fehler bzw. Abbruch kommen, werden alle innerhalb der Transaktion bereits getätigten Änderungen an der Datenbank wieder zurückgenommen.

- Konsistenz (Consistency)

  Eine Transaktion überführt eine Datenbank immer von einem konsistenten Zustand in einen anderen konsistenten Zustand, d.h. alle Integritätsbedingungen der Datenbank werden eingehalten.

- Isolation (Isolation)

  Jede Transaktion läuft isoliert und in jeder Hinsicht unabhängig von anderen Transaktionen ab. Dazu gehört auch, dass jeder Transaktion nur diejenigen Daten aus der Datenbank zur Verfügung gestellt werden, die Teil eines konsistenten Zustands sind. Sollten parallele Transaktionen um Ressourcen konkurrieren, so müssen die Transaktionen serialisiert werden.

- Persistenz (Durability)

  Die Ergebnisse einer erfolgreich beendeten Transaktion bleiben in der Datenbank persistent.

Datenbanksysteme sind Standardsoftware und werden von den unterschiedlichsten Herstellern auf dem Markt angeboten. Soll eine Datenbank zur Verarbeitung von Daten eingesetzt werden, so ist im ersten Schritt ein geeignetes DBS auszuwählen. Die zugehörigen Gefährdungen und Maßnahmen aus dem Baustein B 1.10 *Standardsoftware* sind deshalb zu beachten.

Datenbanken können nicht losgelöst von der Umgebung betrachtet werden, in der sie eingesetzt werden. Ein Einzelplatz-PC ist ebenso denkbar wie ein Großrechnerumfeld oder vernetzte Unix- bzw. Windows-Systeme. Dementsprechend sind in Abhängigkeit des Einsatzumfeldes die Bausteine der entsprechenden Schichten 3 bis 5 zu berücksichtigen.

Gefährdungslage

Neben den grundlegenden Gefährdungen, die prinzipiell für IT-Systeme gelten, existieren Gefährdungen, die speziell die Verfügbarkeit von Datenbanken sowie die Vertraulichkeit oder die Integrität der gespeicherten Daten bedrohen.

Generell steht die Gefährdungslage in Abhängigkeit vom Einsatzszenario und berechtigten Benutzerkreis. Beispielsweise ergibt sich eine erhöhte Gefährdungslage, wenn, anders als gegenüber identifizierbaren Benutzerkreisen innerhalb einer Behörde oder eines Unternehmens, Zugriffe anonymer Benutzern (z. B. Internet-Zugriffe) erlaubt werden.

Eine weiterer Aspekt ergibt sich aus der steigenden Komplexität des DBMS, der sich unter anderem auch in örtlich weit voneinander getrennter Datenhaltung begründet und den damit einhergehenden Anforderungen an sichere Kommunikationswege und konsistente Daten-Synchronisation.

Für den IT-Grundschutz von Datenbanken werden die folgenden Gefährdungen angenommen:

Organisatorische Mängel:
- G 2.22 Fehlende Auswertung von Protokolldaten
- G 2.26 Fehlendes oder unzureichendes Test- und Freigabeverfahren
- G 2.38 Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen
- G 2.39 Mangelhafte Konzeption eines DBMS
- G 2.40 Mangelhafte Konzeption des Datenbankzugriffs
- G 2.41 Mangelhafte Organisation des Wechsels von Datenbank-Benutzern
- G 2.57 Nicht ausreichende Speichermedien für den Notfall
- G 2.110 Mangelhafte Organisation bei Versionswechsel und Migration von Datenbanken

Menschliche Fehlhandlungen:
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten
- G 3.23 Fehlerhafte Administration eines DBMS
- G 3.24 Unbeabsichtigte Datenmanipulation
- G 3.80 Fehler bei der Synchronisation von Datenbanken

Technisches Versagen:
- G 4.26 Ausfall einer Datenbank
- G 4.27 Unterlaufen von Zugriffskontrollen über ODBC
- G 4.28 Verlust von Daten einer Datenbank
- G 4.30 Verlust der Datenbankintegrität/-konsistenz

Vorsätzliche Handlungen
- G 5.9 Unberechtigte IT-Nutzung
- G 5.10 Missbrauch von Fernwartungszugängen
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.64 Manipulation an Daten oder Software bei Datenbanksystemen
- G 5.65 Verhinderung der Dienste eines Datenbanksystems
- G 5.131 SQL-Injection

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Als zentraler Informationsspeicher einer Behörde oder eines Unternehmens empfiehlt es sich, den Datenbank-Server in einem separaten Serverraum aufzustellen oder in einem zentralen Rechenzentrum unterzubringen. Zu realisierende Maßnahmen sind in den Bausteinen B 2.4 *Serverraum* und B 2.9 *Rechenzentrum* beschrieben.

Wird der Datenbank-Server in einem Schutzschrank aufgestellt, ist der Baustein B 2.7 *Schutzschränke* bei der Maßnahmenumsetzung zu berücksichtigen.

Sollen für den Zugriff auf eine Datenbank mobile Engeräte wie beispielsweise entsprechend ausgestattete Mobiltelefone oder PDAs eingesetzt werden, sind die Bausteine B 3.404 *Mobiltelefon* beziehungsweise B 3.405 *PDA* zu berücksichtigen.

Die Gliederung der Sicherheitsmaßnahmen dieses Bausteins orientiert sich an dem Lebenszyklus eines Datenbanksystems. Für den sicheren Einsatz von Datenbanksystemen sollten unter anderem folgende Schritte durchlaufen werden:

1. Planung

Datenbanksysteme sind komplexe Produkte, deren Einsatz und Betrieb systematisch geplant werden muss. Dies mündet unter anderem in einen Anforderungskatalog an die zu beschaffende Software (siehe M 2.80 *Erstellung eines Anforderungskatalogs für Standardsoftware*) sowie in ein Datenbanksicherheitskonzept (siehe M 2.126 *Erstellung eines Datenbanksicherheitskonzeptes*).

2. Schulung der Administratoren und Beschaffung der Software

Bevor die Datenbank-Software produktiv eingesetzt werden kann, müssen die zuständigen Administratoren für den sicheren Betrieb des Datenbanksystems geschult werden (siehe M 3.11 *Schulung des Wartungs- und Administrationspersonals*). Diese Schulungsmaßnahme sollte nach Möglichkeit bereits vor der Beschaffung des Datenbanksystems (siehe M 2.124 *Geeignete Auswahl einer Datenbank-Software*) erfolgen, damit die zuständigen Administratoren frühzeitig effektiv in die Konzeption und den Aufbau einbezogen werden können.

3. Erstellung eines Datenbankkonzeptes / Datenbankmodells

Vor dem Produktivbetrieb des Datenbanksystems ist ein Datenbankkonzept zu erstellen, das sowohl die Installation und Konfiguration der Datenbank-Komponenten, als auch die Struktur der anwendungsspezifischen Datenbank beschreibt. Darüber hinaus ist ein praxisorientiertes Benutzerkonzept zu erstellen. Je nach Volumen und Einsatzbereich der Datenbank sowie der gewählten Datenbank-Standardsoftware kann ein solches Konzept sehr umfangreich sein (M 2.125 *Installation und Konfiguration einer Datenbank*, M 2.126 *Erstellung eines Datenbanksicherheitskonzeptes*, M 2.128 *Zugangskontrolle einer Datenbank* und M 2.129 *Zugriffskontrolle einer Datenbank*).

4. Betrieb des Datenbanksystems

Die Inbetriebnahme und der Betrieb des Datenbanksystems erfordern neben der Umsetzung des Datenbankkonzeptes eine kontinuierliche Überwachung, um die Verfügbarkeit, die Integrität sowie die Vertraulichkeit der Daten sicherzustellen. Die hierfür wichtigsten Maßnahmen betreffen die Aspekte Dokumentation (M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*, M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*), Administration (M 2.130 *Gewährleistung der Datenbankintegrität*, M 2.133 *Kontrolle der Protokolldateien eines Datenbanksystems*) sowie die Nutzung der Datenbank (M 2.65 *Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System*, M 3.18 *Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung*).

5. Notfallvorsorge

Neben der Umsetzung der Maßnahmen zur Einführung und zum störungsfreien Betrieb eines Datenbanksystems gilt es, Ausfällen unterschiedlicher Art vorzubeugen und deren Auswirkungen möglichst gering zu halten. Hierzu sind die datenbankspezifischen Gegebenheiten zu berücksichtigen, um nach einem System- bzw. Datenbankausfall den gestellten Anforderungen hinsichtlich eines zeitnahen Wiederanlaufs des DBS gerecht zu werden und das Risiko eines Datenverlustes zu minimieren (M 6.49 *Datensicherung einer Datenbank*, M 6.50 *Archivierung von Datenbeständen*).

Nachfolgend wird das Maßnahmenbündel für den Baustein "Datenbanken" vorgestellt:

Planung und Konzeption
- M 2.80 (A) Erstellung eines Anforderungskatalogs für Standardsoftware
- M 2.126 (A) Erstellung eines Datenbanksicherheitskonzeptes
- M 2.132 (A) Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen
- M 2.134 (B) Richtlinien für Datenbank-Anfragen
- M 2.363 (B) Schutz gegen SQL-Injection
- M 5.58 (B) Auswahl und Installation von Datenbankschnittstellen-Treibern

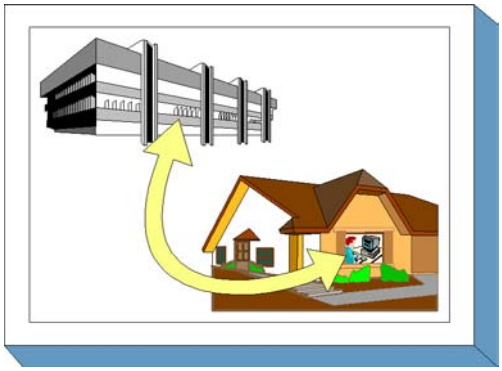
Beschaffung
- M 2.124 (A) Geeignete Auswahl einer Datenbank-Software

Umsetzung
- M 2.125 (A) Installation und Konfiguration einer Datenbank
- M 2.135 (C) Gesicherte Datenübernahme in eine Datenbank
- M 4.7 (A) Änderung voreingestellter Passwörter
- M 4.71 (C) Restriktive Handhabung von Datenbank-Links
- M 4.73 (C) Festlegung von Obergrenzen für selektierbare Datensätze
- M 5.117 (Z) Integration eines Datenbank-Servers in ein Sicherheitsgateway

Betrieb
- M 2.31 (A) Dokumentation der zugelassenen Benutzer und Rechteprofile
- M 2.34 (A) Dokumentation der Veränderungen an einem bestehenden System
- M 2.65 (B) Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
- M 2.127 (B) Inferenzprävention
- M 2.128 (A) Zugangskontrolle einer Datenbank
- M 2.129 (A) Zugriffskontrolle einer Datenbank
- M 2.130 (A) Gewährleistung der Datenbankintegrität
- M 2.131 (C) Aufteilung von Administrationstätigkeiten bei Datenbanksystemen
- M 2.133 (A) Kontrolle der Protokolldateien eines Datenbanksystems
- M 3.18 (A) Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
- M 4.67 (B) Sperren und Löschen nicht benötigter Datenbank-Accounts
- M 4.68 (A) Sicherstellung einer konsistenten Datenbankverwaltung
- M 4.69 (B) Regelmäßiger Sicherheitscheck der Datenbank
- M 4.70 (C) Durchführung einer Datenbanküberwachung
- M 4.72 (Z) Datenbank-Verschlüsselung

Notfallvorsorge
- M 6.48 (A) Verhaltensregeln nach Verlust der Datenbankintegrität
- M 6.49 (A) Datensicherung einer Datenbank
- M 6.50 (Z) Archivierung von Datenbeständen
- M 6.51 (B) Wiederherstellung einer Datenbank

B 5.8 Telearbeit



Beschreibung

Unter Telearbeit versteht man im allgemeinen Tätigkeiten, die räumlich entfernt vom Standort des Arbeit- bzw. Auftraggebers durchgeführt werden, deren Erledigung durch eine kommunikationstechnische Anbindung an die IT des Arbeit- bzw. Auftraggebers unterstützt wird.

Es gibt unterschiedliche Formen von Telearbeit wie z. B. Telearbeit in Satellitenbüros, Nachbarschaftsbüros, mobile Telearbeit sowie Telearbeit in der Wohnung des Arbeitnehmers. Bei der letzteren unterscheidet man zwischen ausschließlicher Teleheimarbeit und alternierender Telearbeit, d. h. der Arbeitnehmer arbeitet teilweise im Büro und teilweise zu Hause.

Dieser Baustein konzentriert sich auf die Formen der Telearbeit, die teilweise oder ganz im häuslichen Umfeld durchgeführt werden. Es wird davon ausgegangen, dass zwischen dem Arbeitsplatz zu Hause und der Institution eine Telekommunikationsverbindung besteht, die den Austausch von Daten oder ggf. auch den Zugriff auf Daten in der Institution ermöglicht.

Die Maßnahmenempfehlungen dieses Bausteins umfassen vier verschiedene Bereiche:

- die Organisation der Telearbeit,
- den Telearbeitsrechner des Telearbeiters,
- die Kommunikationsverbindung zwischen Telearbeitsrechner und Institution und
- den Kommunikationsrechner der Institution zur Anbindung des Telearbeitsrechners.

Die in diesem Baustein aufgeführten Maßnahmenempfehlungen konzentrieren sich auf zusätzliche Sicherheitsanforderungen für ein IT-System, das für die Telearbeit eingesetzt wird. Insbesondere für die technischen Anteile der Telearbeit (Telearbeitsrechner, Kommunikationsverbindung und Kommunikationsrechner) werden sicherheitstechnische Anforderungen formuliert, die bei der konkreten Ausgestaltung durch geeignete IT-Systeme realisiert werden müssen. Für das eingesetzte IT-System muss weiterhin der passende Client-Baustein betrachtet werden, sowie die im Baustein B 2.8 *Häuslicher Arbeitsplatz* erforderlichen Maßnahmen.

Gefährdungslage

Für den IT-Grundschutz der Telearbeit werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:

- G 1.1 Personalausfall

Organisatorische Mängel:

- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- G 2.5 Fehlende oder unzureichende Wartung
- G 2.7 Unerlaubte Ausübung von Rechten (am häuslichen Arbeitsplatz und am Kommunikationsrechner der Institution)
- G 2.22 Fehlende Auswertung von Protokolldaten
- G 2.24 Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
- G 2.49 Fehlende oder unzureichende Schulung der Telearbeiter

- G 2.50 Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Telearbeiter
- G 2.51 Mangelhafte Einbindung des Telearbeiters in den Informationsfluss
- G 2.52 Erhöhte Reaktionszeiten bei IT-Systemausfall
- G 2.53 Unzureichende Vertretungsregelungen für Telearbeit

Menschliche Fehlhandlungen:
- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.13 Übertragung falscher oder nicht gewünschter Datensätze
- G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten
- G 3.30 Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners

Technisches Versagen:
- G 4.13 Verlust gespeicherter Daten

Vorsätzliche Handlungen:
- G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör
- G 5.2 Manipulation an Daten oder Software
- G 5.7 Abhören von Leitungen
- G 5.9 Unberechtigte IT-Nutzung
- G 5.10 Missbrauch von Fernwartungszugängen
- G 5.18 Systematisches Ausprobieren von Passwörtern (am häuslichen Arbeitsplatz und am Kommunikationsrechner)
- G 5.19 Missbrauch von Benutzerrechten
- G 5.20 Missbrauch von Administratorrechten
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.24 Wiedereinspielen von Nachrichten
- G 5.25 Maskerade
- G 5.43 Makro-Viren
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Eine ausreichend sichere Form der Telearbeit wird nur erreicht, wenn IT-Sicherheitsmaßnahmen aus mehreren Bereichen ineinandergreifen und sich ergänzen. Wird einer dieser Bereiche vernachlässigt, ist eine sichere Telearbeit nicht mehr möglich. Die einzelnen Bereiche und wesentlichen Maßnahmen sind:

- *Infrastrukturelle Sicherheit des Telearbeitsplatzes*: Maßnahmen, die am Telearbeitsplatz zu beachten sind, werden im Baustein B 2.8 *Häuslicher Arbeitsplatz* beschrieben.
- *Organisation der Telearbeit*: sichere Telearbeit setzt organisatorische Regelungen und personelle Maßnahmen voraus. Diese werden nachfolgend unter den Oberbegriffen "Organisation" und "Personal" beschrieben. Besonders zu beachten sind die Verpflichtungen des Telearbeiters, seine Einweisung und die Nutzungsregelungen der Kommunikation. Sie sind in den folgenden Maßnahmen beschrieben
  - M 2.113 *Regelungen für Telearbeit*
  - M 2.116 *Geregelte Nutzung der Kommunikationsmöglichkeiten*

  - M 2.117 *Regelung der Zugriffsmöglichkeiten des Telearbeiters*,
  - M 3.21 *Sicherheitstechnische Einweisung und Fortbildung des Telearbeiters*

- *Sicherheit des Telearbeitsrechners*: der Telearbeitsrechner muss so gestaltet sein, dass im unsicheren Einsatzumfeld eine sichere Nutzung möglich ist. Insbesondere darf nur eine autorisierte Person den Telearbeitsrechner offline und online nutzen können. Die notwendigen Maßnahmen sind unter dem Oberbegriff "Hardware/Software" und "Notfallvorsorge" zusammengefasst. Dabei sind insbesondere die Sicherheitsanforderungen aus M 4.63 *Sicherheitstechnische Anforderungen an den Telearbeitsrechner* zu beachten.
- *Sichere Kommunikation zwischen Telearbeitsrechner und Institution*: da die Kommunikation über öffentliche Netze ausgeführt wird, sind besondere Sicherheitsanforderungen für die Kommunikation zwischen Telearbeitsrechner und Institution zu erfüllen. Sie sind in M 5.51 *Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution* beschrieben. Für die Anbindung des Telearbeitsrechners über das öffentliche Netz ist Baustein B 4.5 *LAN-Anbindung eines IT-Systems über ISDN* zu beachten. Für die Anbindung des Telearbeitsrechners über einen Remote-Access-Service (RAS) ist Baustein B 4.4 *Remote Access* zu beachten.
- *Sicherheit des Kommunikationsrechners der Institution*: dieser Rechner stellt eine quasi öffentlich zugängliche Schnittstelle dar, über die der Telearbeiter die IT und die Daten der Institution nutzen kann. Da hier ein Missbrauch durch Dritte verhindert werden muss, sind besondere Sicherheitsanforderungen zu erfüllen, die in M 5.52 *Sicherheitstechnische Anforderungen an den Kommunikationsrechner* beschrieben sind.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Telearbeit" vorgestellt.

Planung und Konzeption

- M 2.113 (A) Regelungen für Telearbeit
- M 2.114 (A) Informationsfluss zwischen Telearbeiter und Institution
- M 2.115 (B) Betreuungs- und Wartungskonzept für Telearbeitsplätze
- M 2.116 (A) Geregelte Nutzung der Kommunikationsmöglichkeiten
- M 2.117 (A) Regelung der Zugriffsmöglichkeiten des Telearbeiters
- M 2.205 (C) Übertragung und Abruf personenbezogener Daten
- M 2.241 (C) Durchführung einer Anforderungsanalyse für den Telearbeitsplatz

Umsetzung

- M 4.63 (A) Sicherheitstechnische Anforderungen an den Telearbeitsrechner
- M 5.51 (A) Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution
- M 5.52 (A) Sicherheitstechnische Anforderungen an den Kommunikationsrechner

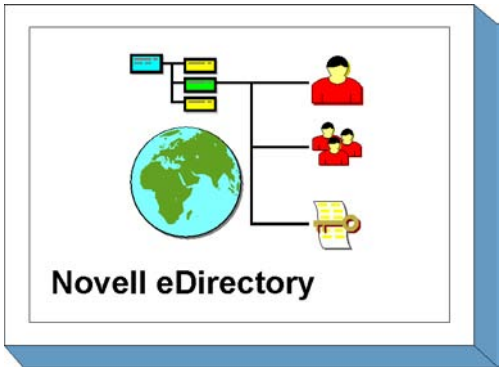
Betrieb

- M 3.21 (A) Sicherheitstechnische Einweisung und Fortbildung des Telearbeiters
- M 3.22 (B) Vertretungsregelung für Telearbeit
- M 4.3 (A) Regelmäßiger Einsatz eines Anti-Viren-Programms
- M 4.33 (A) Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung

Notfallvorsorge

- M 6.38 (B) Sicherungskopie der übermittelten Daten
- M 6.47 (B) Aufbewahrung der Backup-Datenträger für Telearbeit

B 5.9 Novell eDirectory



Beschreibung

Novell eDirectory ist ein komplexes und vielseitiges Produkt, welches

- einerseits innerhalb eines Behörden- oder Unternehmensnetzes das Management der eingebundenen Ressourcen und deren Benutzer plattformübergreifend übernehmen kann und
- andererseits auch als Internet-Informationsbasis mit gesicherten und standardisierten Zugriffsmöglichkeiten via geeigneter Clients einsetzbar ist.

Diese beiden Szenarien ergeben völlig unterschiedliche Gefährdungen für den Einsatz und den Betrieb eines solchen Systems. Vor allem eine Kombination dieser Einsatzszenarien stellt vom Standpunkt der IT-Sicherheit eine Herausforderung dar.

Entsprechend muss für die Sicherheit der in einem eDirectory-Verzeichnis gespeicherten Daten stets auch die Sicherheit des zugrunde liegenden Betriebssystems mit berücksichtigt werden. Letzteres ist jedoch nicht Bestandteil dieses Bausteins und es wird deshalb auf die entsprechenden Beschreibungen zum sicheren Betrieb des genutzten Betriebssystems in den Bausteinen der Schicht 3 verwiesen.

eDirectory ist aus dem Verzeichnisdienst *Novell Directory Services* (NDS) hervorgegangen, das Bestandteil des Betriebssystems *Netware 4* war. Dies war seinerzeit die herausragende Neuerung gegenüber dem Betriebssystem *Netware 3*. Inzwischen positioniert Novell diese Verzeichnisdienste als eigenständiges Produkt *eDirectory* vollständig unabhängig vom Netware-Betriebssystem. eDirectory lässt sich dabei auf einer Vielzahl von Betriebssystemen installieren und betreiben. In der Literatur und in den Quellen wird jedoch häufig weiterhin von "den Novell Directory Services" gesprochen und NDS mit eDirectory synonym gesetzt.

In diesem Baustein wird speziell die eDirectory-Version 8.6 betrachtet, und zwar die englische Version. Die Software unterstützt die Plattformen Netware, Windows NT/2000, Linux sowie Sun Solaris.

eDirectory kann mit spezieller Clientsoftware verwendet werden, wie dem Novell Client für die Windows-Betriebssysteme. Diese Clients sind in den Bootvorgang des jeweiligen Rechners integriert und übernehmen die Authentisierung der Benutzer gegen den Verzeichnisdienst eDirectory. Auch für Unix-Betriebssysteme (Linux, Solaris) gibt es eine ähnliche Möglichkeit, die den Mechanismus der *Pluggable Authentication Modules* (PAM) nutzt. Dabei kommen die *Novell Account Management Modules* zum Einsatz. Auch hier werden Benutzer beim Login gegen den eDirectory-Verzeichnisdienst authentisiert.

Eine andere Möglichkeit bietet der Zugriff über die LDAP-Schnittstelle. Durch die Verwendung dieser standardisierten Schnittstelle ist die Nutzung des eDirectorys auch mit anderen Applikationen und Systemen möglich. Für den Einsatz im Internet ist generell das LDAP-Protokoll die Zugriffsmethode.

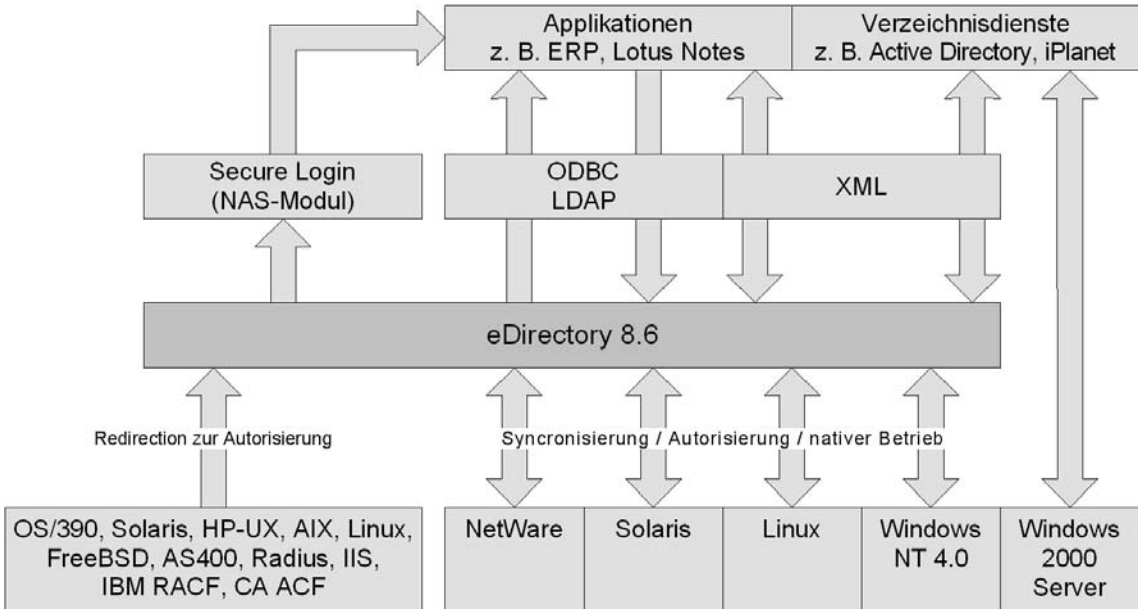


Abbildung: Architekturskizze

Weiterhin bietet die eDirectory-Software eine Vielzahl von Tools, unter anderem den *iMonitor*, der Überwachungs- und Diagnosemöglichkeiten über die Server eines Verzeichnisdienstes von einem Web-Browser aus zur Verfügung stellt.

Gefährdungslage

Aufgrund der Vielzahl an Funktionen und der Komplexität der Software ist ein eDirectory-Verzeichnisdienst einer Reihe von Gefährdungen ausgesetzt. Hinzu kommen die Gefährdungen, die das eingesetzte Betriebssystem betreffen, insbesondere den allgemeinen Serverzugriff und das Dateisystem.

Für den IT-Grundschutz eines Novell eDirectory-Systems werden folgende typische Gefährdungen angenommen:

Höhere Gewalt:
- G 1.2 Ausfall des IT-Systems

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.69 Fehlende oder unzureichende Planung des Einsatzes von Novell eDirectory
- G 2.70 Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Novell eDirectory
- G 2.71 Fehlerhafte oder unzureichende Planung des LDAP-Zugriffs auf Novell eDirectory

Menschliche Fehlhandlungen:
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.13 Übertragung falscher oder nicht gewünschter Datensätze
- G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten
- G 3.34 Ungeeignete Konfiguration des Managementsystems
- G 3.35 Server im laufenden Betrieb ausschalten

- G 3.36 Fehlinterpretation von Ereignissen
- G 3.38 Konfigurations- und Bedienungsfehler
- G 3.43 Ungeeigneter Umgang mit Passwörtern
- G 3.50 Fehlkonfiguration von Novell eDirectory
- G 3.51 Falsche Vergabe von Zugriffsrechten im Novell eDirectory
- G 3.52 Fehlkonfiguration des Intranet-Clientzugriffs auf Novell eDirectory
- G 3.53 Fehlkonfiguration des LDAP-Zugriffs auf Novell eDirectory

Technisches Versagen:

- G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
- G 4.13 Verlust gespeicherter Daten
- G 4.33 Schlechte oder fehlende Authentikation
- G 4.34 Ausfall eines Kryptomoduls
- G 4.44 Ausfall von Novell eDirectory

Vorsätzliche Handlungen:

- G 5.16 Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal
- G 5.17 Gefährdung bei Wartungsarbeiten durch externes Personal
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.19 Missbrauch von Benutzerrechten
- G 5.20 Missbrauch von Administratorrechten
- G 5.65 Verhinderung der Dienste eines Datenbanksystems
- G 5.78 DNS-Spoofing
- G 5.81 Unautorisierte Benutzung eines Kryptomoduls

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den Einsatz der eDirectory-Komponenten sollte bereits bei der Planung ein spezifisches IT-Sicherheitskonzept erstellt werden, welches sich konsistent in das bestehende organisationsweite IT-Sicherheitskonzept integrieren lässt. Das eDirectory-System muss so konfiguriert werden, dass bereits bestehende Sicherheitsanforderungen umgesetzt werden, und hat darüber hinaus weitere, eDirectory-spezifische Anforderungen durchzusetzen.

Ein eDirectory-System wird in der Regel im Umfeld mit weiteren Systemen eingesetzt, welche den Zugriff auf das interne Netz von außen kontrollieren. Hierbei sind insbesondere Firewall-Systeme und Systeme zur Fernwartung zu nennen, mit denen eDirectory zusammenarbeiten muss. Aus diesem Grund sind bei der Durchführung der eDirectory-spezifischen Maßnahmen stets auch die entsprechenden Maßnahmen aus den jeweiligen Bausteinen zusätzlich betroffener Systeme mit zu berücksichtigen. Neben den Bausteinen aus der Schicht 3 sind unter anderem auch die folgenden Bausteine zu nennen:

- B 3.301 *Sicherheitsgateway (Firewall)*, sofern eDirectory-Systeme in einer Firewall-Umgebung eingesetzt werden
- B 4.4 *Remote Access*, wenn der Zugriff auf das eDirectory-System über Einwahlleitungen erfolgt
- B 5.7 *Datenbanken*, allgemein

Für die sichere Implementierung eines eDirectory-Systems sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Installation bis hin zum Betrieb. Die einzelnen Schritte sowie die jeweiligen Maßnahmen, die auf diesem Weg zu beachten sind, sind nachstehend zusammengefasst:

1. Nach der Entscheidung, eDirectory als Verzeichnissystem einzusetzen, muss Software und eventuell zusätzlich benötigte Hardware beschafft werden. Da eDirectory verschiedene Einsatzmöglichkeiten zulässt (siehe oben), hängt die gegebenenfalls zu beschaffende Hardware von den geplanten Einsatzszenarien ab. Daher sind folgende Maßnahmen zu ergreifen:

   - Zunächst muss der Einsatz des eDirectory-Systems geplant werden (siehe Maßnahmen M 2.236 *Planung des Einsatzes von Novell eDirectory* und M 2.237 *Planung der Partitionierung und Replikation im Novell eDirectory*).
   - Parallel dazu ist eine Sicherheitsrichtlinie zu erarbeiten (siehe Maßnahme M 2.238 *Festlegung einer Sicherheitsrichtlinie für Novell eDirectory*), die einerseits bereits bestehende IT-Sicherheitsrichtlinien im Kontext von eDirectory umsetzt und gleichzeitig eDirectory-spezifische Ergänzungen konsistent definiert.
   - Vor der tatsächlichen Verwendung des eDirectory-Systems im Regelbetrieb müssen die Benutzer und Administratoren auf den Umgang mit dem Produkt geschult werden. Insbesondere für Administratoren empfiehlt sich eine intensive Beschäftigung mit der Materie, die auf einen umfassenden Kenntnisstand bezüglich der Sicherheit der eingesetzten Betriebssysteme aufsetzen sollte (siehe M 3.29 *Schulung zur Administration von Novell eDirectory*). Benutzern sollten die verfügbaren Sicherheitsmechanismen der eingesetzten Clients detailliert vermittelt werden (siehe M 3.30 *Schulung zum Einsatz von Novell eDirectory Clientsoftware*).

2. Nachdem die organisatorischen und planerischen Vorbereitungen durchgeführt wurden, kann die Installation des eDirectory-Systems erfolgen. Folgende Maßnahmen sind dabei zu ergreifen:

   - Die Installation kann erst dann als abgeschlossen angesehen werden, wenn die eDirectory-Systeme in einen sicheren Zustand überführt wurden (siehe M 4.153 *Sichere Installation von Novell eDirectory* und M 4.154 *Sichere Installation der Novell eDirectory Clientsoftware*). Dadurch wird sichergestellt, dass in der anschließenden Konfigurationsphase nur berechtigte Administratoren auf das eDirectory-System zugreifen können.
   - Nach der "Rohinstallation" erfolgt eine erstmalige Konfiguration des eDirectory-Systems, siehe M 4.155 *Sichere Konfiguration von Novell eDirectory*, M 4.156 *Sichere Konfiguration der Novell eDirectory Clientsoftware*, M 4.157 *Einrichten von Zugriffsberechtigungen auf Novell eDirectory,* sowie M 4.158 *Einrichten des LDAP-Zugriffs auf Novell eDirectory*.

3. Nach der Konfiguration und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Dabei sind unter Sicherheitsgesichtspunkten folgende Aspekte zu beachten:

   - Ein eDirectory-System ist in der Regel kontinuierlichen Veränderungen unterworfen. Entsprechend müssen die sicherheitsrelevanten Konfigurationsparameter ständig angepasst werden. Weiterhin hängt die Sicherheit bei einer verteilten Softwarearchitektur von der Sicherheit sämtlicher Teilsysteme ab. Dies gilt insbesondere für die eDirectory-Clientsoftware. Die für den sicheren Betrieb relevanten Maßnahmen sind in M 4.159 *Sicherer Betrieb von Novell eDirectory* und M 4.160 *Überwachen von Novell eDirectory*, sowie der Maßnahme zur Kommunikationssicherung (siehe M 5.97 *Absicherung der Kommunikation mit Novell eDirectory*) zusammengefasst.
   - Neben den Maßnahmen zur Absicherung des laufenden Betriebs sind auch die Maßnahmen zur Notfallvorsorge von zentraler Bedeutung. Hinweise zu diesem Thema finden sich in M 6.80 *Erstellen eines Notfallplans für den Ausfall eines Novell eDirectory Verzeichnisdienstes* sowie M 6.81 *Erstellen von Datensicherungen für Novell eDirectory*.

Nachfolgend wird das Maßnahmenbündel für den Baustein "Novell eDirectory" vorgestellt:

Planung und Konzeption

- M 2.236 (A) Planung des Einsatzes von Novell eDirectory
- M 2.237 (B) Planung der Partitionierung und Replikation im Novell eDirectory
- M 2.238 (A) Festlegung einer Sicherheitsrichtlinie für Novell eDirectory
- M 2.239 (A) Planung des Einsatzes von Novell eDirectory im Intranet
- M 2.240 (A) Planung des Einsatzes von Novell eDirectory im Extranet

Umsetzung

- M 3.29 (A) Schulung zur Administration von Novell eDirectory
- M 3.30 (A) Schulung zum Einsatz von Novell eDirectory Clientsoftware
- M 4.153 (A) Sichere Installation von Novell eDirectory
- M 4.154 (A) Sichere Installation der Novell eDirectory Clientsoftware
- M 4.155 (A) Sichere Konfiguration von Novell eDirectory
- M 4.156 (A) Sichere Konfiguration der Novell eDirectory Clientsoftware
- M 4.157 (A) Einrichten von Zugriffsberechtigungen auf Novell eDirectory
- M 4.158 (B) Einrichten des LDAP-Zugriffs auf Novell eDirectory

Betrieb

- M 4.159 (A) Sicherer Betrieb von Novell eDirectory
- M 4.160 (B) Überwachen von Novell eDirectory
- M 5.97 (B) Absicherung der Kommunikation mit Novell eDirectory

Notfallvorsorge

- M 6.80 (A) Erstellen eines Notfallplans für den Ausfall eines Novell eDirectory Verzeichnisdienstes
- M 6.81 (A) Erstellen von Datensicherungen für Novell eDirectory

B 5.10 Internet Information Server

Beschreibung

Der Microsoft Internet Information Server (IIS) stellt die Internet Informationsdienste (WWW-Server, FTP-Server, NNTP-Dienst und SMTP-Dienst) für die Microsoft Betriebssysteme zur Verfügung.

Standardmäßig wird der IIS mit den Serverversionen von Windows NT 4.0 (IIS 4), Windows 2000 (IIS 5), Windows XP Professional (IIS 5.1) und Windows Server 2003 (IIS 6) ausgeliefert.

In diesem Baustein werden spezifische Gefährdungen und Maßnahmen für einen Webserver basierend auf dem IIS 4 oder IIS 5 beschrieben. Für Webserver, die auf einer neueren Version des IIS basieren, können die detaillierten technischen Maßnahmen dieses Bausteins möglicherweise nicht direkt angewandt werden. Zumindest die allgemeineren Maßnahmen sollten jedoch in jedem Fall umgesetzt werden.

Internet Information Server 4.0 (IIS 4)

Viele Windows NT Versionen beinhalten noch eine ältere Version des IIS, meist die Version 2.0. Aufgrund vorhandener Sicherheitsrisiken sollten solche älteren Versionen jedoch nicht mehr eingesetzt werden. Das bedeutet, dass der IIS 4 neu zu installieren ist. Es sollte kein Update von einem installierten IIS 2.0 auf den IIS 4 stattfinden.

Der IIS 4 ist Bestandteil des Windows NT 4.0 Server Option Packs, das eine Reihe von zusätzlichen Dienstprogrammen und Anwendungen enthält, die mit dem IIS 4 zusammenarbeiten. Als typische Microsoft-Anwendung ist der IIS 4 eng mit den Ressourcen des Betriebssystems verzahnt. Der IIS 4 verwendet die Verzeichnisdatenbank von Windows NT, d. h. die Benutzerkonten werden mit Hilfe des Windows NT-Benutzermanagers verwaltet. Außerdem werden vorhandene Windows-NT-Dienstprogramme, wie der Systemmonitor, die Ereignisanzeige und die SNMP-Unterstützung, zur Verwaltung des Webservers genutzt.

Internet Information Server 5.0 (IIS 5.0)

Mit dem Betriebssystem Windows 2000 werden die Internet Informationsdienste durch den IIS 5.0 bereitgestellt. Der IIS 5.0 ist vollständig in das Betriebssystem integriert und wird standardmäßig mit installiert.

Im Vergleich zum IIS 4 enthält die Version 5.0 eine Reihe von neuen Funktionen und Verbesserungen. Beispielsweise wird die MMC-Technologie (Microsoft Management Console) durch die Integration in Windows 2000 vollständig unterstützt und die Verwaltung des Servers durch neue Sicherheitsassistenten, frei zu definierende Fehlermeldungen (für HTTP) und losgelöste Serverprozesse (Start der Internet Informationsdienste ohne Neustart des Computers) vereinfacht. Daneben wurden die ASP-Merkmale durch zusätzliche Methoden ergänzt und die Protokollierungsfunktionen, insbesondere im Bereich Performance und Auslastung, erweitert.

Nach einer Installation der Betriebssysteme Windows 2000 Datacenter Server, Windows 2000 Advanced Server und Windows 2000 Server ist der IIS 5 standardmäßig aktiviert. Nach einer Installation von Windows 2000 Professional ist der IIS 5 standardmäßig nicht aktiviert.

Internet Information Server 5.1 (IIS 5.1)

Der IIS 5.1 wird mit dem Betriebssystem Windows XP Professional ausgeliefert. Nach einer Installation von Windows XP Professional ist der IIS 5.1 standardmäßig nicht aktiviert.

Internet Information Server 6.0 (IIS 6)

Der IIS 6 wird mit dem Betriebssystem Windows Server 2003 ausgeliefert. Gegenüber den Vorgängerversionen wurde diese Version grundlegend überarbeitet und weitgehend neu entwickelt.

Gefährdungslage

Generell hängt die Gefährdungslage vom Einsatzszenario ab. Webserver werden für vielfältige Aufgaben eingesetzt, beispielsweise als einfache Informationsserver im Internet oder Intranet, auf die nur lesend zugegriffen werden darf, aber auch als Basis für weiterführende Anwendungen, z. B. E-Commerce oder E-Government-Anwendungen, die auf Datenbanken zugreifen oder als Entwicklungsserver für neue Applikationen.

Wird der IIS als Internet-Server eingesetzt, zeigt sich eine besondere Gefährdungslage. In diesem Fall ist der Zugriff Externer und Unbekannter auf den Server erwünscht, dabei müssen aber die Verfügbarkeit des Servers, die Integrität der Daten und auch die Vertraulichkeit von Konfigurationsdateien und vorhandenen Skripten gewährleistet sein. Nur durch die Kombination von übergeordneten, organisatorischen Maßnahmen mit technischen Sicherheitsvorkehrungen, wie geeigneten Trenneinrichtungen und der sicheren Konfiguration des Betriebssystems sowie der eigentlichen Internetdienste, kann diese Anforderung erfüllt werden.

Allerdings darf nicht nur die Möglichkeit eines Angriffs von außen betrachtet werden, denn auch innerhalb eines LANs ist ein Angriff auf einen IIS denkbar. Wie jedes vernetzte IT-System ist auch ein Webserver mit IIS vielfältigen Gefahren ausgesetzt, so dass der sicheren Konfiguration des Systems und seiner Komponenten auch im internen Netz eine wichtige Rolle zukommt.

Für den IT-Grundschutz eines IIS-basierenden Webservers werden die folgenden typischen Gefährdungen angenommen:

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.94 Unzureichende Planung des IIS-Einsatzes

Menschliche Fehlhandlungen:
- G 3.56 Fehlerhafte Einbindung des IIS in die Systemumgebung
- G 3.57 Fehlerhafte Konfiguration des Betriebssystems für den IIS
- G 3.58 Fehlkonfiguration eines IIS
- G 3.59 Unzureichende Kenntnisse über aktuelle Sicherheitslücken und Prüfwerkzeuge für den IIS

Technisches Versagen:
- G 4.13 Verlust gespeicherter Daten
- G 4.22 Software-Schwachstellen oder -Fehler
- G 4.39 Software-Konzeptionsfehler

Vorsätzliche Handlungen:
- G 5.2 Manipulation an Daten oder Software
- G 5.20 Missbrauch von Administratorrechten
- G 5.28 Verhinderung von Diensten
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.84 Gefälschte Zertifikate

- G 5.88 Missbrauch aktiver Inhalte
- G 5.108 Ausnutzen von systemspezifischen Schwachstellen des IIS

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Da in einer Einsatzumgebung von vernetzten Systemen der IIS nicht alleine betrachtet werden darf, sind darüber hinaus folgende Bausteine zu berücksichtigen:

- B 3.101 *Servergestütztes Netz*
- B 3.301 *Sicherheitsgateway (Firewall)*
- B 5.4 *Webserver*
- B 3.103 *Server unter Windows NT*, (bei der Verwendung von IIS 4.0)
- B 3.106 *Server unter Windows 2000* (bei der Verwendung von IIS 5.0)

Je nachdem, wie die Administration und Pflege des IIS-Systems erfolgen, sollten gegebenenfalls auch die Bausteine B 4.4 *Remote Access* und B 5.8 *Telearbeit* für die Anbindung externer Anschlusspunkte herangezogen werden.

Für den erfolgreichen Aufbau und Betrieb eines Internet Information Servers sind in den einzelnen Realisierungsphasen (Konzeption, Implementation und Betrieb) eine Reihe von Maßnahmen umzusetzen. Die Realisierungsschritte, die dabei durchlaufen werden, sowie die Maßnahmen, die in den jeweiligen Schritten zu beachten sind, werden nachfolgend aufgeführt. Teilweise stellen diese Maßnahmen "Spezialisierungen" von Maßnahmen aus einem der oben genannten Bausteine dar.

1. Nach der Entscheidung, einen IIS als Webserver einzusetzen, muss die Beschaffung der Software und eventuell zusätzlich benötigter Hardware erfolgen. Die zu beschaffende Soft- und Hardware ist abhängig von den geplanten Einsatzszenarien. Daher sind folgende Maßnahmen durchzuführen:
   - Zunächst muss der Einsatz des IIS-Systems geplant werden (siehe M 2.267 *Planen des IIS-Einsatzes*).
   - Parallel dazu ist eine Sicherheitsrichtlinie zu erarbeiten (siehe M 2.268 *Festlegung einer IIS-Sicherheitsrichtlinie*), in der die bestehenden Sicherheitsrichtlinien für den IIS angewandt und spezialisiert werden.
   - Vor der tatsächlichen Einführung des IIS-Systems müssen die Administratoren auf den Umgang mit dem IIS durch eine Schulung vorbereitet werden. Insbesondere für Administratoren empfiehlt sich aufgrund der Komplexität der Verwaltung eine intensive Schulung. Die Administratoren sollen dabei detaillierte Systemkenntnisse erwerben (siehe M 3.36 *Schulung der Administratoren zur sicheren Installation und Konfiguration des IIS*), so dass eine konsistente und korrekte Systemverwaltung gewährleistet ist.
2. Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt wurden, kann die Installation des Webservers erfolgen. Dabei sind folgenden Maßnahmen zu beachten:
   - Die Installation kann erst dann als abgeschlossen betrachtet werden, wenn die IIS-Systeme in einen sicheren Zustand gebracht wurden. Basis für die sichere Installation des IIS ist ein

abgesichertes Betriebssystem (siehe M 4.174 *Vorbereitung der Installation von Windows NT/2000 für den IIS* und M 4.175 *Sichere Konfiguration von Windows NT/2000 für den IIS*). Es muss sichergestellt werden, dass in der folgenden Konfigurationsphase nur berechtigte Administratoren auf das IIS-System zugreifen können.

- Nach der "Rohinstallation" erfolgt eine erstmalige Konfiguration des IIS-Systems. Bei der Konfiguration sind die relevanten Maßnahmen aus den Bereichen Hardware / Software und Kommunikation zu berücksichtigen.

3. Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:

   - Ein IIS ist in der Regel ständigen Veränderungen unterworfen. Daher müssen sicherheitsrelevante Konfigurationsparameter kontinuierlich angepasst werden. Die für den sicheren Betrieb relevanten Sicherheitseinstellungen sind in den Maßnahmen zur Hardware / Software und Kommunikation zusammengefasst.
   - Neben der Absicherung im laufenden Betrieb spielt jedoch auch die Notfallvorsorge eine wichtige Rolle, da nur so der Schaden im Notfall verringert werden kann. Hinweise zur Notfallvorsorge finden sich in M 6.85 *Erstellung eines Notfallplans für den Ausfall des IIS*.

Nachfolgend wird nun das Maßnahmenbündel für den Baustein IIS vorgestellt.

Planung und Konzeption

- M 2.267 (A) Planen des IIS-Einsatzes
- M 2.268 (A) Festlegung einer IIS-Sicherheitsrichtlinie

Umsetzung

- M 3.36 (A) Schulung der Administratoren zur sicheren Installation und Konfiguration des IIS
- M 4.174 (A) Vorbereitung der Installation von Windows NT/2000 für den IIS
- M 4.175 (A) Sichere Konfiguration von Windows NT/2000 für den IIS
- M 4.178 (A) Absicherung der Administrator- und Benutzerkonten beim IIS-Einsatz
- M 4.179 (A) Schutz von sicherheitskritischen Dateien beim IIS-Einsatz
- M 4.180 (A) Konfiguration der Authentisierungsmechanismen für den Zugriff auf den IIS
- M 4.181 (A) Ausführen des IIS in einem separaten Prozess
- M 4.184 (A) Deaktivieren nicht benötigter Dienste beim IIS-Einsatz
- M 4.185 (A) Absichern von virtuellen Verzeichnissen und Web-Anwendungen beim IIS-Einsatz
- M 4.186 (A) Entfernen von Beispieldateien und Administrations-Scripts des IIS
- M 4.187 (A) Entfernen der FrontPage Server-Erweiterung des IIS
- M 4.188 (B) Prüfen der Benutzereingaben beim IIS-Einsatz
- M 4.189 (B) Schutz vor unzulässigen Programmaufrufen beim IIS-Einsatz
- M 4.190 (B) Entfernen der RDS-Unterstützung des IIS
- M 5.101 (B) Entfernen nicht benötigter ODBC-Treiber beim IIS-Einsatz
- M 5.102 (B) Installation von URL-Filtern beim IIS-Einsatz
- M 5.103 (B) Entfernen sämtlicher Netzwerkfreigaben beim IIS-Einsatz
- M 5.104 (C) Konfiguration des TCP/IP-Filters beim IIS-Einsatz
- M 5.105 (C) Vorbeugen vor SYN-Attacken auf den IIS
- M 5.106 (A) Entfernen nicht vertrauenswürdiger Root-Zertifikate beim IIS-Einsatz
- M 6.86 (B) Schutz vor schädlichem Code auf dem IIS

Betrieb

- M 4.182 (B) Überwachen des IIS-Systems
- M 4.183 (A) Sicherstellen der Verfügbarkeit und Performance des IIS

Notfallvorsorge

- M 6.85 (C) Erstellung eines Notfallplans für den Ausfall des IIS
- M 6.87 (A) Datensicherung auf dem IIS

B 5.11 Apache-Webserver

Beschreibung

Der Apache-Webserver ist seit 1997 der bei weitem am häufigsten eingesetzte Webserver. Laut der Netcraft-Webserverstatistik war im August 2002 auf über 60 Prozent aller betrachteten Webserver ein Apache-Webserver im Einsatz.

Der Apache-Webserver entstand 1995 aus dem bis dahin meist genutzten Webserver, dem *NCSA httpd*, der am National Center for Supercomputing Applications der University of Illinois entwickelt worden war. Da der bisherige Entwickler, Rob McCool, das NCSA verlassen hatte, war die Entwicklung ins Stocken geraten. Eine Gruppe von Webmastern fand sich zusammen, um den *NCSA httpd* weiter zu entwickeln. Da die Weiterentwicklung zunächst in der Form von Patches und Ergänzungen zum *NCSA httpd* erfolgte, bekam das Produkt Namen Apache, von "A patchy server".

Ende 1995 wurde die Version 1.0 des Apache-Webservers veröffentlicht. Nach einer längeren Betatestphase für die Version 2, die sich seit ungefähr 1998 in der Entwicklung befand, wurde im April 2002 mit der Version 2.0.35 die erste "Produktionsversion", beim Apache-Webserver *General Availability Release* genannt, freigegeben.

In der neuen Version des Apache-Webservers hat sich vor allem an der Architektur des Apache-Kerns einiges geändert. Bei der Entwicklung der neuen Version hatten die Autoren das Ziel, die Portierung auf neue Plattformen einfacher zu gestalten, und entwarfen eine modulare Architektur, in der die *Apache Portable Runtime* (APR) eine Abstraktionsschicht zwischen dem unterliegenden Betriebssystem und dem Apache 2.0 darstellt. Die APR stellt für die eigentlichen Apache-Module gewissermaßen ein virtuelles Betriebssystem dar, verwendet aber so weit wie möglich native Betriebssystemaufrufe, um eine bestmögliche Performance zu erzielen.

Gefährdungslage

Für den Grundschutz werden pauschal die folgenden Gefährdungen als typisch für einen Apache-Webserver angenommen:

Organisatorische Mängel:
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- G 2.87 Verwendung unsicherer Protokolle in öffentlichen Netzen
- G 2.97 Unzureichende Notfallplanung bei einem Apache-Webserver

Menschliche Fehlhandlungen:
- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.38 Konfigurations- und Bedienungsfehler
- G 3.62 Fehlerhafte Konfiguration des Betriebssystems für einen Apache-Webserver
- G 3.63 Fehlerhafte Konfiguration eines Apache-Webservers

Technisches Versagen:
- G 4.39 Software-Konzeptionsfehler

Vorsätzliche Handlungen:
- G 5.2 Manipulation an Daten oder Software

- G 5.7 Abhören von Leitungen
- G 5.21 Trojanische Pferde
- G 5.28 Verhinderung von Diensten
- G 5.71 Vertraulichkeitsverlust schützenswerter Informationen
- G 5.85 Integritätsverlust schützenswerter Informationen
- G 5.109 Ausnutzen systemspezifischer Schwachstellen beim Apache-Webserver

Maßnahmenempfehlungen

Seit Version 2 wird neben diversen Unix-Varianten auch Windows als Betriebssystemplattform für den Apache-Webserver voll unterstützt. Zwar gab es auch eine Portierung der Version 1.3 auf Windows, diese galt jedoch bis zuletzt als nicht so stabil wie die Unix-Versionen. Die Maßnahmen in diesem Baustein sind so weit wie möglich so formuliert, dass sie sich sowohl auf einen Apache-Webserver unter Unix als auch unter Windows anwenden lassen. An einigen Stellen wird auf betriebssystemspezifische Aspekte besonders eingegangen.

Für die sichere Planung, Implementierung und den sicheren Betrieb eines Apache-Webservers müssen zunächst die allgemeinen Aspekte berücksichtigt werden, die im Baustein B 5.4 *Webserver* erläutert werden. In diesem Baustein werden vor allem solche Aspekte der Sicherheit betrachtet, die über die allgemeinen Aspekte hinaus speziell für einen Apache-Webserver relevant sind.

Im Rahmen der allgemeinen Planung für den Aufbau eines Webangebots (siehe M 2.172 *Entwicklung eines Konzeptes für die WWW-Nutzung*) wird entschieden, zu welchem Zweck das Webangebot dienen soll und an welche Zielgruppen es sich richtet. Ist im Anschluß daran die Entscheidung gefallen, dass das Webangebot mit einem Apache-Webserver aufgebaut werden soll, muss sich eine detailliertere Planung für dessen Einsatz anschließen (siehe M 2.269 *Planung des Einsatzes eines Apache-Webservers*). Soll der Apache-Webserver in Verbindung mit SSL eingesetzt werden, so muss dies frühzeitig in die Planung einbezogen werden (siehe M 2.270 *Planung des SSL-Einsatzes beim Apache-Webserver*). Der Einsatz von SSL erfordert auch beim Betrieb des Servers einige zusätzliche Maßnahmen (siehe M 5.107 *Verwendung von SSL im Apache-Webserver*).

Die Administratoren müssen für die sichere Installation und den sicheren Betrieb eines Apache-Webservers geschult werden. Wichtige Aspekte, die in einer solchen Schulung abgedeckt werden sollten, sind in M 3.37 *Schulung der Administratoren eines Apache-Webservers* beschrieben.

Bevor der Apache-Webserver auf dem Serverrechner installiert wird, muss zunächst das Betriebssystem geeignet konfiguriert und abgesichert werden (siehe M 4.192 *Konfiguration des Betriebssystems für einen Apache-Webserver*). Die Integrität und Authentizität der zur Installation verwendeten Pakete (Quelltext- oder Binärpakete) muss überprüft werden (siehe M 4.191 *Überprüfung der Integrität und Authentizität der Apache-Pakete*). Bei der eigentlichen Installation und der anschließenden Gundkonfiguration sind eine Reihe von Punkten zu beachten, die in M 4.193 *Sichere Installation eines Apache-Webservers* und M 4.194 *Sichere Grundkonfiguration eines Apache-Webservers* beschrieben werden.

Sollen auf dem Webserver Bereiche nicht öffentlich, sondern nur einem begrenzten Kreis von Besuchern zugänglich sein, so ist M 4.195 *Konfiguration der Zugriffssteuerung beim Apache-Webserver* zu beachten. Beim Betrieb eines Apache-Webservers sind außerdem die in M 4.196 *Sicherer Betrieb eines Apache-Webservers* beschriebenen Aspekte zu beachten.

Falls auf dem Apache-Webserver dynamische Webseiten über Server-Side-Includes, cgi-Programme oder andere Servererweiterungen realisiert werden sollen, so ist M 4.197 *Servererweiterungen für dynamische Webseiten beim Apache-Webserver* zu berücksichtigen. Der Apache-Webserver kann zur Erhöhung der Systemsicherheit unter verschiedenen Unix-Varianten in einem sogenannten chroot-Käfig installiert werden (siehe M 4.198 *Installation eines Apache-Webservers in einem chroot-Käfig*).

Einige Punkte, die bei der Notfallplanung zusätzlich zu den allgemeinen Aspekten der Notfallplanung speziell für einen Apache-Webserver berücksichtigt werden müssen, sind in M 6.89 *Notfallvorsorge für einen Apache-Webserver* zusammen gefasst.

In Beispielen und bei konkreten Empfehlungen wird im Rahmen dieses Bausteins von Version 2.0 eines Apache-Webservers ausgegangen. Wo nicht explizit auf einen Unterschied hingewiesen wird, sollten jedoch die meisten Aussagen auch für die Version 1.3 gelten. Beispiele werden meist in der Syntax angegeben, wie sie für einen Apache-Webserver unter Unix korrekt ist, sie sind aber ohne große Mühe auf die Windows-Version übertragbar.

Nachfolgend sind die Maßnahmen zur Umsetzung von IT-Grundschutz für den Apache-Webserver zusammengefasst. Die Maßnahmen des allgemeinen Webserver-Bausteins und der anderen relevanten Bausteine werden aus Gründen der Übersichtlichkeit hier nicht noch einmal aufgeführt.

Panung und Konzeption
- M 2.269 (A) Planung des Einsatzes eines Apache-Webservers
- M 2.270 (Z) Planung des SSL-Einsatzes beim Apache Webserver

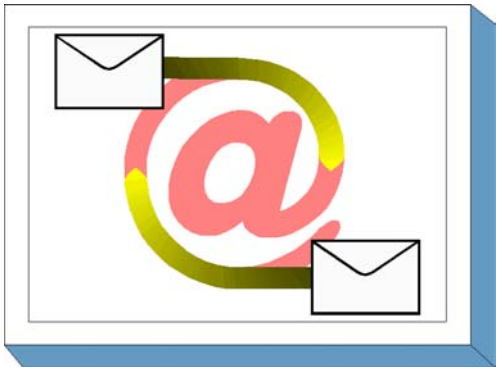
Beschaffung
- M 4.191 (A) Überprüfung der Integrität und Authentizität der Apache-Pakete

Umsetzung
- M 3.37 (A) Schulung der Administratoren eines Apache-Webservers
- M 4.192 (A) Konfiguration des Betriebssystems für einen Apache-Webserver
- M 4.193 (A) Sichere Installation eines Apache-Webservers
- M 4.194 (A) Sichere Grundkonfiguration eines Apache-Webservers
- M 4.195 (A) Konfiguration der Zugriffssteuerung beim Apache-Webserver
- M 4.197 (B) Servererweiterungen für dynamische Webseiten beim Apache-Webserver
- M 4.198 (Z) Installation eines Apache-Webservers in einem chroot-Käfig
- M 5.107 (Z) Verwendung von SSL im Apache-Webserver

Betrieb
- M 4.196 (A) Sicherer Betrieb eines Apache-Webservers

Notfallvorsorge
- M 6.89 (A) Notfallvorsorge für einen Apache-Webserver

B 5.12 Exchange 2000 / Outlook 2000



Beschreibung

Der Exchange 2000 Server ist ein Managementsystem für Nachrichten, das überdies Funktionen im Bereich der Workflow-Unterstützung bietet. Es ist dazu gedacht, in mittleren bis großen Behörden bzw. Unternehmen den internen und externen E-Mail-Verkehr zu regeln. Ebenso werden Newsgroups, Kalender und Aufgabenlisten von Exchange verwaltet.

Outlook 2000 ist ein E-Mail-Client, der Bestandteil des Office 2000 Paketes von Microsoft ist. Neben der reinen E-Mail-Funktionalität bietet er eine Reihe von Zusatzfunktionen, die den Arbeitsprozess in Unternehmen und Behörden erleichtern sollen.

Es handelt sich hierbei um eine typische Client-Server-Anwendung, wobei Exchange 2000 die Server- und Outlook 2000 die Client-Komponente darstellt.

Unterschiede zur Vorgängerversion Exchange 5.5

Die Vorgängerversion von Exchange 2000 Server ist der Exchange 5.5 Server. Zwischen diesen Versionen besteht konzeptionell ein gravierender Unterschied. Exchange 2000 Server integriert sich tief in das Betriebssystem Windows 2000, speziell in das Active Directory. Dies betrifft die Organisation des Exchange Systems, dessen Administration und besonders auch die Sicherheit des Gesamtsystems durch die Verwendung der Systemrichtlinien von Windows 2000.

Das Standort-Konzept (*Site*) von Exchange 5.5 wurde fallen gelassen und stattdessen das *Forest*-Konzept von Windows 2000 übernommen, denen sich sogenannte *Routing Groups* von Exchange 2000 Servern unterordnen. Darüber hinaus haben sich interne Kommunikationsprotokolle geändert. Beispielsweise basiert in der neuen Version die interne E-Mail-Kommunikation innerhalb einer Routing Group ausschließlich auf dem "klassischen" *Simple Mail Transfer Protocol* (SMTP) anstelle der zuvor verwendeten *Remote Procedure Calls* (RPCs).

Weitere Unterschiede ergeben sich aus einer erweiterten Funktionalität und einer Vergrößerung des Leistungsspektrums: Die E-Mail- und Nachrichten-Datenbanken können in separat verwaltete Teile partitioniert und auf verschiedene Server verteilt werden. Dies dient zum einen der Skalierbarkeit des Systems und erhöht zum anderen auch die Ausfallsicherheit. Weiterhin wird eine verteilte Konfiguration unterstützt, eine vereinheitlichte Administration über die *Microsoft Management Console* (MMC) ermöglicht, mehrfache öffentliche Verzeichnisse bereitgestellt, Video- und Datenkonferenzen ermöglicht und *Instant Messaging* unterstützt.

Exchange 2000 Server integriert außerdem in hohem Maße die *Internet Information Services* (IIS) von Windows 2000. Dies führt zu zusätzlichen Gefährdungen und ist für einen gesicherten Betrieb des Systems unbedingt zu berücksichtigen. Betroffen ist davon unter anderem der sogenannte *Web Store* (Installable File System - IFS), der den lokalen und den entfernten (remote) Zugriff auf das Dateisystem erlaubt. Das Laufwerk M (Standardeinstellung) eines jeden Rechners, auf dem Exchange 2000 installiert wird, bietet einen direkten Zugang über das Dateisystem auf diesen *Web Store*. Dieses Laufwerk erhält automatisch eine Netzfreigabe, so dass weitere Applikationen darauf zugreifen können. Ein weiterer Punkt sind die *Web Forms*, die vom Exchange 2000 Server direkt an Browser übermittelt werden, um interaktive Arbeitsprozesse über Browser zu ermöglichen.

Zwischen der Exchange Store Architektur und den Internet Access Protokollen liegt eine spezielle Schicht, der *Exchange Interprocess Communication Layer* EXIPC, auch *Epoxy-Layer* genannt. Dieser besteht aus einem asynchron geteilten Speicherbereich, in welchem sowohl der Prozess *STORE.EXE* als auch die IIS-Protokolle Daten lesen und schreiben können. *STORE.EXE* ist ein wesentlicher Prozess des Exchange Servers. Dadurch wird ein schneller Datenaustausch ermöglicht, der aus Sicherheitssicht jedoch auch problematisch ist.

Die Zusammenarbeit von Client mit Server lässt sich auf vielfältige Art und Weise konfigurieren und betreiben. Hier ergeben sich zum Teil erhebliche Unterschiede in Bezug auf die Sicherheit. Weiterhin ist es möglich, den Exchange 2000 Server so zu konfigurieren, dass mittels des sogenannten *Outlook Web Access* (OWA) direkt über das Internet zugegriffen werden kann. Dies ist von erheblicher sicherheitstechnischer Relevanz, siehe M 4.164 *Browser-Zugriff auf Exchange 2000*.

Allgemeine Gesichtspunkte beim Betrieb eines E-Mail-Systems

Für einen sicheren Betrieb des Exchange 2000 Systems gelten auch allgemeine IT-Sicherheitsaspekte eines E-Mail-Systems, wie z. B. die Frage der Internet-Anbindung, eventuelle unterliegende Verschlüsselungsmaßnahmen, Behandlung aktiver Inhalte, Einsatz von Anti-Viren-Software und vieles mehr. Diesbezüglich wird auf den Baustein B 5.3 *E-Mail* verwiesen. Die dort dargestellten Gefährdungen und Maßnahmen besitzen im Kontext von Exchange/Outlook 2000 uneingeschränkte Gültigkeit.

Wie in der bisherigen Übersicht dargestellt, spielt die Sicherheit von Windows 2000 eine zentrale Rolle für die Sicherheit von Exchange bzw. Outlook. Dies gilt sowohl für die Server als auch die Clients des betrachteten Netzes. In diesem Zusammenhang sei auf die Bausteine B 3.106 Server unter *Windows 2000* und B 3.209 *Client unter Windows XP* sowie die dort aufgeführten Gefährdungen und Maßnahmen verwiesen.

Eine Ende-zu-Ende-Sicherheit auf Anwendungsebene (hier: Outlook-Client) kann mittels Verschlüsselung und Signatur von elektronischen Nachrichten erzielt werden. Die Konfiguration und der Betrieb eines solchen Systems setzen dabei entweder die Verwendung der Microsoft Public Key Infrastruktur (PKI) oder eine Plug-In-Lösung eines Drittherstellers voraus. Theoretisch ist es natürlich möglich, gänzlich auf eine PKI zu verzichten, jedoch sind dann die bekannten Skalierungsprobleme im Schlüsselmanagement oder die Probleme der Vertrauensbeziehungen zu lösen.

Betrachtete Versionen

Im folgenden sind die derzeit aktuellen (Stand Oktober 2001) Produktversionen aufgeführt. In der Folge bezeichnet Exchange 2000 Server jede dieser Produktausprägungen:

- Exchange 2000 Server:

  Dies ist die Grundausstattung des Produktes und richtet sich an kleine bis mittlere Unternehmen bzw. Behörden.

- Exchange 2000 Enterprise Server:

  Diese Ausprägung beinhaltet die Grundfunktionalität von Exchange 2000 sowie Mechanismen für eine bessere Skalierbarkeit des Systems, z. B. Verteilung der E-Mail-Datenbanken auf verschiedene Server, keine Beschränkungen in der Größe von Transaktionsdaten, Vier-Wege-Clustering.

- Exchange 2000 Conferencing Server:

  Diese Version bietet die umfassendste Funktionalität, unter anderem Werkzeuge zur Durchführung von Daten-, Audio- und Videokonferenzen, Load Balancing und Bandbreitenmanagement.

- Outlook 2000, Service Release 1

In diesem Baustein wird die englischsprachige Version des Produktes Exchange 2000 betrachtet. Dies erfolgt vor dem Hintergrund der allgemeinen Empfehlung, stets diejenige Version im Betrieb einzusetzen, für welche Software-Anpassungen und Fehlerbehebungen generell als erstes verfügbar sind.

Für die Office-Anwendung Outlook 2000 wird die deutsche Version betrachtet, da diese in deutschsprachigen Behörden und Unternehmen eine größere Verbreitung findet als die entsprechende englischsprachige Ausgabe.

Für ein Exchange/Outlook 2000 System können folgende Sicherheitsziele unterschieden werden:

1. Zugangssicherheit: Die auf einem Exchange 2000 Server gespeicherten Daten dürfen nur berechtigten Benutzern zugänglich sein. Das heißt, der Zugriff auf den Server muss entsprechend geregelt sein. Dies wird in erster Linie durch geeignete Konfiguration des Windows 2000 Servers erreicht, auf dem die Exchange Services installiert werden. Um Rollenkonflikte und erhebliche zusätzliche Risiken zu vermeiden, sollte dies grundsätzlich ein Member Server des Netzes sein und kein Domänen-Controller.
2. Zugriffskontrolle: Neben der Kontrolle des Serverzugriffs stellt der Zugriff auf Datenbankebene (*Mail Stores*) einen wichtigen Sicherheitsaspekt dar. Hier lässt sich mit Hilfe der Sicherheitseinstellungen des Active Directory (Access Control Lists auf die relevanten Objekte) ein Schutz erreichen.
3. Kommunikationssicherheit: Wenn ein E-Mail-Client auf die Daten des Exchange 2000 Servers zugreift, werden die abgerufenen Daten über eine Netzverbindung (LAN, WAN oder Internet) übertragen. Um Vertraulichkeit und Integrität der Daten zu gewährleisten, lassen sich Schutzmaßnahmen auf verschiedenen Ebenen der Übertragung durchführen.
4. Verfügbarkeit: Um die Produktivität innerhalb eines Unternehmens bzw. einer Behörde nicht zu gefährden, sind Anforderungen an die Verfügbarkeit des Systems zu stellen. Dies umso mehr, als E-Mail oft einen entscheidenden Anteil an der Abwicklung von Geschäftsprozessen hat. Maßnahmen zum Schutz der Verfügbarkeit sind die Verteilung der E-Mail-Datenbanken auf mehrere Server, allgemeine Spiegelungstechniken sowie die Erstellung eines Notfallplans.

Gefährdungslage

Für den IT-Grundschutz eines Exchange 2000 Systems inklusive zugeordneter Outlook 2000 Clients werden die folgenden typischen Gefährdungen angenommen:

Höhere Gewalt:

- G 1.2 Ausfall des IT-Systems

Organisatorische Mängel:

- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.2 Unzureichende Kenntnis über Regelungen
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindungen
- G 2.55 Ungeordnete E-Mail-Nutzung
- G 2.91 Fehlerhafte Planung der Migration von Exchange 5.5 nach Exchange 2000
- G 2.92 Fehlerhafte Regelungen für den Browser-Zugriff auf Exchange
- G 2.95 Fehlendes Konzept zur Anbindung anderer E-Mail-Systeme an Exchange/Outlook

Menschliche Fehlhandlungen:
- G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten
- G 3.38 Konfigurations- und Bedienungsfehler
- G 3.60 Fehlkonfiguration von Exchange 2000 Servern
- G 3.61 Fehlerhafte Konfiguration von Outlook 2000 Clients

Technisches Versagen:
- G 4.22 Software-Schwachstellen oder -Fehler
- G 4.32 Nichtzustellung einer Nachricht

Vorsätzliche Handlungen:
- G 5.9 Unberechtigte IT-Nutzung
- G 5.19 Missbrauch von Benutzerrechten
- G 5.23 Computer-Viren
- G 5.77 Mitlesen von E-Mails
- G 5.83 Kompromittierung kryptographischer Schlüssel
- G 5.84 Gefälschte Zertifikate
- G 5.85 Integritätsverlust schützenswerter Informationen

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Zusätzlich zu der Absicherung der Komponenten von Exchange bzw. Outlook muss noch ein spezifisches Sicherheitskonzept erstellt werden, das sich konsistent in das bestehende betriebsweite Sicherheitskonzept integrieren lässt. Das Exchange/Outlook-System muss so konfiguriert werden, dass bereits bestehende Sicherheitsanforderungen umgesetzt werden. Darüber hinaus sind weitere, für Exchange bzw. Outlook spezifische Anforderungen zu erfüllen.

Ein Exchange/Outlook-System wird in der Regel im Umfeld mit weiteren Systemen eingesetzt, die den Zugriff auf das interne Netz von außen kontrollieren. Hierbei sind insbesondere Firewall-Systeme und Systeme zur Fernwartung zu nennen, mit denen Exchange 2000 zusammenarbeiten muss. Aus diesem Grund sind bei der Durchführung der für Exchange bzw. Outlook spezifischen Maßnahmen stets auch die entsprechenden Empfehlungen aus den jeweiligen Bausteinen zusätzlich betroffener Systeme zu berücksichtigen. Neben den Bausteinen der Schicht 3 sind unter anderem auch die folgenden Bausteine zu nennen:

- B 3.301 Firewall, sofern Exchange 2000 Systeme in einer Firewall-Umgebung eingesetzt werden.
- B 4.4 Remote Access, wenn der Zugriff auf das Exchange-System über Einwahlleitungen erfolgt.

Für die erfolgreiche Implementierung eines Exchange/Outlook-Systems sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung über die Installation bis hin zum Betrieb. Die einzelnen Schritte sowie die jeweiligen Maßnahmen, die auf diesem Weg zu beachten sind, sind nachstehend zusammengefasst:

1. Nach der Entscheidung, Exchange 2000 als internes Kommunikationssystem einzusetzen, muss die Beschaffung der Software und eventuell zusätzlich benötigter Hardware erfolgen. Da Exchange 2000 in verschiedenen Ausprägungen erhältlich ist (siehe oben), hängt das zu beschaffende Softwareprodukt von den geplanten Einsatzszenarien ab. Daher sind folgende Maßnahmen zu ergreifen:

- Zunächst muss der Einsatz des Exchange/Outlook-Systems geplant werden (siehe M 2.247 *Planung des Einsatzes von Exchange/Outlook 2000*).
- Parallel dazu ist eine Sicherheitsrichtlinie zu erarbeiten (siehe M 2.248 *Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000*), die einerseits bereits bestehende Sicherheitsrichtlinien im Kontext von Exchange/Outlook umsetzt und gleichzeitig für Exchange bzw. Outlook spezifische Ergänzungen definiert.
- Vor der tatsächlichen Verteilung des Exchange/Outlook-Systems müssen die Benutzer und Administratoren im Umgang mit den Produkten geschult werden. Insbesondere für Administratoren empfiehlt sich eine intensive und praxisnahe Schulung, die auf fundierte Kenntnisse bezüglich Windows 2000 und dessen Sicherheit aufsetzen sollte (siehe M 3.31 *Schulung zur Systemarchitektur und Sicherheit von Exchange 2000 für Administratoren*). Benutzern sollten die verfügbaren Sicherheitsmechanismen von Outlook 2000 detailliert erläutert werden (siehe M 3.32 *Schulung zu Sicherheitsmechanismen von Outlook 2000 für Benutzer*).

2. Nachdem die organisatorischen und planerischen Vorbereitungen durchgeführt wurden, kann die Installation des Exchange/Outlook-Systems erfolgen. Folgende Maßnahmen sind dabei zu ergreifen:
   - Die Systeme, auf denen Exchange/Outlook installiert werden soll, müssen geeignet abgesichert sein. Empfehlungen für die Betriebssystemplattform des Servers finden sich unter anderem in Baustein B 3.106 *Server unter Windows 2000*.
   - Die Installation kann erst dann als abgeschlossen angesehen werden, wenn die Exchange/Outlook-Systeme in einen sicheren Zustand überführt wurden (siehe M 4.161 *Sichere Installation von Exchange/Outlook 2000*). Dadurch wird sichergestellt, dass in der anschließenden Konfigurationsphase nur berechtigte Administratoren auf das Exchange 2000 System zugreifen können.
   - Nach der Installation erfolgt eine erstmalige Konfiguration des Exchange/Outlook-Systems, siehe M 4.162 *Sichere Konfiguration von Exchange 2000 Server*, M 4.165 *Sichere Konfiguration von Outlook 2000* sowie M 4.164 *Browser-Zugriff auf Exchange 2000*.

3. Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Dabei sind aus Sicht der IT-Sicherheit folgende Aspekte zu beachten:
   - Ein Exchange/Outlook-System ist in der Regel kontinuierlichen Veränderungen unterworfen. Entsprechend müssen die sicherheitsrelevanten Konfigurationsparameter ständig angepasst werden. Weiterhin hängt die Sicherheit bei einer verteilten Software-Architektur von der Sicherheit sämtlicher Teilsysteme ab. Dies gilt insbesondere für die Outlook-Clients. Die für den sicheren Betrieb relevanten Empfehlungen sind in M 4.166 *Sicherer Betrieb von Exchange/Outlook 2000* und den Maßnahmen zur Kommunikationssicherung (siehe M 5.100 *Einsatz von Verschlüsselungs- und Signaturverfahren für die Exchange 2000 Kommunikation*) zusammengefasst.
   - Neben der Absicherung des laufenden Betriebs sind auch die Maßnahmen zur Notfallvorsorge von zentraler Bedeutung. Hinweise zu diesem Thema finden sich in M 6.82 *Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen*.

Nachfolgend wird das Maßnahmenbündel für den Einsatz von Exchange 2000 und Outlook 2000 vorgestellt.

Planung und Konzeption

- M 2.247 (A) Planung des Einsatzes von Exchange/Outlook 2000
- M 2.248 (A) Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000
- M 2.249 (B) Planung der Migration von "Exchange 5.5-Servern" nach "Exchange 2000"

Umsetzung

- M 3.31 (A) Schulung zur Systemarchitektur und Sicherheit von Exchange 2000 für Administratoren
- M 3.32 (A) Schulung zu Sicherheitsmechanismen von Outlook 2000 für Benutzer
- M 4.161 (A) Sichere Installation von Exchange/Outlook 2000
- M 4.162 (A) Sichere Konfiguration von Exchange 2000 Servern
- M 4.163 (A) Zugriffsrechte auf Exchange 2000 Objekte
- M 4.164 (A) Browser-Zugriff auf Exchange 2000
- M 4.165 (A) Sichere Konfiguration von Outlook 2000
- M 5.99 (C) SSL/TLS-Absicherung für Exchange 2000

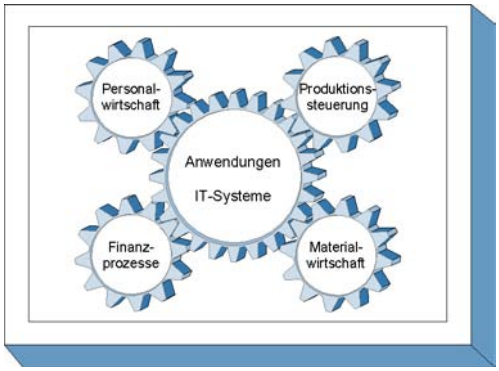
Betrieb

- M 4.166 (A) Sicherer Betrieb von Exchange/Outlook 2000
- M 4.167 (B) Überwachung und Protokollierung von Exchange 2000 Systemen
- M 5.100 (Z) Einsatz von Verschlüsselungs- und Signaturverfahren für die Exchange 2000 Kommunikation

Notfallvorsorge

- M 6.82 (C) Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen

B 5.13 SAP System



SAP Systeme werden in Unternehmen und Behörden eingesetzt, um interne und externe Unternehmens- bzw. Behörden- und Geschäftsabläufe zu automatisieren und technisch zu unterstützen (Enterprise Resource Planning, ERP). Ein SAP System verarbeitet daher typischerweise vertrauliche Daten, so dass ein entsprechender Schutz aller Systemkomponenten und Daten gewährleistet und das Schutzniveau an die Gefährdungslage angepasst werden muss. Daneben spielen auch Integrität und Verfügbarkeit eine wichtige Rolle.

SAP bietet eine umfangreiche Palette an Systemen, Komponenten und Funktionen an, so dass mit dem Begriff "SAP System" nicht eindeutig eine bestimmte Installation oder Gruppe von Komponenten gekennzeichnet werden kann. Im Rahmen dieses Bausteines kann nicht auf alle verfügbaren SAP Produkte eingegangen werden, die Darstellung beschränkt sich daher auf eine typische und in der Praxis häufig anzutreffende Kerninstallation.

Ein Beispiel für ein typisches SAP System ist ein mySAP ERP System, früher SAP R/3 genannt, mit den Enterprise Core Components Human Capital Management (HCM), Finanzen & Controlling (FI/CO), Material Management (MM), Verkauf & Vertrieb (SD), Logistik (PP), Projektmanagement (PS) und Qualitätsmanagement (QM). Als Kernkomponente fungiert hier der so genannte SAP NetWeaver ApplicationServer (ehemals SAP Web Application Server). Weitere Bestandteile der aktuellen NetWeaver-Plattform (derzeit NetWeaver 04) sind SAP XI als Daten-Integrationsplattform zwischen einzelnen SAP Systemen und auch zwischen SAP und Nicht-SAP Systemen sowie das SAP Enterprise Portal als Integrationsplattform für Anwendungen und Anwender. Auch diese beiden Bestandteile werden auf dem SAP NetWeaver ApplicationServer ausgeführt.

Ein kurzer Überblick über SAP Systeme und wichtige Fachbegriffe aus dem SAP Umfeld finden sich in der Maßnahme M 3.53 *Einführung in SAP Systeme*.

Die Gefährdungen und Maßnahmen dieses Bausteines orientieren sich hauptsächlich am SAP NetWeaver ApplicationServer, der vorrangigen technischen Basiskomponente der NetWeaver Plattform. Da auch diese Basiskomponente bereits in mehreren Versionen vorliegt und sich diese in den angebotenen Funktionen unterscheiden, wird bewusst auf die Darstellung versionsbezogener Unterschiede verzichtet. Auf diese Weise wird erreicht, dass der Baustein über längere Zeit angewendet werden kann und auch für bestehende SAP R/3 Systeme eingesetzt werden kann. Im Fokus der Maßnahmen und Gefährdungen steht dabei die Grundabsicherung eines SAP Systems auf Ebene der so genannten Basis-Administration. Die applikations- oder modulbezogene (z. B. HCM, FI) Absicherung ist nicht Teil dieses Bausteines. Da viele Applikationen und Module jedoch die Sicherheitsmechanismen der Basiskomponente nutzen, können die angegebenen Maßnahmen auch hier mit entsprechenden Anpassungen angewendet werden.

Ziel des Bausteines ist nicht, die bestehende, umfangreiche Dokumentation von SAP zu reproduzieren, sondern empfohlene sicherheitsrelevante Vorgehensweisen und beachtenswerte Besonderheiten darzustellen. Ansonsten kann auf die existierende SAP Dokumentation verwiesen werden, die detaillierte technische Darstellungen enthält. Die relevanten SAP Dokumentationen sind zentral in M 2.346 *Nutzung der SAP Dokumentation* zusammengestellt. IT-Sicherheitsbeauftragten und Administratoren hilft der Baustein nicht nur bei der Planung des SAP Einsatzes, er nennt auch die wichtigsten technischen Aspekte, die auch Sicht der IT-Sicherheit zu beachten sind.

Gefährdungslage

Der vorliegende Baustein behandelt Gefährdungen der SAP NetWeaver Basiskomponente SAP NetWeaver ApplicationServer, die im Rahmen der so genannten Basisadministration dieser Komponente in Intranet- und Internet-Szenarien relevant sind.

Generell hängt die Gefährdungslage von SAP Systemen vom Einsatzszenario ab. Ein SAP System in einem isolierten Behörden- oder Unternehmensnetz ist in der Regel weniger gefährdet als ein System, das an das Internet angeschlossen ist. Aber auch in internen Netzen kann mangelnder Schutz auf Netz- oder SAP System-Ebene dazu führen, dass unberechtigte Zugriffsmöglichkeiten bestehen. Dann spielt es eine Rolle, ob auf Daten nur lesend zugegriffen werden kann oder ob die Daten auch verändert werden können. Dies ist generell für Behörden und Unternehmen kritisch und wird beispielsweise auch bei Prüfungen untersucht, die auf dem Sarbanes Oxley Act basieren. In diesem Kontext sind speziell die Probleme unzureichender Berechtigungen und fehlender Funktionstrennung relevant.

Gerade durch den Einsatz von Web-Technologien, wie HTTP-basierten Zugriffsmöglichkeiten und Web-Applikationen mit Internet-Anbindung, hat sich die Gefährdungslage von SAP Systemen stark erhöht. Aufgrund der öffentlichen Netzanbindung von SAP Systemen ergeben sich daher in Folge von unsachgemäßer oder fehlerhafter Konfiguration wesentlich stärkere Gefährdungen. Dies gilt auch für fehlende oder unvollständig etablierte Prozesse, insbesondere in Outsourcing-Szenarien.

Höhere Gewalt:
- G 1.1 Personalausfall

Organisatorische Mängel:
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindungen
- G 2.87 Verwendung unsicherer Protokolle in öffentlichen Netzen
- G 2.108 Fehlende oder unzureichende Planung des SAP Einsatzes

Menschliche Fehlhandlungen:
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.9 Fehlerhafte Administration des IT-Systems
- G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten

Vorsätzliche Handlungen:
- G 5.2 Manipulation an Daten oder Software
- G 5.7 Abhören von Leitungen
- G 5.9 Unberechtigte IT-Nutzung
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.128 Unberechtigter Zugriff auf Daten durch Einbringen von Code in ein SAP System

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für den erfolgreichen Aufbau eines SAP Systems sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der strategischen Entscheidung, über Planung, Konzeption und Installation bis zum Betrieb. Nicht vergessen werden darf dabei die ordnungsgemäße Aussonderung eines Systems, wenn das Ende der Betriebsphase erreicht wird.

Parallel zur Betriebsphase muss die Notfallvorsorge sicherstellen, dass der Betrieb auch im Notfall aufrecht erhalten werden kann. IT-Sicherheitsmanagement und Revision stellen sicher, dass das Regelwerk auch eingehalten wird.

Die Schritte, die dabei zu durchlaufen sind sowie die Maßnahmen, die in den jeweiligen Phasen beachtet werden sollten, sind im Folgenden aufgeführt:

Planungs- und Konzeptionsphase

Ist die Entscheidung für ein SAP System gefallen, muss der Einsatz des SAP Systems geplant und konzipiert werden. Die dabei zu berücksichtigenden Aspekte sind in der Maßnahme M 2.341 *Planung des SAP Einsatzes* zusammengefasst. Wichtig ist dabei, wie die Berechtigungen für die Benutzer eines SAP Systems geplant werden. Die dabei relevanten Themen sind in der Maßnahme M 2.342 *Planung von SAP Berechtigungen* enthalten. Es ist zu bedenken, dass die Sicherheit eines SAP Systems bereits in der Planungs- und Konzeptionsphase entscheidend beeinflusst werden kann, indem sicherheitsrelevante Aspekte berücksichtigt werden. Maßnahmen für die SAP spezifische Benutzerschulung finden sich in M 3.52 *Schulung zu SAP Systemen*, da ausreichende Kenntnisse bei Benutzern und Administratoren von SAP Systemen die Sicherheit beeinflussen.

Besondere Aufmerksamkeit ist der Planung der Sicherheit in solchen Szenarien zu widmen, in denen SAP Systeme einer besonderen Gefährdung ausgesetzt sind. Dabei kann es sich um typische Internet-Szenarien handeln, so dass die Empfehlungen der Maßnahme M 2.344 *Sicherer Betrieb von SAP Systemen im Internet* umgesetzt werden müssen. Es kann sich aber auch um Intranet-Szenarien handeln, beispielsweise wenn ein SAP System von einem Behörden- oder Unternehmensportal aus angesprochen werden soll. Hier werden dann die Empfehlungen der Maßnahme M 2.343 *Absicherung eines SAP Systems im Portal-Szenario* relevant. Ein häufiges Szenario, das mit spezifischen Gefährdungen verbunden ist, ist das Outsourcing eines SAP Systems, denn hier erfolgen Konfiguration und Administration durch behörden- oder unternehmensfremde Personen. Für diesen Fall finden sich Hinweise und Empfehlungen in der Maßnahme M 2.345 *Outsourcing eines SAP Systems*.

Umsetzungsphase

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt worden sind, kann die Installation eines SAP Systems erfolgen. Dabei ist die Maßnahme M 4.256 *Sichere Installation von SAP Systemen* zu beachten.

Die reine Installation eines SAP Systems stellt nur einen geringen Anteil der Arbeiten dar, die in der Umsetzungsphase durchzuführen sind. Der überwiegende Arbeitsaufwand fällt nach der Installation durch die Erstkonfiguration des SAP Systems an. Durch die erste Konfiguration werden die Grundsicherheit bei der Betriebsaufnahme und die Rahmenbedingungen für die zukünftige Sicherheit des SAP Systems festgelegt und definiert. Daher sind in der Umsetzungsphase folgende Aspekte zu berücksichtigen:

Die Erstkonfiguration ist sowohl für den ABAP-Stack als auch für den Java-Stack erforderlich. Es sind insbesondere Situationen zu vermeiden, in denen einer der beiden Stacks unkonfiguriert bleibt, da er nicht genutzt wird. Die entsprechenden Empfehlungen finden sich in folgenden Maßnahmen:

- M 4.258 *Sichere Konfiguration des SAP ABAP-Stacks*
- M 4.266 *Sichere Konfiguration des SAP Java-Stacks*

Kern eines jeden SAP Systems ist die Datenbank und die darin gehaltenen Tabellen mit den Daten. Die Datenbank speichert nicht nur die Geschäftsdaten einer Behörden oder Unternehmens, sondern auch die internen Funktionen und Verwaltungsinformationen des SAP Systems. Sicherheitsprobleme im Bereich der Datenbank betreffen daher sofort immer die Gesamtsicherheit des SAP Systems. Die Datenbank-bezogenen Maßnahmen sind zusammengefasst in:

- M 4.269 *Sichere Konfiguration der SAP System Datenbank*

SAP Systeme sind verteilt aufgebaut und kommunizieren daher über verschiedene Schnittstellen miteinander oder mit anderen externen Client- oder Server-Systemen. Die Absicherung der Kommunikation ist daher eine wichtige Aufgabe. Generell kann ein SAP System viele unterschiedliche Kommunikationskanäle nutzen, die auch von den installierten Applikationen und Modulen abhängen. In der Regel werden jedoch einige wenige Basis-Kommunikationsmechanismen und -Schnittstellen genutzt. Die relevante Einstiegsmaßnahme ist:

- M 5.125 *Absicherung der Kommunikation von und zu SAP Systemen*

Ein SAP System muss an die lokalen funktionalen Anforderungen einer Behörde oder eines Unternehmens angepasst werden. Dies geschieht durch das so genannte Customizing (Anpassung an den Kunden). Die in diesem Kontext relevante Maßnahme ist:

- M 2.348 *Sicherheit beim Customizing von SAP Systemen*

Betrieb

Nach der Erstinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:

Damit Sicherheitsverstöße bemerkt werden, muss eine entsprechende Überwachung des SAP Systems erfolgen. Hinweise dazu finden sich in den Maßnahmen:

- M 4.270 SAP Protokollierung
- M 2.347 Regelmäßige Sicherheitsprüfungen für SAP Systeme

Neuere Versionen der SAP Software bieten die Möglichkeit, ein Computer-Viren-Schutzprogramm anzuschließen, so dass beispielsweise Dokumente und Daten, die an das SAP System gesandt werden, auf Viren geprüft werden können. Hinweise dazu finden sich in:

- M 4.271 *Virenschutz für SAP Systeme*

Da ein SAP System immer Veränderungen unterworfen ist, die sich meist aus veränderten Anforderungen oder Einsatzszenarien ableiten, muss sichergestellt werden, dass das gewünschte Sicherheitsniveau aufrecht erhalten wird. Dies trifft insbesondere für Eigenentwicklungen zu. Die im diesem Kontext relevanten Maßnahmen sind:

- M 2.349 *Sicherheit bei der Software-Entwicklung für SAP Systeme*
- M 2.221 *Änderungsmanagement*

Neuer Code oder andere veränderbare Komponenten müssen in das System eingebracht werden. Dazu steht für ABAP-bezogene Veränderungen das SAP Transportsystem zur Verfügung. Für die Software-Verteilung im Bereich des Java-Stacks wird hingegen ein anderer Mechanismus eingesetzt. In beiden Fällen muss eine Absicherung erfolgen, damit die Mechanismen nicht missbraucht werden können. Die relevanten Maßnahmen sind:

- M 4.272 *Sichere Nutzung des SAP Transportsystems*
- M 4.273 *Sichere Nutzung der SAP Java-Stack Software-Verteilung*

Aussonderung

Empfehlungen zur Deinstallation von SAP Systemen, etwa nach Abschluss des Regelbetriebs, finden sich in der Maßnahme M 2.350 *Aussonderung von SAP Systemen*.

Notfallvorsorge

Empfehlungen zur Notfallvorsorge für SAP Systeme finden sich in der Maßnahme M 6.97 *Notfallvorsorge für SAP Systeme*.

Nachfolgend werden alle Maßnahmen für SAP Systeme vorgestellt:

Planung und Konzeption

- M 2.341 (A) Planung des SAP Einsatzes
- M 2.342 (A) Planung von SAP Berechtigungen
- M 2.343 (C) Absicherung eines SAP Systems im Portal-Szenario
- M 2.344 (C) Sicherer Betrieb von SAP Systemen im Internet
- M 2.345 (C) Outsourcing eines SAP Systems
- M 2.346 (A) Nutzung der SAP Dokumentation
- M 3.52 (A) Schulung zu SAP Systemen
- M 3.53 (Z) Einführung in SAP Systeme

Umsetzung

- M 4.256 (A) Sichere Installation von SAP Systemen
- M 4.257 (A) Absicherung des SAP Installationsverzeichnisses auf Betriebssystemebene
- M 4.258 (A) Sichere Konfiguration des SAP ABAP-Stacks
- M 4.259 (A) Sicherer Einsatz der ABAP-Stack Benutzerverwaltung
- M 4.260 (A) Berechtigungsverwaltung für SAP Systeme
- M 4.261 (B) Sicherer Umgang mit kritischen SAP Berechtigungen
- M 4.262 (C) Konfiguration zusätzlicher SAP Berechtigungsprüfungen
- M 4.263 (A) Absicherung von SAP Destinationen
- M 4.264 (A) Einschränkung von direkten Tabellenveränderungen in SAP Systemen
- M 4.265 (B) Sichere Konfiguration der Batch-Verarbeitung im SAP System
- M 4.266 (A) Sichere Konfiguration des SAP Java-Stacks
- M 4.267 (A) Sicherer Einsatz der SAP Java-Stack Benutzerverwaltung
- M 4.268 (A) Sichere Konfiguration der SAP Java-Stack Berechtigungen
- M 4.269 (A) Sichere Konfiguration der SAP System Datenbank
- M 5.125 (B) Absicherung der Kommunikation von und zu SAP Systemen
- M 5.126 (A) Absicherung der SAP RFC-Schnittstelle
- M 5.127 (B) Absicherung des SAP Internet Connection Framework (ICF)
- M 5.128 (B) Absicherung der SAP ALE (IDoc/BAPI) Schnittstelle
- M 5.129 (C) Sichere Konfiguration der HTTP-basierten Dienste von SAP Systemen

Betrieb

- M 4.270 (A) SAP Protokollierung
- M 2.347 (B) Regelmäßige Sicherheitsprüfungen für SAP Systeme
- M 2.348 (C) Sicherheit beim Customizing von SAP Systemen
- M 2.349 (C) Sicherheit bei der Software-Entwicklung für SAP Systeme
- M 2.221 (A) Änderungsmanagement
- M 4.271 (C) Virenschutz für SAP Systeme
- M 4.272 (A) Sichere Nutzung des SAP Transportsystems
- M 4.273 (A) Sichere Nutzung der SAP Java-Stack Software-Verteilung

Aussonderung

- M 2.350 (A) Aussonderung von SAP Systemen

Notfallvorsorge

- M 6.97 (A) Notfallvorsorge für SAP Systeme

G 1 Gefährdungskatalog Höhere Gewalt

G 1.1 Personalausfall

Durch Krankheit, Unfall, Tod oder Streik kann Personal unvorhersehbar ausfallen. Desweiteren ist auch der vorhersagbare Personalausfall bei Urlaub, Fortbildung oder einer regulären Beendigung des Arbeitsverhältnisses zu berücksichtigen, insbesondere wenn die Restarbeitszeit z. B. durch einen Urlaubsanspruch verkürzt wird.

Schlüsselstellung im IT-Bereich

In allen Fällen kann die Konsequenz sein, dass entscheidende Aufgaben aufgrund des Personalausfalls im IT-Einsatz nicht mehr wahrgenommen werden. Dies ist besonders dann kritisch, wenn die betroffene Person im IT-Bereich eine Schlüsselstellung einnimmt und aufgrund fehlenden Fachwissens anderer nicht ersetzt werden kann. Störungen des IT-Betriebs können die Folge sein.

Verlust von Wissen und Geheimnissen

Ein Personalausfall kann zusätzlich einen empfindlichen Verlust von Wissen und Geheimnissen nach sich ziehen, der die nachträgliche Übertragung der Tätigkeiten auf andere Personen unmöglich macht.

Beispiele:

- Aufgrund längerer Krankheit blieb der Netzadministrator vom Dienst fern. In der betroffenen Firma lief das Netz zunächst fehlerfrei weiter. Nach zwei Wochen jedoch war nach einem Systemabsturz niemand in der Lage, den Fehler zu beheben. Dies führte zu einem Ausfall des Netzes über mehrere Tage.
- Während des Urlaubs des Administrators muss für Datensicherungszwecke auf die Backupbänder im Datensicherungstresor zurückgegriffen werden. Der Zugangscode zum Tresor wurde erst kürzlich geändert und ist nur dem Administrator bekannt. Erst nach mehreren Tagen konnte die Datenrestaurierung durchgeführt werden, da der Aufenthaltsort des Administrators zuerst ermittelt werden musste.

G 1.2 Ausfall des IT-Systems

Ausfall zentraler Komponenten

Der Ausfall einer Komponente eines IT-Systems kann zu einem Ausfall des gesamten IT-Betriebs führen. Insbesondere zentrale Komponenten eines IT-Systems sind geeignet, solche Ausfälle herbeizuführen, z. B. LAN-Server, Datenfernübertragungseinrichtung. Auch der Ausfall von Komponenten der technischen Infrastruktur, beispielsweise Klima- oder Stromversorgungseinrichtungen, kann zu einem Ausfall des IT-Systems beitragen.

Technisches Versagen/ menschliche Fehlhandlungen

Technisches Versagen (z. B. G 4.1 *Ausfall der Stromversorgung*) muss nicht zwingend als Ursache für den Ausfall eines IT-Systems angenommen werden. Ausfälle lassen sich auch oft auf menschliches Fehlverhalten (z. B. G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*) oder vorsätzliche Handlungen (z. B. G 5.4 *Diebstahl*, G 5.102 *Sabotage*) zurückführen. Auch durch höhere Gewalt (z. B. Feuer, Blitzschlag, Chemieunfall) können Schäden eintreten, allerdings sind diese Schäden meist um ein Vielfaches höher.

Werden auf einem IT-System zeitkritische IT-Anwendungen betrieben, sind die Folgeschäden nach Systemausfall entsprechend hoch, wenn es keine Ausweichmöglichkeiten gibt.

Beispiele:

- Durch Spannungsspitzen in der Stromversorgung wird das Netzteil eines wichtigen IT-Systems zerstört. Da es sich um ein älteres Modell handelt, steht nicht unmittelbar Ersatz bereit. Die Reparatur nimmt einen Tag in Anspruch, in dieser Zeit ist der gesamte IT-Betrieb nicht verfügbar.
- Es wird eine Firmware in ein IT-System eingespielt, die nicht für diesen Systemtyp vorgesehen ist. Das IT-System startet daraufhin nicht mehr fehlerfrei und muss vom Hersteller wieder betriebsbereit gemacht werden.
- Bei einem Internet Service Provider führte ein Stromversorgungsfehler in einem Speichersystem dazu, dass dieses abgeschaltet wurde. Obwohl der eigentliche Fehler schnell behoben werden konnte, ließen sich die betroffenen IT-Systeme anschließend nicht wieder hochfahren, da Inkonsistenzen im Dateisystem auftraten. Bis alle Folgeprobleme behoben waren, waren mehrere der vom ISP betriebenen Webserver tagelang nicht erreichbar.

Ausfall einer Archivkomponente

- In elektronischen Archiven kann der Zeitpunkt der erstmaligen Archivierung als Entstehungszeitpunkt von Dokumenten missinterpretiert werden, wenn keine anderweitigen Beweisverfahren, z. B. Zeitstempeldienste, zur Beglaubigung eingesetzt werden. Dies gilt vor allem für Geschäftsprozesse, in die die elektronische Archivierung von massenhaft anfallenden Belegdaten transparent eingebunden ist. Im vorliegenden Fall konnte aufgrund des Ausfalls einer Archivkomponente ein Teil von Belegdaten erst um einen Tag verzögert archiviert werden. Durch die Verwendung von WORM-Medien wurde die Reihenfolge der physikalischen Archivierung der Geschäftsbelege trotzdem nachweisbar dokumentiert, es wurde jedoch kein Nachweis für die ansonsten nicht auftretende Verzögerung durch die ausgefallene Archivkomponente geführt. Dadurch entstand bei einer späteren Prüfung der Eindruck einer nachträglichen Manipulation.

G 1.3 Blitz

Freisetzung elektrischer Energie

Der Blitz ist die wesentliche während eines Gewitters bestehende Gefährdung für ein Gebäude und die darin befindliche Informationstechnik. Blitze erreichen bei Spannungen von mehreren 100.000 Volt Ströme bis zu 200.000 Ampere. Diese enorme elektrische Energie wird innerhalb von 50-100 Mikrosekunden freigesetzt und abgebaut. Ein Blitz mit diesen Werten, der in einem Abstand von ca. 2 km einschlägt, verursacht auf elektrischen Leitungen im Gebäude immer noch Spannungsspitzen, die zur Zerstörung empfindlicher elektronischer Geräte führen können. Diese indirekten Schäden nehmen mit abnehmender Entfernung zu.

Gebäudeschäden

Schlägt der Blitz direkt in ein Gebäude ein, werden durch die dynamische Energie des Blitzes Schäden hervorgerufen. Dies können Beschädigungen des Baukörpers (Dach und Fassade), Schäden durch auftretende Brände oder Überspannungsschäden an elektrischen Geräten sein.

Über das regional unterschiedliche Blitzschlagrisiko erteilt der Deutsche Wetterdienst entsprechende Auskünfte.

Beispiele:

- Auf einem deutschen Großflughafen schlug ein Blitz in unmittelbarer Nähe neben dem Tower ein. Trotz der installierten äußeren Blitzschutzanlage (Blitzableiter) wurde die automatische Löschanlage im IT-Bereich ausgelöst und dadurch der gesamte Flughafenbetrieb für 2 Stunden lahmgelegt.
- Neben direkten Schäden haben Blitzschläge auch oft weitreichendere Folgen. Häufig finden sich Meldungen wie diese: Im April 1999 führte ein Blitzeinschlag in eine Hochspannungsleitung im Raum Darmstadt zu einem kurzzeitigen Stromausfall, von dem ca. 80.000 Personen betroffen waren.

G 1.4 Feuer

Neben direkten durch das Feuer verursachten Schäden an einem Gebäude oder dessen Einrichtung lassen sich Folgeschäden aufzeigen, die insbesondere für die Informationstechnik in ihrer Schadenswirkung ein katastrophales Ausmaß erreichen können. Löschwasserschäden treten beispielsweise nicht nur an der Brandstelle auf. Sie können auch in tiefer liegenden Gebäudeteilen entstehen. Bei der Verbrennung von PVC entstehen Chlorgase, die zusammen mit der Luftfeuchtigkeit und dem Löschwasser Salzsäure bilden. Werden die Salzsäuredämpfe über die Klimaanlage verteilt, können auf diese Weise Schäden an empfindlichen elektronischen Geräten entstehen, die in einem vom Brandort weit entfernten Teil des Gebäudes stehen. Aber auch "normaler" Brandrauch kann auf diesem Weg beschädigend auf die IT-Einrichtung einwirken.

Ein Brand entsteht nicht nur durch den fahrlässigen Umgang mit Feuer (z. B. Adventskranz, Schweiß- und Lötarbeiten), sondern auch durch unsachgemäße Benutzung elektrischer Einrichtungen (z. B. unbeaufsichtigte Kaffeemaschine, Überlastung von Mehrfachsteckdosen). Technische Defekte an elektrischen Geräten können ebenfalls zu einem Brand führen.

Die Ausbreitung eines Brandes kann unter anderem begünstigt werden durch:

- Aufhalten von Brandabschnittstüren durch Keile,
- Unsachgemäße Lagerung brennbarer Materialien,
- Nichtbeachtung der einschlägigen Normen und Vorschriften,
- Fehlen von Brandmeldeeinrichtungen,
- Fehlen von Handfeuerlöschern bzw. automatische Löscheinrichtungen,
- mangelhaft vorbeugenden Brandschutz (z. B. Fehlen von Brandabschottungen auf Kabeltrassen).

Beispiele:

- Anfang der 90er Jahre erlitt im Frankfurter Raum ein Großrechenzentrum einen katastrophalen Brandschaden, der zu einem kompletten Ausfall führte.
- Immer wieder kommt es vor, dass elektrische Kleingeräte wie z. B. Kaffeemaschinen oder Halogenlampen unsachgemäß installiert sind oder betrieben werden und dadurch Brände verursachen.

G 1.5 Wasser

Der unkontrollierte Eintritt von Wasser in Gebäuden oder Räumen kann beispielsweise bedingt sein durch:

- Regen, Hochwasser, Überschwemmung,
- Störungen in der Wasser-Versorgung oder Abwasser-Entsorgung,
- Defekte der Heizungsanlage,
- Defekte an Klimaanlagen mit Wasseranschluss,
- Defekte in Sprinkleranlagen,
- Löschwasser bei der Brandbekämpfung und
- Wassersabotage z. B. durch Öffnen der Wasserhähne und Verstopfen der Abflüsse.

Unabhängig davon, auf welche Weise Wasser in Gebäude oder Räume gelangt, besteht die Gefahr, dass Versorgungseinrichtungen oder IT-Komponenten beschädigt oder außer Betrieb gesetzt werden (Kurzschluss, mechanische Beschädigung, Rost etc.). Wenn zentrale Einrichtungen der Gebäudeversorgung (Hauptverteiler für Strom, Telefon, Daten) in Kellerräumen ohne selbsttätige Entwässerung untergebracht sind, kann eindringendes Wasser sehr hohe Schäden verursachen.

Beispiele:

- Viele Gewerbebetriebe, auch große Unternehmen, tragen der Hochwassergefährdung nicht hinreichend Rechnung. So wurde ein Unternehmen bereits mehrere Male durch Hochwasserschäden am Rechenzentrum "überrascht". Das Rechenzentrum schwamm im wahrsten Sinne des Wortes innerhalb von 14 Monaten zum zweiten Mal davon. Der entstandene Schaden belief sich auf mehrere hunderttausend Euro und ist nicht von einer Versicherung gedeckt.
- In einem Serverraum verlief eine Wasserleitung unterhalb der Decke, die mit Gipskarton verkleidet war. Als eine Verbindung undicht wurde, wurde dies nicht rechtzeitig erkannt. Das austretende Wasser sammelte sich zunächst an der tiefsten Stelle der Verkleidung, bevor es dort austrat und im darunter angebrachten Stromverteiler einen Kurzschluss verursachte. Dies führte dazu, dass bis zur endgültigen Reparatur sowohl die Wasser- als auch die Stromversorgung des betroffenen Gebäudeteils abgeschaltet werden musste.

G 1.6 Kabelbrand

Wenn ein Kabel in Brand gerät, sei es durch Selbstentzündung oder durch Beflammung, hat dies verschiedene Folgen:

- Die Verbindung kann unterbrochen werden.
- Es können sich aggressive Gase entwickeln. Diese können zum einen korrosiv sein, also die Informations- und Kommunikationstechnik in Mitleidenschaft ziehen. Sie können aber auch toxisch sein, also zu Personenschäden (z. B. Vergiftung) führen.

"aggressive" Gase

- An Kabeln, deren Isolationsmaterial nicht flammwidrig bzw. selbstverlöschend ist, kann sich ein Feuer ausbreiten. Selbst Brandabschottungen verhindern dies nicht vollständig, sie verzögern die Ausbreitung.

Ausbreitung durch Kabelschächte

- Bei dicht gepackten Trassen kann es zu Schwelbränden kommen, die über längere Zeit unentdeckt bleiben und so zur Ausbreitung des Feuers führen, lange bevor es offen ausbricht.

Beispiel:

In einem ostdeutschen Verwaltungsgebäude wurden die vorhandenen Elektroleitungen aus Kostengründen nicht ersetzt, sondern wider besseres Wissen überlastet. Die notwendigen Anpassungsarbeiten wurden nicht durchgeführt, da in Kürze ein neu erstelltes Verwaltungsgebäude bezogen werden sollte.

Die überlasteten Leitungen erhitzten sich und durch die sehr dichte Verlegung kam es zu einem Hitzestau, der dann zu einem Schwelbrand führte. Dieser wurde erst dann entdeckt, als die Leitungen durch die große Hitze versagten. Bis die vom Brand betroffenen Arbeitsplätze wieder ordnungsgemäß benutzt werden konnten, vergingen zwei Tage.

G 1.7 Unzulässige Temperatur und Luftfeuchte

Jedes Gerät hat einen Temperaturbereich, innerhalb dessen seine ordnungsgemäße Funktion gewährleistet ist. Überschreitet die Raumtemperatur die Grenzen dieses Bereiches nach oben oder unten, kann es zu Betriebsstörungen und zu Geräteausfällen kommen.

IT-Systeme als Heizung

So wird z. B. in einem Serverraum durch die darin befindlichen Geräte elektrische Energie in Wärme umgesetzt und daher der Raum aufgeheizt. Bei unzureichender Lüftung kann die zulässige Betriebstemperatur der Geräte überschritten werden. Bei Sonneneinstrahlung in den Raum sind Temperaturen über 50°C nicht unwahrscheinlich.

Zu Lüftungszwecken werden oft die Fenster des Serverraumes geöffnet. In der Übergangszeit (Frühjahr, Herbst) kann das bei großen Temperaturschwankungen dazu führen, dass durch starke Abkühlung die zulässige Luftfeuchte überschritten wird.

Fehler auf Langzeitspeichermedien

Bei der Lagerung von Langzeitspeichermedien können zu große Temperaturschwankungen oder zu große Luftfeuchtigkeit zu Datenfehlern und reduzierter Speicherdauer führen. Einige Hersteller geben die optimalen Lagerbedingungen für Langzeitspeichermedien mit Temperaturen von 20 bis 22°C und einer Luftfeuchtigkeit von 40% an.

Beispiel:

In einer Bonner Behörde wurde die gesamte Steuerungs- und Auswerteelektronik einer Sicherungseinrichtung in einem Raum untergebracht, der gerade genug Platz ließ, um die Türen der Geräteschränke zu öffnen. Aus Sicherheitsgründen waren sowohl die Schränke als auch der Raum mit festen Türen verschlossen.

Nach der Fertigstellung der Anlage im Herbst lief die Anlage störungsfrei. Im folgenden Sommer zeigten sich zuerst unerklärliche Funktionsfehler und bald Totalabstürze des Systems, alles ohne erkennbare Systematik. Tagelanges Suchen mit hohem technischen und personellem Aufwand bei geöffneten Türen erbrachte keine Ergebnisse. Nur durch Zufall wurde schließlich die Überhitzung der Anlage bei Außentemperaturen über 30°C als Ursache der Störungen erkannt und durch ein Kühlgerät erfolgreich abgestellt.

G 1.8 Staub, Verschmutzung

Staub stört Elektronik

Trotz zunehmender Elektronik in der IT kommt sie noch nicht ohne mechanisch arbeitende Komponenten aus. Zu nennen sind Disketten, Fest- und Wechselplatten, Diskettenlaufwerke, Drucker, Scanner etc, aber auch Lüfter von Prozessoren und Netzteile. Mit steigenden Anforderungen an die Qualität und die Schnelligkeit müssen diese Geräte immer präziser arbeiten. Bereits geringfügige Verunreinigungen können zu einer Störung eines Gerätes führen. Staub und Verschmutzungen können beispielsweise durch

- Arbeiten an Wänden, Doppelböden oder anderen Gebäudeteilen,
- Umrüstungsarbeiten an der Hardware bzw.
- Entpackungsaktionen von Geräten (z. B. aufwirbelndes Styropor)

in größerem Maße entstehen, die entsprechende Ausfälle der Hardware verursachen können.

Vorhandene Sicherheitsschaltungen in den Geräten führen meist zu einem rechtzeitigen Abschalten. Das hält zwar den Schaden, die Instandsetzungskosten und die Ausfallzeiten klein, führt aber dazu, dass das betroffene Gerät nicht verfügbar ist.

Beispiele:

- Bei der Aufstellung eines Servers in einem Medienraum, zusammen mit einem Kopierer und einem Normalpapier-Faxgerät, traten nacheinander die Lähmung des Prozessor-Lüfters und des Netzteil-Lüfters aufgrund der hohen Staubbelastung des Raumes auf. Der Ausfall des Prozessor-Lüfters führte zu sporadischen Server-Abstürzen. Der Ausfall des Netzteil-Lüfters führte schließlich zu einer Überhitzung des Netzteils mit der Folge eines Kurzschlusses, was schließlich einen Totalausfall des Servers nach sich zog.
- Um eine Wandtafel in einem Büro aufzuhängen, wurden von der Haustechnik Löcher in die Wand gebohrt. Der Mitarbeiter hatte hierzu sein Büro für kurze Zeit verlassen. Nach Rückkehr an seinen Arbeitsplatz stellte er fest, dass sein PC nicht mehr funktionierte. Ursache hierfür war Bohrstaub, der durch die Lüftungsschlitze in das PC-Netzteil eingedrungen war.

G 1.9 Datenverlust durch starke Magnetfelder

Typische Datenträger mit magnetisierbaren Speichermedien sind Disketten, Wechselplatten, Kassetten und Bänder. Informationen werden über Schreib-/Leseköpfe aufgebracht. Die derart magnetisierten Datenträger sind empfindlich gegenüber magnetischer Störstrahlung, so dass die Nähe zu solchen Strahlungsquellen vermieden werden sollte.

Je nach Stärke der Strahlung führt diese zu mehr oder weniger großen Datenverlusten. Besonders kritisch ist dies bei Dateien, die aufgrund ihrer internen Formatierung bereits durch geringfügige Veränderungen gänzlich unbrauchbar werden (z. B. Postscript-Dateien, Datenbanken).

Beispiele für Quellen magnetischer Störstrahlung sind**:**

- Elektromotoren,
- Transformatoren,
- Ausweiselesegeräte auf Magnetfeldbasis.

G 1.10 Ausfall eines Weitverkehrsnetzes

Werden auf IT-Systemen, die über Weitverkehrsnetze verbunden sind, zeitkritische IT-Anwendungen betrieben, sind die durch einen Netzausfall möglichen Schäden und Folgeschäden entsprechend hoch, wenn keine Ausweichmöglichkeiten (z. B. Anbindung an ein zweites Kommunikationsnetz) vorgesehen sind.

Im Rahmen der Liberalisierung des Telekommunikationsmarktes bietet nicht nur die Deutsche Telekom AG ihre Dienste für die Bereitstellung von Kommunikationsverbindungen zum Daten- und Sprachtransfer an. Viele, teilweise sehr kleine Netzbetreiber, konkurrieren mit günstigen Kommunikationsentgelten untereinander und mit der Deutschen Telekom AG. Daher sollte ein Kunde sich informieren, mit welcher Güte dieser Dienst tatsächlich erbracht werden kann, indem er den Netzbetreiber um detaillierte Auskünfte über Backup-Strategien oder Notfallplanungen bittet.

G 1.11 Technische Katastrophen im Umfeld

Probleme im Umfeld einer Behörde bzw. eines Unternehmens können zu Schwierigkeiten im Betrieb bis hin zu Arbeitsausfällen führen. Dies können technische Unglücksfälle, Havarien, aber auch gesellschaftliche oder politische Unruhen wie Demonstrationen oder Krawalle sein (siehe auch G 1.12 *Beeinträchtigung durch Großveranstaltungen*).

Die Liegenschaften einer Organisation können verschiedenen Gefährdungen aus dem Umfeld durch Verkehr (Straßen, Schiene, Luft, Wasser), Nachbarbetrieben oder Wohngebieten ausgesetzt sein. Diese können beispielsweise durch Brände, Explosionen, Stäube, Gase, Sperrungen, Strahlung, Emissionen (chemische Industrie) verursacht sein.

Vorbeugungs- oder Rettungsmaßnahmen können die Liegenschaften dabei direkt betreffen. Durch die Komplexität der Haustechnik und der IT-Einrichtungen kann es aber auch zu indirekten Problemen kommen.

Beispiel:

Bei einem Brand in einem chemischen Betrieb in unmittelbarer Nähe eines Rechenzentrums (ca. 1000 m Luftlinie) entstand eine mächtige Rauchwolke. Das Rechenzentrum besaß eine Klima- und Lüftungsanlage, die über keine Außenluftüberwachung verfügte. Nur durch die Aufmerksamkeit eines Mitarbeiters (der Unfall geschah während der Arbeitszeit), der die Entstehung und Ausbreitung verfolgte, konnte die Außenluftzufuhr rechtzeitig manuell abgeschaltet werden.

G 1.12 Beeinträchtigung durch Großveranstaltungen

Großveranstaltungen aller Art können zu Behinderungen des ordnungsgemäßen Betriebs einer Behörde bzw. eines Unternehmens führen. Hierzu gehören u. a. Straßenfeste, Konzerte, Sportveranstaltungen, Arbeitskämpfe oder Demonstrationen. Ausschreitungen im Umfeld solcher Veranstaltungen können zusätzlich Auswirkungen wie die Einschüchterung bis hin zur Gewaltanwendung gegen das Personal oder das Gebäude nach sich ziehen.

Beispiele:

- Während der heißen Sommermonate fand eine Demonstration in der Nähe eines Rechenzentrums statt. Die Situation eskalierte und es kam zu Gewalttätigkeiten. In einer Nebenstraße stand noch ein Fenster des Rechenzentrumsbereiches auf, durch das ein Demonstrant eindrang und die Gelegenheit nutzte, IT-Hardware mit wichtigen Daten zu entwenden.
- Beim Aufbau einer Großkirmes wurde aus Versehen eine Stromleitung gekappt. Dies führte in einem hierdurch versorgten Rechenzentrum zu einem Ausfall, der jedoch durch die vorhandene Netzersatzanlage abgefangen werden konnte.

G 1.13 Sturm

Die Auswirkungen eines Sturms oder Orkans auf Außeneinrichtungen, die zum Betrieb eines Rechenzentrums mittelbar benötigt werden, werden häufig unterschätzt. Außeneinrichtungen können hierdurch beschädigt oder abgerissen werden. Abgerissene und vom Sturm fortgeschleuderte Gegenstände können weitere Folgeschäden verursachen. Weiterhin können dadurch technische Komponenten in ihrer Funktion beeinträchtigt werden.

Beispiele:

lose verlegte Kühlleitungen

- Kühlleitungen der Klimaanlage eines Rechenzentrums waren auf dem Dach als flexible Hart-PVC-Schläuche verlegt, aber über weite Strecken auf der Dachhaut weder beschwert noch befestigt. Sie wurden vom Orkan gepackt und vom Dach des Gebäudes gefegt. Dabei rissen sie aus den Verbindungen. Die Kühlflüssigkeit lief aus und das System musste für mehrere Stunden stillgelegt werden. Für die Dauer des Sturmes konnten wegen der Gefahr, vom Dach geweht zu werden, keinerlei Reparaturen vorgenommen werden. Der Serverpark fiel für fast 12 Stunden aus. Er versorgt ca. 12.000 Nutzer.

durch Sturm abgerissene Verkleidung

- In einem anderen Fall stürzte eine Lamellenwand, welche die Rückkühlwerke auf dem Dach des Prozessrechenzentrums eines Industriebetriebs optisch verkleidete, ein. Die scharfen Kanten der Bleche durchschnitten die Elektroleitungen der Rückkühlwerke. Es gab einen Kurzschluss mit Lichtbogen, der die vom Sturm mit hoch gerissene Dachhaut in Brand steckte. Gleichzeitig wirkte die umgestürzte Verkleidung geringfügig als Windschutz - ließ aber genug Wind durch, um das Feuer zu entfachen. Der Brand setzte sich in der Isolierung zwischen Trapezblech und Dichtungsbahnen fort. Nur durch einen glücklichen Zufall konnte ein Totalschaden verhindert werden.

G 1.14 Datenverlust durch starkes Licht

Typische Datenträger mit optischen Speichermedien sind CD-ROM, CD-RW, DVD-RAM, DVD-RW und MO. Informationen werden über Schreib-/Leseköpfe sowie Laser aufgebracht. Die derart beschriebenen Datenträger sind empfindlich gegenüber starkem Licht, insbesondere im UV-Bereich, so dass die Nähe zu solchen Lichtquellen vermieden werden sollte.

Je nach Stärke und Dauer der Strahlung führt diese zu mehr oder weniger großen Datenverlusten. Besonders kritisch ist dies bei Dateien, die aufgrund ihrer internen Formatierung bereits durch geringfügige Veränderungen gänzlich unbrauchbar werden (z. B. Postscript-Dateien, Datenbanken oder verschlüsselte Dateien).

Beispiele für starke Lichtquellen sind**:**

- Sonnenlicht (vor allem an wolkenfreien Sommertagen oder in Höhenlagen),
- Halogenlampen,
- spezielle Neonröhren.

G 1.15 Beeinträchtigung durch wechselnde Einsatzumgebung

Mobile Geräte werden in sehr unterschiedlichen Umgebungen eingesetzt und sind dadurch einer Vielzahl von Gefährdungen ausgesetzt. Dazu gehören beispielsweise schädigende Umwelteinflüsse wie zu hohe oder zu niedrige Temperaturen, ebenso wie Staub oder Feuchtigkeit. Zu anderen Problemen, die durch die Mobilität der Geräte entstehen, gehören beispielsweise Transportschäden.

Unbekannte Umgebung - unbekannte Risiken

Ein wichtiger Aspekt bei mobilen Geräten ist aber auch, dass sie sich in Bereichen mit unterschiedlichem Sicherheitsniveau bewegen. Bei einigen Umgebungen ist das Sicherheitsniveau den Benutzern durchaus bekannt, bei anderen nicht. Neben der Beweglichkeit ist auch die Kommunikationsfähigkeit mit anderen IT-Systemen ein Grund für den Einsatz von PDAs, Laptops und anderen mobilen Geräten. Daher müssen auch die Probleme betrachtet werden, die durch die Interaktion mit anderen IT-Systemen ausgelöst werden können. Innerhalb der eigenen Organisation kann die Vertrauenswürdigkeit von IT-Systemen bis zu einem gewissen Grad eingeschätzt werden. Dies ist allerdings in fremden Umgebungen schwierig. Die Kommunikation mit unbekannten IT-Systemen und Netzen kann immer Gefährdungspotential für das eigene mobile System und dessen Anwendungen und Daten enthalten. Bei der Kontaktaufnahme mit anderen IT-Systemen könnten beispielsweise auch Computerviren oder Trojanische Pferde mit übertragen werden.

Daher muss auch nach der Rückkehr von mobilen Systemen immer kritisch hinterfragt werden, wo dieser PDA oder Laptop schon überall gewesen ist, und die entsprechenden Vorsichtsregeln sind zu beachten.

Ein weiteres Problem bei der Nutzung von fremden Infrastrukturen, wie z. B. beim Herunterladen von Informationsangeboten auf Messen, ist die häufig unzureichende Transparenz der angebotenen Dienste. Viele Diensteanbieter sammeln Kundendaten, um Profile erstellen zu können, um einerseits ihren Kunden besser auf sie zugeschnittene Dienste anbieten zu können, aber auch um diese andererseits an andere Anbieter weiterverkaufen zu können. Es könnten beispielsweise Profile erstellt werden, alleine indem die Informationen über Aufenthaltsorte und das Kommunikationsverhalten des Benutzers ausgewertet werden (welche Dienste, wann, wie oft, mit wem). Auch bei Anwendungen, die vollständig auf dem eigenen mobilen Endgerät ablaufen, kann es vorkommen, dass diese Daten sammeln (z. B. über Nutzungshäufigkeit und -art) und weitergeben, sobald das Gerät online geht.

Immer wieder werden mobile Endgeräte verloren oder gestohlen. Je kleiner und begehrter solche Geräte sind, wie beispielsweise PDAs, desto höher ist dieses Risiko. Neben dem unmittelbaren Verlust kann dabei durch den Verlust bzw. die Offenlegung wichtiger Daten weiterer Schaden entstehen.

G 1.16 Ausfall von Patchfeldern durch Brand

Patchfelder und Leitungsverteiler, auf die die internen Leitungen des Hausnetzes und die externen des öffentlichen Netzes auflaufen, können durch einen Brand so stark beschädigt werden, dass eine reibungslose Datenübertragung darüber nicht mehr möglich ist. Der Schaden wird dabei nicht ausschließlich durch die Hitze des Feuers verursacht. Allein schon der Brandrauch kann die empfindliche Anschlusstechnik massiv beschädigen. Der Einsatz von Löschmitteln (Wasser, Pulver, Schaum) führt zu weiteren Schäden.

Nach einem solchen Schadensereignis ist es dann in der Regel nicht mehr möglich, bereitstehende Ersatz-Hardware einfach an derart beschädigte Patchfelder bzw. Leitungsverteiler anzuschließen, um so zumindest einen Notbetrieb rasch wieder aufnehmen zu können.

Im Allgemeinen sind sehr umfangreiche, kosten- und zeitintensive Reparaturarbeiten erforderlich, die mit einem längeren Ausfall der IT einhergehen.

G 1.17 Ausfall oder Störung eines Funknetzes

In Funknetzen werden Informationen mittels elektromagnetischer Funkwellen übertragen. Strahlen andere elektromagnetische Quellen im gleichen Frequenzspektrum Energie ab, können diese die drahtlose Kommunikation stören und im Extremfall den Betrieb des WLANs verhindern. Dies kann unbeabsichtigt durch andere technische Systeme (z. B. Bluetooth-Geräte, andere WLANs, Mikrowellenöfen, medizinische Geräte, Funk-Überwachungskameras, etc.) oder aber durch absichtliches Betreiben einer Störquelle (Jammer) als so genannter Denial-Of-Service-Angriff erfolgen. Darüber hinaus sind auch Denial-Of-Service-Angriffe möglich, z. B. durch wiederholtes Senden bestimmter Steuer- und Managementsignale, die zum Verlust der Verfügbarkeit des Funknetzes führen können.

Beispiele:

- Bei einer ungeeignet gewählten Montageposition für eine Außenantenne und mangelhaft geplantem Blitz- und Witterungsschutz kann ein WLAN durch Blitzeinschlag oder Witterungseinflüsse ausfallen.
- Bei WLAN-Systemen, die nach dem Standard IEEE 802.11b und IEEE 802.11g im ISM-Band bei 2,4 GHz operieren, können Störungen durch eine Vielzahl anderer in diesem Frequenzband zugelassener Funksysteme, wie beispielsweise Bluetooth, Mikrowellenherde oder andere WLAN-Netze, hervorgerufen werden.

G 2 Gefährdungskatalog Organisatorische Mängel

G 2.1	Fehlende oder unzureichende Regelungen	
G 2.2	Unzureichende Kenntnis über Regelungen	
G 2.3	Fehlende, ungeeignete, inkompatible Betriebsmittel	
G 2.4	Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen	
G 2.5	Fehlende oder unzureichende Wartung	
G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen	
G 2.7	Unerlaubte Ausübung von Rechten	
G 2.8	Unkontrollierter Einsatz von Betriebsmitteln	
G 2.9	Mangelhafte Anpassung an Veränderungen beim IT-Einsatz	
G 2.10	Nicht fristgerecht verfügbare Datenträger	
G 2.11	Unzureichende Trassendimensionierung	
G 2.12	Unzureichende Dokumentation der Verkabelung	
G 2.13	Unzureichend geschützte Verteiler	
G 2.14	Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen	
G 2.15	Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System	
G 2.16	Ungeordneter Benutzerwechsel bei tragbaren PCs	
G 2.17	Mangelhafte Kennzeichnung der Datenträger	
G 2.18	Ungeordnete Zustellung der Datenträger	
G 2.19	Unzureichendes Schlüsselmanagement bei Verschlüsselung	
G 2.20	Unzureichende oder falsche Versorgung mit Verbrauchsgütern	
G 2.21	Mangelhafte Organisation des Wechsels zwischen den Benutzern	
G 2.22	Fehlende Auswertung von Protokolldaten	
G 2.23	Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Netz	**entfallen**
G 2.24	Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes	
G 2.25	Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten	

G 2.26	Fehlendes oder unzureichendes Test- und Freigabeverfahren	
G 2.27	Fehlende oder unzureichende Dokumentation	
G 2.28	Verstöße gegen das Urheberrecht	
G 2.29	Softwaretest mit Produktionsdaten	
G 2.30	Unzureichende Domänenplanung	
G 2.31	Unzureichender Schutz des Windows NT Systems	
G 2.32	Unzureichende Leitungskapazitäten	
G 2.33	Nicht gesicherter Aufstellungsort von Novell Netware Servern	
G 2.34	Fehlende oder unzureichende Aktivierung von Novell Netware Sicherheitsmechanismen	
G 2.35	Fehlende Protokollierung unter Windows 95	**entfallen**
G 2.36	Ungeeignete Einschränkung der Benutzerumgebung	
G 2.37	Unkontrollierter Aufbau von Kommunikationsverbindungen	
G 2.38	Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen	
G 2.39	Mangelhafte Konzeption eines DBMS	
G 2.40	Mangelhafte Konzeption des Datenbankzugriffs	
G 2.41	Mangelhafte Organisation des Wechsels von Datenbank-Benutzern	
G 2.42	Komplexität der NDS	
G 2.43	Migration von Novell Netware 3.x nach Novell Netware Version 4	
G 2.44	Inkompatible aktive und passive Netzkomponenten	
G 2.45	Konzeptionelle Schwächen des Netzes	
G 2.46	Überschreiten der zulässigen Kabel- bzw. Buslänge oder der Ringgröße	
G 2.47	Ungesicherter Akten- und Datenträgertransport	
G 2.48	Ungeeignete Entsorgung der Datenträger und Dokumente am häuslichen Arbeitsplatz	
G 2.49	Fehlende oder unzureichende Schulung der Telearbeiter	
G 2.50	Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Telearbeiter	
G 2.51	Mangelhafte Einbindung des Telearbeiters in den Informationsfluss	

G 2.52	Erhöhte Reaktionszeiten bei IT-Systemausfall	
G 2.53	Unzureichende Vertretungsregelungen für Telearbeit	
G 2.54	Vertraulichkeitsverlust durch Restinformationen	
G 2.55	Ungeordnete E-Mail-Nutzung	
G 2.56	Mangelhafte Beschreibung von Dateien	
G 2.57	Nicht ausreichende Speichermedien für den Notfall	
G 2.58	Novell Netware und die Datumsumstellung im Jahr 2000	**entfallen**
G 2.59	Betreiben von nicht angemeldeten Komponenten	
G 2.60	Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement	
G 2.61	Unberechtigte Sammlung personenbezogener Daten	
G 2.62	Ungeeigneter Umgang mit Sicherheitsvorfällen	
G 2.63	Ungeordnete Faxnutzung	
G 2.64	Fehlende Regelungen für das RAS-System	
G 2.65	Komplexität der SAMBA-Konfiguration	
G 2.66	Unzureichendes IT-Sicherheitsmanagement	
G 2.67	Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten	
G 2.68	Fehlende oder unzureichende Planung des Active Directory	
G 2.69	Fehlende oder unzureichende Planung des Einsatzes von Novelle eDirectory	
G 2.70	Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Novell eDirectory	
G 2.71	Fehlerhafte oder unzureichende Planung des LDAP-Zugriffs auf das Novell eDirectory	
G 2.72	Unzureichende Migration von Archivsystemen	
G 2.73	Fehlende Revisionsmöglichkeit von Archivsystemen	
G 2.74	Unzureichende Ordnungskriterien für Archive	
G 2.75	Mangelnde Kapazität von Archivdatenträgern	
G 2.76	Unzureichende Dokumentation von Archivzugriffen	
G 2.77	Unzulängliche Übertragung von Papierdaten in elektonische Archive	
G 2.78	Unzulängliche Auffrischung von Datenbeständen bei der Archivierung	
G 2.79	Unzulängliche Erneuerung von digitalen Signaturen bei der Archivierung	

G 2.1 Fehlende oder unzureichende Regelungen

Die Bedeutung übergreifender organisatorischer Regelungen und Vorgaben für das Ziel IT-Sicherheit nimmt mit dem Umfang der Informationsverarbeitung, aber auch mit dem Schutzbedarf der zu verarbeitenden Informationen zu.

Von der Frage der Zuständigkeiten angefangen bis hin zur Verteilung von Kontrollaufgaben kann das Spektrum der Regelungen sehr umfangreich sein. Auswirkungen von fehlenden oder unzureichenden Regelungen werden beispielhaft in den Gefährdungen G 2.2 ff. beschrieben.

Vielfach werden nach Veränderungen technischer, organisatorischer oder personeller Art, die wesentlichen Einfluss auf die IT-Sicherheit haben, bestehende Regelungen nicht angepasst. Veraltete Regelungen können dem störungsfreien IT-Betrieb entgegen stehen. Probleme können auch dadurch entstehen, dass Regelungen unverständlich oder zusammenhanglos formuliert sind und dadurch missverstanden werden.

Dass Regelungsdefizite schadensfördernde Auswirkungen haben können, machen folgende **Beispiele** deutlich:

- Durch eine mangelhafte Betriebsmittelverwaltung kann der termingerechte Arbeitsablauf in einem Rechenzentrum schon durch eine unterbliebene Druckerpapierbestellung stark beeinträchtigt werden.
- Neben einer Beschaffung von Handfeuerlöschern muss auch deren Wartung geregelt sein, um sicherzustellen, dass diese im Brandfall auch funktionstüchtig sind.
- Bei einem Wasserschaden wird festgestellt, dass dieser auch den darunter liegenden Serverraum in Mitleidenschaft zieht. Durch eine unzureichende Schlüsselverwaltung kann der Wasserschaden im Serverraum allerdings nicht unmittelbar behoben werden, weil keiner informiert ist, wo sich der Schlüssel zum Serverraum gerade befindet. Dadurch steigt der Schaden erheblich.

G 2.2 Unzureichende Kenntnis über Regelungen

Die Festlegung von Regelungen allein sichert den störungsfreien IT-Einsatz noch nicht. Allen Mitarbeiter müssen die geltenden Regelungen auch bekannt sein, vor allem den Funktionsträgern. Der Schaden, der sich aus einer unzureichenden Kenntnis über bestehende Regelungen ergeben kann, darf sich nicht mit den Aussagen entschuldigen lassen: "Ich habe nicht gewusst, dass ich dafür zuständig bin." oder "Ich habe nicht gewusst, wie ich zu verfahren hatte."

Beispiele:

- Werden Mitarbeiter nicht über die Verfahrensweise des Umgangs mit übersandten Datenträgern und E-Mails unterrichtet, besteht die Gefahr, dass ein Computer-Virus im Unternehmen bzw. in der Behörde verbreitet wird.
- In einer Bundesbehörde wurden farblich unterschiedliche Papierkörbe aufgestellt, von denen eine Farbe für die Entsorgung zu vernichtender Unterlagen bestimmt war. Die meisten Mitarbeiter waren von dieser Regelung nicht unterrichtet.
- In einer Bundesbehörde gab es eine Vielzahl von Regelungen zur Durchführung von Datensicherungen, die mündlich zwischen dem IT-Sicherheitsbeauftragten und dem IT-Referat sukzessiv vereinbart wurden. Eine Nachfrage ergab, dass die betroffenen IT-Benutzer keine Kenntnis und keinen Ansprechpartner über die getroffenen "Vereinbarungen" hatten. Die Regelungen zur Datensicherung waren auch nicht dokumentiert. Viele Benutzer haben deshalb auch von den lokalen Daten ihres Arbeitsplatzrechners keine Datensicherung angefertigt, obwohl nur auf den Servern kontinuierliche Datensicherungen zentral durchgeführt werden.
- In einem Rechenzentrum wurde als neue Regelung festgelegt, dass bei Problemen mit der Einbruch- oder Brandmeldeanlage eine Besetzung der Pförtnerloge auch nachts erfolgt. Der Pförtnerdienst war über diese eingeführte Regelung vom Sicherheitsverantwortlichen nicht informiert worden. Als Folge war das Rechenzentrum für mehrere Wochen nachts unzureichend geschützt.

G 2.3 Fehlende, ungeeignete, inkompatible Betriebsmittel

Eine nicht ausreichende Bereitstellung von Betriebsmitteln kann einen IT-Betrieb erheblich beeinträchtigen. Störungen können sich ergeben, weil benötigte Betriebsmittel nicht in ausreichender Menge vorhanden sind oder nicht termingerecht bereit gestellt wurden.

Ebenso kann es vorkommen, dass ungeeignete oder sogar inkompatible Betriebsmittel beschafft werden, die infolgedessen nicht eingesetzt werden können.

Beispiele:

- Für den neu angemieteten Internet-Anschluss wird vergessen, das Entgelt für die Einrichtung an den Betreiber zu überweisen mit der Folge, dass der Anschluss nicht freigeschaltet wird. Das IT-Verfahren, das diesen Anschluss nutzen soll, kann daher nur mit Verspätung in Betrieb genommen werden.
- Ein ungeeignetes Betriebsmittel ist zum Beispiel eine komplexe und zeitkritische Anwendung, z. B. eine grafikintensive CAD-Anwendung, die auf einem nicht ausreichend leistungsfähigen Rechner installiert werden soll.
- Ein Beispiel für inkompatible Betriebsmittel sind Verbindungskabel unterschiedlicher Pin-Belegung zum Anschluss von Druckern.
- Bei der Vielzahl von Möglichkeiten, Daten zwischen zwei IT-Systemen auszutauschen, taucht häufig das Problem auf, dass jeder der beiden Rechner mindestens drei Schnittstellen zum Datenaustausch besitzt, diese aber leider nicht kompatibel sind. Typische Fragen vor jedem Datenaustausch sind beispielsweise: Diskette, CD-ROM, DVD, USB-Stick, Bluetooth?
- Auf den Arbeitsplatz-PCs soll eine neue Version des Betriebssystems aufgespielt werden. Teilweise sind allerdings verwendete Hardwarekomponenten mit der neuen Betriebssystem-Version nicht lauffähig, da keine Treiberunterstützung für die neue Betriebssystem-Version angeboten wird.
- Der Plattenplatz bei PCs und Servern steigt ständig. Leider wird häufig vergessen, IT-Komponenten und Datenträger zu beschaffen, die für eine regelmäßige Datensicherung ausreichend Kapazität bieten.

G 2.4 Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen

Nach der Einführung von Maßnahmen, die der Sicherheit der IT dienen (z. B. Datensicherung, Zutrittskontrolle, Vorgaben für Verhalten bei Notfällen), müssen diese auch konsequent umgesetzt werden. Finden keine oder nur unzureichende Kontrollen der Sicherheitsmaßnahmen statt, wird weder deren Missachtung noch ihre effektive Wirksamkeit festgestellt. Eine rechtzeitige und der jeweiligen Situation angemessene Reaktion wird dadurch verhindert.

Darüber hinaus gibt es Sicherheitsmaßnahmen, die nur mit der Durchführung entsprechender Kontrollen ihre Wirkung entfalten. Hierzu zählen beispielsweise Protokollierungsfunktionen, deren Sicherheitseigenschaften erst mit der Auswertung der Protokolldaten zum Tragen kommen.

Beispiele:

- Zur Vorbereitung von Straftaten kommt es vor, dass Schließzylinder in Außentüren und Toren von nicht autorisierten Personen ausgetauscht werden. Gerade wenn es sich um Zugänge handelt, die selten genutzt werden oder lediglich als Notausgänge vorgesehen sind, werden diese bei Streifengängen nur in Panikrichtung geprüft. Die Funktionalität der Schließzylinder wird dabei oft vernachlässigt.
- In einer Behörde werden einige Unix-Server zur externen Datenkommunikation eingesetzt. Aufgrund der zentralen Bedeutung dieser IT-Systeme sieht das IT-Sicherheitskonzept vor, dass die Unix-Server wöchentlich einer Integritätsprüfung unterworfen werden. Da diese Überprüfungen nicht regelmäßig nachgehalten werden, fällt erst bei der Klärung eines Sicherheitsvorfalls auf, dass die IT-Abteilung auf solche Integritätsprüfungen verzichtet hat. Als Grund wurde die mangelhafte personelle Ausstattung der Abteilung genannt.
- In einem Unternehmen wurde die Rolle des z/OS-Security-Auditors nicht besetzt. Dies hatte zur Folge, dass die Einstellungen im RACF im Laufe der Zeit nicht mehr den Sicherheitsvorgaben des Unternehmens entsprachen. Erst nach einem Produktionsausfall wurde bemerkt, dass einige Anwender mehr Rechte hatten, als sie für ihre Tätigkeit benötigten. Eine für die Produktion wichtige Anwendung war von ihnen versehentlich gestoppt worden.

G 2.5 Fehlende oder unzureichende Wartung

Die Funktionsfähigkeit der eingesetzten Technik muss gewährleistet bleiben. Durch regelmäßige Wartung kann die Funktionsfähigkeit der eingesetzten Technik gefördert werden. Werden Wartungsarbeiten nicht oder nur unzureichend durchgeführt, können daraus unabsehbar hohe Schäden oder Folgeschäden entstehen.

Beispiele:

- Die Batterien einer unterbrechungsfreien Stromversorgung (USV) verfügen infolge fehlender Wartung über eine unzureichende Kapazität (zu geringer Säuregehalt). Die USV kann einen Stromausfall nicht mehr ausreichend lange überbrücken.
- Die Feuerlöscher verfügen aufgrund fehlender Wartung nicht mehr über einen ausreichenden Druck, so dass ihre brandbekämpfende Wirkung nicht mehr vorhanden ist.
- Der Laserdrucker fällt aufgrund Überhitzung aus, weil ein Lüftungsgitter nicht vorschriftsmäßig gereinigt wurde.
- Im Serverraum stehen viele Geräte mit eigener Hitzeentwicklung. Kommen dazu noch hochsommerliche Temperaturen und eine nicht ausreichende Klimatisierung (z. B. fehlende Klimaanlage) des Raumes hinzu, kann es vereinzelt zu temperaturbedingten Geräteausfällen kommen. Wenn eine Klimaanlage fest installiert ist, muss diese daher auch regelmäßig gewartet und gereinigt werden, um eine verlässliche Funktion sicherzustellen.

G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen

Gelangen Unbefugte in schutzbedürftige Räume, können sich Gefährdungen nicht nur durch vorsätzliche Handlungen, sondern auch durch unbeabsichtigtes Fehlverhalten ergeben. Eine Störung des Betriebsablaufs tritt allein schon dadurch ein, dass aufgrund des unbefugten Zutritts eine Feststellung möglicher Schäden erforderlich wird. Dabei ist zu beachten, dass auch dienstlich genutzte Räume im häuslichen Umfeld zu diesen schutzbedürftigen Räumen zu zählen sind.

Beispiele:

- Beim Reinigungspersonal wird eine Urlaubsvertretung eingesetzt. Die Urlaubsvertretung übernimmt eigenmächtig - obwohl sie nicht eingewiesen wurde - die Reinigung des Rechenzentrums. Dort öffnet sie den alarmüberwachten Notausgang und löst hierdurch einen Fehlalarm aus.
- Bei einem Einbruch in einem Bürogebäude sind auf den ersten Blick nur die Kaffeekasse und zwei neue Laptops verschwunden. Trotzdem müssen alle Akten gesichtet werden, ob wesentliche Teile fehlen und alle IT-Systeme daraufhin geprüft werden, ob unbefugt auf sie zugegriffen wurde.
- Dienstlich genutzte Räume im häuslichen Umfeld können z. B. auch Telearbeitsplätze sein. Hier muss es nicht immer der Eindringling von Außen (Einbrecher) sein, sondern denkbar sind auch neugierige Gäste im Rahmen einer Hausparty, die unbefugt und vorsätzlich an Arbeitsplatzdaten gelangen möchten.
- Eine weitere Möglichkeit, ohne böse Absicht, sind die Kinder des Telearbeiters, die an dem häuslichen Arbeitsplatzrechner Computerspiele ausführen möchten und eventuell aus Unkenntnis wichtige Daten zerstören bzw. einen Virus in das System bringen.

Ebenfalls vorkommen kann z. B., dass Gegenstände wie Spielzeug oder Nahrungsmittel in Disketten- oder CD-ROM-Laufwerke eingebracht werden, die die Funktion derart beeinflussen, dass diese unbrauchbar werden.

Einbruchsicherungen gegen Diebstahl (z. B. abschließbare Fenstergriffe, Sicherheitsschlösser und Sicherheitsverglasung an Haustüren) werden im privaten Umfeld für den häuslichen Arbeitsplatz oft aus Kostengründen nicht realisiert. Dadurch ist bei Telearbeitsplätzen der Schutz vor Einbrüchen niedriger.

G 2.7 Unerlaubte Ausübung von Rechten

Rechte wie Zutritts-, Zugangs- und Zugriffsberechtigungen werden als organisatorische Maßnahmen eingesetzt, um eine sichere und ordnungsgemäße IT-Nutzung zu gewährleisten. Werden solche Rechte an die falsche Person vergeben oder wird ein Recht unautorisiert ausgeübt, können sich eine Vielzahl von Gefährdungen ergeben, die die Vertraulichkeit und Integrität von Daten oder die Verfügbarkeit von Rechnerleistung beeinträchtigen.

Beispiele:

- Der Arbeitsvorbereiter, der keine Zutrittsberechtigung zum Datenträgerarchiv besitzt, entnimmt in Abwesenheit des Archivverwalters Magnetbänder, um Sicherungskopien einspielen zu können. Durch die unkontrollierte Entnahme wird das Bestandsverzeichnis des Datenträgerarchivs nicht aktualisiert, die Bänder sind für diesen Zeitraum nicht auffindbar.
- Ein Mitarbeiter ist erkrankt. Ein Zimmerkollege weiß aufgrund von Beobachtungen, wo dieser sein Passwort auf einem Merkzettel aufbewahrt und verschafft sich Zugang zum Rechner des anderen Mitarbeiters. Da er erst kürzlich durch ein Telefonat mitbekommen hat, dass der Kollege noch eine fachliche Stellungnahme abzugeben hatte, nimmt er hier unberechtigterweise diese Aufgabe im Namen seines Kollegen wahr, obwohl er zu der Thematik nicht auf dem aktuellen Sachstand ist. Eine daraus folgende Erstellung einer Ausschreibungsunterlage in der Verwaltungsabteilung fordert im Pflichtenheft daher eine längst veraltete Hardwarekomponente, weil die dortigen Mitarbeiter der fachlichen Stellungnahme des erfahrenen Kollegen uneingeschränkt vertraut haben.

G 2.8 Unkontrollierter Einsatz von Betriebsmitteln

Betriebsmittel - gleich welcher Art - dürfen nur entsprechend dem Verwendungszweck eingesetzt werden. Die für die Beschaffung und den Einsatz der Betriebsmittel verantwortlichen Personen müssen sowohl den unkontrollierten Einsatz verhindern als auch den korrekten Einsatz überwachen. Wird jedoch der Einsatz von Betriebsmitteln nicht ausreichend kontrolliert, können als Folge vielfältige Gefährdungen auftreten.

Beispiele:

- Der Einsatz privater Datenträger durch Mitarbeiter kann zu einem Befall des dienstlichen PCs durch Computer-Viren führen.
- Falsche Reinigungsmittel können zu einer Beschädigung von Monitoren führen.
- Ungeeignete Tinte für Tintenstrahldrucker kann zu einer Verunreinigung oder Fehlfunktion des Druckers führen.
- In einem Betrieb wurde der Verbrauch von DVDs nicht kontrolliert. Erst bei einer zufälligen Plausibilitätsprüfung stellte sich heraus, dass im letzten halben Jahr unerklärbar viele DVDs verbraucht worden waren. Bei Nachfragen stellte sich heraus, dass viele Mitarbeiter diese benutzten, um kleinere Datenmengen für den Datenaustausch aufzuspielen. Anschließend hatten sie die DVDs weggeworfen, weil ihnen nicht erklärt worden war, dass diese im Gegensatz zu den bis dahin genutzten CD-ROMs wiederverwendet werden konnten.

G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz

Die speziell für den Einsatz von Informationstechnik geschaffenen organisatorischen Regelungen, aber auch das gesamte Umfeld einer Behörde bzw. eines Unternehmens unterliegen ständigen Veränderungen. Sei es nur, dass Mitarbeiter ausscheiden oder hinzukommen, Mitarbeiter das Büro wechseln, neue Hardware oder Software beschafft wird, der Zulieferbetrieb für die Betriebsmittel Konkurs anmeldet. Dass sich bei einer ungenügenden Berücksichtigung der vorzunehmenden organisatorischen Anpassungen Gefährdungen ergeben, zeigen folgende Beispiele:

- Vor Urlaubsantritt vergisst ein Mitarbeiter, der Urlaubsvertretung Zugriffsrechte auf alle von dieser benötigten Dateien und Verzeichnisse zu übertragen. Hierdurch können sich Verzögerungen im IT-Betrieb ergeben.
- Durch bauliche Änderungen im Gebäude werden bestehende Fluchtwege verändert. Durch mangelhafte Unterrichtung der Mitarbeiter ist die Räumung des Gebäudes nicht in der erforderlichen Zeit möglich.
- Durch eine Umstellung eines IT-Verfahrens werden größere Mengen an Druckerpapier benötigt. Durch fehlende Unterrichtung der Beschaffungsstelle kommt es zu Engpässen im IT-Betrieb.
- Beim Empfang elektronischer Dokumente werden diese nicht automatisch auf Makro-Viren überprüft, da dieses Problem noch nicht bekannt ist oder kein Virenprüfprogramm vorhanden ist.
- Bei der Übermittlung elektronischer Dokumente wird nicht darauf geachtet, diese in einem für die Empfängerseite lesbaren Format abzuspeichern.

G 2.10 Nicht fristgerecht verfügbare Datenträger

Die korrekte Verwendung von Datenträgern ist für ein IT-Verfahren von besonderer Bedeutung. Bereits geringfügige Fehler - z. B. mangelhafte Kennzeichnung, falscher Aufbewahrungsort, fehlende Ein- oder Ausgabebestätigungen im Datenträgerarchiv - können dazu führen, dass ein Datenträger nicht in der erforderlichen Zeit aufgefunden werden kann. Die resultierenden Verzögerungen können zu erheblichen Schäden führen.

Beispiele:

- Datensicherungsbänder werden versehentlich in ein externes Datensicherungsarchiv ausgelagert. Eine erforderliche Datenrekonstruktion wird erheblich verzögert, weil die Wiederbeschaffung der Bänder nicht unverzüglich möglich ist.
- Datensicherungsbänder unterschiedlichen Inhalts werden versehentlich gleich gekennzeichnet. Der Archivverwalter gibt unabsichtlich das aktuellere Magnetband zum Löschen frei. Folglich steht nur noch eine überalterte Datensicherung zur Verfügung.
- Bandverwaltungssysteme im z/OS-Betriebssystem verwenden Batch-Jobs, um Datensicherungsbänder mit erreichtem *Expiration Date* zu erkennen und zum Überschreiben frei zu geben. Bricht dieser Batch-Job ab oder läuft erst gar nicht an, so stehen unter Umständen nicht genug Leerbänder (*Scratch Tapes*) für die Folgesicherungen zur Verfügung und es kann zu Engpässen in der Bandverarbeitung kommen.

G 2.11 Unzureichende Trassendimensionierung

Bei der Planung von Netzen, Serverräumen oder Rechenzentren wird oft der Fehler begangen, die funktionale, kapazitive oder sicherheitstechnische Auslegung ausschließlich am aktuellen Stand auszurichten. Dabei wird übersehen, dass

- die Kapazitäten des Netzes und der Rechner aufgrund steigender Datenvolumina oder Einsatz neuer Dienste und Dienstleistungen erweitert werden müssen,
- Änderungen technischer Standards bauliche oder sicherheitstechnische Anpassungen nach sich ziehen können,
- Erweiterungen des Netzes nicht auszuschließen sind
- neue Forderungen an das Netz die Verlegung anderer Kabel erforderlich machen.

Beispiele:

- Eine Erweiterung von Netzen ist nur in dem Umfang möglich, wie es die vorhandenen, verlegten Kabel zulassen oder der zur Verfügung stehende Platz für zusätzliche Kabel erlaubt. Gerade in geschlossenen Trassen (Rohre, estrichüberdeckte Fußbodenkanäle etc.) ist es trotz noch vorhandenen Platzes oft nicht möglich, zusätzliche Kabel einzuziehen, ohne neue und alte Kabel zu beschädigen. Als Ausweg bleibt dann nur, die vorhandenen Kabel aus der Trasse herauszuziehen und alle Kabel, die alten und die neuen, gleichzeitig neu einzuziehen. Die dadurch entstehenden Betriebsbeeinträchtigungen und Kosten sind beträchtlich.

  kein Austausch einzelner Kabel möglich

- Die Planung eines Rechenzentrum erfolgte zunächst allein unter ästhetischen Gesichtspunkten. Infrastrukturelle und sicherheitstechnische Anforderungen standen im Hintergrund und wurden erst nach der Rohbauerstellung konkreter definiert. Die Fertigstellung des Baus verzögerte sich extrem, weil erforderliche Trassen nicht zur Verfügung standen und Räume nicht bedarfsgerecht dimensioniert und positioniert waren. Änderungen während des späteren Betriebs waren nur unter großen Umständen zu bewältigen.

  Trassen nicht eingeplant

- In einem Unternehmen wurde nach zehn Jahren Betriebszeit eine vollständig neue Netzstruktur und IT-Verkabelung geplant. Auf Nachfrage stellte sich heraus, dass im folgenden Jahr eine Erneuerung der TK-Anlage und der TK-Verkabelung geplant war, die bislang zusammen mit der IT-Verkabelung in derselben Trasse geführt wurde. Ohne Koordinierung dieser beiden Maßnahmen wären doppelte Arbeiten an den Trassen erforderlich geworden und es wären möglicherweise zu kleine Trassen geplant worden.

  schlechte Koordination

G 2.12 Unzureichende Dokumentation der Verkabelung

Ist aufgrund unzureichender Dokumentation die genaue Lage von Leitungen nicht bekannt, so kann es bei Bauarbeiten außerhalb oder innerhalb eines Gebäudes zu Beschädigungen von Leitungen kommen. Dabei kann es zu längeren Ausfallzeiten oder unter Umständen sogar zu lebensbedrohenden Gefahren, z. B. durch Stromschlag, kommen.

Eine unzureichende Dokumentation erschwert zudem Prüfung, Wartung und Reparatur von Leitungen sowie Rangierungen, wie sie z. B. bei Änderungen im Endgeräte-Bereich (Umzug, Neuzugang) erforderlich werden.

Beispiel:

- In einer größeren Behörde wurde die Verkabelung der IT durch eine externe Firma vorgenommen. Die Anfertigung einer Dokumentation war im Leistungsumfang nicht enthalten. Da nach Fertigstellung der Verkabelung mit der Firma kein Wartungsvertrag abgeschlossen wurde, verfügte die Behörde nicht über die notwendige Dokumentation. Erweiterungen des Netzes konnten nur mit erheblichen Verzögerungen vorgenommen werden.

G 2.13 Unzureichend geschützte Verteiler

Verteiler des Stromversorgungsnetzes sind vielfach frei zugänglich und unverschlossen in Fluren oder Treppenhäusern untergebracht. Somit ist es jedermann möglich, diese Verteiler zu öffnen, Manipulationen vorzunehmen und ggf. einen Stromausfall herbeizuführen.

G 2.14 Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen

Ein nicht nach ergonomischen Gesichtspunkten eingerichteter Arbeitsplatz oder das Arbeitsumfeld (z. B. Störungen durch Lärm oder Staub) können dazu führen, dass die zur Verfügung stehende IT nicht oder nicht optimal genutzt werden kann.

Die meisten der denkbaren Störungen wirken sich nicht direkt auf die IT aus. Vielmehr werden die Benutzer in der Form beeinflusst, dass sie ihren Aufgaben nicht mit entsprechender Konzentration nachgehen können. Die Störungen reichen von Lärm oder starkem, unorganisiertem Kundenverkehr bis zu ungünstiger Beleuchtung, schlechter Belüftung und ähnlichem. Als erste Anzeichen solcher Störungen kann sich Aufgabenerledigung verlangsamen und die Anzahl kleiner Fehler zunehmen (Zeichendreher, Schreibfehler). Dadurch wird nicht nur das direkte Arbeitsergebnis beeinträchtigt. Auch die gespeicherten Daten enthalten eventuell Fehler, die Integrität der Daten wird vermindert.

G 2.15 Vertraulichkeitsverlust schutzbedürftiger Daten im Unix-System

Durch verschiedene Unix-Programme ist es möglich, Daten abzufragen, die das IT-System über die Benutzer speichert. Hiervon sind auch solche Daten betroffen, die Auskunft über das Leistungsprofil eines Benutzers geben können. Datenschutzrechtliche Gesichtspunkte müssen deshalb genauso beachtet werden wie die Gefahr, dass solche Informationen Missbrauchsmöglichkeiten erleichtern.

Beispiel:

Mit einem einfachen Programm, das in einem bestimmten Zeitintervall die Informationen, die der Befehl *who* liefert, auswertet, kann jeder Benutzer ein genaues Nutzungsprofil für einen Account erstellen. Z. B. lassen sich auf diese Weise die Abwesenheitszeiten des oder der Systemadministratoren feststellen, um diese Zeiten für unberechtigte Handlungen zu nutzen. Desweiteren lässt sich feststellen, welche Terminals für einen privilegierten Zugang zugelassen sind.

Weitere Programme mit ähnlichen Missbrauchsmöglichkeiten sind *finger* oder *ruser*.

G 2.16 Ungeordneter Benutzerwechsel bei tragbaren PCs

Der Benutzerwechsel bei tragbaren PCs wie Laptops oder Notebooks wird oftmals durch die einfache Übergabe des Gerätes vorgenommen. Dies hat zur Folge, dass meist nicht sichergestellt wird, dass auf dem Gerät keine schutzbedürftigen Daten mehr gespeichert sind und dass das Gerät nicht mit einem Computer-Virus verseucht ist. Zudem ist nach einiger Zeit nicht mehr nachvollziehbar, wer den tragbaren PC wann genutzt hat oder wer ihn zurzeit benutzt. Der ungeordnete Benutzerwechsel ohne Speicherkontrollen und ohne entsprechende Dokumentation kann damit zur Einschränkung der Verfügbarkeit des Geräts und zum Vertraulichkeitsverlust von Restdaten der Festplatte führen.

G 2.17 Mangelhafte Kennzeichnung der Datenträger

Unterbleibt eine ordnungsgemäße Kennzeichnung der ausgetauschten Datenträger, so ist für den Empfänger oft nicht nachvollziehbar, wer den Datenträger übersandt hat, welche Informationen darauf gespeichert sind oder welchem Zweck sie dienen. Wenn mehrere Datenträger ein- und desselben Absenders eingehen, kann bei fehlender Kennzeichnung die Reihenfolge verwechselt werden.

Beispiel:

Absender A verschickt an den Empfänger E eine Diskette mit Informationen, bei denen großes Gewicht auf deren Integrität gelegt wird. Am nächsten Tag stellt A fest, dass die Daten fehlerhaft waren, verschickt eine korrigierte Version und kündigt diese beim Empfänger telefonisch an. Auf dem Postweg überholt nun die zweite Diskette die erste, so dass der Empfänger aufgrund mangelhafter Kennzeichnung glaubt, die zuerst erhaltene Diskette enthielte die falschen Daten.

G 2.18 Ungeordnete Zustellung der Datenträger

Bei ungeordneter Zustellung von Datenträgern besteht die Gefahr, dass vertrauliche, auf dem Datenträger gespeicherte Daten in unbefugte Hände gelangen oder das gewünschte Ziel nicht rechtzeitig erreichen.

Beispiele:

- eine fehlerhafte Adressierung kann dazu führen, dass der Datenträger einem unautorisierten Empfänger übergeben wird,
- eine unzureichende Verpackung kann zu einer Beschädigung des Datenträgers führen, aber auch einen unbefugten Zugriff ermöglichen, der nicht festgestellt werden kann,
- eine fehlende Festlegung der Verantwortung beim Empfänger kann zur Folge haben, dass ein eingegangener Datenträger erst verspätet bearbeitet wird,
- eine nicht festgelegte Versandart kann bewirken, dass der Datenträger zu spät zugestellt wird, da die falsche Versandart ausgewählt wurde,
- eine fehlende Festlegung der Verantwortung beim Absender kann zur Folge haben, dass eine terminlich zugesicherte Zustellung der Datenträger nicht eingehalten werden kann.

G 2.19 Unzureichendes Schlüsselmanagement bei Verschlüsselung

Werden zum Schutz der Vertraulichkeit zu übermittelnder Daten Verschlüsselungssysteme eingesetzt, so kann aufgrund eines unzureichenden Schlüsselmanagements der gewünschte Schutz unterlaufen werden, wenn

- die Schlüssel in einer ungesicherten Umgebung erzeugt oder aufbewahrt werden,
- ungeeignete oder leicht erratbare Schlüssel eingesetzt werden,
- die zur Verschlüsselung bzw. Entschlüsselung eingesetzten Schlüssel nicht auf einem sicheren Weg den Kommunikationspartner erreichen.

Beispiele:

- Einfachstes **Negativbeispiel** ist der Versand der verschlüsselten Informationen **und** des benutzten Schlüssels auf ein- und derselben Diskette. In diesem Fall kann jeder, der in den Besitz der Diskette gelangt, die Informationen entschlüsseln, vorausgesetzt, dass das bei der Verschlüsselung eingesetzte Verfahren bekannt ist.

schlechte Zufallsquelle

- Kryptographische Schlüssel werden im Allgemeinen durch Zufallsprozesse erzeugt und evtl. nachbearbeitet. Wenn die verwendete Zufallsquelle ungeeignet ist, können Schlüssel erzeugt werden, die unsicher sind.

schlechte Wahl der Schlüssel

- Bei der Erzeugung von kryptographischen Schlüsseln, insbesondere von Masterkeys, ist es für die Sicherheit entscheidend, dass keine schwachen kryptographischen Schlüssel erzeugt werden. Dies können Schlüssel sein, die leicht zu erraten sind, oder Schlüssel, die für die Verschlüsselung ungeeignet sind (Beispiel: schwache und semischwache DES-Schlüssel). Wenn bei der Ableitung von Schlüsseln aus Masterkeys nicht überprüft wird, ob dabei ein schwacher Schlüssel erzeugt wurde, kann dadurch ein schwacher Schlüssel im Wirkbetrieb zum Einsatz kommen.
- Werden beim Triple-DES identische Teilschlüssel verwendet, bewirkt die Triple-DES-Verschlüsselung nur eine einfache DES-Verschlüsselung. Der Sicherheitsgewinn geht verloren.

Aber nicht nur die Offenlegung, sondern auch der Verlust von kryptographischen Schlüsseln kann zu großen Problemen führen. Kryptographische Schlüssel können

- verloren oder vergessen werden,
- nicht mehr zugreifbar sein, z. B. wenn der Schlüsselinhaber die Firma verlassen hat oder
- zerstört werden, indem sie versehentlich gelöscht werden oder indem sie verändert werden, z. B. durch Datenträgerversagen oder Bitfehler.

Wenn die Schlüssel nicht mehr verfügbar sind, können damit geschützte Daten nicht mehr entschlüsselt oder auf ihre Authentizität überprüft werden.

G 2.20 Unzureichende oder falsche Versorgung mit Verbrauchsgütern

Viele im Büroalltag eingesetzte Geräte wie Faxgeräte, Drucker, Datensicherungslaufwerke usw. benötigen für einen reibungslosen und unterbrechungsfreien Betrieb Verbrauchsgüter in ausreichender Menge. Fehlen Verbrauchsgüter, kann der Betriebsablauf empfindlich gestört werden. In Notfällen kann die Handlungsfähigkeit stark beeinträchtigt sein und hohe Folgekosten verursachen, weil Verbrauchsgüter nicht in ausreichender Menge zur Verfügung stehen.

Beispiele:

- Eingehende Faksimiles können nicht ausgedruckt werden, obwohl sie ordnungsgemäß empfangen wurden, wenn der Papier- oder der Tonervorrat aufgebraucht sind. Der Puffer-Speicher kann aufgrund seiner begrenzten Speicherkapazität die Abweisung oder den Verlust von Fax-Sendungen nur herauszögern, aber nicht langfristig verhindern.
- Es wird ein neues Bandlaufwerk beschafft, das mit den alten Bändern nicht kompatibel ist. Neue passende Bänder sind nicht beschafft worden, daher können tagelang keine Datensicherungen angefertigt werden.
- Ein wichtiger Druckjob steht an. Die beschaffte Tonerkartusche zur Reserve passt jedoch nicht für den Drucker.

G 2.21 Mangelhafte Organisation des Wechsels zwischen den Benutzern

Arbeiten mehrere Benutzer zeitlich versetzt an einem Einzelplatz-IT-System, so findet zwangsläufig ein Wechsel zwischen den Benutzern statt. Ist dieser nicht ausreichend organisiert und geregelt, wird er unter Umständen nicht sicherheitsgerecht durchgeführt. Hierdurch können Missbrauchsmöglichkeiten entstehen, wenn z. B.

- laufende Anwendungen nicht korrekt abgeschlossen werden,
- aktuelle Daten nicht gespeichert werden,
- Restdaten im Hauptspeicher oder in temporären Dateien verbleiben,
- der vorhergehende Benutzer sich nicht am IT-System abmeldet und
- der neue Benutzer sich nicht ordnungsgemäß am IT-System anmeldet.

G 2.22 Fehlende Auswertung von Protokolldaten

Die meisten IT-Systeme und Anwendungen bieten Funktionalitäten an, um die Nutzung der Operationen, ihre Reihenfolge und ihre Auswirkungen zu protokollieren.

Im Lebenszyklus eines IT-Systems kommen verschiedene Protokollierungskonzepte zum Einsatz. Während der Entwicklungsphase werden ausführliche Protokolle erstellt, um im Fehlerfall die Protokolldaten für eine detaillierte Problemanalyse heranziehen zu können und die Fehlerbehebung zu erleichtern.

In der Einführungsphase werden Protokolle genutzt, um unter anderem die Performance des IT-Systems in der Produktivumgebung zu optimieren oder um die Wirksamkeit des Sicherheitskonzepts erstmals in der Praxis zu überprüfen.

In der Produktivphase werden Protokolle hauptsächlich auf die Sicherstellung des ordnungsgemäßen Betriebs bezogen. Protokolldaten dienen dann dem Zweck, nachträglich feststellen zu können, ob Sicherheitsverletzungen im IT-System stattgefunden haben oder ob ein Angriffsversuch unternommen wurde. Protokolldaten werden für die Fehleranalyse im Schadensfall und zur Ursachenermittlung bzw. zur Integritätsprüfung genutzt. Die Protokollierung kann auch der Täterermittlung und damit auch der Abschreckung von potenziellen Tätern dienen. Durch regelmäßige Auswertung der Protokolldaten können vorsätzliche Angriffe auf ein IT-System unter Umständen frühzeitig erkannt werden. Findet die Auswertung der Protokolldaten nicht oder nur unzureichend statt, können diese nicht für Präventivmaßnahmen genutzt werden.

Bei einigen IT-Systemen oder Anwendungen fehlen ausreichende Protokollierungsmöglichkeiten. Häufig ist es mit systemeigenen Mitteln nicht oder nur schwer möglich, bei der Protokollierung nach der Art der Ereignisse zu differenzieren. Teilweise ist überhaupt keine Protokollierung vorgesehen.

Beispiele:

- Ein nicht autorisierter Benutzer versucht, Zugriff auf einen Datenbank-Server zu erlangen, indem er zu bekannten Benutzernamen die entsprechenden Passwörter rät. Die erfolglosen Authentisierungsversuche werden im System protokolliert. Aufgrund fehlender Auswertung der Protokolldateien werden die Angriffsversuche nicht erkannt. Der unautorisierte Benutzer kann unerkannt den Angriffsversuch gegebenenfalls bis zum Erfolg fortsetzen.
- Auf einem nicht vernetzten Windows 95-Rechner gibt es keine Möglichkeit, die Aktivitäten eines oder mehrerer Benutzer benutzerspezifisch zu protokollieren. Es ist daher nicht festzustellen, ob Sicherheitsverletzungen im IT-System stattgefunden haben oder ob ein solcher Versuch unternommen wurde.

G 2.23 Schwachstellen bei der Einbindung von DOS-PCs in ein servergestütztes Netz

Diese Gefährdung ist mit Version 2006 entfallen.

G 2.24 Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes

Bei einem nicht durch eine Firewall geschützten Netz, das mit einem externen Netz wie dem Internet gekoppelt ist, können aus dem externen Netz verschiedene Daten des internen Netzes wie z. B. Mailadressen, IP-Nummern, Rechnernamen und Benutzernamen abgerufen werden. Dadurch lassen sich Rückschlüsse auf die interne Netzstruktur und dessen Anwender ziehen. Je mehr Informationen ein Angreifer über potentielle Angriffsziele hat, desto mehr Angriffsmöglichkeiten hat er. Wenn ein Angreifer z. B. Benutzernamen eines IT-Systems kennt, kann er versuchen, die zugehörigen Passwörter zu erraten oder über Wörterbuchattacken herauszufinden (siehe G 5.18 *Systematisches Ausprobieren von Passwörtern*).

G 2.25 Einschränkung der Übertragungs- oder Bearbeitungsgeschwindigkeit durch Peer-to-Peer-Funktionalitäten

In einem servergestützten Netz können auf Clients aktivierte Peer-to-Peer-Funktionalitäten die verfügbare Übertragungsbandbreite einschränken, da dasselbe physikalische Medium beansprucht wird. Beispielsweise erfolgen Zugriffe auf Dateien des Servers unter Umständen mit erheblichen Verzögerungen, wenn gleichzeitig über die Peer-to-Peer-Funktionen große Dateien von Client zu Client kopiert werden.

Ein Arbeitsplatz-Computer kann in einem Peer-to-Peer-Netz als "Server", d. h. als Applikations- oder Dateianbieter für andere Rechner, eingesetzt werden. Dabei wird er durch die zu verwaltenden Peer-to-Peer-Funktionalitäten unter Umständen erheblich belastet, wodurch die lokale Bearbeitungsgeschwindigkeit deutlich abnimmt.

G 2.26 Fehlendes oder unzureichendes Test- und Freigabeverfahren

Wird neue Hard- oder Software nicht oder nur unzureichend getestet und ohne Installationsvorschriften freigegeben, kann es passieren, dass Fehler in der Hard- oder Software nicht erkannt werden oder dass die notwendigerweise einzuhaltenden Installationsparameter nicht erkannt bzw. nicht beachtet werden. Diese Hardware-, Software- oder Installationsfehler, die aus einem fehlenden oder unzureichenden Software-Test- und Freigabeverfahren resultieren, stellen eine erhebliche Gefährdung für den IT-Betrieb dar.

Im Vertrauen auf eine problemlose Installation neuer Hard- bzw. Software wird oftmals übersehen, dass mögliche Schäden in keinem Verhältnis zu dem Aufwand stehen, den ein geordnetes Test- und Freigabeverfahren erfordert. Programme oder IT-Systeme werden unzureichend getestet und mit Fehlern in eine Produktionsumgebung eingebracht. Die Fehler wirken sich in der Folge störend auf den bis zu diesem Zeitpunkt problemlosen Betrieb aus.

Beispiele für solche Schäden werden nachfolgend aufgezeigt:

- Programme oder Programm-Updates lassen sich nicht sinnvoll nutzen, da für ein annehmbares Verarbeitungstempo mehr Ressourcen (z. B. Hauptspeicher, Prozessorkapazität) als erwartet benötigt werden. Wird dies nicht im Test erkannt, kann das zu erheblichen Fehl- oder Folgeinvestitionen führen. Nicht selten führten Entscheidungen gegen weitere Investitionen dazu, dass ein Softwareprodukt zwar gekauft und bezahlt, jedoch nie benutzt wurde. **Ressourcen**
- Eingeübte Arbeitsabläufe werden nach Installation neuer Software maßgeblich behindert. Der mit der Installation des Programms beabsichtigte Nutzen stellt sich erst bedeutend später ein, da die Mitarbeiter im Vorfeld nicht geschult bzw. nicht über die neuen Funktionen des Programms informiert wurden. **Arbeitsbehinderungen**
- Durch das Einspielen eines Updates einer DBMS-Standardsoftware, das mit Fehlern behaftet ist, steht die Datenbank nicht mehr zur Verfügung oder es kommt zu Datenverlust.
- Einige Software-Produkte installieren die Microsoft Server Desktop Engine (MSDE) als Datenbank, ohne dass dies vom Benutzer bemerkt wird. Hierbei handelt sich um eine Ausprägung des Microsoft SQL Servers mit den typischen Gefährdungen eines Datenbanksystems. Oft sind die Benutzer des Produktes bzw. die Administratoren, die das Produkt installieren, nicht ausreichend über diese Gefährdungen informiert und versäumen, sicherheitsrelevante Maßnahmen zu ergreifen. So wird häufig in Verbindung mit MSDE ein Benutzerkonto in der Datenbank für den Administrator angelegt, das in der Grundinstallation über keinen Passwortschutz verfügt. Auf diese Weise können Angreifer einen Vollzugriff auf die Daten und gegebenenfalls sogar auf das Betriebssystem erhalten.

G 2.27 Fehlende oder unzureichende Dokumentation

Verschiedene Formen der Dokumentation können betrachtet werden: die Produktbeschreibung, die Administrator- und Benutzerdokumentation zur Anwendung des Produktes und die Systemdokumentation.

Eine fehlende oder unzureichende Dokumentation der eingesetzten IT-Komponenten kann sowohl im Auswahl- und Entscheidungsprozess für ein Produkt, als auch bei einem Schadensfall im Wirkbetrieb erhebliche Auswirkungen haben.

Schadensbehebung ohne Dokumentation schwierig

Bei einer unzureichenden Dokumentation kann sich im Schadensfall, beispielsweise durch den Ausfall von Hardware bzw. Fehlfunktionen von Programmen, die Fehlerdiagnose und -behebung erheblich verzögern oder völlig undurchführbar sein.

Dies gilt auch für die Dokumentation von Leitungswegen und Verkabelungen innerhalb der Gebäude-Infrastruktur. Ist aufgrund unzureichender Dokumentation die genaue Lage von Leitungen nicht bekannt, so kann es bei Bauarbeiten außerhalb oder innerhalb eines Gebäudes zu Beschädigungen von Leitungen kommen. Dabei kann es zu längeren Ausfallzeiten (Eintritt eines Notfalls) oder unter Umständen sogar zu lebensbedrohenden Gefahren, z. B. durch Stromschlag, kommen.

Beispiele:

vertrauliche Informationen versehentlich offen gelegt

- Wenn von einem Programm Arbeitsergebnisse in temporären Dateien zwischengespeichert werden, ohne dass dies ausreichend dokumentiert ist, kann dies dazu führen, dass die temporären Dateien nicht angemessen geschützt und vertrauliche Informationen offengelegt werden. Durch fehlenden Zugriffsschutz auf diese Dateien oder eine nicht korrekte physikalische Löschung der nur temporär genutzten Bereiche können Informationen Unbefugten zugänglich werden.
- Bei Installation eines neuen Softwareproduktes werden bestehende Konfigurationen abgeändert. Andere, bislang fehlerfrei laufende Programme sind danach falsch parametrisiert und stürzen ggf. ab. Durch eine detaillierte Dokumentation der Veränderung bei der Installation von Software ließe sich der Fehler schnell lokalisieren und beheben.

Dokumentationspflicht vergessen

- In einer größeren Behörde wurde die Verkabelung der IT durch eine externe Firma vorgenommen. Die Anfertigung einer Dokumentation war im Leistungsumfang nicht enthalten. Da nach Fertigstellung der Verkabelung mit der Firma kein Wartungsvertrag abgeschlossen wurde, verfügte die Behörde nicht über die notwendige Dokumentation. Erweiterungen des Netzes konnten nur mit erheblichen Verzögerungen vorgenommen werden (siehe auch G 2.12 *Unzureichende Dokumentation der Verkabelung)*.
- In einer z/OS-Installation wurden jeden Abend automatisch Batch-Jobs zur Verarbeitung von Anwendungsdaten gestartet. Für die Verarbeitung war es wichtig, dass die Batch-Jobs in der richtigen Reihenfolge abliefen. Als eines Abends die Automation versagte, mussten die Jobs manuell gestartet werden. Aufgrund fehlender Dokumentation wurden die Batch-Jobs in der falschen Reihenfolge gestartet. Dies führte zu Abbrüchen in der

Verarbeitung der Anwendungsdaten und zu Verzögerungen in der Produktion um mehrere Stunden.

G 2.28 Verstöße gegen das Urheberrecht

Der Einsatz nicht-lizenzierter Software kann einen Verstoß gegen das Urheberrecht darstellen und sowohl zu zivil- als auch strafrechtlichen Konsequenzen führen.

Behörden und Unternehmen, in denen Raubkopien zum Einsatz kommen, können im Rahmen des Organisationsverschuldens, unabhängig von der Schuldform (Vorsatz oder Fahrlässigkeit) vom Urheberrechtseigentümer schadensersatzpflichtig gemacht werden.

Beispiel:

In einem Unternehmen wurde eine große Anzahl Benutzeroberflächen eingesetzt, ohne dass die hierfür erforderlichen Lizenzen erworben wurden. Die Kosten für die erforderliche Nachlizenzierung sowie den Schadensersatz an den Urheberrechtseigentümer beliefen sich auf ein Vielfaches der Lizenzgebühren.

G 2.29 Softwaretest mit Produktionsdaten

Vielfach ist zu beobachten, dass Softwaretests mit Produktionsdaten vollzogen werden. Als wesentliche Gründe werden hierfür angeführt, dass nur im direkten Vergleich mit vorhandenen Arbeitsergebnissen eine abschließende Beurteilung über die Funktion und Performance des Produktes möglich ist. Darüber hinaus sind mangelndes Sicherheitsbewusstsein, überzogenes Vertrauen in die zu testende Software und Unkenntnis über mögliche schädliche Auswirkungen ursächlich für diese Vorgehensweise.

Beim Test mit Produktionsdaten kann es zu folgenden Problemen kommen:

- Software wird mit Kopien von Produktionsdaten in isolierter Testumgebung getestet:

  Wenn neue Software mit nicht anonymisierten Daten getestet wird, erhalten evtl. nicht befugte Mitarbeiter, bzw. Dritte, die mit dem Softwaretest beauftragt worden sind, hierbei Einblick in Dateien mit evtl. vertraulichen Informationen.

- Software wird mit Produktionsdaten im Wirkbetrieb getestet:

  Fehlfunktionen von Software während des Testens können über den oben geschilderten Fall hinaus beispielsweise dazu führen, dass neben der Vertraulichkeit der Produktionsdaten auch deren Integrität und Verfügbarkeit beeinträchtigt werden.

  Aufgrund der Inkompatibilität unterschiedlicher Programme können Seiteneffekte auftreten, die bei anderen Systemkomponenten zu nachhaltigen Beeinträchtigungen führen können. Bei vernetzten Systemen kann das von Performanceverlusten bis hin zum Systemabsturz des Netzes reichen.

  Durch fehlerhaftes Verhalten der zu testenden Software oder Bedienfehler können Produktionsdaten ungewollt verändert werden. Möglicherweise wird diese Veränderung nicht festgestellt. Da Datenbestände, um unnötige Redundanz zu vermeiden, zunehmend durch unterschiedliche Programme gemeinsam genutzt werden, können sich diese Fehler auch auf andere IT-Anwendungen auswirken. Im Schadensfall ist nicht nur der Aufwand für die Rekonstruktion der Daten notwendig, darüber hinaus müssen bereits erstellte Arbeitsergebnisse auf ihre Integrität überprüft werden.

G 2.30 Unzureichende Domänenplanung

Eine unzureichende Planung der Domänen und ihrer Vertrauensbeziehungen in einem Windows NT Netz kann dazu führen, dass Vertrauensbeziehungen zu Domänen bestehen, die nicht als vertrauenswürdig zu betrachten sind. Damit ist es Benutzern der betreffenden Domänen unter Umständen möglich, auf Ressourcen der vertrauenden Domäne zuzugreifen, ohne dass dies dort beabsichtigt ist oder auch nur erkannt wird. Dies kann insbesondere dann geschehen, wenn die Zugriffsrechte der vertrauenden Domäne in der Annahme, dass keine andere Domäne auf die lokalen Ressourcen zugreift, relativ weitgehend festgesetzt wurden.

Umgekehrt können fehlende Vertrauensbeziehungen zwischen Domänen dazu führen, dass sich Benutzer unnötigerweise explizit bei fremden Domänen authentisieren müssen, was bei mangelnder Koordination der Passwörter zwischen diesen Domänen zu Verwirrung führt. Der Benutzer muss sich dann eine Vielzahl von Passwörtern merken, was zu einer Beeinträchtigung der Sicherheit führen kann, wenn er sich die Passwörter aufschreibt.

G 2.31 Unzureichender Schutz des Windows NT Systems

Windows NT wird mit sehr weitgehenden Zugriffsrechten auf das Dateisystem und auf die Registrierung ausgeliefert. Wenn diese Zugriffsrechte nicht nach der Installation entsprechend den lokalen Sicherheitsanforderungen strikter eingestellt werden, besitzt effektiv jeder Benutzer Zugriff auf alle Dateien und auf die gesamte Registrierung, d.h. der Zugriffsschutz ist de facto ausgeschaltet.

Weiterhin ist Windows NT nicht in der Lage, den Zugriff auf Disketten- und CD-ROM-Laufwerke sowie auf Bänder zu kontrollieren, so dass hier eine Möglichkeit zu unzulässigem Datenimport und -export besteht, wenn nicht durch zusätzliche Maßnahmen der Zugriff auf diese Datenträger eingeschränkt oder zumindest auf organisatorischer Ebene kontrolliert wird.

G 2.32 Unzureichende Leitungskapazitäten

Bei der Planung von Netzen wird oft der Fehler begangen, die Kapazitätsauslegung ausschließlich am aktuellen Bedarf vorzunehmen. Dabei wird übersehen, dass die Kapazitätsanforderungen an das Netz stetig steigen, z. B. wenn neue IT-Systeme in das Netz integriert werden oder das übertragene Datenvolumen zunimmt.

Wenn die Kapazität des Netzes nicht mehr ausreicht, wird die Übertragungsgeschwindigkeit und ggf. auch die Erreichbarkeit im Netz für alle Benutzer stark eingeschränkt. Beispielsweise werden Dateizugriffe auf entfernten IT-Systemen erheblich verzögert, wenn gleichzeitig das Netz von anderen Benutzern stark in Anspruch genommen wird, wie durch das Verschieben von großen Dateien von einem IT-System zum anderen.

Beispiel:

Eine verteilte Organisation baut für die Datenkommunikation ein Netz über ISDN-So-Verbindungen auf. Nach Einführung eines graphisch orientierten, firmeneigenen Intranet kommt die Datenkommunikation fast zum Stillstand. Erst das Umstellen auf S2M-Übertragungswege schafft die nötige Übertragungskapazität.

G 2.33 Nicht gesicherter Aufstellungsort von Novell Netware Servern

Die Aufstellung von Novell Netware Servern in einer nicht gesicherten Umgebung (z. B. Flure, nicht verschlossene Serverräume) stellt eine erhebliche Gefährdung für die IT-Sicherheit dar.

Direkte Eingaben an der Server-Konsole bzw. das Laden von NLMs (Netware Loadable Modules) am Server können dazu führen, dass die installierten Sicherheitsmechanismen außer Kraft gesetzt werden, ohne dass dieser Umstand dem Administrationspersonal bzw. dem IT-Sicherheitsmanagement bekannt wird.

Beispiel:

Durch das Laden spezieller NLMs ist es möglich, einen Supervisor-äquivalenten Benutzer zu generieren bzw. einen existierenden Benutzer mit Supervisor-äquivalenten Rechten zu versehen.

G 2.34 Fehlende oder unzureichende Aktivierung von Novell Netware Sicherheitsmechanismen

Das Netzbetriebssystem Novell Netware verfügt über eine Sammlung an Sicherheitsmechanismen, die den unerlaubten Zugriff auf Dateien des Servers abwehren.

Diese Sicherheitsmechanismen werden jedoch nicht automatisch aktiviert, sondern müssen durch die Systemadministration nach dem erstmaligen Start des Servers eingerichtet werden.

Werden die Sicherheitsmechanismen eines Novell Netware Servers nicht oder nur unzureichend installiert, so kann der unerlaubte Zugriff auf schützenswerte Dateien entscheidend erleichtert werden.

G 2.35 Fehlende Protokollierung unter Windows 95

Auf einem nicht vernetzten Windows 95-Rechner gibt es keine Möglichkeit, die Aktivitäten eines oder mehrerer Benutzer benutzerspezifisch zu protokollieren. Es ist daher nicht festzustellen, ob Sicherheitsverletzungen im IT-System stattgefunden haben oder ob ein solcher Versuch unternommen wurde.

Hinweis:

Der Inhalt dieser Gefährdung wurde in G 2.22 *Fehlende Auswertung von Protokolldaten* integriert und ist mit der Version entfallen.

G 2.36 Ungeeignete Einschränkung der Benutzerumgebung

Verschiedene Betriebssysteme (z. B. Windows 95, Windows NT) und PC-Sicherheitsprodukte bieten die Möglichkeit, die Benutzerumgebung individuell für jeden Benutzer einzuschränken. Dabei bestehen prinzipiell zwei Möglichkeiten:

1. Bestimmte Funktionalitäten werden erlaubt, alle anderen sind verboten.
2. Bestimmte Funktionalitäten werden verboten, alle anderen sind erlaubt.

In beiden Fällen besteht die Möglichkeit, den Benutzer derart einzuschränken, dass dieser wesentliche Funktionen nicht mehr ausführen kann oder dass sogar ein sinnvolles und effizientes Arbeiten mit dem PC nicht mehr möglich ist.

G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindungen

Beim Einsatz von Kommunikationskarten innerhalb eines IT-Systems (Fax-, Modem- oder ISDN-Karten) ist für den Benutzer nicht immer offensichtlich, was außer seinen Nutz- und Protokollinformationen zusätzlich übertragen wird. Nach Aktivierung einer Kommunikationskarte ist es grundsätzlich möglich, dass diese, ohne Initiierung durch den Benutzer, Verbindungen zu einer nicht gewünschten Gegenstelle aufbaut oder durch Dritte über dem Benutzer nicht bekannte Remote-Funktionalitäten angesprochen wird.

Beispiele:

- Bei der erstmaligen Konfiguration einer Faxkarte wurde der Benutzer vom Installationsprogramm nach der Landesvorwahl von Schweden gefragt. Zu vermuten ist, dass der Kartenhersteller über den Einsatz seines Produkts, evtl. aus Gründen des Produkt-Marketings, informiert werden wollte.
- Eine große Anzahl von Modem-Karten unterstützt den ferngesteuerten Zugriff auf IT-Systeme. Zwar lassen sich diese Zugriffe über teilweise sogar auf den Karten integrierte Mechanismen (Callback-Option und Rufnummernauthentisierung) absichern, voreingestellt ist dies jedoch nicht. Ein so konfiguriertes IT-System lässt sich von außen über die Modemkarte vollständig manipulieren.

G 2.38 Fehlende oder unzureichende Aktivierung von Datenbank-Sicherheitsmechanismen

Jede Datenbank-Standardsoftware stellt in der Regel eine Reihe von Sicherheitsmechanismen bereit, mittels derer die Daten vor unberechtigtem Zugriff oder Ähnlichem geschützt werden können. Sie sind jedoch nicht unbedingt automatisch aktiv, sondern müssen vom Datenbank-Administrator meistens manuell eingeschaltet werden. Wird davon kein Gebrauch gemacht, so kann weder die Vertraulichkeit noch die Integrität der Daten gewährleistet werden. In diesem Fall ist es dann meistens nicht möglich, solche Schutzverletzungen zu erkennen und zu protokollieren. Der Verlust bzw. die Manipulation von Daten bis hin zur Zerstörung der Datenbank selbst kann die Folge sein.

Beispiel:

Bei der Datenbank MS Access ist die Aktivierung des Passwortschutzes optional. Hierdurch kann es auf einfache Weise zu einem unberechtigten Zugang zum Datenbanksystem und damit auch zu einem unberechtigten Zugriff auf die dort gespeicherten Daten kommen. Eine Kontrolle der Datenbanknutzung ist in diesem Fall nicht möglich.

G 2.39 Mangelhafte Konzeption eines DBMS

In der Konzeption eines Datenbank-Managementsystems (DBMS) werden die Anforderungen an Auswahl, Aufbau, Betrieb und eventuell Erweiterung des geplanten Systems festgelegt.

Die Auswahl und der Einsatz einer Datenbank-Standardsoftware erfordert sorgfältige Planung, Installation und Konfiguration des Datenbank-Managementsystems (DBMS), um einen störungsfreien Einsatz zu gewährleisten. Die Vielzahl möglicher Gefährdungen sollen durch die nachfolgenden Beispiele verdeutlicht werden.

Auswahl einer ungeeigneten Datenbank-Standardsoftware

- Es wird ein DBMS ausgewählt, welches in der geplanten Einsatzumgebung nicht lauffähig ist. Dies kann daraus resultieren, dass das DBMS an ein bestimmtes Betriebssystem gebunden ist oder die Mindestanforderungen an die Hardware nicht erfüllt werden.
- Das ausgewählte DBMS stellt ein Sicherheitsrisiko dar, weil die vom Hersteller zur Verfügung gestellten Sicherheitsmechanismen nicht ausreichen, um die geforderte Verfügbarkeit, Integrität und Vertraulichkeit der Daten zu gewährleisten.

Fehlerhafte Installation bzw. Konfiguration der Datenbank-Standardsoftware

- Die empfohlenen Sicherheitsmaßnahmen werden fehlerhaft, unvollständig oder gar nicht durchgeführt.

  Beispiele:

  Die Kontrolldateien eines Datenbanksystems werden nicht gespiegelt bzw. die gespiegelte Kontrolldatei wird nicht auf einer anderen Festplatte abgelegt. Ein Plattencrash führt dabei mit großer Wahrscheinlichkeit zur Zerstörung der Datenbank.

  Während der Installation wird der automatisch erzeugten Systemadministrator-Kennung ein triviales Passwort zugewiesen, das nachfolgend nicht abgeändert wird.

- Die physikalischeVerteilung der Daten ist unzureichend (falls das DBMS eine physikalische Verteilung vorsieht). Werden anwendungsspezifische Daten nicht physikalisch voneinander getrennt gespeichert, kann bereits der Ausfall einer einzigen Festplatte zu einem Komplettausfall aller Anwendungen führen.
- Durch falsche Parametereinstellungen kann der Zugriff auf bestimmte Daten verhindert werden.

  Beispiel:

  Durch eine falsche Ländereinstellung in einer Datenbank-Software kann die Darstellung von Umlauten unmöglich gemacht werden.

Fehlerhafte Konzeption der Datenbank

Im Datenbankkonzept werden neben den einzelnen Tabellen und ihren Spalten und Schlüsseln auch die Relationen der Tabellen untereinander dargestellt.

Einem Element einer Tabelle können kein, ein oder mehrere Elemente einer anderen Tabelle zugeordnet sein. Aus diesen Relationen ergeben sich Restriktionen, die bei Lösch-, Update- oder Einfüge-Operationen zu erfüllen sind, um die Datenbank-Integrität zu erhalten.

Beispiel:

Jeder Einwohner muss einen Wohnort haben. Einwohner können mehrere Wohnorte besitzen. Sollte ein Einwohner sterben, so fallen auch alle zugeordneten Wohnorte weg. Mehrere Einwohner können sich einen Wohnort teilen. Wohnorte können leer stehen.

In der Datenbank wird eine solche Relation durch eine zusätzliche Tabelle dargestellt, die für jedes Element der Relation (im Beispiel Einwohner / Wohnort) als Verweise auf die Datensätze die Schlüssel der zugehörigen Datensätze der einzelnen Tabellen enthält. Wenn ein Datensatz in der Tabelle der Einwohner oder der Wohnorte gelöscht wurde, darf es auch in der Tabelle zur Zuordnungsrelation keinen Verweis mehr auf diesen Datensatz geben. Die Einhaltung solcher Bedingungen kann in der Datenbank selbst definert werden, durch Bedingungen oder automatisch ablaufende Prozeduren.

Aus dem Zusammenwirken dieser Konstrukte kann es zu kaskadierenden Datenbankoperationen kommen, die aber in verschiedenen DBMS durch unterschiedliche Einschränkungen begrenzt werden.

- Fehlende Relationen zwischen einzelnen Tabellen können, wenn nicht die Anwendung diese Funktionalität nachbildet, zu einem Verlust der sogenannten referenziellen Datenbankintegrität führen.

  Beispiel:

  Ein Wohnort wird ohne Prüfung gelöscht, ob diesem noch Einwohner zugeordnet sind.

- Werden Datenbanktrigger falsch eingesetzt, kann es zu Inkonsistenzen der Daten kommen, wenn die Anwendung dies nicht selbst berücksichtigt.

  Beispiel:

  Ein Einwohner verstirbt und wird daher aus der Datenbank gelöscht. Nachdem die Löschoperation durchgeführt ist, werden durch einen Delete-Trigger alle Datensätze in der zusätzlichen Tabelle gelöscht, die die verschiedenen Wohnorte des verstorbenen Einwohners beschreiben.

- Durch eine mangelhafte Konzeption des Einsatzes von Datenbanktriggern kann es zu einem Verlust der Datenintegrität oder unkontrollierten Datenmanipulationen kommen.

G 2.40 Mangelhafte Konzeption des Datenbankzugriffs

Die Benutzer greifen über ein Datenbank-Managementsystem (DBMS) auf eine oder mehrere Datenbanken zu. Dieser Zugriff geschieht direkt oder aber von einer Anwendung aus. Um die Integrität einer Datenbank zu gewährleisten, müssen alle Datenbankzugriffe von einer zentralen Stelle aus kontrolliert werden. Bei mangelhafter Konzeption des Datenbankzugriffs kann es unter anderem zu folgenden Sicherheitsproblemen kommen:

Benutzerberechtigungen

- Ist der Berechtigungsumfang für die Benutzer zu restriktiv definiert, kann dies dazu führen, dass bestimmte Arbeiten von diesen nicht durchgeführt werden können.
- Ist der Berechtigungsumfang dagegen zu umfangreich, kann dies dazu führen, dass Daten unberechtigt manipuliert bzw. eingesehen werden können.
- Wird den Benutzern erlaubt, direkt auf die Datenbank zuzugreifen (im Gegensatz zum Zugriff aus einer Anwendung heraus), so besteht prinzipiell die Gefahr des Integritätsverlustes der Datenbank durch Datenmanipulationen, deren Auswirkungen die Benutzer nicht unbedingt abschätzen können.

Hinweis: Wie die eigentlichen Daten einer Datenbank werden auch die Eigenschaften der einzelnen Datenbankobjekte, wie z. B. Struktur, Indizes, Schlüssel einer Tabelle, wiederum in Tabellen gespeichert, auf die über SQL-Befehle zugegriffen werden kann.

- Werden Datenbankobjekte nicht explizit durch ein entsprechendes Berechtigungs- und Zugriffskonzept geschützt, so besteht die Gefahr, dass die Datenbankobjekte selbst manipuliert werden (Manipulation von Feldern einer Tabelle oder von Tabellen-Indizes etc.). Dies kann zu einer Vielzahl von Problemen bis hin zur Zerstörung der Datenbank führen.

Hinweis: Für die Vergabe von Zugriffsrechten entsteht durch den Einsatz von Data-Warehouse, Online Analytic Processing (OLAP)-Systemen und Query-Tools häufig ein Sicherheitskonflikt. Einerseits sollen möglichst viele Daten aus heterogenen Datenquellen für die Entscheidungsträger zur Auswertung herangezogen werden können, andererseits müssen sensible Daten vor unberechtigtem Zugriff geschützt werden. Die Herausforderung besteht darin, die Zugriffsrechte so zu gestalten, dass sie sowohl dem Datenschutz und den Anforderungen an die Vertraulichkeit sensibler Daten als auch den Analyseanforderungen gerecht werden.

Remote-Zugriff

- Wird die Datenbank in einem Netz zur Verfügung gestellt, können bei mangelnden Sicherheitsvorkehrungen im Bereich des Remote-Zugriffs auf die Datenbank sowohl Daten manipuliert als auch unberechtigt eingesehen werden (siehe hierzu auch G 5.64 *Manipulation an Daten oder Software bei Datenbanksystemen*).

Datenbankabfragen

- Ohne eine aufgabenspezifische Einschränkung der Zugriffsrechte für die verschiedenen Benutzergruppen kann es zum Verlust der Vertraulichkeit schutzbedürftiger Daten durch unautorisierten Zugriff kommen.
- Die Anfragen und Aufrufe von Benutzern oder Anwendungen an die Datenbank müssen einer gemeinsam vereinbarten Syntax oder einem normierten Sprachumfang folgen, der vom jeweils angesprochenen DBMS zur Verfügung gestellt wird (z. B. ANSI-SQL-99 für eine relationale Datenbank). Hält sich die aufrufende Seite nicht an diese Syntax, kann dies dazu führen, dass Datenbankanfragen vom DBMS nicht bearbeitet werden können und zurückgewiesen werden. Diese Gefährdung besteht insbesondere, wenn DBMS verschiedener Anbieter eingesetzt und von einer zentralen Anwendung angesprochen werden.
- Die Verwendung von nicht exakt formulierten Datenbankabfragen kann dazu führen, dass durch eine Änderung der Datenbankobjekte die Datenbankabfrage falsche oder unerwartete Ergebnisse liefert. Unter Umständen kann auch das gesamte Datenbanksystem durch sinnlose Anfragen so in Anspruch genommen werden, dass der eigentliche Zweck nicht mehr erfüllt werden kann.

Beispiele:

- Die Abfrage "SELECT * FROM Tabelle" liefert alle Attribute bzw. Felder eines Tupels bzw. Datensatzes. Die Reihenfolge der Felder wird dabei von der technischen Struktur der Tabelle vorgegeben. Wird nun ein Feld in der Tabelle hinzugefügt oder gelöscht, d. h. die technische Struktur der Tabelle wird verändert, so hat dies unter Umständen fatale Auswirkungen auf eine Anwendung, in der eine solche Datenbankabfrage benutzt wird.
- Es werden vorsätzlich viele weit gefasste Abfragen an die Datenbank gerichtet, um die Ansprechbarkeit der Datenbank zu verhindern (siehe G 5.65 *Verhinderung der Dienste eines Datenbanksystems*).

G 2.41 Mangelhafte Organisation des Wechsels von Datenbank-Benutzern

Teilen sich mehrere Benutzer einer Datenbank den gleichen Arbeitsplatz, so besteht die Gefahr von ungewollten oder gezielten Datenmanipulationen, wenn der Wechsel zwischen den Benutzern nicht organisiert ist bzw. der Wechsel nicht ordnungsgemäß durchgeführt wird. Auch ist dann die Vertraulichkeit der Daten nicht mehr gewährleistet.

Beispiel:

Wird eine Anwendung, die auf eine Datenbank zugreift, vor einem Benutzerwechsel nicht ordnungsgemäß verlassen, so führen die unterschiedlichen Berechtigungsprofile der betroffenen Benutzer zu den oben genannten Gefährdungen. Auch wird dabei der Protokollmechanismus der Datenbank unterlaufen, da dieser die Datenmodifikationen und Aktivitäten der aktiven Benutzer-Kennung festhält. Diese Kennung stimmt aber in einem solchen Fall nicht mit dem tatsächlichen Benutzer überein. Dadurch können Datenmodifikationen nicht mehr eindeutig einem Benutzer zugeordnet werden.

G 2.42 Komplexität der NDS

Die Netware Verzeichnisdienste NDS (Netware Directory Services) ermöglichen das Einrichten einer gemeinsamen, dezentralen Verzeichnisdatenbank aller logischen und physischen Ressourcen in einem Netz. Jede Netzressource wird durch einen eindeutigen Eintrag in dieser Datenbank repräsentiert, wobei es keine Rolle spielt, wo sich die Ressourcen tatsächlich befinden. Der Zugang zum Netz bzw. der Zugriff auf eine Netzressource erfolgt dabei, anders als bei Novell Netware 3.x, nicht über einen bestimmten Netware 4.x Server, sondern über den Verzeichnisdienst des Novell Netzes (siehe M 2.151 *Entwurf eines NDS-Konzeptes*).

Die NDS ist die zentrale Komponente der Ressourcenverwaltung von Novell Netware 4.x und die Anforderungen an deren korrekte Funktionsweise sind entsprechend hoch. Aufgrund der komplexen Administrationsmöglichkeiten kann es zum Verlust der Verfügbarkeit, Vertraulichkeit sowie Integrität und dabei beispielsweise zu folgenden konkreten Gefährdungen kommen:

- Der Zugang eines Benutzers zum Netz erfolgt über die Authentisierung gegenüber der NDS. Diese Anmeldung findet am nächstgelegenen Netware 4-Server statt, der die Master-Partition des Verzeichnisbaums oder eine Kopie davon gespeichert hat. Existieren zu wenige Kopien im Netz, müssen sich alle Benutzer an den gleichen Servern beglaubigen. Jeder Anmeldevorgang bedeutet zusätzliche Serverbelastung und zusätzliche Netzlast. Dies kann zu längeren Wartezeiten bei der Anmeldung führen sowie die Verfügbarkeit beeinträchtigen.

  Werden keine Kopien der Master-Partition auf weiteren Netware 4-Servern angelegt, ist eine Anmeldung am Netz bei einem Fehler in der NDS-Datenbank nicht mehr möglich.

- Werden beim Entwurf des Verzeichnisbaumes zu viele Organisationen und Unterorganisationen ineinander verschachtelt, erhöht sich der Administrationsaufwand erheblich. Außerdem wird dann das Auffinden von Netzressourcen für die Administratoren und die Benutzer unübersichtlich.

- Wenn in einem WAN-Verbund nicht an jedem Standort eine Reproduktion der zugehörigen Partitions des Standortes gespeichert wird, ist eine Anmeldung am Netz bei einem Ausfall des WANs für die betroffenen Standorte nicht mehr möglich.

- Werden zuviele Reproduktionen einer Partition in einem WAN-Verbund eingerichtet, entsteht sehr hoher Netzverkehr im WAN, da bei jeder Anmeldung das Anmeldedatum des Benutzers in allen Reproduktionen geändert werden muss.

- In den verschiedenen Versionen und Patchleveln von Novell Netware Version 4 kann auch das Modul *DS.NLM* verschiedene Versionen aufweisen. Diese Information wird jedoch von den Netware 4-Servern genutzt, um Änderungswünsche an der NDS-Datenbank zu filtern. Dies kann u. U. dazu führen, dass sich die Netware 4-Server untereinander nicht über die Änderungen an der NDS informieren können, so dass es dort zu Inkonsistenzen kommt.

G 2.43 Migration von Novell Netware 3.x nach Novell Netware Version 4

Sind in einem Netz sowohl Netware 3.x als auch Netware 4.x Server vorhanden, so können prinzipiell zwei Szenarien unterschieden werden:

- die Netware 3.x Server wurden migriert und damit in die NDS integriert
- Netware 3.x und Netware 4.x Server arbeiten im Parallelbetrieb

In diesem Zusammenhang sind die folgenden konkreten Gefährdungen zu beachten:

- Bei einer Migration eines Netware 3.x Servers wird ein Großteil seiner NLMs ersetzt, so dass er vom Netware-Administrator über einen Netware 4.x Server kontrolliert werden kann. Ein solcher migrierter Netware 3.x Server kann ohne aufwendige Maßnahmen nicht mehr von seinem zuständigen Netware 4.x Server getrennt werden, um wieder als eigenständiger Netware 3.x Server im Netz fungieren zu können.
- Wird nach der Migration eines Netware 3.x Servers keine Bindery Emulation auf dem Netware 4.x Server aktiviert, können sich Benutzer mit der alten Client-Software nicht mehr am Netware 4 Netz anmelden.
- Werden die Netware 3.x Server getrennt als eigenständiges Netz betrieben, entsteht ein sehr hoher administrativer Aufwand, da dann die Benutzer weiterhin an allen Netware 3.x Servern einzeln und zusätzlich in der NDS verwaltet werden müssen.

G 2.44 Inkompatible aktive und passive Netzkomponenten

Durch inkompatible aktive Netzkomponenten können Probleme verursacht werden, die im Umfeld nicht oder noch nicht vollständig standardisierter Kommunikationsverfahren auftreten, wie z. B. ATM oder Tag-Switching. Um das betreffende Kommunikationsverfahren nutzen zu können, sind die Hersteller aufgrund der fehlenden oder nur teilweise vorhandenen Standards gezwungen, proprietäre Implementierungen einzusetzen.

Inkompatibilitätsprobleme dieser Art können entstehen, wenn bestehende Netze um aktive Netzkomponenten anderer Hersteller ergänzt werden oder wenn Netze mit Netzkomponenten unterschiedlicher Hersteller aufgebaut werden.

Werden aktive Netzkomponenten mit unterschiedlichen Implementierungen des gleichen Kommunikationsverfahrens gemeinsam in einem Netz betrieben, kann es zu einem Verlust der Verfügbarkeit des gesamten Netzes, von einzelnen Teilbereichen oder bestimmter Dienste kommen. Zwei Fälle können je nach Art der Inkompatibilität unterschieden werden:

- Durch nicht interoperable Implementierungen eines Kommunikationsverfahrens kann über die zugehörigen Komponenten hinweg keine Kommunikation erfolgen.

  Beispiel: ATM-Komponenten können unterschiedliche Signalisierungsprotokolle verwenden, z. B. gemäß UNI (User Network Interface) Version 3.0 und UNI Version 3.1, die nicht interoperabel zueinander sind.

- Auch auf aktiven Netzkomponenten, die prinzipiell interoperabel sind, können spezifische Dienste unterschiedlich implementiert sein. Dies hat zur Folge, dass die betreffenden Dienste nicht oder nicht netzweit zur Verfügung stehen, obwohl eine Kommunikation über diese Komponenten hinweg möglich ist.

  Beispiel: Es existieren proprietäre Implementierungen redundanter LAN Emulation Server für ATM-Netze. Besteht ein ATM-Netz z. B. aus zwei ATM-Switches, von denen ein Switch über eine solche proprietäre Implementierung verfügt und der andere nicht, kann zwar eine Kommunikation via LANE (LAN Emulation) erfolgen, der proprietär implementierte Dienst jedoch nicht genutzt werden.

Aber auch die Kombination von inkompatiblen passiven Netzkomponenten kann die Verfügbarkeit eines Netzes gefährden. So existieren für Twisted-Pair-Kabel Ausführungen in 100 und 150 Ohm, die nicht ohne einen entsprechenden Umsetzer zusammen verwendet werden dürfen. Eine ungeeignete Kombination von aktiven und passiven Netzkomponenten kann die Verfügbarkeit ebenfalls beeinträchtigen, wenn beispielsweise ein Netzzugangsprotokoll auf einem nicht hierfür definierten Medium betrieben wird. Beispielsweise lässt sich ATM nicht über ein 50 Ohm Koaxialkabel betreiben.

G 2.45 Konzeptionelle Schwächen des Netzes

Die Planung des Auf- und Ausbaus eines Netzes ist ein kritischer Erfolgsfaktor für den Netzbetrieb. Insbesondere bei den immer kürzer werdenden Innovationszyklen in der IT können sich Netze, die auf Grund ihrer Konzeption nicht neuen Erfordernissen angepasst werden können, schnell zu einem Engpass entwickeln:

- Abhängig von einer Anforderungsermittlung von Netzteilnehmern (z. B. Arbeitsgruppen) an die Vertraulichkeit der Daten und die Integrität des Netzes muss das Netz entsprechend konzipiert worden sein. Ansonsten können vertrauliche Daten einer Arbeitsgruppe von anderen, hierzu unbefugten Netzteilnehmern mitgelesen werden. Unter diesem Aspekt kann die Vertraulichkeit auch durch den Umzug von Arbeitsgruppenteilnehmern oder der ganzen Arbeitsgruppe verloren gehen, wenn es nicht möglich ist, im Netz neue vertrauliche Bereiche einzurichten bzw. zu ändern. Diese Gefährdung betrifft analog die Integrität des Netzes bzw. die Integrität von Netzsegmenten.

  Beispiel: Für eine Arbeitsgruppe mit besonderen Anforderungen an Vertraulichkeit und Integrität ihrer Daten wurde ein eigenes Teilnetz eingerichtet, welches durch einen Router abgetrennt ist. Dieses Segment ist durch die Kabelführung auf ein Gebäude beschränkt. Nach einem Umzug mehrerer Mitglieder dieser Arbeitsgruppe in andere Gebäude müssen diese über das normale Produktivnetz miteinander kommunizieren. Die Vertraulichkeit und auch die Integrität der Daten kann nicht mehr gewährleistet werden.

- Werden neue Anwendungen mit einem höheren als zum Planungszeitpunkt berücksichtigten Bandbreitenbedarf auf dem Netz betrieben, kann dies schnell zu einem Verlust der Verfügbarkeit des gesamten Netzes führen, wenn die Netzinfrastruktur in Folge konzeptioneller Schwächen nicht mehr ausreichend skaliert werden kann (Verlust der Verfügbarkeit durch Überlastung). Abhängig von der gewählten Segmentierung des Netzes kann der Verlust der Verfügbarkeit auch nur einzelne Segment des Netzes betreffen.

  Beispiel: In den heute noch häufig vorzufindenden, bedarfsorientiert gewachsenen Netzen, sind aus historischen Gründen vielfach Backbone-Segmente mit niedriger maximaler Bandbreite, wie z. B. Token-Ring- oder Ethernet-Segmente, vorhanden. Durch diese Beschränkung der Geschwindigkeit im Backbone-Bereich ist bei hoher zusätzlicher Last die Verfügbarkeit des gesamten Netzes betroffen.

- Netze, die ausschließlich zum Anschluss proprietärer Systeme geeignet sind, können ebenfalls einen Verlust der Verfügbarkeit bedingen, wenn hierfür ungeeignete Systeme an das Netz angeschaltet werden (Verlust der Verfügbarkeit durch nicht interoperable Netzkomponenten).

  Beispiel: Nicht systemneutrale Netze sind vorrangig im Großrechnerumfeld zur Vernetzung der Großrechner mit den zugehörigen Terminals anzutreffen. Häufig sind dies Netze, die für den Terminal- oder

Druckerbetrieb installiert wurden und nicht für den Betrieb von anderen Architekturen (z. B. Ethernet) geeignet sind. Dies betrifft sowohl die eingesetzte Verkabelung als auch die aktiven Netzkomponenten. Wird es dennoch versucht, wird das proprietäre Netz im allgemeinen nicht mehr verfügbar sein. Eine Möglichkeit zur Integration zweier Architekturen kann u. U. die Kopplung über ein Gateway darstellen.

- Beim Einsatz von aktiven Netzkomponenten, die nicht für den Einsatz bestimmter Protokolle vorgesehen sind, können ggf. zusätzlich erforderliche Dienste oder Protokolle nicht verwendet werden.

  Beispiel: In einem Netz, welches ausschließlich mit aktiven Netzkomponenten aufgebaut ist, die nur IP-Routing oder IP-Switching unterstützen, kann kein Novell Netware-Netzbetriebssystem auf der Basis von SPX/IPX betrieben werden.

- Beim Einsatz von passiven Netzkomponenten, die eine Einschränkung der auf ihnen zu betreibenden Netzzugangsprotokollen mit sich bringen, kann das Netz in Zukunft u. U. nicht mehr skaliert werden.

  Beispiel: In einem Netz, welches ausschließlich mit 50 Ohm Koaxialkabel aufgebaut ist, kann kein ATM benutzt werden. An Netzen, die mit 150 Ohm Twisted-Pair-Kabeln aufgebaut sind, können keine 100 Ohm Ethernet-Komponenten betrieben werden. Die Folge der o. a., zum Teil historisch bedingten konzeptionellen Schwächen, sind kostenintensive Veränderungen der Netzinfrastruktur.

Netze können zwar anwendungs-, system- und dienstneutral ausgeführt sein, aber durch eine sehr heterogene Komponentenlandschaft einen Betreuungsaufwand erfordern, der durch das Betriebspersonal nicht mehr geleistet werden kann. Dies kann zu einem Verlust der Verfügbarkeit des Netzes führen, wenn Störungen oder Ausfälle passiver oder aktiver Netzkomponenten aufgrund mangelnder personeller Ressourcen nicht mehr schnell genug beseitigt werden können.

G 2.46 Überschreiten der zulässigen Kabel- bzw. Buslänge oder der Ringgröße

Je nach Kabeltyp, Topologie und Übertragungsverfahren sehen die betreffenden Standards maximale Kabel- bzw. Buslängen sowie maximale Ringgrößen vor, um die Funktionsfähigkeit des Netzes im Sinne dieses Standards zu garantieren. Überhöhte Kabellängen wie auch überhöhte Bus- oder Ringlängen verlängern die Signallaufzeiten über das für das betreffende Übertragungsverfahren vorgesehene Maß hinaus, so dass die Verfügbarkeit des jeweiligen Netzsegments oder die Kommunikationsbandbreite herabgesetzt wird.

Die auftretenden Phänomene sind vom Zugriffsverfahren abhängig:

- Bei Netzsegmenten, auf denen das Zugriffsverfahren CSMA/CD (Carrier Sense Multiple Access/Collision Detection) verwendet wird, greifen alle Endgeräte gleichberechtigt zu, obwohl das Medium jeweils nur exklusiv durch ein Endgerät genutzt werden kann. Hierzu prüft jedes Endgerät zunächst, ob das Medium für die Benutzung zur Verfügung steht (Carrier Sense). Ist dies der Fall, beginnt das betreffende Endgerät mit der Übertragung. Geschieht dies durch mehrere Endgeräte gleichzeitig (Multiple Access), kommt es zu einer Kollision, die von den sendenden Endgeräten erkannt wird (Collision Detection) und zu einer erneuten Prüfung des Mediums mit anschließender Wiederholung der Übertragung führt.

  Wird die maximal definierte Signallaufzeit auf dem Medium überschritten, können Kollisionen ggf. im vorgesehenen Zeitintervall (Collision Detection) nicht erkannt werden. Dies bedeutet, dass ein Endgerät bereits begonnen hat, Daten zu übertragen, während ein anderes Endgerät das Übertragungsmedium noch als frei betrachtet. In diesem Fall kommt es zu so genannten späten Kollisionen, die das betreffende Datenpaket unbrauchbar machen und in Abhängigkeit der Länge des Datenpakets das Medium über Gebühr blockieren. Die nutzbare Übertragungsbandbreite auf dem Medium kann dadurch stark eingeschränkt werden. Einen Verlust von Informationen tritt in der Regel, trotz des Verlustes von einzelnen Datenpaketen, durch die Sicherung des Netzzugangsprotokolls nicht auf. Beispielsweise verwenden Ethernet oder Fast Ethernet das CSMA/CD Übertragungsverfahren.

- Übertragungsverfahren, die auf dem Token-Passing-Verfahren basieren, verwenden ein spezielles Datenpaket (das so genannte Token), um festzulegen, welches Endgerät das Medium belegen darf. Erhält ein Endgerät das Token, belegt es das Medium und gibt das Token in Abhängigkeit des implementierten Token-Passing-Verfahrens an das nächste Endgerät weiter. Hiermit ist gewährleistet, dass das Medium immer nur durch ein einziges Endgerät belegt wird.

  Wesentlich für Netzsegmente, auf denen ein Token-Passing-Verfahren betrieben wird, ist eine synchrone Datenübertragung mit konstanter Bitrate. Ist das Medium belegt, werden die betreffenden Zeitintervalle für die unterschiedlichen Bits für die Übertragung der Datenpakete genutzt, ist das Medium frei, werden die Zeitintervalle für die Weitergabe des Tokens

genutzt. Bei einer Überschreitung der maximal vorgesehenen Signallaufzeit kann die für das betreffende Übertragungsverfahren vorgesehene konstante Bitrate nicht mehr eingehalten werden, so dass die Kommunikation zum Erliegen kommt. Beispielsweise basieren Token Ring oder FDDI auf dem Token-Passing-Verfahren.

Neben einer Verlängerung der Signallaufzeit erhöhen längere Kabel die Dämpfung. Bei Überschreitung der Kabellängen im Hinblick auf den betreffenden Standard kann die Dämpfung des Kabels so groß werden, dass die verschiedenen Signalpegel nicht mehr wie im Standard festgelegt voneinander unterschieden werden können. Die Kommunikation über die betreffenden Adern oder Glasfasern kann in diesem Fall nicht über die gesamte Länge sichergestellt werden.

G 2.47 Ungesicherter Akten- und Datenträgertransport

Werden Dokumente, Datenträger oder Akten zwischen der Institution und anderen Stellen, zum Beispiel dem häuslichen Arbeitsplatz, transportiert, besteht die Gefahr, dass sie

- auf dem Transportweg verloren gehen,
- auf dem Transportweg entwendet werden,
- auf dem Transportweg gelesen oder manipuliert werden und
- an einen falschen Empfänger übergeben werden.

Insbesondere wenn es sich um Unikate handelt, können Zerstörung, Vertraulichkeitsverlust oder Manipulation größere Schäden verursachen.

G 2.48 Ungeeignete Entsorgung der Datenträger und Dokumente

Wenn Datenträger oder Dokumente nicht geeignet entsorgt werden, können hieraus unter Umständen Informationen extrahiert werden, die Dritten nicht in die Hände fallen sollten.

Beispiele:

- Angreifer müssen nicht immer komplizierte technische Attacken austüfteln, um über Schwachstellen in IT-Systemen an Informationen zu gelangen. Viel einfacher und erfolgreicher kann die Informationsgewinnung aus der Mülltonne (Dumpster Diving) sein. Büromüll ist im Allgemeinen nicht einmal sehr schmutzig und kann sehr viele interessante und weiterverwertbare Sachen enthalten, wie beispielsweise Disketten, CD-ROMs, interne Telefonbücher oder auch die aktuellen Erfolgsbilanzen.
- CD-ROMs können zur Wiederverwertung an vielen Stellen abgegeben werden. Leider wird hierbei häufig nicht bedacht, dass auch CD-ROMs mit "alten" Datensicherungen oder anderen Dateien für Externe noch interessante Informationen enthalten können. Auch das Zerkratzen der Oberfläche hilft hier nicht, um Interessierte an der Auswertung von Informationen erfolgreich zu hindern.

Auch alte oder defekte IT-Systeme enthalten häufig eine Vielzahl von spannenden Informationen. So hat eine Test-Kaufreihe einer Computer-Zeitschrift ergeben, dass auf 90 % der gebraucht gekauften Festplatten noch die vollständigen Informationen der vorherigen Besitzer enthalten waren.

Beispiele:

- Zwei Wissenschaftler vom Massachusetts Institute of Technology haben untersucht, wie viele sensitive Daten über den Handel mit gebrauchten Computern und Computerkomponenten in die falschen Hände gelangen. Das erschreckende Ergebnis war auch hier, dass nur 10 % der IT-Komponenten so gesäubert worden war, dass keine Daten rekonstruiert werden konnten. Die übrigen Platten enthielten unter anderem Pornographie, Liebesbriefe, Kreditkartennummern oder Patientendaten. Der "Hauptgewinn" war eine Festplatte, die zuvor offensichtlich in einem Geldautomaten eingebaut war, und auf der neben Kontonummern und Kontoständen auch ein Teil der verwendeten Software zu finden war.
- Der Käufer eines ausgemusterten Behördencomputers wandte sich an Datenschutzbeauftragte und Presse, nachdem er darauf die nur scheinbar gelöschten Daten eines Nachlassgerichtes rekonstruieren konnte.

Sind für Telearbeiter am häuslichen Arbeitsplatz keine geeigneten Möglichkeiten vorhanden, um Datenträger und Dokumente geeignet zu entsorgen, wandern diese erfahrungsgemäß meist in den Hausmüll. Auch dort, wo unterwegs gearbeitet wird, besteht die bedauerliche Neigung, Entwürfe und anderes "Unnützes" direkt in die nächsten Papierkörbe zu geben oder einfach liegen zu lassen, sei es im Hotel oder in der Bahn.

Beispiel:

- So wurden bereits aus Patientenakten von den Nachbarskindern Papierflugzeuge gebastelt. Diese waren von einem Telearbeiter als Altpapier zur Entsorgung vor die Haustür gestellt worden. Da die brisanten Papierflugzeuge anschließend überall in der Nachbarschaft zu finden waren, war dies bald als Nachricht über den schlechten Datenschutz einer Klinik in der Lokalpresse zu lesen.

G 2.49 Fehlende oder unzureichende Schulung der Telearbeiter

Telearbeiter sind am häuslichen Arbeitsplatz weitestgehend auf sich allein gestellt. Das bedeutet, dass sie sich besser mit der eingesetzten IT auskennen müssen als ihre Kollegen in der Institution, die meist kurzfristig auf IT-Systemspezialisten vor Ort zurückgreifen können. Ist der Telearbeiter nicht ausreichend im Umgang mit der IT geschult, kann dies bei Problemen zu erhöhten Ausfallzeiten führen, da ggf. ein IT-Betreuer aus der Institution zum häuslichen Arbeitsplatz des Telearbeiters fahren muss, um dort die Probleme zu beseitigen.

Beispiel:

Der Telearbeiter sollte in der Lage sein, selbstständig Sicherungskopien seiner Daten herzustellen. Wird dem Telearbeiter ein zusätzliches Speichermedium (z. B. Bandlaufwerk) zur Verfügung gestellt, so muss er in den Gebrauch eines solchen eingewiesen werden.

G 2.50 Verzögerungen durch temporär eingeschränkte Erreichbarkeit der Telearbeiter

Üblicherweise hat ein Telearbeiter keine festen Arbeitszeiten am häuslichen Arbeitsplatz. Lediglich feste Zeiten der Erreichbarkeit werden vereinbart. Bei alternierender Telearbeit sind seine Arbeitszeiten zwischen häuslichem Arbeitsplatz und dem innerbetrieblichen Arbeitsplatz verteilt. Ergibt sich kurzfristig das Problem, dass Informationen vom Telearbeiter eingeholt oder Informationen an den Telearbeiter übergeben werden müssen, kann es aufgrund der schwierigen Erreichbarkeit zu Verzögerungen kommen. Selbst eine Übermittlung der Informationen über E-Mail verkürzt nicht notwendigerweise die Reaktionszeit, da nicht sichergestellt werden kann, dass der Telearbeiter die E-Mail zeitnah liest.

G 2.51 Mangelhafte Einbindung des Telearbeiters in den Informationsfluss

Da Telearbeiter nicht täglich in der Institution sind, sondern überwiegend zu Hause arbeiten, haben sie weniger Gelegenheit, am direkten Informationsaustausch mit Vorgesetzten und Arbeitskollegen teilzuhaben. Es besteht die Gefahr, dass sie vom betrieblichen Geschehen abgeschnitten werden und sich dadurch auch die Identifizierung mit der Institution verringert.

Darüber hinaus ist nicht auszuschließen, dass durch einen mangelhaften Informationsfluss für IT-Sicherheit notwendige Informationen nicht ausreichend oder nicht rechtzeitig den Telearbeiter erreichen. Beispielsweise kann die kurzfristige Weitergabe von Computer-Viren-Meldungen erschwert sein.

G 2.52 Erhöhte Reaktionszeiten bei IT-Systemausfall

Findet beim Telearbeiter zu Hause ein IT-Systemausfall statt, den er nicht selbständig beheben kann oder darf, so muss entweder ein IT-Systemverantwortlicher zu ihm nach Hause kommen oder das IT-System muss zu seiner Institution gebracht werden, damit es dort repariert werden kann. Dies nimmt einige Zeit in Anspruch, so dass der Telearbeiter mit erhöhten Ausfallzeiten rechnen muss. Gleiche Probleme entstehen bei Wartungsarbeiten oder bei der Neuinstallation von Komponenten oder Software.

G 2.53 Unzureichende Vertretungsregelungen für Telearbeit

Die Aufgaben des Telearbeiters sind in der Regel so konzipiert, dass er weitestgehend selbständig arbeiten kann. Dies birgt die Gefahr in sich, dass es im Krankheitsfall schwierig ist, eine entsprechende Vertretung für den Telearbeiter bereitzustellen. Insbesondere kann es zu Problemen führen, die erforderlichen Unterlagen oder die Daten aus dem Telearbeitsrechner für den Vertreter bereitzustellen, wenn keine Zutrittsmöglichkeiten zum häuslichen Arbeitsplatz des Telearbeiters bestehen.

G 2.54 Vertraulichkeitsverlust durch Restinformationen

Bei elektronischer Datenübermittlung oder Datenträgerweitergabe passiert es immer wieder, dass dabei auch Informationen weitergegeben werden, die die Institution nicht verlassen sollten. Als mögliche Ursachen für die unbeabsichtigte Weitergabe von Informationen lassen sich folgende Beispiele anführen:

- Eine Datei enthält Textpassagen, die als "versteckt" oder "verborgen" formatiert sind. Solche Textpassagen können Bemerkungen enthalten, die nicht für den Empfänger bestimmt sind.
- Dateien, die mit Standardsoftware wie Textverarbeitungsprogrammen oder Tabellenkalkulationen erstellt worden sind, können Zusatzinformationen über Verzeichnisstrukturen, Versionsstände, Bearbeiter, Kommentare, Bearbeitungszeit, letztes Druckdatum, Dokumentnamen und -beschreibungen enthalten. Besonders hervorzuheben sind in diesem Zusammenhang Funktionen, die mehreren Bearbeitern das gemeinsame Bearbeiten eines Dokuments erlauben. Solche Funktionen löschen Textpassagen, die ein Bearbeiter löscht oder überschreibt, nicht wirklich aus dem Dokument, sondern markieren diese nur als gelöscht und erlauben es späteren Bearbeitern, Änderungen ganz oder teilweise rückgängig zu machen. Praktisch alle aktuellen Office-Suites (Microsoft Office, StarOffice, OpenOffice) bieten diese Möglichkeit. Werden die Daten solcher Änderungen nicht vor der Weitergabe entfernt, so erhält der Empfänger neben dem tatsächlichen Dokument unter Umständen eine große Menge weiterer Informationen.
- Praktisch alle aktuellen Office-Suites besitzen die Möglichkeit der Schnellspeicherung von erstellten Dokumenten. Dies führt dazu, dass nur die Änderungen an einem Dokument gespeichert werden. Dieser Vorgang nimmt vergleichsweise weniger Zeit in Anspruch als ein vollständiger Speichervorgang, bei dem die Office-Suite das vollständige überarbeitete Dokument speichert. Ein vollständiger Speichervorgang erfordert jedoch weniger Festplattenspeicher als eine Schnellspeicherung. Der entscheidende Nachteil ist jedoch, dass bei einer Schnellspeicherung die Datei unter Umständen Textfragmente enthalten kann, die der Verfasser nicht weitergeben möchte.
- Eine weitere Möglichkeit, wie Informationen weitergegeben werden können, die nicht für Externe bestimmt sind, stellen Funktionen dar, die es beispielsweise erlauben, in ein Textdokument oder eine Präsentation eine Tabelle aus einem Tabellenkalkulationsdokument so einzubetten, dass die Tabelle direkt im Textdokument bearbeitet werden kann. Wird ein solches Textdokument weitergegeben, so können unter Umständen sehr viel mehr Informationen aus dem Tabellenkalkulationsdokument übertragen werden, als im Textdokument sichtbar ist.
- Wird eine Datei auf eine Diskette kopiert, so wird der erforderliche physikalische Speicherbereich (Block) vollständig aufgefüllt. Benötigt das Original einen Block nicht vollständig, so wird dieser (nach dem End-Of-File Kennzeichen) mit beliebigen "Restinformationen" des IT-Systems aufgefüllt.

- Auf z/OS-Systemen werden gelöschte Member nicht sofort in der Bibliothek (*PDS - Partitioned Dataset*) überschrieben. Lediglich der Eintrag des Members im Verzeichnis (*Directory*) des *PDS* wird gelöscht. Erst wenn im *PDS* freier Speicherplatz benötigt wird, werden die Informationen des alten Members überschrieben. Noch nicht überschriebene Daten lassen sich mit Hilfsprogrammen auslesen. **z/OS-Systeme**
- Werden in z/OS-Systemen Dateien auf einer Festplatte gelöscht, so wird die Datei im *Volume Table of Content (VTOC)* als gelöscht gekennzeichnet, die Datei selbst auf der Festplatte jedoch nicht gelöscht. Die Datei wird erst überschrieben, wenn neue Daten auf der Festplatte gespeichert werden sollen und kein freier Platz verfügbar ist. Gelingt es, die Speicherstelle der Datei aus dem *VTOC* auszulesen, so ist es möglich, die Datei mit speziellen Programmen zu editieren und wieder herzustellen. Dies gilt ebenso für Bänder, die zwar als Leer-Bänder gekennzeichnet, aber noch nicht überschrieben sind.

Restinformationen auf Datenträgern

Bei den meisten Dateisystemen werden Dateien, die vom Benutzer über einen Löschbefehl gelöscht werden, nicht wirklich in dem Sinn gelöscht, dass die Information anschließend nicht mehr vorhanden ist. Normalerweise werden lediglich die Verweise auf die Datei aus den Verwaltungsinformationen des Dateisystems (etwa aus der Dateizuordnungstabelle (*File Allocation Table*) beim FAT-Dateisystem) gelöscht und die zu der Datei gehörenden Blöcke als "frei" markiert. Der tatsächliche Inhalt der Blöcke auf dem Datenträger bleibt jedoch erhalten und kann mit entsprechenden Werkzeugen rekonstruiert werden.

Wenn Datenträger an Dritte weitergegeben werden, beispielsweise

- wenn ein Rechner ausinventarisiert wurde und verkauft wird,
- wenn ein defektes Gerät zur Reparatur gegeben oder im Rahmen der Garantie ausgetauscht wird oder
- wenn ein Datenträger im Rahmen des Datenträgeraustauschs an einen Geschäftspartner weitergegeben wird

können auf diese Weise sensitive Informationen nach draußen gelangen.

Beispiele:

- Die Forscher Simson Garfinkel und Abhi Shelat vom MIT kauften zwischen 2000 und 2002 bei verschiedenen Händlern über das Online-Auktionshaus eBay eine größere Anzahl gebrauchter Festplatten und untersuchten diese auf enthaltene Restinformationen. Sie fanden eine erschreckende Menge an Daten, beispielsweise
  - interne Vermerke von Unternehmen, bei denen es um Personalsachen ging,
  - eine große Anzahl von Kreditkartennummern,
  - medizinische Informationen,
  - E-Mails.

und vieles mehr. Ihre Ergebnisse veröffentlichten sie in einem Journal der IEEE.

- Ein Benutzer entdeckte durch Benutzung eines anderen Editors per Zufall, dass die kurz vor der Versendung stehende Datei diverse URLs enthielt, inklusive Benutzername und Passwort für einen WWW-Server. Mit URL (Uniform Resource Locator) wird die Adresse eines WWW-Dokuments bezeichnet. Der Zugriff auf die WWW-Seite kann passwortgeschützt sein.
- Eine Behörde hatte mit dem Programm Microsoft Powerpoint erstellte Präsentationen in Dateiform an Externe weitergegeben. Später stellte sich heraus, dass neben den Präsentationen auch Informationen über die Rechnerumgebung des Benutzers mitgeliefert worden waren, wie etwa darüber, welche Newsgruppen ein Benutzer abonniert hat und welche News er schon gelesen hat. Die Powerpoint-Datei enthielt u. a. folgende Einträge:

  de.alt.drogen! s21718 0

  de.alt.dummschwatz! s125 0
- Zwei Verkäufer konkurrierender Firmen tauschten ihre Präsentationen aus, die sie bei einer Veranstaltung gehalten hatten. Eines der Powerpoint-Dokumente enthielt eine kleine Tabelle mit Endkunden-Preisen für die Produkte der einen Firma. Beim Öffnen der Präsentation entdeckte der Empfänger, dass diese kleine Tabelle Teil eines sehr umfangreichen Tabellenkalkulationsdokuments war, das in die Präsentation eingebettet worden war, und das die gesamte Preiskalkulation des Konkurrenzunternehmens enthielt.

G 2.55 Ungeordnete E-Mail-Nutzung

Bei ungeordneter Nutzung von E-Mails besteht die Gefahr, dass sensitive Daten Unbefugten zur Kenntnis gelangen oder das gewünschte Ziel nicht rechtzeitig erreichen.

Beispiele:

- Eine fehlerhafte Adressierung kann dazu führen, dass die E-Mail an einen unautorisierten Empfänger übersandt wird.

  Werden Verteilerlisten nicht gepflegt, können E-Mails Empfängern zugestellt werden, die von der Versendung hätten ausgeschlossen sein müssen.

- Eine falsche Versandmethode kann zu Übertragungs- oder Empfangsproblemen führen. Wenn beispielsweise die Datei nicht mit *uuencode* in eine 7-Bit ASCII-Darstellung umgewandelt wurde, kann sie nach dem Empfang fehlerhaft konvertiert und damit nicht lesbar sein. Wenn die Datenmenge zu groß ist, kann eines der an der Übertragung beteiligten IT-Systeme die Weitergabe verweigern.
- Fehlende oder mangelhafte organisatorische Regelungen beim Empfänger können zur Folge haben, dass eine empfangene E-Mail erst verspätet bearbeitet wird.
- Fehlende oder mangelhafte organisatorische Regelungen beim Absender können zur Folge haben, dass ein terminlich zugesichertes Absenden der Daten nicht eingehalten werden kann.

G 2.56 Mangelhafte Beschreibung von Dateien

Werden beim elektronischen Dateiaustausch die übertragenen Dateien nicht gut genug beschrieben, so ist für den Empfänger oft nicht nachvollziehbar, wer diese übersandt hat, welche Informationen sie enthalten oder welchem Zweck sie dienen.

Wenn mehrere E-Mails ein- und desselben Absenders eingehen, kann bei fehlender oder schlechter Kennzeichnung die Reihenfolge verwechselt werden.

Beispiel:

Absender A verschickt an die Empfängerin E eine E-Mail mit mehreren Dateien. Am nächsten Tag stellt A fest, dass eine Datei noch Fehler enthielt und verschickt eine korrigierte Version mit der Bitte, die vorhergehende E-Mail zu löschen. Nachdem E die alte E-Mail gelöscht hat, stellt sie fest, dass die aktuelle E-Mail nur die korrigierte Datei enthält.

G 2.57 Nicht ausreichende Speichermedien für den Notfall

Wenn Daten nach ihrer Zerstörung wiederhergestellt werden müssen, ist es vielen Fällen notwendig, die gesicherten Daten zunächst auf getrennten Speichermedien wiedereinzuspielen. Dies ist insbesondere bei komplexeren Datenstrukturen wie z. B. bei Datenbanken notwendig, da die Wiederherstellung nicht immer reibungslos und fehlerfrei funktioniert. Wird die hierfür benötigte Speicherkapazität nicht für den Notfall vorgehalten, kann es durch übereiltes Handeln während des Notfalls zu weiteren Datenverlusten kommen.

Beispiel:

In einem Unternehmen mit einer großer Datenbank-Applikation wurde die Datenbank als inkonsistent vom Datenbankmanagementsystem (DBMS) gemeldet. Daraufhin nahm das Systemmanagement die Datenbank außer Betrieb und restaurierte den letzten gesicherten Datenbestand im Produktionssystem. Von der scheinbar korrupten Datenbank wurden nur Log- und Konfigurationsdateien vorher gesichert. Durch diese Aktion gingen alle Datenänderungen seit der letzten Sicherung verloren, da aufgrund eines bis dahin unbekannten Fehlers im DBMS das Nachfahren der Änderungen nicht möglich war. Die Analyse der Log- und Konfigurationsdateien ergab dann, dass die Datenbank in Wirklichkeit gar nicht inkonsistent gewesen war. Hätte ausreichend Plattenplatz zur Verfügung gestanden, um die Rekonstruktion parallel durchzuführen, wäre das alte produktive System ohne Datenverlust nach Erkennung und Behebung der nur scheinbaren Inkonsistenz wieder einsatzbereit gewesen.

G 2.58 Novell Netware und die Datumsumstellung im Jahr 2000

Diese Gefährdung ist mit der Version November 2004 entfallen.

G 2.59 Betreiben von nicht angemeldeten Komponenten

In der Regel sollten alle Komponenten eines Netzes der Systemadministration bekannt sein. Es muss auf organisatorischer Ebene gewährleistet sein, dass neue Komponenten bei der Systemadministration angemeldet und freigegebenen werden, z. B. durch eine automatische Meldung der Beschaffungsstelle oder einen entsprechenden Antrag der die Komponenten betreibenden Organisationseinheit.

Nicht angemeldete Komponenten stellen ein Sicherheitsrisiko dar, da sie nicht in organisatorische innerbetriebliche Abläufe und Kontrollen eingebunden sind. Dies kann einerseits zu Gefahren für die Benutzer der nicht angemeldeten Komponenten führen (z. B. Datenverlust, da das System nicht in die Datensicherung eingebunden ist), aber auch zur Gefährdung anderer Netzkomponenten, z. B. können durch nicht erfasste Zugangspunkte zum Netz Schwachstellen entstehen, wenn diese schlecht oder gar nicht gegen unbefugten Zugriff abgesichert sind. Da eine solche Komponente nicht der Kontrolle des Netzmanagements und/oder des Systemmanagements unterliegt, können insbesondere Fehlkonfigurationen des lokalen Systems zu einem Sicherheitsloch führen.

Beispiel:

Der Administrator wartet über das Systemmanagementsystem die Passwörter (Community Names) für das verwendete Netzmanagementsystem, welches auf SNMP basiert. Eine Arbeitsgruppe beschließt den Kauf eines neuen Netz-PCs, vergisst diesen jedoch der zentralen Administration zu melden. Die Installationseinstellung für das Passwort (Community Name) des lokalen SNMP-Dämons lautet "public". Dieses Passwort ist wohl bekannt. Angreifer können nun einen SNMP-basierten Angriff starten, da sie vollen Zugriff auf die SNMP-Daten besitzen. Der so kompromittierte PC kann als Ausgangspunkt für weitere Angriffe auf das interne Netz dienen. So könnten dort z. B. Passwort-Sniffer installiert werden.

G 2.60 Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement

Werden für die Bereiche Netzmanagement und/oder Systemmanagement keine organisationsübergreifenden Managementstrategien festgelegt, kann es insbesondere in mittleren und großen Netzen mit mehreren Managementdomänen durch Fehlkoordination der einzelnen Subdomänen zu schwerwiegenden Problemen durch Fehlkonfiguration kommen, die bis hin zu völligem Systemzusammenbruch auf Netzebene führen können.

Aus diesem Grund ist die Festlegung und Durchsetzung einer Managementstrategie zwingend erforderlich. Im folgenden werden einige Beispiele für Probleme durch eine fehlende oder unzureichende Strategie für das Netz- und Systemmanagement gegeben.

Fehlende Bedarfsanalyse vor Festlegung der Managementstrategie

Um eine Netz- und/oder Systemmanagementstrategie festlegen zu können, ist eine vorangehende Bedarfsanalyse durchzuführen. Ohne die Feststellung des Managementbedarfs (etwa: Welche verwaltbaren Netzkoppelelemente existieren? Wie dynamisch ist der zu verwaltende Softwarebestand?) können Anforderungen an die Managementstrategie nicht formuliert werden. Da die Managementstrategie zudem Einfluss auf das zu beschaffende Softwareprodukt hat, kann dies zu Fehlentscheidungen führen.

Wird dann z. B. ein Managementprodukt eingeführt, das einen zu geringen Funktionsumfang besitzt, so kann diese Funktionslücke zusätzlich zu einem Sicherheitsproblem werden, da die nötige Funktion "von Hand" bereitgestellt werden muss. In größeren Systemen kann dies dann leicht zu Fehlkonfigurationen führen.

Beschaffung von nicht managebaren Komponenten

Wird ein Rechnerverbund mit Hilfe eines Netz- und/oder eines Systemmanagementsystems verwaltet, so ist bei der Beschaffung neuer Komponenten darauf zu achten, dass sie in das jeweilige Managementsystem integrierbar sind, damit sie in das Management einbezogen werden können. Ist dies nicht der Fall, so fällt mindestens zusätzlicher Verwaltungsaufwand an, da auch auf den nicht mit dem Managementsystem verwalteten Komponenten die festgelegte Managementstrategie durchgesetzt werden muss. Da jedoch diese Komponenten insbesondere nicht in die automatisierten Verwaltungsabläufe des Managementsystems integriert sind, kann es hier zu Fehlkonfigurationen kommen. Dies birgt durch nicht abgestimmte Konfigurationen ein Sicherheitsrisiko.

Nicht koordiniertes Managen von benachbarten Bereichen (Communities, Domänen)

Existieren in einem durch ein Managementsystem verwalteten Rechnernetz mehrere Verwaltungsbereiche, die jeweils von einem eigenen Systemmanager betreut werden, so sind deren Kompetenzen durch die Managementstrategie eindeutig festzulegen. Ist dies nicht der Fall, kann es durch unkoordiniertes Management einzelner Komponenten zu Sicherheitsproblemen kommen.

Werden z. B. einerseits einzelne Komponenten wie Netzkoppelelemente fälschlicherweise von zwei Verwaltungsbereichen verwaltet (dies kann etwa geschehen, wenn keine unterschiedlichen SNMP-"Passwörter" (Community Strings) verwendet werden), so führt das unkoordinierte Einstellen von Konfigurationsparametern unter Umständen zu Sicherheitslücken.

Werden andererseits Komponenten (etwa Drucker) gemeinsam von zwei Verwaltungsbereichen genutzt und wurde z. B. die Vertrauensstellung des jeweils anderen Verwaltungsbereiches (z. B. Windows NT Netzwerkfreigaben) nicht korrekt eingerichtet, so kann dies unbeabsichtigt zu Sicherheitsproblemen führen, wenn nun auch unberechtigten Dritten der Zugriff gestattet wird.

Nicht integrierte Verwaltungssoftware

Beim Verwalten von mittleren und großen Systemen kann es vorkommen, dass nach Einführung des Managementsystems neue Komponenten in das System integriert werden sollen, deren Verwaltung Funktionen erfordern, die das eingesetzte Managementsystem nicht unterstützt. Dies gilt insbesondere für den Bereich Applikationsmanagement. Wird zur Verwaltung der neuen Komponente nun eine Verwaltungssoftware eingesetzt, die nicht in das eingesetzte Managementsystem integriert werden kann (z. B. über eine Programmierschnittstelle, oder durch den Einsatz von so genannten Gateways), so ist ein koordiniertes Einbinden in das Managementsystem nicht möglich. Dadurch unterliegt die neue Komponente jedoch nicht dem "automatisierten" Management, was ein Verwalten "von Hand" nötig macht. Die festgelegte Managementstrategie muss nun für zwei Systeme umgesetzt werden, dies kann jedoch zu Fehlkonfigurationen führen, die Sicherheitslücken bedingen können.

G 2.61 Unberechtigte Sammlung personenbezogener Daten

Beim Einsatz von Managementsystemen fallen im Rahmen des normalen Ablaufes auch viele Protokolldaten an, die in der Regel automatisch erzeugt und ausgewertet werden. Dies trifft im besonderen Maße auf die Bereiche der Netz- und Systemüberwachung zu. Ohne ausführliche Protokollierung der Systemaktivitäten ist es z. B. auch nicht möglich, Sicherheitsverletzungen aufzudecken. Eine Anforderung im Rahmen der Überwachung ist jedoch auch die eindeutige Zuordnung bestimmter Zugriffe zu Benutzern. Damit müssen die überwachten Benutzeraktivitäten aber personenbezogen protokolliert werden. In der Regel wird durch die Managementstrategie organisationsübergreifend und im Einvernehmen mit dem Datenschutzbeauftragten festgelegt, welche Benutzeraktivitäten aus Sicherheitsgründen überwacht werden sollen. Hierüber sind die betroffenen Benutzer entsprechend zu informieren. Die Einhaltung der durch die Managementstrategie festgelegten Vorgaben ist jedoch im Rahmen der Systemrevision zu überprüfen. Es ist zudem möglich, dass das Managementsystem im Rahmen einer regulären Funktion temporäre Protokolldateien erstellt, die z. B. im wenig geschützten Bereich für temporäre Dateien abgelegt werden. Die Protokolldateien sind dann potentiell zumindest für die Zeit ihrer Existenz zugreifbar und können zudem Benutzerinformationen enthalten.

G 2.62 Ungeeigneter Umgang mit Sicherheitsvorfällen

Sicherheitsvorfälle mit dem Potential großer Schäden werden in der Praxis nie ausgeschlossen werden können. Die gilt auch dann, wenn eine Reihe von Sicherheitsmaßnahmen umgesetzt sind. Wird auf akute Sicherheitsvorfälle nicht angemessen reagiert, so können sich daraus unter Umständen große Schäden bis hin zu Katastrophen entwickeln.

Beispiele dafür sind:

Arbeitsausfälle

- Es treten zunächst sporadisch, dann massenhaft neue Computer-Viren mit Schadfunktionen auf. Erfolgt keine rechtzeitige Reaktion, können unter Umständen ganze Organisationseinheiten arbeitsunfähig werden. Konkret ist dies bei Auftreten des Computer-Virus "Melissa" beobachtet worden.

Imageverlust

- Auf einem Webserver finden sich unerklärlich veränderte Inhalte. Wird dies nicht als Hinweis auf mögliche Hacker-Attacken weiterverfolgt, können weitere Angriffe auf den Server u. U. auch zu großem Imageverlust führen.
- In der Protokollierung einer Firewall finden sich Ungereimtheiten. Wird dies nicht als Hacking-Versuch untersucht, können ggf. tatsächlich externe Angreifer die Firewall überwinden.
- Es werden Sicherheitslücken in den verwendeten IT-Systemen bekannt. Werden diese Informationen nicht rechtzeitig beschafft und notwendige Gegenmaßnahmen nicht zügig umgesetzt, so besteht die Gefahr, dass die Sicherheitslücken von Innen- oder Außentätern missbraucht werden.

Folgeschäden

- Es ergeben sich Hinweise auf manipulierte Unternehmensdaten. Wird dies nicht zum Anlass genommen, den Manipulationen nachzugehen, so können auch unerkannte Manipulationen schwere Folgeschäden nach sich ziehen, wie zum Beispiel fehlerhafte Lagerbestände, falsche Buchhaltung oder unkontrolliert abgeflossene Finanzmittel.
- Wird Hinweisen auf Kompromittierung von vertraulichen Unternehmensdaten nicht nachgegangen, können weitere vertrauliche Daten abfließen.

Diese Beispiele verdeutlichen, dass bei Sicherheitsvorfällen eine schnelle Benachrichtigung zuständiger Stellen, eine zügige Reaktion und eine Unterrichtung der potentiell Betroffenen zur Schadensminimierung oder -prävention notwendig ist.

Fehlentscheidungen

Wenn für die Behandlung von Sicherheitsvorfällen keine geeignete Vorgehensweise definiert ist, können außerdem falsche Entscheidungen getroffen werden, die z. B. dazu führen

- dass Pressevertreter falsche Auskünfte erhalten,
- dass die betroffenen Systeme bzw. Komponenten trotz schwerer Sicherheitslücken nicht abgeschaltet werden,
- dass Systeme bzw. einzelne Komponenten bei relativ unbedeutenden Sicherheitslücken völlig abgeschaltet werden,
- dass keinerlei Ausweichmaßnahmen vorgesehen sind, wie z. B. der Austausch kompromittierter Komponenten, kryptographischer Verfahren oder Schlüssel.

G 2.63 Ungeordnete Faxnutzung

Bei ungeordneter Nutzung von Faxgeräten oder Faxservern besteht die Gefahr, dass sensitive Daten Unbefugten zur Kenntnis gelangen oder das gewünschte Ziel nicht rechtzeitig erreichen.

Beispiele:

- Eine fehlerhafte Adressierung kann dazu führen, dass ein Fax an einen unautorisierten Empfänger übersandt wird. **falsche Adressierung**

  Werden Adressbücher und Verteillisten nicht gepflegt, können Faxe Empfängern zugestellt werden, die von der Versendung hätten ausgeschlossen sein müssen.

- Eine fehlerhafte Administration eines Faxservers kann dazu führen, dass eingehende Faxe an Mitarbeiter zugestellt werden, die von dem Inhalt keine Kenntnis erlangen sollen.

- Fehlende oder mangelhafte organisatorische Regelungen beim Empfänger können zur Folge haben, dass ein empfangenes Fax erst verspätet bearbeitet wird. **unzuverlässige Bearbeitung**

- Fehlende oder mangelhafte organisatorische Regelungen beim Absender können zur Folge haben, dass ein terminlich zugesichertes Absenden einer Nachricht per Fax nicht eingehalten werden kann.

- Fehlende Sensibilisierung der Benutzer bei der Verwendung von Faxservern kann dazu führen, dass versehentlich ein Entwurf versandt wird, der so die Organisation nicht verlassen sollte.

G 2.64 Fehlende Regelungen für das RAS-System

Fehlende Regelungen für das RAS-System stellen eine erhebliche Gefährdung des Gesamtsystems dar. Da sich ein RAS-System aus verschiedenen Komponenten zusammensetzt, ergeben sich zunächst die jeweiligen Gefährdungen aus dem Bereich "organisatorische Mängel" der Einzelkomponenten, wie sie den jeweiligen Bausteinbeschreibungen zu entnehmen sind.

Im RAS-Umfeld sind folgende Gefährdungen besonders hervorzuheben:

Fehlende oder mangelhafte Planung des RAS-Systems

- Ein RAS-System sollte nicht "organisch wachsen". Vielmehr sollte vor der Nutzung eines RAS-Zuganges - gleichgültig, wie komplex der Zugang gestaltet ist - eine Planung erfolgen. Die Erfahrung zeigt, dass insbesondere beim stetigen Ausbau von RAS-Zugängen komplexe Hard- und Software-Szenarien entstehen können, die dann nicht mehr beherrscht werden können. Dies kann dazu führen, dass Sicherheitseinstellungen falsch gewählt werden, inkompatibel zueinander sind oder sich gegenseitig aufheben.

Fehlendes RAS-Sicherheitskonzept

- Ohne durchgängiges und verbindliches Sicherheitskonzept bleibt es in der Regel einzelnen Administratoren und RAS-Benutzern überlassen, die Sicherheitseinstellungen nach "Gutdünken" vorzunehmen. Dies kann zu inkompatiblen Sicherheitseinstellungen führen, die entweder die Verbindungsaufnahme verhindern oder den Aufbau ungesicherter Verbindungen ermöglichen. Da mittels RAS angebundene IT-Systeme jedoch in vielen Fällen die gleichen Zugriffsmöglichkeiten wie direkt im LAN befindliche IT-Systeme haben, wird dadurch u. U. die Sicherheit des LANs beeinträchtigt.

Von den Vorgaben abweichende Installation

- Die Sicherheit eines RAS-Systems basiert auf dem Zusammenspiel der physikalischen Komponenten (Rechner, Netzkoppelelemente), deren Verbindungsstruktur (Netzaufteilung, Verbindungstopologie) und den Konfigurationen der jeweiligen Software-Komponenten. Die im Rahmen des RAS-Sicherheitskonzeptes festgelegten Regelungen und deren Umsetzung durch entsprechende Konfigurationseinstellungen können die gewünschte Sicherheit jedoch nur dann erbringen, wenn das tatsächlich installierte System mit dem geplanten System übereinstimmt. Oft ergeben sich jedoch, z. B. aufgrund von fehlenden Detailinformationen während der Planungsphase, in der Installationsphase Änderungen im physikalischen Aufbau. Werden die Änderungen nicht erfasst, dokumentiert und auf Auswirkungen auf die IT-Sicherheit analysiert, so kann die Sicherheit des LANs durch Inkompatibilitäten von Systemaufbau und Konfiguration des RAS-Systems gefährdet sein.

Fehlende Regelungen für die RAS-Nutzung

- Fehlende Regelungen für die RAS-Nutzung stellen eine besondere Gefährdung dar. Der RAS-Benutzer ist während der Nutzung in der Regel auf sich alleine gestellt. Existieren für den RAS-Einsatz keine dedizierten Regeln oder sind diese den Benutzern nicht bekannt, so können durch den Benutzer unbewusst Sicherheitslücken geschaffen werden. Regelungen, deren Einhaltung alleine der Verantwortung des einzelnen Benutzers unterliegen, werden von diesen nicht immer vollständig eingehalten, beispielsweise aufgrund fehlendem technischen Verständnis.

- Durch fehlende Beachtung datenschutzrechtlicher Belange bei der Übertragung personenbezogener Daten zwischen den Komponenten des RAS-Systems kann es zu Gesetzesverstößen kommen. So ist z. B. bei der Einrichtung automatisierter Abrufverfahren durch die beteiligten Stellen zu gewährleisten, dass die Zuverlässigkeit des Abrufverfahrens kontrolliert werden kann (siehe § 10 Abs. 2 Bundesdatenschutzgesetz).

Fehlende Beachtung datenschutzrechtlicher Belange

Beispiele:

- Inkompatible Sicherheitseinstellungen: Der Administrator des RAS-Systems lässt nur mit Tripel-DES-Verfahren verschlüsselte Verbindungen zu, ein Benutzer hat jedoch für den RAS-Client keine Verschlüsselung konfiguriert. Eine Verbindung wird daher nicht aufgebaut.
- Von der Planung abweichende Installation: Aufgrund inkompatibler Anschlüsse zwischen RAS-Server und Übergabepunkt des Telekommunikationsanbieters (z. B. ISDN-Endgeräteanschluss gegenüber ISDN-Anlagenanschluss) sowie ungünstiger Leitungsführung wird bei der Installation des RAS-Systems entschieden, dass eine zusätzliche kleine ISDN-Anlage installiert wird, welche kompatible Anschlüsse zu beiden Seiten hin anbietet. Da dieses zusätzliche Gerät in der Planung nicht erfasst wurde, wird versäumt, es im RAS-Sicherheitskonzept zu berücksichtigen. Bei aufgebauter RAS-Verbindung ist es nun möglich, z. B. über den mit einem Standardpasswort gesicherten Fernwartungszugang, auf das Gerät zugreifen.

G 2.65 Komplexität der SAMBA-Konfiguration

SAMBA ist ein freies Programmpaket für Unix-Betriebssysteme, das unter anderem Datei-, Druck- und Authentisierungsdienste über das SMB (Server Message Block) bzw. CIFS (Common Internet File System) Protokoll zur Verfügung stellt. Wichtigste Beispiele für SMB/CIFS-Clients sind sicherlich die Betriebssysteme der Microsoft Windows-Familie. Hierdurch ist es beispielsweise möglich, dass Windows 9x- oder Windows NT-Rechner direkt auf freigegebene Dateien auf einem Unix-Server zugreifen können. Ein Umweg über die Protokolle FTP oder NFS und die Installation zusätzlicher Software auf Client-Seite entfallen. In der aktuellen Version bildet SAMBA eine ganze Reihe der Funktionen eines Windows NT Servers nach, sodass ein Unix-System mit SAMBA in vielen Fällen einen solchen Server ersetzen kann.

unbemerkte Seiteneffekte

Die Konfiguration von SAMBA geschieht hauptsächlich auf der Server-Seite in der Datei *smb.conf*, insbesondere werden hier die freigegebenen Verzeichnisse und Drucker sowie diverse Einstellungen zur Authentisierung eingetragen. Hierzu existiert eine ganze Reihe von Parametern, die in den einzelnen Abschnitten der Datei *smb.conf* gesetzt werden können. Eine bestimmte Funktion des SAMBA-Servers wird in der Regel durch mehrere verschiedene Parameter gesteuert. Je nach Anwendungsfall kann das Zusammenspiel dieser Parameter untereinander sehr komplex sein, so dass die Gefahr besteht, dass der Administrator die Wirkung einer bestimmten Parameter-Kombination falsch interpretiert. Insbesondere besteht die Gefahr, dass bei Modifikation eines bestimmten Parameters unbemerkte Seiteneffekte entstehen, die die Sicherheit des Servers u. U. beeinträchtigen.

Zugriffsrechte auf Verzeichnisse/Dateien

Die zuvor beschriebene Problematik wird bei der Konfiguration der Zugriffsrechte auf Verzeichnisse und Dateien noch verstärkt. Hier sind nicht nur die Einstellungen in der Datei *smb.conf*, sondern auch die Zugriffsrechte auf dem (Unix-)Dateisystem zu berücksichtigen, auf dem die Verzeichnisse bzw. Dateien vorgehalten werden. Die tatsächlichen Rechte, die für den Benutzer beim Zugriff über SAMBA gültig sind, lassen sich über die Datei *smb.conf* auf zwei verschiedenen Wegen beeinflussen: Einerseits können direkt Zugriffsbeschränkungen für die einzelnen Freigaben eines SAMBA-Servers vergeben werden (z. B. über den Parameter *valid users*). Andererseits existieren in der Datei *smb.conf* Parameter (z. B. *force user*), mit denen konfiguriert werden kann, wie sich verzeichnis- und dateibasierte Zugriffsbeschränkungen auf die tatsächlich gültigen Rechte des Benutzers auswirken. Hier kann leicht eine Fehlkonfiguration entstehen, die dazu führt, dass Benutzer zu weitreichende Zugriffsrechte auf Verzeichnisse bzw. Dateien erhalten.

Beispiel:

Der Administrator eines SAMBA-Servers vergibt verzeichnis- bzw. dateibasierte Zugriffsrechte auf dem lokalen Dateisystem des Servers. Hierzu setzt er auf allen freigegebenen Bereichen geeignete Permissions und Ownerships. In der Datei *smb.conf* ist jedoch die Zeile

```
force user = root
```

enthalten. Dies bedeutet, dass Zugriffe auf das Dateisystem unter dem Benutzer-Account "root" durchgeführt werden, unabhängig davon, welcher Benutzer sich am Server angemeldet hat. In der Regel führt dies dazu, dass verzeichnis- und dateibasierte Zugriffsbeschränkungen ignoriert werden.

G 2.66 Unzureichendes IT-Sicherheitsmanagement

Unkoordinierte Vorgehensweise

Die Komplexität der heute vielerorts eingesetzten IT-Systeme und ihre zunehmende Vernetzung macht ein organisiertes Vorgehen bei der Planung, Durchführung und Kontrolle des IT-Sicherheitsprozesses zwingend erforderlich. Die Erfahrung zeigt, dass es nicht genügt, lediglich die Umsetzung von Maßnahmen anzuordnen, da die einzelnen Betroffenen, insbesondere die IT-Benutzer dadurch häufig aufgrund fehlender Fachkenntnisse und unzureichender zeitlicher Ressourcen überfordert sind. In der Konsequenz wird es häufig unterlassen, überhaupt Sicherheitsmaßnahmen umzusetzen, so dass kein befriedigender IT-Sicherheitszustand erreicht wird. Selbst wenn ein solcher einmal erreicht wurde, bedarf er der ständigen Pflege, um ihn dauerhaft im laufenden Betrieb aufrechtzuerhalten.

Mangelhafte Gesamtorganisation

Ein unzureichendes IT-Sicherheitsmanagement ist häufig Symptom einer mangelhaften Gesamtorganisation des IT-Sicherheitsprozesses und damit des gesamten IT-Betriebs. Beispiele für konkrete Gefährdungen, die aus einem unzureichenden IT-Sicherheitsmanagement resultieren, sind:

- *Fehlende persönliche Verantwortung:* Wird in einer Organisation kein IT-Sicherheitsmanagement-Team eingerichtet bzw. kein IT-Sicherheitsbeauftragter ernannt und die persönliche Verantwortung für die Umsetzung von Einzelmaßnahmen nicht eindeutig festgelegt, so ist es wahrscheinlich, dass viele IT-Benutzer ihre Verantwortung für die IT-Sicherheit durch Verweis auf übergeordnete Hierarchieebenen ablehnen. Folglich unterbleibt die Umsetzung von Maßnahmen, die ja zunächst fast immer einen Mehraufwand im gewohnten Arbeitsablauf darstellt.
- *Mangelnde Unterstützung durch die Leitungsebene:* In der Regel gehören IT-Sicherheitsbeauftragte nicht der Behörden- bzw. Unternehmensleitung an. Unterbleibt seitens dieser eine unmissverständliche Unterstützung der IT-Sicherheitsverantwortlichen bei ihrer Arbeit, so werden sie es mitunter schwer haben, notwendige Maßnahmen auch von IT-Benutzern, die in der Linienstruktur über ihnen stehen, wirksam einzufordern. Eine vollständige Umsetzung des IT-Sicherheitsprozesses ist unter diesen Umständen nicht gewährleistet.
- *Unzureichende strategische und konzeptionelle Vorgaben:* In vielen Organisationen wird die Erstellung eines IT-Sicherheitskonzept in Auftrag gegeben, dessen Inhalt nur wenigen Insidern bekannt ist und dessen Vorgaben an Stellen, an denen organisatorischer Aufwand zu betreiben wäre, bewusst oder unbewusst nicht eingehalten werden. Sofern das IT-Sicherheitskonzept strategische Zielsetzungen enthält, werden diese vielfach als bloße Sammlung von Absichtserklärungen betrachtet, und es werden für deren Umsetzung keine genügenden Ressourcen zur Verfügung gestellt. Vielfach wird fälschlicherweise davon ausgegangen, dass in einer automatisierten Umgebung Sicherheit automatisch produziert werde. Schadensfälle in der eigenen oder in ähnlich strukturierten Organisationen sind bisweilen Auslöser für mehr oder minder heftigen Aktionismus, bei dem häufig bestenfalls Teilaspekte verbessert werden.
- *Unzureichende oder fehlgeleitete Investitionen:* Wird die Leitungsebene einer Organisation nicht durch regelmäßige und mit klaren Priorisierungen

versehene IT-Sicherheitsreports über den Sicherheitszustand der IT-Systeme und Anwendungen und über vorhandene Mängel unterrichtet, ist es wahrscheinlich, dass nicht genügend Ressourcen für den IT-Sicherheitsprozess bereitgestellt oder diese nicht sachgerecht eingesetzt werden. In letzterem Fall kann es dazu kommen, dass einem übertrieben hohen Sicherheitsniveau in einem Teilbereich schwerwiegende Mängel in einem anderen gegenüberstehen. Häufig ist auch zu beobachten, dass teure technische Sicherungssysteme falsch eingesetzt werden und somit unwirksam sind oder gar selbst zur Gefahrenquelle werden.

- *Unzureichende Durchsetzbarkeit von Maßnahmenkonzepten:* Zur Erreichung eines durchgehenden IT-Sicherheitsniveaus ist es erforderlich, dass unterschiedliche Zuständigkeitsbereiche innerhalb einer Organisation miteinander kooperieren. Fehlende strategische Leitaussagen und unklare Zielsetzungen führen mitunter zu unterschiedlicher Interpretation der Bedeutung der IT-Sicherheit. Dies kann zur Konsequenz haben, dass die notwendige Kooperation wegen vermeintlich fehlender Notwendigkeit oder ungenügender Priorisierung der Aufgabe "IT-Sicherheit" letztlich unterbleibt und somit die Durchsetzbarkeit der IT-Sicherheitsmaßnahmen nicht gegeben ist.
- *Fehlende Aktualisierung im IT-Sicherheitsprozess:* Neue IT-Systeme oder neue Bedrohungen beeinflussen den IT-Sicherheitszustand innerhalb einer Organisation. Ohne effektives Revisionskonzept verringert sich das IT-Sicherheitsniveau. Aus realer Sicherheit wird somit schleichend eine gefährliche Scheinsicherheit, da das Bewusstsein für die neuen Bedrohungen häufig fehlt.

G 2.67 Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten

Wenn die Vergabe von Zugangs- und Zugriffsrechten schlecht geregelt ist, führt das schnell zu gravierenden Sicherheitslücken, z. B. durch Wildwuchs in der Rechtevergabe.

hoher Arbeitsaufwand

In vielen Organisationen ist die Verwaltung von Zugangs- und Zugriffsrechten eine extrem arbeitsintensive Aufgabe, weil sie schlecht geregelt ist oder die falschen Tools dafür eingesetzt werden. Dadurch kann z. B. viel "Handarbeit" erforderlich sein, die gleichzeitig wiederum sehr fehleranfällig ist. Außerdem sind in diesem Prozess dann auch häufig viele unterschiedliche Rollen und Personengruppen eingebunden, so dass hier auch leicht der Überblick über durchgeführte Aufgaben verloren geht.

Überblick geht verloren

Weiterhin gibt es auch Organisationen, in denen kein Überblick über alle auf den verschiedenen IT-Systemen eingerichteten Benutzer und deren Rechteprofil vorhanden ist. Typischerweise führt das dazu, dass sich Accounts finden von Benutzern, die die Behörde bzw. das Unternehmen längst verlassen haben oder die durch wechselnde Tätigkeiten zu viele Rechte aufgehäuft haben.

Wenn die Tools zur Verwaltung von Zugangs- und Zugriffsrechten schlecht ausgewählt wurden, sind diese oft nicht flexibel genug, um auf Änderungen in der Organisationsstruktur oder auf Wechsel der IT-Systeme angepasst zu werden.

Falsche Rolleneinteilung

Die Rollentrennung von Benutzern kann falsch vorgenommen worden sein, so dass Sicherheitslücken entstehen, beispielsweise durch falsche Zuordnung von Benutzern in Gruppen oder zu großzügige Rechtevergabe. Benutzer können Rollen zugeordnet werden, die nicht ihren Aufgaben entsprechen (zu viel oder zu wenig Rechte) oder die sie aufgrund ihrer Aufgaben nicht haben dürfen (Rollenkonflikte).

G 2.68 Fehlende oder unzureichende Planung des Active Directory

Die globale Struktur des Active Directory, also die Gliederung in Domänen, hat weitreichende Auswirkungen auf die Sicherheit einer Windows 2000 Installation. Problematische Aspekte ergeben sich hier besonders dann, wenn für die verschiedenen Domänen unterschiedliche Sicherheitsanforderungen bestehen oder Domänen zu verschiedenen Organisationsbereichen gehören.

Bei fehlender oder unzureichender Planung ergeben sich beispielsweise folgende domänenübergreifende Gefährdungen:

inkompatible Schemaänderungen

- Alle Domänen in einem Active Directory müssen das gleiche Schema verwenden. Soll auch nur in einer Domäne eine Software installiert werden, die eine Schemaänderung benötigt, müssen alle anderen Domänen diese Änderung mit tragen. Inkompatible Schemaänderungen durch verschiedene Softwareprodukte können dann dazu führen, dass Software nicht installiert werden kann oder fehlerhaft abläuft.

Datenschutz

- Bestimmte Benutzerdaten aus dem Active Directory (Global Catalog) stehen in jeder Domäne zur Verfügung. Dies kann unter Aspekten des Datenschutzes problematisch sein.

verzögerte Kontosperrung

- Administratoren der Forest Root Domain haben weitreichende Befugnisse auch in anderen Domänen.
- Ist eine Domäne auf mehrere Standorte verteilt, die nur unzureichend miteinander vernetzt sind, kann es zu lange dauern, bis eine Kontosperrung in allen Standorten wirksam wird. Daher kann sich ein Benutzer, dessen Konto gesperrt worden ist, u. U. noch an anderen Standorten am System unberechtigt anmelden.

Auch innerhalb einer Domäne muss der Aufbau des Active Directory sorgfältig geplant werden, da sich sonst beispielsweise folgende Gefährdungen ergeben:

- Werden Rechner und Benutzerkonten in den voreingestellten Containern *Computer* und *Benutzer* unterhalb der Domäne angeordnet, ist keine Gruppenrichtlinien-Konfiguration entsprechend verschiedener Typen von Benutzerkonten oder verschiedener Computertypen möglich.
- Werden Organisations-Einheiten (OUs) tief geschachtelt, so kann die Struktur der Domäne unüberschaubar werden, so dass das Active Directory anfälliger für Fehlkonfigurationen wird. Zudem sinkt die Performance des Active Directory Dienstes mit der Schachtelungstiefe, wenn OUs zu tief, d. h. über mehr als 4 Ebenen, geschachtelt werden.

G 2.69 Fehlende oder unzureichende Planung des Einsatzes von Novell eDirectory

Als Werkzeug für das Ressourcenmanagement in Netzen ist eDirectory für den Einsatz in einer heterogenen IT-Umgebung unter einer Vielzahl unterstützter Betriebssysteme ausgelegt. Die Sicherheit des Gesamtsystems ist naturgemäß abhängig von der Sicherheit jedes Teilsystems. Die Betriebssystemsicherheit und speziell die Sicherheit des Dateisystems sind die Basis, auf die sich die Sicherheit von eDirectory stützt.

Da sich eDirectory sowie die einsetzbare Clientsoftware auf einer Vielzahl von Betriebssystemen installieren und betreiben lassen, kann sich daraus eine hohe Vielfalt der bei den eingesetzten Betriebssystemen jeweils vorzunehmenden Sicherheitseinstellungen ergeben. Dies erhöht die Anforderungen an die Planung und setzt entsprechende Kenntnisse sämtlicher involvierter Betriebssysteme voraus. Es besteht deshalb die Gefahr, dass der Einsatz von eDirectory nicht detailliert und tief genug geplant wird, wenn die Gesamtlösung sehr heterogen ist.

Unzulänglicher Betrieb des Verzeichnisdienstes

Für den Einsatz im Intranet ist speziell die Planung der Baumstruktur und die Abbildung der Unternehmensinfrastruktur darin von großer Bedeutung. Bei fehlerhafter Planung besteht die Gefahr von Inkonsistenzen und übermäßiger Komplexität im Aufbau des Verzeichnisdienstes. Daraus können in der Folge Fehlkonfigurationen und falscher oder unzulänglicher Betrieb des Systems resultieren.

Inkonsistenz der Sicherheitsrichtlinien zwischen einzelnen Baum-Hierarchien

Die globale Baumstruktur des eDirectory-Verzeichnisdienstes hat weitreichende Auswirkungen auf die Sicherheit einer eDirectory-Installation. Problematische Aspekte ergeben sich hier besonders dann, wenn die verschiedenen Teilbäume unterschiedliche Sicherheitsanforderungen haben oder zu verschiedenen Organisationsbereichen gehören. Durch die impliziten Vererbungsmechanismen und die Komplexität der Regeln für die Berechnung der tatsächlich wirksamen, effektiven Rechte einzelner Objekte stellt dies hohe Anforderungen an die Planung des Systems.

Die implizit eingesetzte CA (Zertifizierungsstelle) ist wesentlicher Bestandteil der Sicherheit von eDirectory. Auch hier kann eine fehlerhafte Planung die Sicherheit des Verzeichnisdienstes beeinträchtigen.

Unklarheit über die tatsächlich angewendeten effektiven Rechte

Die Planung der Zugriffsmöglichkeiten auf den Verzeichnisdienst ist ein Kernthema für die Systemsicherheit. Dies gilt sowohl für den Einsatz im Intranet als auch besonders für den Einsatz von eDirectory als LDAP-Server im Internet.

Ungewollte Zugriffsmöglichkeiten auf den Verzeichnisdienst

Weiterhin ist die Planung der Administration des Verzeichnisdienstes ein wichtiges Thema. eDirectory erlaubt die Umsetzung eines Rollen-basierten Administrationskonzeptes sowie die Delegation von Administrationsaufgaben. Dies ist speziell unter dem Aspekt der Sicherheitsadministration wichtig. Die Planung der Administration erfordert äußerste Sorgfalt und Umsicht, anderenfalls besteht die Gefahr, dass unautorisierte Systemnutzer ungewollte Zugriffsmöglichkeiten erhalten.

Darüber hinaus bietet die eDirectory-Software das *iMonitor-Tool*, welches einen Web-basierten Monitorzugriff auf die eDirectory-Server und das

Verzeichnissystem gestattet. Eine fehlerhafte Planung des Einsatzes dieser Funktionalität erlaubt unter Umständen unautorisierten Benutzern den Zugang zu Interna der eDirectory-Installation.

Ein wichtiger Punkt im Betrieb von eDirectory ist auch die Partitionierung des Verzeichnisdienstes und dessen Replikation. Hier kann eine unzulängliche Planung mangelhafte Performance, Inkonsistenzen in der Datenhaltung bis hin zu Datenverlusten zur Folge haben.

Inkonsistenz der Sicherheitsrichtlinien zwischen eDirectory und der jeweiligen Betriebssystemumgebung

Der eDirectory-Verzeichnisdienst erlaubt eine rollenbasierte Administration der Verzeichnisdatenbank sowie die Delegation einzelner Administrationsaufgaben. Die Planung der Administrationsrollen und der Delegationsmöglichkeiten hat dabei in Übereinstimmung mit der festzulegenden Sicherheitsrichtlinie (siehe M 2.238 *Festlegung einer Sicherheitsrichtlinie für Novell eDirectory*) zu erfolgen. Bei fehlender oder fehlerhafter Planung der Administrationsaufgaben besteht die Gefahr, dass das System unsicher oder unzulänglich administriert wird.

Unzulängliche Administration des Verzeichnissystems

eDirectory erlaubt die Synchronisation von Verzeichnisdaten mit weiteren Verzeichnisdiensten via DirXML. DirXML besteht aus einem Kern (*engine*) und spezialisierten Treibern (z. B. für Windows 2000 Active Directory, Lotus Notes, SAP R/3, Netscape, etc.) für den Austausch von Verzeichnisinformationen im XML-Format. Dabei können die fremden Verzeichnisdienste über einen so genannten *Publisher Channel* dem eDirectory Änderungen mitteilen. Bei entsprechenden Rechten, die vom jeweils betrachteten Zielsystem abhängen, werden diese Änderungen dann auch im eDirectory aktiv. Die externen Verzeichnisse können sich umgekehrt beim eDirectory einschreiben, um Änderungen des eDirectory-Informationsstandes über diesen Kanal (*subscriber channel*) zu erfahren und ihr Verzeichnis daraufhin abzugleichen. Diese Synchronisation bedarf einer detaillierten Planung, da anderenfalls sensitive Daten unter Umständen ungewollt automatisiert nach außen vervielfältigt werden. Umgekehrt können unter Umständen ungewollt bestehende Daten auf diesem Weg überschrieben werden. Um die Daten beim Transport zu schützen, kann SSL eingesetzt werden. Hierbei können Fehler in der Planung den Verlust von Integrität und Vertraulichkeit von Verzeichnisdaten nach sich ziehen.

Nicht zuletzt ist die Verwendung von Login-Skripts für Benutzer und Benutzergruppen zu planen. Bei fehlender oder unzulänglicher Planung können hierbei Inkonsistenzen zur festgelegten Sicherheitsrichtlinie auftreten.

Darüber hinaus können sich bei fehlender oder unzureichender Planung auch folgende Probleme ergeben:

- Der Administrationszugriff auf das System kann unzureichend gesichert sein,
- der Betrieb der Public-Key-Infrastruktur kann unzulänglich sein,
- die Systemperformance zu gering sein und
- es kann zu Datenverlusten kommen, sofern Replikation und Backup nicht ausreichend berücksichtigt wurden.

G 2.70 Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Novell eDirectory

Die Partitionierung und die Replizierung des eDirectory-Verzeichnisdienstes ist ein wesentlicher Aspekt bei der Planung des Einsatzes.

Bei der Partitionierung handelt es sich um eine Aufteilung der Verzeichnisdaten des eDirectory in einzelne Teilbereiche (Partitionen). Diese Aufteilung kann nicht beliebig erfolgen, sondern muss gewissen Regeln entsprechen, die sich aus der Logik der hierarchischen Baumstruktur ergeben. Zweck der Partitionierung ist zum einen eine Lastverteilung des Verzeichnissystems auf mehrere Teile, zum anderen kann damit eine physikalische Trennung der Aufbewahrungsorte von Verzeichnisdaten - z. B. den Standorten einer Organisation entsprechend - erreicht werden. Weiterhin können Partitionen auch Verwaltungseinheiten des Verzeichnissystems darstellen.

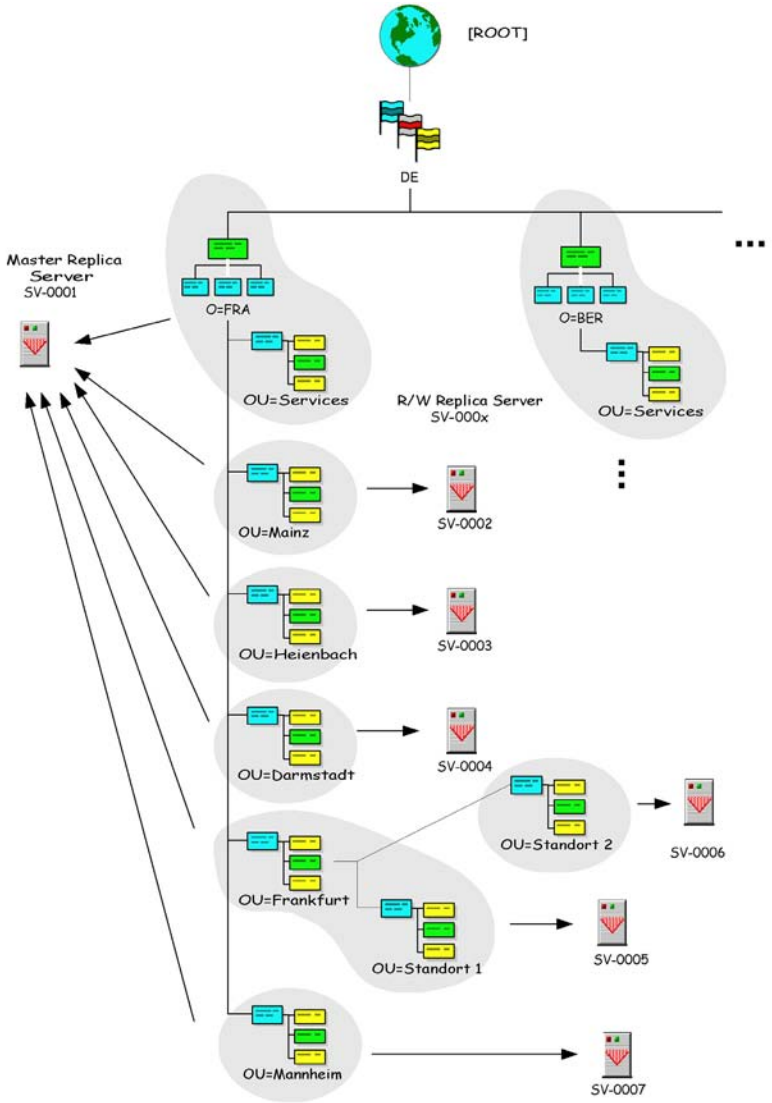


Abb.: Beispiel für einen partitionierten eDirectory Verzeichnisdienst

Die Replizierung von Partitionen des eDirectory dient in erster Linie der Erhöhung der Verfügbarkeit und der Lastverteilung des Verzeichnissystems. Weiter wird durch die Redundanz in der Datenhaltung die Ausfallsicherheit verbessert.

Die Planung ist auch deshalb von entscheidender Bedeutung, da nachträgliche Änderungen an den Partitions- und Replikationseinstellungen zwar möglich sind, jedoch unter Umständen Inkonsistenzen nach sich ziehen können.

Zeitfenster mit Inkonsistenzen

Bei Änderungen am eDirectory dauert es naturgemäß eine gewisse Zeit, bis sich die neuen Einstellungen überall hin ausgebreitet haben. Somit kann sich ein Zeitfenster ergeben, innerhalb dessen das eDirectory inkonsistent ist. Solche Inkonsistenzen können vor allem in der Definition der Authentisierungsdaten oder auch der Zugriffsrechte auf eDirectory-Objekte ein Problem darstellen.

Eine Partitionierung des eDirectory-Verzeichnisses hat direkte Konsequenzen für die Vererbung von Zugriffsrechten (Access Control Lists, ACL). Um die Vererbungsregeln bei einem bestehenden eDirectory-Baum zu erhalten, wird bei einer Partitionierung dem Wurzelobjekt der neuen Partition die übergeordnete ACL als *inherited ACL* vom System zur Kenntnis gebracht.

erhöhter Administrationsaufwand

Die Festlegung der Partitionierung des eDirectory-Verzeichnisdienstes hat direkte Auswirkung auf die Replizierungsaktivitäten des Gesamtsystems. Um effizient über den Gesamtbaum nach Objekten suchen zu können (*Tree walking*), legt das eDirectory automatisch so genannte *Subordinate Reference Replicas* an, welche im Wesentlichen Sprungadressen enthalten. Ist die Planung unzulänglich (z. B. bei zu flacher Baumstruktur), so werden hier sehr umfassende Replizierungsringe erzeugt. Wird ein Replizierungsring sehr groß, so besteht eine gewisse Wahrscheinlichkeit, dass zumindest ein eDirectory-Server des Ringes momentan nicht erreichbar ist. In einem solchen Fall werden Fehler- und Statusmeldungen auf jedem weiteren eDirectory-Server des Replizierungsrings erzeugt. Dies kann zu erhöhtem Administrationsaufwand führen, der sich über große Teile des Verzeichnisbaums erstrecken kann.

Weitere Problemfelder sind in G 2.42 *Komplexität der NDS* beschrieben.

Außerdem kann eine fehlerhafte oder unzureichende Planung der Partitionierung und der Replizierung des Verzeichnisdienstes auch zu Datenverlusten sowie Inkonsistenzen in der Datenhaltung, einer mangelhaften Verfügbarkeit des Verzeichnisdienstes und einer insgesamt schlechten Systemperformance bis hin zu Systemausfällen führen.

G 2.71 Fehlerhafte oder unzureichende Planung des LDAP-Zugriffs auf Novell eDirectory

Die LDAP-Zugriffsmöglichkeit auf den Verzeichnisdienst von eDirectory ist ein wesentliches Leistungsmerkmal des Softwareprodukts. Der Zugriff durch die Benutzer erfolgt über das LDAP v3-Protokoll, welches einen weitverbreiteten Internet-Standard darstellt. Betreiber, die eDirectory als eBusiness-Plattform verwenden, stellen ihren Benutzern dabei in der Regel spezielle Clients zur Verfügung. Einfache Web-Browser oder E-Mail-Clients können jedoch ebenfalls als LDAP-Clients agieren.

Die LDAP-Schnittstelle ist außerdem auch dazu geeignet, dass Netzapplikationen und deren Services darüber auf den Verzeichnisdienst zugreifen. Dieser Zugriff bedarf eingehender Planung, insbesondere auch in Bezug auf die für den sinnvollen Einsatz der Anwendungen benötigten eDirectory-Rechte.

verschiedene Verbindungsarten

Die Planung des LDAP-Zugriffs hängt also wesentlich vom Einsatzszenario des eDirectory ab. Prinzipiell gibt es aus Sicht des eDirectory drei verschiedene Verbindungsarten für einen LDAP-Client:

- als [Public] Objekt (*Anonymous Bind*): Hierbei werden keine Authentisierungsinformationen abgefragt und das [Public] Objekt besitzt standardmäßig stets das uneingeschränkte Browse-Recht auf den Verzeichnisbaum.
- als Proxy User (*Proxy User Anonymous Bind*): Diese Konfigurationsmöglichkeit kann anstelle des anonymen Login gewählt werden. Der Proxy User ist dabei eDirectory-seitig entsprechend zu konfigurieren.
- als NDS User (*NDS User Bind*): Hierbei meldet sich der Benutzer mit seinen eDirectory-Rechten am Verzeichnisdienst an. Das entsprechende Benutzerobjekt muss beim eDirectory angelegt sein.

Was darf im Klartext übertragen werden?

Es muss in der Planung berücksichtigt werden, ob und welche Daten im Klartext gemäß den organisationsinternen Sicherheitsrichtlinien übertragen werden dürfen. Dies gilt für den Einsatz im Intranet sowie besonders für die Anbindung an das Internet.

Dabei geht es z. B. darum, ob Benutzerpasswörter im Klartext übermittelt werden dürfen und wie konsequent der Einsatz der SSL-Verschlüsselung umgesetzt wird. Damit unterstützt eDirectory entsprechend dem Standard LDAP v3 zwei Verbindungsarten:

- *anonymous bind*: ohne Benutzername und Passwort,
- *clear-text password bind*: Benutzername und Klartextpasswort zur Authentisierung.

Zusätzlich wird LDAP über SSL unterstützt. Seitens eDirectory muss konfiguriert werden, ob die ersten beiden Verbindungsarten unterstützt werden.

Außerdem wird SSL in zwei Modi unterstützt: ein- und zweiseitige Authentisierung. Bei beidseitiger Authentisierung müssen die erforderlichen Credentials, unter anderem das Wurzelzertifikat der Zertifizierungsstelle, allgemein zugänglich sein.

Fehlkonfigurationen

Durch die oben beschriebene Vielfalt der Konfigurationsoptionen für den LDAP-Zugriff auf den eDirectory-Verzeichnisdienst können sich schnell Fehlkonfigurationen ergeben. Konsequenzen solcher Fehlkonfigurationen könnten sein:

- Falsche Vergabe von Zugriffsrechten,
- unautorisierte Zugriffsmöglichkeiten auf den eDirectory-Verzeichnisdienst,
- Übermittlung von Benutzerpasswörtern im Klartext,
- Ausspähen von unverschlüsselten Informationen,
- Fehler beim LDAP-Zugriff, insbesondere für netzbasierte Anwendungen, sowie
- unzureichende Produktivität des Gesamtsystems.

G 2.72 Unzureichende Migration von Archivsystemen

Archivierte Daten sollen typischerweise über einen sehr langen Zeitraum gespeichert bleiben. Während dieses Zeitraums können die zugrundeliegenden technischen Systemkomponenten, Speichermedien und Datenformate physikalisch bzw. technologisch altern und dadurch unbrauchbar werden. Außerdem können sich im Laufe der Zeit Probleme mit der Kompatibilität der verwendeten Datenformate ergeben.

Alterung von Komponenten

Wenn auf die Alterung des bestehenden Systems nicht reagiert wird, ist langfristig damit zu rechnen, dass

- archivierte Rohdaten physikalisch nicht mehr von den Archivmedien lesbar sind,
- archivierte Daten durch physikalische Fehler an Archivsystem und -medien verändert werden,
- Ersatzteile für Hardware-Komponenten nicht mehr lieferbar sind,
- Ergänzungen für Software-Komponenten nicht mehr lieferbar sind,
- verwendete Datenformate nicht mehr den Integritätsanforderungen entsprechen,
- elektronische Signaturen unbrauchbar werden,
- verschlüsselte Daten für Unberechtigte lesbar werden.

Alterung kryptographischer Verfahren

Auch wenn rechtzeitig Systemkomponenten ausgetauscht oder die Daten kopiert werden, so können trotzdem noch Probleme durch die Verwendung kryptographischer Verfahren auftreten. Beispielsweise könnten Schwachstellen in integritätssichernden Verfahren entstehen, da Verschlüsselungs- und Signaturalgorithmen im Laufe der Zeit und mit steigender Rechenleistung an Schutzwirkung verlieren können (siehe auch G 2.79 *Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung*).

Beispiele:

- Durch physikalische Langzeiteinflüsse (Materialverschleiß, Verformung, Verkratzen von Medienoberflächen, Weichmacher) können Datenträger beschädigt werden. Je nach Verwendungszweck des betroffenen Datenträgers als System- oder Archivmedium kann der Betrieb des Archivsystems gestört oder die auf den Archivmedien gespeicherten Daten verloren gehen.
- Der Hersteller eines Archivsystems hatte in den Kontextdaten für Dokumente ein Debug-Feld vorgesehen. In der Pilotphase des Archivsystems wurden Dokumente aus dem normalen Geschäftsbetrieb zu Testzwecken archiviert, wobei der Teststatus in der Debug-Information festgehalten wurde. Beim Übergang in die Betriebsphase wurden die Testdokumente dann nicht gelöscht, da sie auf WORM-Datenträgern archiviert waren, sondern es wurden die mit der betreffenden Debug-Information markierten Dokumente nicht mehr angezeigt. Das Nachfolgesystem wurde von einem anderen Hersteller geliefert, der Debug-Informationen auf eine andere Weise darstellte. Bei der anschließenden Migration der Archivdaten auf das neue Archivsystem wurde jedoch versehentlich das alte Debug-Feld

nicht ausgewertet. Die alten Testdokumente befanden sich nach der Migration der Daten weiterhin im Archiv, tauchten bei einer späteren Recherche jedoch plötzlich als vermeintlich authentische Dokumente auf.

- Elektronische Signaturverfahren könnten durch Ausprobieren der Signaturschlüssel oder durch mathematische Verfahren kompromittiert werden. Sofern dies innerhalb des Archivierungszeitraums eintritt, ist es möglich, elektronische Signaturen auch rückwirkend zu fälschen.

G 2.73 Fehlende Revisionsmöglichkeit von Archivsystemen

Die Revision eines Archivierungsvorgangs muss sowohl organisatorische als auch technische Kriterien berücksichtigen. Die Prüfung von Archivsystemen muss daher neben der Begutachtung der Systemkonfiguration auch die Prüfung der Vergabe und Nutzung von Zugriffsrechten umfassen.

Wenn das ausgewählte Archivsystem hierbei nicht die notwendige technische Unterstützung liefert, z. B. in Form von speziellen Benutzerkonten für die Revision, Monitoring-Werkzeugen, integritätsgeschützten Protokolldateien (siehe G 2.76 *Unzureichende Dokumentation von Archivzugriffen*), kann der Prüfungsvorgang sehr aufwendig werden. Dadurch besteht außerdem die Gefahr, dass dieser nur unvollständig stattfindet und wesentliche Punkte übersehen werden. Der Revisionsvorgang des Archivierungsprozesses kann hierdurch insgesamt gefährdet werden.

Mittelbar können sich hieraus rechtliche und wirtschaftliche Nachteile ergeben, z. B. durch den Wegfall der Nachweiskraft archivierter Dokumente.

G 2.74 Unzureichende Ordnungskriterien für Archive

Elektronische Archive können sehr große Datenmengen beinhalten. Zur Ablage und zum Wiederauffinden einzelner Datensätze dienen Ordnungskriterien, die in Indexdaten des Dokumentenmanagementsystems (DMS) und Indexdaten des Archivsystems zu unterscheiden sind.

Dokumentenmanagementsystem

Ordnungskriterien des DMS dienen dazu, den Kontext und Inhaltsangaben zusammen mit dem jeweiligen Dokument zu verwalten. Eine ungeeignete Auswahl von Kontextkriterien hätte hier zur Folge, dass archivierte Dokumente nicht oder nur mit großem Aufwand wieder zu recherchieren wären oder die Semantik archivierter Dokumente nicht eindeutig bestimmbar wäre. Eine große Zahl von Kontextkriterien andererseits steigert den Verwaltungsaufwand und reduziert mit wachsender Zahl archivierter Dokumente die Performance des Dokumentenmanagementsystems.

Archivsystem

Ordnungskriterien des Archivsystems hingegen sind eher technischer Natur. Sie dienen der Identifikation einzelner Rohdaten und der Organisation der Ablage der Rohdaten auf Speichermedien. Ihre Auswahl wird in der Regel nicht durch das DMS, sondern durch den Aufbau des Archivservers und der zugrundeliegenden Speicherarchitektur bestimmt. Eine wesentliche Anforderung ist die Eindeutigkeit der Dokumentkennung. Sollte diese Anforderung verletzt werden, d. h. wenn zwei Dokumente dieselbe Dokumentkennung erhalten, so kann je nach Suchverfahren beim Abrufen ein falsches Dokument an das DMS zurückgegeben und dort mit einem neuen Dokumentkontext versehen werden. Das nicht gefundene Dokument wäre zwar physikalisch vorhanden, würde aber nicht mehr eindeutig einem Vorgang im DMS zuzuordnen sein.

eindeutige Kennzeichnung

Die Revisionssicherheit des Archivierungsprozesses bezieht sich wesentlich auf die eindeutige Kennzeichnung aller verwalteten Dokumente sowie die Nachweisbarkeit der Verknüpfung von Dokument und Kontextinformationen.

G 2.75 Mangelnde Kapazität von Archivdatenträgern

Eine falsche Einschätzung des Datenaufkommens bei der Archivierung kann dazu führen, dass zu kleine Archivmedien verwendet werden und daher die Archivierung unvollständig oder verzögert erfolgt.

Änderungshäufigkeit von Dokumenten

Bei der Abschätzung des benötigten Datenvolumens wird häufig nur die erwartete maximale Größe der zu speichernden Dokumente als einzige Einflussgröße zugrundegelegt. Tatsächlich jedoch kann der Speicherbedarf bei Archivsystemen ein Vielfaches davon betragen, da hierbei auch die Art der Datenablage sowie die Änderungshäufigkeit von Dokumenten einen wesentlichen Einfluss haben.

Bei einer Archivierung auf WORM-Medien (Write Once Read Multiple) werden beispielsweise die Dokumente zwangsläufig in mehreren Versionen abgelegt, d. h. nach jeder Änderung wird ein neues Dokument gespeichert. Dadurch kann sich auch bei kleinen Dokumenten mit hoher Änderungsfrequenz ein hohes Datenvolumen ergeben. Alte Versionen der Dokumente können nachträglich nicht mehr vom Archivmedium gelöscht werden. Neben Kapazitätsengpässen kann dies auch zu Datenschutz- oder Vertraulichkeitsproblemen führen, da Daten nur als "zu löschen" markiert, aber nicht tatsächlich gelöscht werden.

G 2.76 Unzureichende Dokumentation von Archivzugriffen

Ebenso wie bei anderen IT-Systemen bestehen auch bei Archivsystemen Manipulationsmöglichkeiten, wenn diese schlecht geschützt sind. Benutzer könnten versuchen, gefälschte Dokumente in das Archiv einzubringen und durch Angabe entsprechender Kontextinformationen diese Dokumente bestehenden Verwaltungsvorgängen zuzuweisen oder komplett neue Vorgänge zu fälschen. Systemadministratoren könnten Manipulationen am Archivsystem vorbei durchführen und die Manipulation durch Veränderung von Protokolldateien verbergen.

Protokolldateien werden oft vernachlässigt

Üblicherweise wird Protokolldateien ein geringerer Wert beigemessen als den zu archivierenden Dokumenten selbst. Dies äußert sich häufig in geringeren Aufbewahrungsfristen für Protokolldateien und im weniger sorgsamen Umgang mit Protokolldateien.

Wenn archivierte Dokumente in spätere Verwaltungsvorgänge einfließen sollen, ist es unerlässlich, die Authentizität nachweisen zu können, also korrekte von manipulierten Dokumenten unterscheiden und im Falle von strittigen Dokumenten die Dokumenthistorie belegen zu können. Dies wird gefährdet durch

- eine nicht ausreichende Protokollierung der Archivzugriffe, insbesondere der Speichervorgänge,
- einen nicht ausreichenden Schutz der Protokolldaten vor Manipulation durch Benutzer sowie Systemadministratoren,
- den Verlust von Protokolldaten,
- zu kurze Aufbewahrungsfristen der Protokolldaten.

Sofern die zu archivierenden Dokumente nach Vertraulichkeitsstufen klassifiziert sind, muss auch immer nachvollziehbar sein, wer zu welchem Zeitpunkt Einsicht in Dokumente genommen hat. Dies ist nicht mehr gewährleistet, wenn Lesezugriffe und Suchanfragen nicht dokumentiert werden.

Beispiele:

- Im Rahmen einer Archiv-Recherche wird ein Dokument aufgefunden, das in einem laufenden Verwaltungsvorgang eine Person in bestimmter Weise belastet. Anhand der mitgespeicherten Kontextinformationen wird das Dokument als authentisch bewertet. Das Dokument wurde aber seinerzeit von einem Unberechtigten erzeugt, der bewusst falsche Kontextinformationen (u. a. Ersteller des Dokuments und Erstelldatum) angegeben hatte, um später die fragliche Person belasten zu können. Da die Protokolldateien der Archivzugriffe zwischenzeitlich gelöscht wurden, kann dies aber nun nicht mehr erkannt werden. Der betroffene Mitarbeiter wird dadurch fälschlich belastet.
- Ein Benutzer mit administrativen Privilegien manipuliert Dateien im Cache-Bereich des Archivsystems, bevor diese auf dauerhaften Medien abgelegt werden. Die Manipulation ist nicht nachvollziehbar, da der Benutzer am Archivsystem vorbei sowohl die Daten selbst als auch die Protokolldateien manipuliert hat.

G 2.77 Unzulängliche Übertragung von Papierdaten in elektronische Archive

In vielen elektronischen Archiven werden regelmäßig Dokumente gespeichert, die ursprünglich nur in Papierform vorlagen und daher in eine elektronische Form übertragen werden müssen. Dies erfolgt unter Wahrung ausgewählter Merkmale des Originaldokuments. Je nach Verwendungszweck des Dokuments ergeben sich hier unterschiedliche Anforderungen. Dies kann die Übereinstimmung des äußeren Erscheinungsbilds der Kopie mit dem Original sein, wenn beispielsweise eine Bilddatei verwendet wird. Es kann auch die Übereinstimmung von Textausschnitten, z. B. unter Verwendung einer Textdatei, oder die Abbildung weiterer Merkmale, z. B. Biometriedaten oder Kontextdaten, gefordert sein.

Die Ablage als Text- oder Bilddatei allein reicht für den Nachweis der Originaltreue des Dokuments nicht immer aus, da sowohl Manipulationen als auch Fehler auftreten können:

Manipulation

- Mit Text- und Bildverarbeitungsprogrammen können bestehende Dokumente manipuliert werden.

Fehler beim Einscannen

- Durch Fehler beim Einscannen kann die Semantik der aufgenommenen Daten verfälscht werden, wodurch Fehlinterpretationen und -berechnungen ausgelöst werden können. Beispielsweise könnten wichtige Teile des Dokuments beim Scanvorgang vergessen werden.

In einigen Archivierungsszenarien ist vorgesehen, die in Papierform vorliegenden Dokumente nach dem Einscannen aus Platzgründen zu vernichten. Hierbei muss davon ausgegangen werden, dass nach Vernichtung des Originaldokumentes der spätere Nachweis der Originaltreue von Kopie und Dokument nicht mehr direkt erbracht werden kann.

Dies bedeutet, dass alle für spätere Nachweiszwecke notwendigen Merkmale des Originaldokuments bereits in der Phase der Übertragung in elektronischer Form erfasst und nachvollziehbar mitgespeichert werden müssen. Werden hierbei Merkmale nicht berücksichtigt oder vergessen (z. B. die Anzahl der Seiten eines Originaldokumentes), kann das die Nachweiskraft der Dokumente erheblich einschränken, da Nacherhebungen von Merkmalen des Originaldokuments oftmals nicht mehr möglich sind.

Eine unzulängliche Vorgehensweise bei der Übertragung der Dokumente gefährdet die Wirksamkeit und Nachvollziehbarkeit des nachfolgenden Verarbeitungsprozesses für Dokumente und letztlich die Korrektheit der archivierten Dokumente.

Beispiele:

Originale werden vernichtet

- Der eingehende Schriftverkehr einer Behörde wird zur späteren elektronischen Weiterverarbeitung eingescannt und im Archiv abgelegt. Gelegentlich wird jedoch vergessen, die Rückseite eines Briefes einzuscannen. Da der eingehende Schriftverkehr nach dem Einscannen vernichtet wird, kann der Originalzustand des Briefes nicht mehr nachgewiesen werden.

Text wird falsch erkannt

- Beim Einscannen und automatischen Erfassen von Text werden Passagen ausgelassen oder verfälscht, die vom OCR-Programm (Optical Character

Recognition - Verfahren zur Erkennung von Text aus Bilddateien) nicht korrekt erkannt worden sind. Das kann z. B. in schwacher Farbe oder undeutlicher Schrift gedruckten Text betreffen, aber auch handschriftliche Ergänzungen in Dokumenten oder ein verwischtes Druckbild von Tintenstrahldruckern. Falsch erkannte Rechnungsbeträge (nicht erkannte Kommata, etc.) sind ebenfalls eine mögliche Fehlerquelle für spätere Missverständnisse.

- Manuelle Unterschriften unter Dokumenten werden als Bild eingescannt. Bei einem späteren Rechtsstreit über die Echtheit von Dokument und Unterschrift kann ein graphologisches Gutachten keine eindeutige Aussage mehr liefern, da die vorgelegte Bilddatei mit einem Bildbearbeitungsprogramm manipuliert bzw. ein anderes Dokument kopiert worden sein könnte. Merkmale des Originaldokuments, wie z. B. Beschaffenheit und Zusammensetzung des verwendeten Papiers oder die Andruckstärke bei der händischen Unterschrift, sind nicht mehr nachvollziehbar.

händische Unterschrift ist nicht überprüfbar

G 2.78 Unzulängliche Auffrischung von Datenbeständen bei der Archivierung

Datenträger können physikalisch wie technologisch veralten. Datenformate werden ebenfalls gelegentlich um neue syntaktische bzw. strukturelle Merkmale erweitert. Beides kann dazu führen, dass archivierte Daten nicht mehr lesbar sind (siehe G 2.72 *Unzureichende Migration von Archivsystemen*).

Daher sollten elektronisch archivierte Dokumente in größeren Zeitabständen auf neue Datenträger kopiert bzw. in neue, aktuellere Datenformate übertragen werden. Hierbei besteht die Gefahr, dass Daten bei der Übertragung auf neue Datenträger aus ihrem Dokumentkontext gelöst werden oder beim Umkopieren in andere Datenformate unbeabsichtigt semantische Änderungen vorgenommen werden.

Daneben bestehen Manipulationsmöglichkeiten während der Übertragung der Daten auf ein neues Speichermedium. Hierbei können selbst auf WORM-Medien abgelegte Daten "geändert" werden.

Nach der Migration der Datenbestände kann die Notwendigkeit bestehen, alte Datenträger zu vernichten. Hierzu wird auf die Gefährdung G 2.81 *Unzureichende Vernichtung von Datenträgern bei der Archivierung* verwiesen.

Beispiele:

- Im Rahmen der Migration der Datenbestände werden Vorversionen von versioniert gespeicherten Dokumenten aus Platzgründen gelöscht, obwohl diese aus Nachweisgründen noch benötigt werden.
- Es werden Dateien, die ursprünglich auf WORM-Medien änderungssicher ("revisionssicher") gespeichert waren, auf neue Datenträger übertragen. Dabei werden Dateien während des Kopiervorgangs ausgetauscht, d. h. einzelne Dateien werden nicht auf das neue Medium übernommen, stattdessen werden gefälschte Dateien eingefügt.

G 2.79 Unzureichende Erneuerung von digitalen Signaturen bei der Archivierung

Die Algorithmen und Schlüssellängen, die bei digitalen Signaturen verwendet werden, müssen in regelmäßigen Abständen an den aktuellen Stand der Technik angepasst werden, damit ihre Schutzwirkung gewährleistet ist (siehe G 4.47 *Veralten von Kryptoverfahren*). Das bedeutet, dass die verwendeten kryptographischen Schlüssel und die zugehörigen Zertifikate nur eine begrenzte Zeit zuverlässige Gültigkeit besitzen. Gemessen an der angestrebten Archivierungsdauer sind dies verhältnismäßig kurze Zeiträume. Um die Beweiskraft digitaler Signaturen zu erhalten, muss daher rechtzeitig die elektronische Signatur jedes einzelnen Dokuments erneuert werden.

Bei der regelmäßigen Neusignatur der archivierten Dokumente können u. a. folgende Sicherheitsprobleme auftreten:

- Wenn Dokumente mit einer vormals ungültigen oder fehlenden elektronischen Signatur fälschlicherweise eine gültige neue Signatur erhalten, so können diese Dokumente fortan fälschlicherweise als authentisch angesehen werden.

"versehentliche" Neusignatur

- Es könnte passieren, dass Dokumente bei einer Neusignatur vergessen werden, d. h. keine neue gültige Signatur erhalten, obwohl sie vormals gültig signiert waren. Dadurch kann die Authentizität bzw. Integrität des betreffenden Dokuments fortan möglicherweise nicht mehr nachgewiesen werden, wenn kein alternativer Nachweis anhand anderer Merkmale möglich ist.

Dokumente werden vergessen

- Zum Zeitpunkt der Neusignatur könnte das zu Grunde liegende kryptographische Verfahren bereits kompromittiert oder der ursprüngliche Signaturschlüssel bekannt geworden sein (z. B. durch massiven Rechenaufwand ermittelt). Dadurch könnten Unbefugte Dokumente erzeugen und mit einer technisch gültigen Signatur, gegebenenfalls auch mit beliebigen Zeitsignaturen (Zeitstempel), versehen. Gelingt es, diese Dokumente in den Prozess der Neusignatur einzubringen, so können diese Dokumente fälschlicherweise als authentisch angesehen werden.

kompromittierte kryptographische Verfahren

G 2.80 Unzureichende Durchführung von Revisionen bei der Archivierung

Die elektronische Archivierung stellt sehr hohe Anforderungen an den Prozess der Umwandlung von Papierdokumenten in elektronische Dokumente. Die bei der Archivierung auszuführenden Tätigkeiten sollten in einer Verfahrensdokumentation genau beschrieben sein und durch eine Protokollierung, die aufzeichnet, welcher Benutzer wann welche Aktivitäten im Archiv ausgeführt hat, nachvollziehbar gemacht werden.

Zu seltene und zu ungenaue Überprüfung der Arbeitsvorgänge bei der Archivierung oder der aufgezeichneten Protokolldaten kann mittelbar dazu führen, dass die Ordnungsmäßigkeit des Archivierungsprozesses und damit die Richtigkeit der archivierten Dokumente selbst angezweifelt wird.

G 2.81 Unzureichende Vernichtung von Datenträgern bei der Archivierung

Archivsysteme mit ihren Speichermedien bieten alleine für sich in der Regel keinen Zugriffsschutz auf die gespeicherten Daten. Diese Funktion wird stattdessen vom übergeordneten Dokumenten-Management-System (DMS) erfüllt. Sind Archivdatenträger außerhalb der Archivumgebung (Archivsystem und DMS) zugänglich, ist davon auszugehen, dass jeder, der das Medium lesen kann, auf die dort gespeicherten Informationen zugreifen kann.

Missbrauch alter Archivmedien

Besonders wenn archivierte Daten auf neue Datenträger umkopiert werden, besteht ein erhebliches Risiko, dass alte, nicht mehr gebrauchte Archivmedien, die nicht ordnungsgemäß und vollständig zerstört werden, zur Informationsgewinnung missbraucht werden.

einmalige Verschlüsselung schützt nicht dauerhaft

Auch bei verschlüsselt archivierten Daten kann eine nicht ordnungsgemäße Vernichtung von Datenträgern ein Problem darstellen, da die Sicherheit von Kryptoalgorithmen immer nur zeitlich begrenzt garantiert werden kann (siehe G 4.47 *Veralten von Kryptoverfahren*). Eine einmalige Verschlüsselung schützt deshalb nicht dauerhaft vor Datenmissbrauch.

G 2.82 Fehlerhafte Planung des Aufstellungsortes von Speicher- und Archivsystemen

Aufgrund der Sensitivität der gespeicherten Daten sowie der sehr langen Aufbewahrungszeit sind bei Speicher- oder Archivsystemen erhebliche Anforderungen an die Qualität der Datenspeicherung zu stellen. Die Wahl des Aufstellungsortes für das Speicher- oder das Archivsystem hat hierauf hohen Einfluss.

In diesem Zusammenhang sind folgende potentielle Sicherheitsprobleme zu beachten:

- **Unzulängliche klimatische Bedingungen**

  Eine zu hohe oder zu niedrige Temperatur kann ebenso wie eine zu hohe Luftfeuchtigkeit zu Fehlfunktionen in technischen Komponenten von Archiv- und Speichersystemen und zur Beschädigung von Archiv- und Speichermedien führen. Häufige Schwankungen der klimatischen Bedingungen verstärken diesen Effekt. Auch durch Sekundärschäden können derartige Klimabelastungen hervorgerufen werden. Ein Beispiel dafür ist die Ausdünstung von Wänden, die nach einem Brand im Nachbarraum auftreten kann.

- **Unzureichender physikalischer Schutz**

  Durch unzureichenden Schutz des Speicher- oder Archivsystems gegen unbefugten Zutritt und Zugriff können vorsätzliche Handlungen (z. B. Diebstahl, Manipulation oder Sabotage) begünstigt werden.

- **Unzureichender Schutz gegen sonstige Umgebungseinflüsse**

  Auch durch sonstige Umgebungseinflüsse (z. B. Erschütterungen oder eine hohe Staubbelastung) können Schäden an technischen Komponenten des Archivsystems oder an Speichermedien hervorgerufen werden. Besonders ärgerlich ist das, wenn die schädigenden Einflüsse sogar vorhersehbar waren, wie z. B. bei Bauarbeiten.

Beispiel:

Durch Ansiedlung des zentralen IT-Bereichs nahe an Produktionsanlagen kommt es dort gelegentlich zu Erschütterungen. Als Folge treten immer wieder Störungen in den technischen Komponenten des Archivsystems auf, das ebenfalls im IT-Bereich betrieben wird.

G 2.83 Fehlerhafte Outsourcing-Strategie

Die Entscheidung, ein Outsourcing-Vorhaben durchzuführen, ist eine weitreichende Entscheidung. Durch diese begibt sich ein Unternehmen oder eine Behörde in ein enges Abhängigkeitsverhältnis zu dem Outsourcing-Dienstleister. Daher haben diesbezügliche Fehlentscheidungen langfristige und schwerwiegende Folgen. Diese können organisatorische, technische und auch gravierende finanzielle Auswirkungen sein.

Sicherheitsprobleme (z. B. bei mangelhafter Verfügbarkeit) beim Outsourcing-Dienstleister können nicht nur teuer, sondern auch existenzbedrohend sein. Jedoch können auch Fehleinschätzungen der auslagernden Organisation gravierende Folgen haben. Wird beispielsweise der Aufwand (z. B. Erstellung von Dokumentationen, Tests, Absicherung von Systemen) unterschätzt, so sind zeitliche Verzögerungen zu erwarten. Um verlorene Zeit einzuholen und Geld zu sparen, wird erfahrungsgemäß häufig der Testaufwand reduziert, was zu Abstrichen bei der Sicherheit führen kann.

G 2.84 Unzulängliche vertragliche Regelungen mit einem externen Dienstleister

Wenn Situationen eintreten, die nicht eindeutig vertraglich geregelt sind, können (z. B. im Rahmen eines Outsourcing-Vorhabens) Nachteile für den Auftraggeber entstehen.

So kann beispielsweise ein Outsourcing-Auftraggeber für Sicherheitsmängel zur Verantwortung gezogen werden, die im Einflussbereich des Outsourcing-Dienstleisters liegen, aber vertraglich nicht eindeutig geregelt sind.

Ein Hauptgrund für Probleme zwischen den Vertragspartnern sind zu optimistische Kostenschätzungen. Wenn sich herausstellt, dass der Outsourcing-Dienstleister zu den kalkulierten und angebotenen Kosten die Dienstleistung nicht erbringen kann oder Uneinigkeit darüber besteht, was "selbstverständlich" ist, kann das direkt zu Sicherheitsproblemen führen. Erfahrungsgemäß wird an der IT-Sicherheit gespart, wenn in anderen Bereichen ein Kostendruck entsteht, dem so begegnet werden kann, ohne dass Folgen unmittelbar sichtbar werden. Der Ausgestaltung der vertraglichen Regelungen zwischen Auftraggeber und Auftragnehmer kommt daher eine entscheidende Bedeutung zu. Nur was von Anfang an vertraglich fixiert ist, wird auch später sicher in die Tat umgesetzt!

Weitere **Beispiele** für Folgen aus unzulänglichen vertraglichen Regelungen mit externen Dienstleistern sind:

- **Auskunftspflicht** Der Auftraggeber kann seiner Auskunftspflicht gegenüber Aufsichtsbehörden oder Wirtschaftsprüfern nicht nachkommen, wenn der Dienstleister keinen Zutritt zu seinen Räumlichkeiten oder keinen Zugang zu den notwendigen Unterlagen gewährt.
- **Gesetze** Der Auftraggeber muss sich für Verstöße gegen geltende Gesetze verantworten, wenn der Dienstleister nicht auf die Einhaltung dieser Gesetze verpflichtet wurde.
- **Missverständnisse** Aufgaben, Leistungsparameter und Aufwände wurden ungenügend oder missverständlich beschrieben, so dass aus Unkenntnis oder wegen fehlender Ressourcen Sicherheitsmaßnahmen nicht umgesetzt werden.
- **Anpassungen** Der Auftraggeber kann neuen Anforderungen (z. B. fachlich, gesetzliche Vorschriften, Verfügbarkeit, technische Entwicklung) nicht nachkommen, wenn Änderungsmanagement und Systemanpassungen nicht ausreichend vertraglich geregelt wurden.
- **Verantwortung** Bei Outsourcing-Vorhaben ist die Behörden- bzw. Unternehmensleitung des Auftraggebers unter Umständen voll verantwortlich für die ausgelagerten Geschäftsbereiche, kann dieser Verantwortung aber wegen fehlender Kontrollmöglichkeiten nicht gerecht werden.
- **Schutzbedarf** Ausgelagerte Daten oder Systeme werden ungenügend geschützt, wenn ihr Schutzbedarf dem Outsourcing-Dienstleister unbekannt ist.
- **Sanktionen** Die Dienstleistungsqualität ist schlecht, und es gibt keine Eingriffsmöglichkeiten, weil keine Sanktionen vertraglich festgelegt wurden.

- Der Dienstleister zieht qualifiziertes Personal ab oder Vertreter des Stammpersonals sind nicht ausreichend vorbereitet, was zu Sicherheitsproblemen führen kann. **Personal**

Besondere Probleme treten häufig dann auf, wenn Dienstleistungsverträge beendet werden (siehe G 2.85 *Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens*) und diese Situation nur unzureichend vertraglich geregelt wurde.

G 2.85 Unzureichende Regelungen für das Ende des Outsourcing-Vorhabens

Wird ein Outsourcing-Vorhaben durchgeführt, so kommt es in der Regel zu Know-how-Verlust beim Auftraggeber und zu einer Abhängigkeit des Auftraggebers vom Outsourcing-Dienstleister. Daher können unzureichende Regelungen für eine mögliche Kündigung des Vertragsverhältnisses gravierende Folgen für den Auftraggeber haben. Dies ist erfahrungsgemäß immer dann besonders problematisch, wenn ein aus Sicht des Auftraggebers kritischer Fall unerwartet eintritt, wie beispielsweise Insolvenz oder Verkauf des Outsourcing-Dienstleisters.

Beispiele:

- Ein Konkurrent des Auftraggebers kauft den Outsourcing-Dienstleister.
- Eine nationale Sicherheitsbehörde hat Prozesse zu einem Rechenzentrum ausgelagert, das später von einem ausländischen Unternehmen gekauft wird.
- Es gibt juristische Auseinandersetzungen zwischen Auftraggeber und Outsourcing-Dienstleister wegen schlechter Dienstleistungsqualität oder gravierender Sicherheitsmängel, in deren Folge ein Vertragspartner den Vertrag kündigen möchte.

Ohne ausreichende interne Vorsorge sowie genaue Vertragsregelungen besteht immer die Gefahr, dass sich der Auftraggeber nur schwer aus dem abgeschlossenen Vertrag mit dem Outsourcing-Dienstleister lösen kann. In diesem Fall ist es schwer bis unmöglich, den ausgelagerten Bereich beispielsweise auf einen anderen Dienstleister zu übertragen oder ihn wieder in das eigene Unternehmen einzugliedern, falls dies geboten erscheint.

Im Folgenden sind beispielhaft weitere Probleme aufgelistet, die in dieser Situation auftreten können:

- Durch unflexible Kündigungsrechtregelungen kann der Vertrag nicht im Sinne des Auftraggebers bedarfsgerecht beendet werden.
- Zu kurze Kündigungszeiten führen bei Kündigung durch den Dienstleister dazu, dass keine Zeit für einen geordneten Übergang bleibt.
- Unzureichende Regelungen über das Eigentumsrecht an eingesetzter Hard- und Software (Schnittstellenprogramme, Tools, Batchabläufe, Makros, Lizenzen, Backups) können einen geregelten Übergang, beispielsweise auf einen neuen Outsourcing-Dienstleister, verhindern.
- Unzureichende Regelungen über das Überlassen von Dokumentationen können dazu führen, dass die IT-Systeme nicht geregelt weiterbetrieben werden.
- Unzureichende Regelungen für das Löschen von Daten beim Outsourcing-Dienstleister können dazu führen, dass vertrauliche Daten Dritten bekannt werden.
- Der Auftraggeber kann seine Aufgaben unter Umständen nicht mehr erfüllen, da die Verfügbarkeit nicht mehr gewährleistet ist.
- In der Endphase des Auflösungsprozesses sind eventuell Daten und Systeme nicht mehr ausreichend geschützt, da diese als "Alt-Systeme" angesehen werden.

G 2.86 Abhängigkeit von einem Outsourcing-Dienstleister

Durch ein Outsourcing-Vorhaben gerät der Auftraggeber immer in die Abhängigkeit vom Outsourcing-Dienstleister. Daraus ergeben sich folgende typische Gefahren:

Know-how-Verlust

- Durch das Auslagern von Geschäftsprozessen geht intern das entsprechende Know-how verloren.
- Mitarbeiter des Auftraggebers verlassen das Unternehmen oder werden versetzt und nehmen ihr Know-how mit.

Kontrollverlust

- IT-Systeme und Ressourcen werden dem Outsourcing-Dienstleister überlassen, so dass über diese keine vollständige Kontrolle mehr besteht.
- Auftraggeber und Auftragnehmer schätzen den Schutzbedarf der ausgelagerten Informationen unterschiedlich ein, beispielsweise aufgrund von Missverständnissen in der Kommunikation oder einer anderen Sicherheitskultur. Damit können dann die ergriffenen Sicherheitsmaßnahmen unzureichend oder falsch gelagert sein.

Aus einer zu großen Abhängigkeit können sich außerdem folgende Konsequenzen ergeben, die es zu bedenken gilt:

Probleme bei Wechsel des Dienstleister

- Insourcing ist im Allgemeinen teuer und im Extremfall sogar unmöglich.
- Ein Wechsel des Dienstleisters ist im Allgemeinen schwierig und kann zu existenzbedrohenden Situationen (Verfügbarkeit, Kosten) führen.
- Auf Veränderung der Rahmenbedingungen (z. B. Eigentümerwechsel beim Outsourcing-Dienstleister, Änderung der Gesetzeslage, Zweifel an der Zuverlässigkeit des Outsourcing-Dienstleisters) kann unter Umständen nicht angemessen reagiert werden.

Erkennt der Outsourcing-Dienstleister eine große Abhängigkeit des Auftraggebers, so können sich zudem auch folgende Probleme ergeben:

- Der Dienstleister führt drastische Preiserhöhungen durch.
- Es kommt zu schlechter Dienstleistungsqualität.
- Die Drohung, die Dienstleistung sofort einzustellen, wird als Druckmittel (z. B. bei Kündigung des Vertrages oder bei Streitigkeiten) benutzt.

G 2.87 Verwendung unsicherer Protokolle in öffentlichen Netzen

Bei der Kommunikation über öffentliche Netze, insbesondere das Internet, existiert eine Reihe von Gefahren, die aus der Verwendung unsicherer Protokolle entstehen.

Vertraulichkeitsverlust übertragener Daten bei Klartextprotokollen

Eine wichtige Gefahr ist, dass vertrauliche Informationen in fremde Hände gelangen können. Als unsichere Protokolle müssen insbesondere solche Protokolle gelten, bei denen Informationen im Klartext übertragen werden. Da der Weg der Datenpakete im Internet nicht vorhersagbar ist, können in diesem Fall die übertragenen Informationen an verschiedensten Stellen mitgelesen werden. Besonders kritisch ist dies, wenn es sich um

- Authentisierungsdaten wie Benutzernamen und Passwörter,
- Autorisierungsdaten, beispielsweise Transaktionsnummern beim Electronic Banking oder Electronic Brokerage,
- andere vertrauliche Informationen, beispielsweise in Dokumenten, die per E-Mail verschickt werden, handelt.

Telnet, http, ftp, SMTP usw.

Protokolle, bei denen sämtliche Informationen im Klartext übertragen werden, sind beispielsweise

- das Hypertext Transfer Protocol *http*, das bei der Kommunikation zwischen Webbrowsern und Webservern verwendet wird,
- das *telnet* Protokoll, das noch an einigen Stellen für Remote Logins verwendet wird,
- das File Transfer Protocol *ftp*, das noch häufig für den Zugriff auf Server benutzt wird, die Dateien zum Download bereitstellen,
- das Simple Mail Transfer Protocol *smtp*, das zur Übertragung von E-Mail verwendet wird,
- die Protokolle *rsh* (Remote Shell), *rlogin* (Remote Login) und andere verwandte Protokolle.

Bei solchen Protokollen können sämtliche übertragenen Informationen auf jedem Rechner, über den eine entsprechende Verbindung läuft, mitgelesen und gegebenenfalls auch verändert werden. Kritisch ist beispielsweise die Übertragung von Kreditkartennummern oder Passwörtern über http-Verbindungen im WWW.

Mittels Password-Sniffings können in einem ersten Schritt Passwörter bei der Übertragung zu einem System abgefangen werden. Dies erlaubt dem Angreifer anschließend auf dieses IT-System zu gelangen, um dann weitere Angriffe lokal auf dem Rechner durchzuführen.

Man-in-the-middle Angriffe und Session Hijacking

Bei den erwähnten Protokollen (besonders bei *http* oder *telnet*) drohen auch sogenannte Man-in-the-middle-Angriffe oder Session Hijacking (siehe G 5.89 *Hijacking von Netz-Verbindungen*). Bei dieser Art von Angriffen ist ein Angreifer nicht nur dazu in der Lage, Informationen mitzulesen, sondern kann darüber hinaus aktiv Schaden anrichten, indem laufende Transaktionen

verändert werden. Beispielsweise können Preise oder Bestellmengen bei Geschäften über das Internet so verändert werden, dass der Besteller nur die Artikel oder Lieferadresse sieht und bestätigt bekommt, die er eingibt, während der Angreifer eine wesentlich höhere Menge und eine andere Lieferadresse an den Verkäufer schickt.

Neben den erwähnten Protokollen, bei denen sämtliche Informationen im Klartext übertragen werden, existieren auch solche, bei denen zumindest die Übertragung der Authentisierungsdaten verschlüsselt erfolgt. Dabei droht jedoch immer noch das Mitlesen der übertragenen Nutzinformation.

G 2.88 Störung des Betriebsklimas durch ein Outsourcing-Vorhaben

Outsourcing-Vorhaben haben je nach Art und Umfang nicht nur Auswirkungen auf die Geschäftsprozesse, sondern auch auf das Personal innerhalb eines Unternehmens oder einer Behörde. Dabei sind neben den vom Auftraggeber erwarteten Positiveffekten aus Sicht der Arbeitnehmer jedoch auch negative Effekte möglich. **Beispiele** dafür sind:

- Im Outsourcing-Bereich kann es zu einem Stellenabbau und damit verbunden zu Versetzungen oder Kündigungen von Mitarbeitern kommen.
- Durch die Auslagerung von Geschäftsvorfällen werden gewohnte Arbeitsprozesse geändert.
- Vor, während oder nach der Einführung eines Outsourcing-Vorhabens kann es zu hohen Arbeitsbelastungen kommen.
- Durch die Zusammenarbeit mit Mitarbeitern eines Outsourcing-Dienstleisters oder externen Beratern kann es erforderlich sein, dass einzelne Mitarbeiter Kompetenzen und Zuständigkeiten abgeben müssen. Genauso kann sich aber auch ergeben, dass Mitarbeiter neue Zuständigkeiten übernehmen müssen und sich dadurch überfordert fühlen.
- Durch Umstrukturierungen im Zusammenhang mit einem Outsourcing-Vorhaben kann es auch dazu kommen, dass Mitarbeiter den Arbeitgeber wechseln müssen (z. B. Übergang zu einer Tochterfirma oder Übernahme durch den Outsourcing-Dienstleister). Dabei kann der Mitarbeiter auch dazu gezwungen sein, schlechtere Bedingungen zu akzeptieren oder dies zumindest so empfinden.

Durch diese oder ähnlich Veränderungen kann das Betriebsklima nachhaltig gestört werden. Mögliche Gefährdungspotenziale sind unter anderem:

- Mitarbeiter oder ehemalige Mitarbeiter können Racheakte verüben. **vorsätzliche Handlungen**
- Die Mitarbeiter sind schlecht motiviert und vernachlässigen unabsichtlich oder mutwillig Pflichten, insbesondere Sicherheitsmaßnahmen. **Pflichtverletzung**
- Know-how-Träger (wie beispielsweise IT-Leiter und Administratoren) können während der Einführungsphase kündigen. In Folge könnte dadurch das Outsourcing-Vorhaben nicht bedarfsgerecht oder gar nicht umgesetzt werden, was wiederum existenzbedrohend sein kann. Oftmals ist der Outsourcing-Dienstleister sogar darauf angewiesen, dass die entscheidenden Know-how-Träger geordnet zu ihm wechseln. **Know-how-Verlust**

G 2.89 Mangelhafte IT-Sicherheit in der Outsourcing-Einführungsphase

Ein Outsourcing-Vorhaben wird in der Regel in mehreren Schritten umgesetzt. Die Einführungsphase geht meist mit drastischen internen Veränderungen auf Seiten des Auftraggebers einher. Zusätzlich wird ein Outsourcing-Vorhaben von stringenten terminlichen und finanziellen Randbedingungen begleitet. Oft bleibt keine Zeit für regelmäßige Sicherheitskontrollen und Audits. Um Termine und Budgets während der Einführungsphase einzuhalten, leidet oftmals die Arbeitsqualität und Sicherheitskonzepte werden vernachlässigt. Dies hat jedoch gravierenden Einfluss auf die IT-Sicherheit. Mögliche weitere Gefährdungen der IT-Sicherheit sind unter anderem:

Nichts hält länger als Zwischenlösungen!

- Der Betrieb von Übergangslösungen erfolgt unter geringen Sicherheitsstandards. Dabei wird häufig argumentiert: "Hauptsache, es läuft!" Oft werden solche Übergangslösungen dann jedoch aus verschiedenen Gründen auf Jahre hin weiterbetrieben.
- Aus Zeit- und Ressourcengründen werden "Altsysteme" vernachlässigt, während an den neuen Systemen gearbeitet wird.

Ausgelöst durch die hohe Arbeitsbelastung und den Zeitdruck werden die Probleme durch bewusste oder unbewusste Nachlässigkeiten oder Fehler verstärkt. Gründe können sein:

- Während der Einführungsphase muss ein Parallelbetrieb der von der Auslagerung betroffenen Systeme erfolgen.
- Durch die Anbindung an den Outsourcing-Dienstleister entstehen viele neue organisatorische und technische Schnittstellen.
- Mitarbeiter müssen in neue Aufgaben eingearbeitet werden, so dass zusätzlich Ressourcen gebunden sind.
- Ein Outsourcing-Vorhaben geht einher mit dem Einsatz neuer Soft- und Hardware. Gefahren resultieren dabei aus fehlerhaften oder gänzlich fehlenden Tests, aus Unerfahrenheit mit neuen Sicherheitsmechanismen, aus Installations- und Administrationsfehlern oder aber aus Softwarefehlern.

IT-Sicherheitsmängel können sich jedoch auch aus organisatorischen Schwächen während der Einführungsphase ergeben. Die Gründe können beispielsweise folgende sein:

Anlaufschwierigkeiten bei der Kommunikation

- Die Zusammenarbeit zwischen den Mitarbeitern des Auftraggebers und denen des Outsourcing-Dienstleister oder externer Berater funktioniert nicht richtig. Ursachen können etwa Kommunikationsprobleme technischer oder persönlicher Art sein. Da am Anfang auch die Ansprechpartner der Gegenseite noch unbekannt sind, können in dieser Phase außerdem Angriffe über "Social Engineering" besonders leicht erfolgreich sein.
- Entscheidungshierarchien funktionieren noch nicht oder Ansprechpartner und Zuständigkeiten sind noch nicht geklärt oder wechseln häufig. Als Folge werden Entscheidungen gar nicht oder nur sehr zögerlich getroffen. Das führt dann unter Umständen dazu, dass Sicherheitsvorschriften nicht eingehalten, umgangen oder nicht kontrolliert werden.

Diese Gesamtproblematik führte beispielsweise auch für ein namhaftes Finanzinstitut zu Problemen: Während an der Einrichtung eines neuen Webservers gearbeitet wurde, wurde das "Altsystem" nicht mehr ausreichend gewartet und war Ziel eines Angriffes, bei dem Kundendaten kompromittiert wurden. Das Ereignis wurde durch die Medien einem Millionenpublikum bekannt gemacht.

G 2.90 Schwachstellen bei der Anbindung an einen Outsourcing-Dienstleister

Die Durchführung eines Outsourcing-Vorhabens verlangt in aller Regel den Zugriff des Dienstleisters auf interne Ressourcen des Auftraggebers. Dies wird häufig durch eine gegenseitige Anbindung von Teilen der jeweiligen IT-Infrastruktur realisiert. Zum beschleunigten Informationsaustausch zwischen Auftraggeber und Auftragnehmer werden möglicherweise spezielle Informationskanäle (z. B. dedizierte Standleitungen, VPN-Verbindungen, Zugänge für die Remote-Wartung) eingerichtet.

Ist diese Anbindung nicht gesichert oder treten bei der Absicherung Schwachstellen auf, so ergeben sich zwangsläufig eine Reihe von Gefährdungen:

- Die Vertraulichkeit der Kommunikation kann gefährdet sein.
- Die Integrität von übermittelten Datensätzen ist nicht mehr garantiert.
- Der Empfang von übermittelten Informationen und Nachrichten könnte abgestritten werden.
- Es wird Externen ein für die tatsächlichen Bedürfnisse des Dienstleisters zu umfassender Einblick in Interna des Auftraggebers gegeben.
- Es entstehen zusätzliche Zugangsmöglichkeiten für Außenstehende zum Intranet der Organisation und damit Gefahrenquellen.
- Bei offenen oder schlecht gesicherten IT-Zugängen ergeben sich Manipulationsmöglichkeiten.
- Es könnten vertrauliche Informationen und geistiges Eigentum an Außenstehende weitergegeben werden.
- Externe Systemzugriffe werden unter Umständen nicht ausreichend kontrolliert.

Die IT-Anbindung zwischen auslagernder Organisation und Outsourcing-Dienstleister kann auch komplett ausfallen. Dabei können Daten, deren Übertragung vor dem Ausfall noch nicht vollständig abgeschlossen war, zerstört oder inkonsistent werden. In Abhängigkeit von der Dauer und Art des Ausfalles können die Konsequenzen auch existenzbedrohend sein. Diese Gefahr wird verstärkt, wenn kein Notfallvorsorgekonzept (siehe G 2.93 *Unzureichendes Notfallvorsorgekonzept beim Outsourcing*) existiert.

G 2.91 Fehlerhafte Planung der Migration von Exchange 5.5 nach Exchange 2000

Häufiger als eine Neuinstallation eines Exchange 2000 E-Mail-Systems ist in der Praxis die Migration einer bestehenden Exchange 5.5 Installation nach Exchange 2000. In vielen Fällen ist diese Umstellung verbunden mit einem Betriebssystemwechsel von Windows NT nach Windows 2000. Für den Betrieb eines Exchange 2000 Servers ist dieser Betriebssystemwechsel sogar Voraussetzung.

Mit dem Betriebssystemwechsel ist auch eine Umstellung des NT-Domänenkonzeptes auf den Verzeichnisdienst Active Directory von Windows 2000 erforderlich. Dies ist eine planerische und organisatorische Herausforderung, die speziell aus Sicherheitssicht eine sorgfältige Einarbeitung und eine grundlegende Neuplanung verlangt (siehe M 2.249 *Planung der Migration von "Exchange 5.5-Servern" nach "Exchange 2000"*).

Folgende Sicherheitsprobleme können bei einer fehlerhaften Planung der Migration auftreten:

- Die Konfigurationen einer *NT-Domäne* könnte falsch oder inkonsistent in das *Active Directory* von Windows 2000 abgebildet werden, da dies eine vollständige Neukonzeption der bisherigen Infrastruktur umfasst. Weiterhin könnte eine fehlerhafte Anbindung an das Active Directory zur Folge haben, dass die Systemrichtlinien von Windows 2000 und die *Access Control Lists* (ACL) nicht wirksam sind. **Domänen**
- Eine oder mehrere Exchange 5.5 *Site(s)* könnten unzulänglich auf eine Exchange 2000 *Routing Group* abgebildet werden, da dies unter Umständen eine Umstrukturierung der Exchange-Server bedeutet. Die Gefahr besteht hier in erster Linie in einem Funktionsausfall durch fehlerhafte Protokolleinstellungen oder sonstige Fehlkonfigurationen. **Sites**
- Unter Umständen wird die Administration des Systems unsachgemäß geplant und die Administrationsgrenzen unklar definiert, da sich die Administrationsgrenzen durch Einführung der Administrationsgruppen in Exchange 2000 im Vergleich zu Exchange 5.5 ändern können. Die Administratorrolle unter Exchange 5.5 existiert in Exchange 2000 nicht mehr und es müssen entsprechende Domänenbenutzer konfiguriert werden. Wird für diese Benutzergruppe die Rechtevergabe falsch geplant, so kann dies zu Sicherheitslücken oder auch zur Behinderung der Administration des Systems führen. **Rollen und Gruppen**
- Die geforderten organisationsweiten Sicherheitsrichtlinien könnten durch eine falsche Planung der Migration der Sicherheitseinstellungen ungenügend umgesetzt werden. Dies betrifft sowohl die Zugriffsmöglichkeiten auf den Server an sich als auch auf die dort gespeicherten Daten. **Richtlinien**
- Daten und Informationen könnten bei der Migration verloren gehen, besonders wenn das System während der Migrationsphase abstürzt. **Datenverlust**
- Durch notwendige Nachbesserungen der Konfiguration an den Produktivsystemen könnte sich ein Produktivitätsausfall ergeben. **Ausfall**

G 2.92 Fehlerhafte Regelungen für den Browser-Zugriff auf Exchange

WebDAV

Exchange 2000 bietet - wie auch schon Exchange 5.5 - die Möglichkeit, über einen Browser auf das eigene E-Mail-Konto zuzugreifen. Neu in Exchange 2000 ist dabei die Unterstützung des *WebDAV*-Protokolls, das auf HTTP aufsetzt. Dadurch kann auf das *Installable File System* (IFS) zugegriffen werden und damit wird die Funktionalität des *Web Store* und der *Web Forms* unterstützt. Hierzu werden die *Internet Information Services* (IIS) verwendet, die fester Bestandteil der Installation von Exchange 2000 Server sind.

Grundsätzlich besteht die Gefahr, dass es bei unsachgemäßer Planung und fehlerhaften Regelungen für diese Funktionalität möglich wird, unkontrolliert von außen auf das interne Netz zuzugreifen.

schwache Authentisierung und Verschlüsselung

Fehlkonfigurationen betreffen in erster Linie die Authentisierung des Webclients gegenüber dem Exchange 2000 Server sowie die geschützte Übertragung der Informationen über das IP-Netz. Sind die geforderten Authentisierungsmethoden zu schwach, so können unter Umständen Unbefugte auf E-Mail-Daten und Systemressourcen zugreifen. Sind die eingesetzten Verschlüsselungsmechanismen nicht hinreichend stark, so besteht die Gefahr, dass Daten abgehört werden. Bei nicht ausreichenden Authentisierungs- und Verschlüsselungsmechanismen können bestehende Verbindungen unter Umständen durch unbefugte Dritte übernommen werden. Weiterhin besteht die Gefahr, dass über den OWA-Kanal Viren oder anderer schädlicher Code auf den E-Mail-Server gelangen.

Das Gefahrenpotential ist darüber hinaus vielfältig. Beispiele für weitere mögliche Folgen sind:

- E-Mail-Adressen könnten ausgespäht werden.
- Unbefugte könnten Zugriff auf E-Mail-Funktionen erlangen.
- Spam-Attacken könnten ermöglicht werden.
- Unbefugte könnten interne Informationen über das Unternehmen bzw. die Behörde erlangen.
- Es könnten sich direkte Angriffsmöglichkeiten auf das interne Netz ergeben.

G 2.93 Unzureichendes Notfallvorsorgekonzept beim Outsourcing

Versäumnisse im Bereich der Notfallvorsorge haben beim Outsourcing schnell gravierende Folgen. Zusätzliche Schwierigkeiten ergeben sich dadurch, dass Probleme generell auf drei kritische Bereiche verteilt sein können. Es sind dies:

unterschiedliche Zuständigkeiten

1. IT-Systeme beim Auftraggeber
2. IT-Systeme beim Outsourcing-Dienstleister
3. Schnittstellen (z. B. Netzverbindung, Router, Telekommunikations-Provider) zwischen Auftraggeber und Dienstleister

Im Falle eines Fehlers muss dieser zunächst korrekt lokalisiert werden, was je nach Fehlerart schwierig ist, da unterschiedliche Fehler zu gleichen Symptomen führen können, z. B. Ausfall der Kommunikationsverbindung und Ausfall eines Systems beim Dienstleister. Erst nachdem der Fehler identifiziert worden ist, können sinnvolle Notfallmaßnahmen eingeleitet werden.

Versäumnisse bei den Notfallvorsorgekonzepten für die IT-Systeme von Auftraggeber bzw. Dienstleister sowie der Schnittstellen führen im Falle eines Teil- oder Totalausfalls immer zu unnötig langen Ausfallzeiten mit entsprechenden Folgen für die Produktivität bzw. Dienstleistung des Auftraggebers.

G 2.94 Unzureichende Planung des IIS-Einsatzes

Der IIS bietet vielfältige Einsatzmöglichkeiten, z. B. als einfacher Informationsserver im Intranet. Auch als Basis für komplexe Webanwendungen im Internet ist der IIS geeignet. Aus diesen Einsatzumgebungen resultieren unterschiedliche Anforderungen an die Sicherheit des IIS. Die Absicherung eines aus dem Internet erreichbaren Servers ist in der Regel mit einem viel höheren Aufwand verbunden als die Absicherung eines Servers im LAN, auf den nur vertrauenswürdige Benutzer zugreifen.

Erfolgt vor der Installation keine ausreichende Planung, z. B. in welche Systemumgebung der Server einzubinden ist, welche Protokolle verwendet werden und wie der Zugriff (Authentisierung) geregelt wird, besteht die Gefahr, dass bestehende Risiken nicht berücksichtigt werden.

Die Verfügbarkeit und Performance sind für den Erfolg eines Internet-Angebots von entscheidender Bedeutung. Lange Wartezeiten werden von keinem Anwender auf Dauer akzeptiert, deshalb muss ein Internet-Server ständig verfügbar und seine Reaktionszeit möglichst kurz sein. Bei unzureichender Ressourcenplanung, die Netzkapazitäten und Systemressourcen berücksichtigen muss, kann die Akzeptanz der Benutzer für eine Web-Seite sinken.

G 2.95 Fehlendes Konzept zur Anbindung anderer E-Mail-Systeme an Exchange/Outlook

Gegebene IT-Landschaften sind meist heterogen, sowohl in Bezug auf die verwendeten Betriebssysteme als auch in Bezug auf die Anwendungen. Dies spiegelt häufig die Historie des Wachsens und Zusammenwachsens der Organisationsstruktur im Unternehmen bzw. in der Behörde wider.

Connectors

Exchange 2000 ist eng mit dem Betriebssystem Windows 2000 verzahnt und harmoniert nur mühsam mit Fremdsystemen. Zur Interaktion mit anderen E-Mail-Systemen bietet Exchange 2000 sogenannte *Connectors* an, mit denen sich das Exchange-System mit Fremdsystemen verbinden lässt.

Aus Sicherheitssicht besteht die Gefahr, dass unter Windows 2000 getroffene Sicherheitseinstellungen, die sich auf das Exchange 2000 E-Mail-System beziehen, außerhalb des homogenen Microsoft-Umfeldes keine Gültigkeit haben.

Inkonsistenzen

Ebenso besteht natürlich auch umgekehrt die Gefahr, dass die festgelegten Sicherheitsrichtlinien der Fremdsysteme keine Gültigkeit für das Exchange 2000 System haben. Bei der separaten Administration verschiedener Teilsysteme können stets Inkonsistenzen auftreten.

Eine unsachgemäße Anbindung fremder E-Mail-Systeme kann zudem den Verlust von Daten oder eine Blockade des Systems zur Folge haben.

G 2.96 Veraltete oder falsche Informationen in einem Webangebot

Die Korrektheit und Aktualität der Informationen, die eine Organisation in einem Webangebot veröffentlicht, hat nicht nur Einfluss auf den Erfolg des Webangebots alleine. Werden im WWW falsche Informationen veröffentlicht, so kann das Ansehen der Organisation in der Öffentlichkeit empfindlichen Schaden nehmen.

In manchen Fällen drohen auch finanzielle Verluste oder rechtliche Konsequenzen (beispielsweise Abmahnungen), wenn falsche Informationen veröffentlicht werden. Noch schlimmer können die Auswirkungen sein, wenn irrtümlich interne (vertrauliche oder gar geheime) Informationen auf den Webserver gelangen, die eigentlich gar nicht veröffentlicht werden dürften.

Selbst dann, wenn bestimmte Informationen auf dem Webserver nur veraltet sind, kann dies nachteilige Auswirkungen haben. Wenn beispielsweise veraltete Kontaktinformationen veröffentlicht werden, kann dies zu einer Störung der betroffenen Geschäftsprozesse führen.

Beispiel:

- Im Jahr 2002 fanden Reporter auf dem Webserver eines schwedischen Unternehmens eine Datei mit einem Quartalsbericht dieses Unternehmens, der erst einige Tage später hätte veröffentlicht werden sollen. Dies führte unter anderem zu zeitweiligen Kursverlusten der Aktien des Unternehmens.

G 2.97 Unzureichende Notfallplanung bei einem Apache-Webserver

Eine unzureichende Planung für Notfälle kann Probleme, die beim Betrieb eines Apache-Webservers auftreten, wesentlich verschlimmern und Ausfallzeiten verlängern.

Zusätzlich zu allgemeinen Fehlern, die oft im Bereich Notfallvorsorge gemacht werden, können bei einem Apache-Webserver einige spezielle Fehler passieren, die eine schnelle Reaktion auf Zwischenfälle sehr erschweren oder gar unmöglich machen können. Einige dieser Fehler werden im folgenden beschrieben.

- **Nicht vorhandene Installationspakete**
  Wird nach einem Notfall (etwa einem Hackereinbruch) eine Neuinstallation eines Apache-Webservers nötig, so kann es zu erheblichen Verzögerungen führen, wenn die bei der Installation verwendeten Pakete (Quelltexte oder Distributionspakete) nicht mehr verfügbar sind. Sind die Installationspakete zwar verfügbar, aber beispielsweise auf dem Webserverrechner selbst und nicht auf einem anderen Rechner oder einem schreibgeschützten Datenträger gespeichert, so müssen sie nach einem Hackereinbruch als unsicher angesehen werden.

- **Nicht dokumentierte Installationsoptionen und -prozeduren**
  Ist nicht bekannt, mit welchen Kompilierungs- und Installationsoptionen der Apache-Webserver installiert wurde, so kann es sehr schwierig sein, wieder eine funktionell gleichwertige Installation herzustellen. Dies gilt besonders dann, wenn beispielsweise externe Module bei der Übersetzung eingebunden wurden.

- **Undokumentierte oder schlecht dokumentierte Konfiguration**
  Existiert keine oder nur eine unzureichende Dokumentation der Konfiguration, so kann es sehr schwierig sein, nach einem Notfall überhaupt wieder eine funktionierende Konfiguration herzustellen. Schlechte Dokumentation kann auch dazu führen, dass Konfigurationsfehler zunächst nicht entdeckt werden und bei auftretenden Problemen eine aufwendige Fehlersuche erforderlich wird.

- **Fehlende Versionsverwaltung für Konfigurationsdateien**
  Bei der Systemwiederherstellung nach einem Notfall kann es wünschenswert sein, einen älteren Stand der Konfiguration wieder herzustellen. Wird für die Konfigurationsdateien (insbesondere die Datei *httpd.conf*) keine Versionsverwaltung durchgeführt, so kann dies schwierig oder gar unmöglich sein.

G 2.98 Fehlerhafte Planung und Konzeption des Einsatzes von Routern und Switches

Bei der Planung des Einsatzes aktiver Netzkomponenten stehen meistens die Aspekte Funktionalität und Leistungsfähigkeit im Vordergrund. Wenn der Betrieb von Routern und Switches, als zentrale Elemente in Netzen, nicht in das unternehmensweite Sicherheitskonzept eingebunden wird, kann der sichere Einsatz dieser Komponenten nicht sichergestellt werden.

Die Fehler bei der Planung des Einsatzes von Routern und Switches fallen meist in eine der folgenden Kategorien:

Unzureichende Berücksichtigung des Einsatzzwecks der Geräte

Bei der Planung des Einsatzes von Routern und Switches ist in erster Linie der Einsatzzweck dieser Komponenten entscheidend. Oft wird der Einsatzzweck der Komponenten bei der Planung nicht ausreichend berücksichtigt, beispielsweise beim Einsatz von VLANs. Entgegen öfters gehörter Werbeaussagen wurden VLANs nicht entwickelt, um Sicherheitsanforderungen bei der Trennung von Netzen zu erfüllen. VLANs bieten eine Vielzahl von Angriffspunkten, so dass insbesondere für die Trennung von schutzbedürftigen Netzen immer zusätzliche Maßnahmen umzusetzen sind.

Auch bei der Planung des Einsatzes von Routing-Protokollen können Fehler gemacht werden. Wenn Router im Bereich von demilitarisierten Zonen (DMZs) eingesetzt werden kann die Verwendung von dynamischen Routing-Protokollen die Verfügbarkeit, Vertraulichkeit und die Integrität des zu schützenden Netzes gefährden.

Unzureichende Berücksichtigung von Sicherheitsmechanismen

Bei der Planung werden oft die vorhandenen Sicherheitsmechanismen (sowohl im bestehenden Netz als auch bei den Netzkomponenten, deren Einsatz geplant wird) nicht ausreichend berücksichtigt. Beispielsweise können zusätzliche Maßnahmen erforderlich werden, falls ein Gerät bestimmte Sicherheitsmechanismen nicht unterstützt. Wenn dies nicht bereits in der Planungsphase berücksichtigt wird, kann es später zu Problemen führen, wenn die Notwendigkeit erkannt wird.

Ein wichtiger Punkt, der beispielsweise bei der Planung oft nicht berücksichtigt wird, ist die Einrichtung eines gesonderten Administrationsnetzes (Out-of-Band Management). Falls die gewählten oder vorhandenen Geräte nur unsichere Protokolle wie SNMPv1, SNMPv2 oder Telnet unterstützen, so ist die Einrichtung eines Administrationsnetzes unbedingt erforderlich. Dies wird in vielen Fällen nicht beachtet, mit der Folge, dass später unter Umständen die Einrichtung des Administrationsnetzes auf Schwierigkeiten stößt, weil die notwendigen Anschlüsse nicht vorhanden sind.

Fehlende oder mangelhafte Information und Dokumentation

Gelegentlich sind in der Planungsphase notwendige Informationen nicht vorhanden, da entweder keine entsprechende Dokumentation vom Anbieter zur Verfügung gestellt wurde oder die betreffenden Dokumente nicht berücksichtigt werden. Fehlentscheidungen, die auf Grund mangelhafter Dokumentation gemacht wurden, sind oft nur schwer zu korrigieren, wenn sich beispielsweise später herausstellt, dass ein Gerät bestimmte Funktionen nicht oder nur unzureichend unterstützt.

G 2.99 Unzureichende oder fehlerhafte Konfiguration der zSeries-Systemumgebung

Das Ressourcenangebot der zSeries-Architektur gestattet den Betrieb mehrerer Produktions- und Testsysteme auf einem physischen Rechner. Daraus resultiert ein hohes Gefahrenpotential, weil eine fehlerhafte Abgrenzung der zSeries-Systemumgebungen unter Umständen den ungewollten Zugriff auf fremde Ressourcen ermöglicht.

Shared DASD (Direct Access Storage Device)

- Im LPAR-Betrieb ist es möglich, die Platten eines z/OS-Betriebssystems so zu konfigurieren, dass sie durch alle z/OS-Systeme des Rechners verwendet werden können (durch Konfiguration entsprechender Subchannel-Adressen über den *Host Configuration Definition Prozess*). Damit verbunden ist die Gefahr, dass die Datentrennung zwischen den LPARs nicht mehr gewährleistet ist.
- Es ist möglich, Platten einer LPAR1 an einer anderen LPAR2 *Online* zu setzen. Die Daten der neuen Platte stehen dann an der LPAR2 zur Verfügung und können entsprechend den RACF-Definitionen dieser LPAR2 bearbeitet werden. Sind die RACF-Definitionen der LPAR2 schwächer als die der LPAR1, können die Daten unter Umständen unbefugt manipuliert oder gelesen werden.

Unsachgemäße Trennung Test-Produktion

Sicherheitsprobleme können auch durch eine unsachgemäße Trennung von Test- und Produktionsumgebungen entstehen. Werden Test und Produktion auf unterschiedlichen LPARs (noch besser unterschiedlichen zSeries Systemen) betrieben, ist die Abgrenzung leichter zu realisieren. Der Betrieb von Test und Produktion auf der gleichen LPAR ist prinzipiell möglich (hier sollte auf jeden Fall die Gefährdung G 3.70 *Unzureichender Dateischutz des z/OS-Systems* beachtet werden), jedoch ist die Trennung hierbei ungleich schwieriger. Werden die Umgebungen nicht richtig voneinander abgegrenzt, so ist es möglich, dass Testdaten in die Produktion gelangen bzw. Produktionsdaten zum Testen verwendet werden. Beides beinhaltet ein hohes Gefahrenpotential.

Beispiel:

- Ein Outsourcing-Dienstleister betrieb in seinem Rechenzentrum die Anwendungen von zwei konkurrierenden Unternehmen aus dem Bereich der Automobilindustrie auf dem gleichen z/OS-System. Aufgrund einer unsicheren Konfiguration war es dem Kunden B möglich, Platten des Kunden A online zu nehmen. Kunde B nutzte dies aus, um sich durch Ausspähen der Daten Wettbewerbsvorteile gegenüber dem Kunden A zu verschaffen.

G 2.100 Fehler bei der Beantragung und Verwaltung von Internet-Domainnamen

Internet-Domainnamen (meist einfach kurz "Domains" genannt) können nicht beliebig gewählt werden, sondern müssen bei Registrierungsstellen (*Registrars*) angemeldet werden. Eine Registrierungsstelle kann Namen für eine oder mehrere sogenannte "Top-Level-Domains" vergeben (beispielsweise verwaltet die DeNIC GmbH die Top-Level-Domain *.de*). Domains werden nicht "gekauft", sondern nur jeweils für einen bestimmten Zeitraum registriert. Ist dieser Zeitraum abgelaufen, so muss die Registrierung gegen Zahlung einer Gebühr verlängert werden. Im Zusammenhang mit der Registrierung und dem Verlängern der Registrierung von Domainnamen werden häufig Fehler gemacht, die gegebenenfalls erhebliche Kosten und einen Ansehensverlust der Institution zur Folge haben können. Einige dieser Fehler werden im folgenden kurz erläutert:

Nichtberücksichtigung "verwandter" Domainnamen

Oft wird nur der "richtige" Domainname, den die Organisation wirklich benutzen möchte (etwa *firmenname.de*), registriert. Dabei wird übersehen, dass "verwandte" Domainnamen (bspw. *firmenname.com* oder *firmenname.info*) von Internetbenutzern, welche die "richtige" Domain der Firma noch nicht kennen, einfach ausprobiert werden.

Domain-Grabber

Es kommt häufig vor, dass "verwandte" Domainnamen von unseriösen Anbietern registriert werden, die unter dem Namen dann beispielsweise Websites mit pornographischen Inhalten betreiben. Zwar können solche Angebote oft gerichtlich untersagt und abgeschaltet werden, da aber ein solcher Prozess oft längere Zeit dauert, kann inzwischen das Ansehen der Organisation beträchtlichen Schaden nehmen.

Beispielsweise musste eine deutsche Universität im Jahr 2000 gerichtlich gegen einen Pornoanbieter vorgehen, der den "*com*-Domainnamen" der Universität benutzte. Im Jahr 2004 gelang es einem Jugendlichen, sich durch Ausnutzung eines "Verfahrensfehlers" für kurze Zeit die deutsche Domain eines Online-Auktionshauses übertragen zu lassen, was für ziemliches Aufsehen in der Presse sorgte.

Diebstahl von Zugangsdaten und Kreditkarten-informationen

Schlimmere Folgen als nur einen Imageschaden kann es haben, wenn Betrüger einen "verwandten" Domainnamen dazu benutzen, um dort einen Webauftritt aufzubauen, der dem echten Webauftritt täuschend ähnlich sieht und der arglose Besucher dazu verleitet, dort Zugangsdaten für den echten Webauftritt oder Kreditkarteninformationen für Bezahlvorgänge einzugeben. Die Betrüger benutzen diese Daten dann, um sich Zugang zum echten Webserver zu verschaffen oder mit den gestohlenen Kreditkarteninformationen einzukaufen. Solche Vorfälle wurden bereits mehrfach bekannt.

Verletzung von Markenrechten

Bei der Registrierung von Domainnamen wird oft nicht geprüft, ob der gewählte Name nicht registrierte Markennamen anderer Firmen verletzt. Solche Markenrechtsverletzungen werden meist prompt bemerkt. Marken-inhaber oder auf Abmahnungen spezialisierte Anwälte bzw. Organisationen recherchieren regelmäßig nach neuen Domains, die eventuell Markenrechte

verletzen und schicken meist kostenpflichtige Abmahnungen. Zusätzlich kann der Inhaber einer Marke gerichtlich die Rückgabe oder Löschung der Domain verlangen. Dies kann neben erheblichen Kosten auch erhebliche Imageschäden nach sich ziehen.

Fehler bei der Verlängerung von Domainnamen und beim Wechsel der Registrierungsstelle

Domainnamen müssen regelmäßig gegen Zahlung einer Verwaltungsgebühr beim zuständigen Registrar "verlängert" werden. Wird die Gebühr nicht rechtzeitig bezahlt, so geht das Recht an dem Domainnamen verloren und andere Organisationen können den Domainnamen registrieren. Ist der betreffende Domainname nicht firmenspezifisch, so gibt es schlimmstenfalls keine Möglichkeit, die verlorene Domain zurück zu erhalten. Der zusätzliche Imageschaden, der eventuell dadurch entsteht, dass eine derart "verwaiste" Domain womöglich von einem Pornoanbieter oder einer radikalen Organisation registriert wird, die von dort aus denn anstößige oder gar illegale Inhalte verbreiten, kann in diesem Fall erheblich sein.

Nepper, Schlepper, Bauernfänger

Es ist auch vorgekommen, dass weniger seriöse Registrierungsstellen Kunden ihrer Konkurrenten anriefen und behaupteten, die Registrierung sei abgelaufen und müsste gegen eine erneute Zahlung an sie erneuert werden. Wenn dadurch überraschte Kunden dann die Gebühr an die betreffende Stelle bezahlten, vollzogen sie gleichzeitig einen Wechsel der Registrierungsstelle.

Fehlerhafte Anordnung der *Primary Nameserver*

Bei der Registrierung eines Domainnamens müssen mindestens zwei Nameserver angegeben werden, die als *Primary Nameserver* für diese Domain agieren. Falls diese beiden Nameserver in demselben Netzsegment angesiedelt sind, so kann durch einen Ausfall des Netzkoppelelements, das dieses Netzsegment mit dem Internet verbindet, die Namensauflösung für die komplette Domain lahmgelegt werden. Dies führt letztlich dazu, dass auf keinen der unter dem Domainnamen angebotenen Dienste wie Webserver oder E-Mail mehr zugegriffen werden kann.

Beispielsweise wurde im Jahr 2001 die Domain eines großen Softwarehauses durch einen DDoS (Distributed Denial of Service) Angriff auf den Router, der die Primary Name Server für die Domain mit dem Internet verband, für mehrere Stunden praktisch komplett lahmgelegt. Als Reaktion auf diesen Angriff wurden die Nameserver in verschiedene Netzsegmente verlegt.

G 2.101 Unzureichende Notfallvorsorge bei einem Sicherheitsgateway

Eine unzureichende Planung für Notfälle kann Probleme, die beim Betrieb eines Sicherheitsgateways auftreten, wesentlich verschlimmern und Ausfallzeiten verlängern.

Zusätzlich zu allgemeinen Fehlern, die oft im Bereich Notfallvorsorge gemacht werden, können bei einem Sicherheitsgateway einige spezielle Fehler gemacht werden, die eine schnelle Reaktion auf Zwischenfälle sehr erschweren oder gar unmöglich machen können. Einige dieser Fehler werden im folgenden beschrieben.

- Existieren keine Planungen für das Vorgehen bei Notfällen und keine entsprechenden Handlungsanweisungen, so ist eine effiziente Reaktion meist überhaupt nicht möglich. Bei komplexen Systemen wie mehrstufigen Sicherheitsgateways kann es zu zusätzlichen Problemen kommen, wenn Abhängigkeiten zwischen einzelnen Komponenten nicht bekannt oder nicht dokumentiert sind, oder wenn sie bei der Planung nicht korrekt berücksichtigt werden.
- Sind für wichtige Hardwarekomponenten keine Austauschteile beziehungsweise -geräte verfügbar und sind mit den Herstellern oder Lieferanten keine entsprechenden Vereinbarungen (beispielsweise Service-Level-Agreements oder Vor-Ort-Austausch innerhalb eines garantierten Zeitraums) getroffen, so kann dies zu erheblichen Ausfallzeiten und Kosten führen.
- Existiert keine oder nur eine unzureichende Dokumentation der Konfiguration und der wichtigsten Betriebsparameter, so kann es sehr schwierig sein, nach einem Notfall überhaupt wieder eine funktionierende Konfiguration herzustellen. Schlechte Dokumentation kann auch dazu führen, dass Konfigurationsfehler zunächst nicht entdeckt werden und bei auftretenden Problemen eine aufwendige Fehlersuche erforderlich wird.
- Sind die für eine Fehlerdiagnose benötigten Werkzeuge und Programme nicht verfügbar oder sind die Administratoren nicht in der Lage, diese richtig einzusetzen, so kann dies zu erheblichen Verzögerungen führen.
- Werden wichtige Daten bei der Protokollierung nicht erfasst, so kann dies die korrekte Einschätzung von Art und Schwere eines Vorfalls erschweren oder unmöglich machen.
- Bei der Systemwiederherstellung nach einem Notfall kann es wünschenswert sein, einen älteren Stand der Konfiguration wieder herzustellen. Wird für die Konfigurationsdaten (insbesondere die Paketfilterregeln) keine Versionsverwaltung durchgeführt, so kann dies schwierig oder gar unmöglich sein.

G 2.102 Unzureichende Sensibilisierung für IT-Sicherheit

Die Aktivitäten zur Sensibilisierung für IT-Sicherheitsfragen müssen sich an der IT-Umgebung der jeweiligen Institution orientieren, um auch die richtigen Bereiche zu adressieren. Dadurch muss unter Umständen eine Vielzahl von Themengebieten angesprochen werden. Hierfür müssen die Schulungsaktivitäten sorgfältig geplant und organisiert werden. Die Erfahrung zeigt, dass es nicht genügt, lediglich die Umsetzung von bestimmten Sensibilisierungsmaßnahmen anzuordnen. Folgende Fallstricke erschweren häufig eine nachhaltige Sensibilisierung:

- Es fehlt Unterstützung durch das Management der verschiedenen Ebenen, was dazu führen kann, dass
  - Mitarbeiter von verschiedenen Bereichen für Schulungen zur IT-Sicherheit nicht freigestellt werden,
  - die Teilnahme weder seitens der Mitarbeiter noch seitens derer Vorgesetzte ernst genommen wird, da auch die Vorgesetzten die Bedeutung von IT-Sicherheit für den Organisationserfolg nicht kommunizieren oder sogar IT-Sicherheit als unwesentlich abtun.
- Die Planung der Sensibilisierungsmaßnahmen ist mangelhaft.
- Das Ziel des Sensibilisierungsprogramms ist nicht oder unklar definiert.
- Es findet keine Erfolgskontrolle statt. Wenn aber Erfolgsmeldungen fehlen, entzieht das Management schnell die Unterstützung oder priorisiert solche Projekte niedriger.
- Es werden nur einzelne Aktionen und Schulungen zur IT-Sicherheit durchgeführt. Wenn diese nicht in Zusammenhang mit anderen IT-Sicherheitsmaßnahmen stehen, können diese unter Umständen mehr Schaden als Nutzen anrichten. Beispielsweise können Mitarbeiter hierdurch verwirrt oder demotiviert werden.
- Es werden zu wenige finanzielle oder personelle Ressourcen zur Durchführung von IT-Sicherheitskampagnen zur Verfügung gestellt. Häufig werden teure Sicherheitskomponenten angeschafft oder mit hohem Aufwand Sicherheitskonzeptionen erarbeitet, ohne dass die Benutzer in deren Anwendung bzw. Umsetzung geschult werden. Dadurch können die ausgeklügelsten Sicherheitslösungen sinnlos werden.

G 2.103 Unzureichende Schulung der Mitarbeiter

IT-Benutzer aller Art werden häufig zu wenig in der Bedienung der von ihnen eingesetzten IT-Systeme geschult. Dies trifft leider sogar öfters auf Administratoren und Benutzerbetreuer zu. Vielfach werden teure Systeme und Anwendungen angeschafft, aber keine oder nur unzureichend Mittel für die Schulung der IT-Benutzer bereitgestellt.

Dies kann durch unabsichtliche Fehlbedienungen, falsche Konfiguration und ungeeignete Betriebsmittel zu gravierenden Sicherheitsproblemen führen. Häufig wenden Benutzer neu eingeführte Sicherheitsprogramme deswegen nicht an, weil sie nicht wissen, wie sie bedient werden und eine selbständige Einarbeitung oft als zu zeitaufwendig im täglichen Arbeitsablauf gesehen wird. Daher reicht die Beschaffung und Installation einer Sicherheitssoftware noch lange nicht aus.

Beispiele:

- Während der Datenerfassung erschien eine dem Benutzer nicht bekannte Fehlermeldung. Da bei den meisten Fehlermeldungen das Anklicken von "ok" bisher keinen Schaden verursachte, wählte er an diesem Fall auch "ok". Nur diesmal bewirkte dies das Herunterfahren des Systems und folglich den Verlust der bis dahin eingegebenen Daten.
- Ein teures Firewall-System wurde beschafft. Der Administrator eines anderen IT-Systems wurde "durch Handauflegen" zum Administrator dieses Firewall-Systems bestimmt. Da er als unabkömmlich galt und alle verfügbaren Mittel für die System-Beschaffung verwendet worden waren, wurde er aber weder in der Bedienung der System-Plattform noch für den eingesetzten Firewall-Typ ausgebildet. Externe Seminare wurden aus Geldmangel verweigert, nicht einmal zusätzliche Handbücher angeschafft. Zwei Monate nach Inbetriebnahme des Firewall-Systems stellte sich heraus, dass durch eine Fehlkonfiguration der Firewall interne Systeme aus dem Internet frei zugänglich waren.
- In einem Unternehmen wurde die Migration auf ein neues Betriebssystem vorbereitet. Der dafür verantwortliche Mitarbeiter war zwar ein ausgezeichneter Kenner der bis dahin eingesetzten Plattform, kannte sich aber mit den diskutierten neuen Systemen nicht aus und erhielt auch keine dem entsprechende Schulung. Daher besuchte er einige kostenfreie Veranstaltungen eines Herstellers, dessen Produkte er auch danach favorisierte. Dies führte zu einer kostenintensiven Fehlentscheidung durch Einführung eines ungeeigneten Produktes.
- Für die Internet-Nutzung während der Dienstreisen wurden auf den Notebooks der Mitarbeiter Personal Firewalls installiert. Die Mitarbeiter wurden nicht dazu geschult, eine Abstimmung der Einstellungen der Firewall mit den Bedürfnissen der Mitarbeiter fand nicht statt. Viele Mitarbeiter haben daraufhin die Firewall abgeschaltet, um problemlos alle Internet-Seiten zu erreichen, die sie brauchten. Das Ergebnis war, dass schon nach einigen Wochen viele der Rechner mit Schadprogrammen verseucht waren. Neben dem Datenverlust war der Ansehensschaden erheblich, da sich ein Schadprogramm über Mails an Kunden weitergesendet hatte.

G 2.104 Inkompatibilität zwischen fremder und eigener IT

Bei der zunehmenden Mobilität von IT-Systemen und IT-Benutzern tritt häufiger das Problem auf, dass sich IT-Systeme aufgrund von Inkompatibilität nicht wie geplant nutzen lassen. Dies ist natürlich ärgerlich, wenn IT-Geräte extra mitgenommen wurden, sich aber nicht nutzen lassen. Darüber hinaus können Versuche, die IT-Systeme doch zu verbinden, zu Schäden an den Geräten oder den gespeicherten Daten führen.

Beispiele:

- Ein Laptop ist mit allen wichtigen Daten für ein Kundengespräch vorbereitet worden. Dieser lässt sich aber beim Kunden nicht mit der dortigen IT koppeln und auch die Daten können wegen unterschiedlicher Schnittstellen nicht auf einen anderen Rechner dort transferiert werden. Dadurch sind die Aufwände und Bemühungen, die in die Vorbereitungen des Gesprächs gesteckt wurden, vergebens.
- Beim Versuch, zwischen zwei IT-Systemen Daten auszutauschen, wird ein Treiber-Problem gemeldet. Auf Anraten eines anderen Besprechungsteilnehmers wird auf dem einem IT-System ein neuer Treiber installiert. Dies führt dazu, dass sich das System nicht mehr starten lässt.

G 2.105 Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen

Wenn Informationen, Geschäftsprozesse und IT-Systeme unzureichend abgesichert sind (beispielsweise durch ein unzureichendes IT-Sicherheitsmanagement), kann dies dazu führen, dass eine Institution gegen Rechtsvorschriften mit Bezug zur Informationsverarbeitung oder gegen bestehende Verträge mit Geschäftspartnern verstößt. Häufig ist die jeweilige Gesetzeslage von der Art der Institution bzw. der betriebenen Geschäftsprozesse und Dienstleistungen sowie den nationalen Vorschriften abhängig. Folgende Beispiele verdeutlichen dies:

- Der Umgang mit personenbezogenen Daten ist in Deutschland über eine Vielzahl von Vorschriften geregelt. Dazu gehören das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze, aber auch eine Vielzahl bereichsspezifischer Regelungen.

  Werden bei der Kommunikation zwischen zwei Geschäftsbereichen personenbezogene Daten (z. B. vertrauliche Patientendaten) ungeschützt über öffentliche Netze übertragen, kann dies unter Umständen rechtliche Konsequenzen nach sich ziehen.

- Bei einem Unternehmen ist die Geschäftsführung dazu verpflichtet, bei allen Geschäftsprozessen eine angemessene Sorgfalt anzuwenden. Hierzu gehört auch die Beachtung anerkannter Sicherheitsmaßnahmen. In Deutschland gibt es verschiedene Rechtsvorschriften wie KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich), GmbHG (Gesetz betreffend die Gesellschaften mit beschränkter Haftung) oder AktG (Aktiengesetz), aus denen sich zu Risikomanagement und IT-Sicherheit Handlungs- und Haftungsverpflichtungen der Geschäftsführung bzw. des Vorstands eines Unternehmens ableiten lassen.

- Die ordnungsmäßige Verarbeitung von buchungsrelevanten Daten ist in verschiedenen Gesetzen und Vorschriften geregelt. In Deutschland sind dies unter anderem das Handelsgesetzbuch (z. B. HGB §§ 238 ff.) und die Abgabenordnung (AO). Die ordnungsmäßige Verarbeitung von Informationen umfasst natürlich deren sichere Verarbeitung. Beides muss in vielen Ländern regelmäßig nachgewiesen werden, beispielsweise durch Wirtschaftsprüfer im Rahmen der Prüfung des Jahresabschlusses. Falls hierbei gravierende Sicherheitsmängel festgestellt werden, kann kein positiver Prüfungsbericht erstellt werden.

- In vielen Branchen (z. B. der Automobil-Industrie) ist es üblich, dass Hersteller ihre Zulieferer zur Einhaltung bestimmter Qualitäts- und Sicherheitsstandards verpflichten. In diesem Zusammenhang werden zunehmend auch Anforderungen an IT-Sicherheit gestellt. Verstößt ein Vertragspartner gegen vertraglich geregelte Sicherheitsanforderungen, kann dies Vertragsstrafen nach sich ziehen, aber auch Vertragsauflösungen bis hin zum Verlust von Geschäftsbeziehungen.

Nur wenige Sicherheitsanforderungen ergeben sich unmittelbar aus Gesetzen. Im Allgemeinen orientiert sich die Gesetzgebung aber am Stand der Technik als allgemeine Bewertungsgrundlage für den Grad der erreichbaren Sicherheit. Wenn also bei einer Institution die vorhandenen Sicherheitsmaßnahmen in

keinem gesunden Verhältnis zu den zu schützenden Werten stehen, kann dies gravierende Konsequenzen nach sich ziehen.

G 2.106 Störung der Geschäftsabläufe aufgrund von IT-Sicherheitsvorfällen

Sicherheitsvorfälle können durch ein singuläres Ereignis oder eine Verkettung unglücklicher Umstände ausgelöst werden und dazu führen, dass Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen und IT-Systemen beeinträchtigt werden. Dies wirkt sich dann schnell negativ auf wesentliche Fachaufgaben und Geschäftsprozesse aus. Auch wenn längst nicht alle Sicherheitsvorfälle anschließend in der Öffentlichkeit bekannt werden, können sie trotzdem zu negativen Auswirkungen in den Beziehungen zu Geschäftspartnern und Kunden führen. Dabei ist es nicht einmal so, dass die beträchtlichsten und weitreichendsten Sicherheitsvorfälle durch die größten Sicherheitsschwachstellen ausgelöst wurden. In vielen Fällen haben kleine Ursachen zu riesigen Schäden geführt, weil verschiedene Faktoren ungeahnte Verkettungen nach sich gezogen haben.

Beispiele:

- Ein Computerproblem führte dazu, dass an allen US-amerikanischen Flughäfen für mehr als zwei Stunden von zwei Fluglinien keine Maschinen starten konnten. Als Ursache wurde eine Fehlfunktion in einer Datenbank genannt, die laufende Informationen über die anstehenden Flüge bereitstellt. Als Folge konnten hunderte Flüge nicht starten, auch im Anschluss gab es massive Verspätungen, mehrere Tausend Passagiere saßen fest.
- Fehlende Plausibilitätskontrollen führen immer wieder dazu, dass kleine Fehler in Benutzereingaben erhebliche Auswirkungen nach sich ziehen. So brach an der Londoner Börse der FTSE-Index um 200 Punkte ein, nachdem ein Broker versehentlich eine Null zuviel an eine Order gehängt hatte.

  Bei einer Hotelkette wurde statt dessen eine Null bei der Eingabe in die Angebotsdatenbank vergessen, was dazu führte, dass Luxusappartements im Südpazifik für ein Zehntel des eigentlichen Preises angeboten wurden.
- Nach einem schiefgelaufenen Software-Update war bei einem großen Unternehmen über 16 Stunden das Netz nicht mehr verfügbar. Dadurch konnten 5000 Mitarbeiter nicht ihren normalen Tätigkeiten nachgehen und 1700 Kundenanfragen nicht bearbeitet werden. Wichtige Termine konnten dadurch nicht eingehalten werden. Neben der ohnehin hohen Belastung für die Administration fielen zusätzlich 6000 Anfragen an den Benutzersupport an.

G 2.107 Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes IT-Sicherheitsmanagement

IT-Sicherheit ist eine Voraussetzung für die Gewährleistung der einwandfreien Funktion einer Institution. Gleichzeitig ist aber aufgrund der Vielfältigkeit dieses Themas eine absolute IT-Sicherheit praktisch nicht erreichbar. Aus diesem Grund ist es essenziell, die richtigen Prioritäten zu setzen und an denjenigen Stellen zu investieren, die den größten Mehrwert für die Institution bringen. Dies ist eine Entscheidung, die nur mit Hilfe eines institutionsübergreifenden IT-Sicherheitsmanagements getroffen werden kann.

Durch ein IT-Sicherheitsmanagement werden als erstes die tatsächlichen Sicherheitsanforderungen der Institution festgelegt und die Risiken bei ihrer Nichteinhaltung betrachtet. Auf dieser Basis muss entschieden werden, ob

- Ressourcen in Schutzmaßnahmen investiert werden,
- durch Umstrukturierung oder Verlagerung von Aufgaben sich der Aufwand für den Schutz auf ein vertretbares Maß reduziert,
- Risiken akzeptiert werden.

Diese Überlegungen sind für das Vorgehen in Bezug auf IT-Sicherheit grundlegend und müssen in entsprechenden Dokumentationen festgehalten werden. Fehlendes oder unzureichendes IT-Sicherheitsmanagement kann dementsprechend zu folgenden Fehlern führen:

- Oft wird in teure Sicherheitslösungen investiert, ohne dass eine Basis an notwendigen organisatorischen Regelungen vorhanden ist. Nicht geklärte Zuständigkeiten und Verantwortlichkeiten können trotz teurer Investitionen zu schweren IT-Sicherheitsvorfällen führen.

  Vorfall aus der Praxis: In einem Unternehmen wurde eine teure Firewall beschafft, aber die Administratoren unzureichend geschult und Verantwortlichkeiten nicht klar zugewiesen. Dadurch wurde die Firewall nicht sicher und für die Sicherheitsbedürfnisse des Unternehmens angemessen konfiguriert. Da immer wieder Dienste durch unterschiedliche Administratoren freigeschaltet wurden, blieb die Funktionalität weitgehend ungenutzt und es kam zu Sicherheitsvorfällen.

- Es wird in den Bereichen in IT-Sicherheit investiert, die entsprechende Mittel zur Verfügung haben und deren Verantwortliche für IT-Sicherheit besonders sensibilisiert sind. Andere Bereiche, die vielleicht für die Erfüllung der Fachaufgaben wichtiger sind, werden aufgrund von knappen Mitteln oder Desinteresse der Verantwortlichen vernachlässigt.

  Vorfall aus der Praxis: Um die Verfügbarkeit der Anwendung "Buchhaltung" zu erhöhen, wurde ein teures Cluster-System angeschafft. Die für den Kundendienst notwendigen Anwendungen laufen dagegen aufgrund von knappen finanziellen Mitteln in dem Bereich immer noch auf einem alten Server, der jederzeit ausfallen könnte. Die Verfügbarkeit der Kundendienst-Anwendung ist für das Unternehmen wichtiger, leider wurden aber in diesem Fall die Prioritäten bei der Mittelvergabe nicht berücksichtigt.

- Bei Investitionen in einzelnen Teilbereichen ist es erforderlich, das gesamte Sicherheitskonzept zu betrachten.

  Vorfall aus der Praxis: Eine Abteilung wird mit einer neuen Sicherheitslösung ausgerüstet. Die Stromversorgung bleibt jedoch weiterhin sehr schlecht gesichert, da eine alte und lange nicht getestete USV eingesetzt wird. Dadurch bleiben im Gesamtsystem erhebliche Sicherheitslücken.

- Durch die einseitige Erhöhung des Schutzes einzelner Grundwerte kann sich der Gesamtschutz verringern.

  Vorfall aus der Praxis: Nach dem Einsatz einer hochwertigen Verschlüsselungsroutine bei der Rechnungserstellung wurde die Geschwindigkeit der Arbeitsabläufe sehr schwer beeinträchtigt. Es wurde nicht berücksichtigt, dass die Verfügbarkeit der Systeme viel wichtiger war als ihre Vertraulichkeit.

- Ein inhomogener und unkoordinierter Einsatz von IT-Produkten kann zu hohem finanziellen und personellen Ressourceneinsatz führen.

  Vorfall aus der Praxis: In einem großen Unternehmen gab es mehrere Bereiche, die sich mit Informationssicherheit beschäftigt haben. Es stellte sich heraus, dass von zwei Bereichen unabhängig voneinander jeweils Firmenlizenzen eines Viren-Suchprogramms eingekauft wurden. Im gesamten Unternehmen fanden sich zudem verschiedene Verschlüsselungsprodukte für den selben Einsatz. Dies erschwerte die Administration und führte zu einer erhöhten Fehleranfälligkeit.

G 2.108 Fehlende oder unzureichende Planung des SAP Einsatzes

Wird ein SAP System ohne ausreichende Planung eingesetzt, so kann dies zu einer Vielzahl von Problemen führen. Unter anderem kommt es dabei immer auch zu Sicherheitsproblemen. Im Folgenden sind nur einige Probleme dargestellt, die jedoch deutlich machen, dass eine gute Planung vor dem Einsatz eines SAP Systems notwendig ist:

- In einem mittelständischen Unternehmen soll ein SAP System eingeführt werden. Es wurde sich für eine Installation auf einem Rechner entschieden (Single-Host-Installation). Aus Zeitgründen wurde keine Ressourcen-Planung durchgeführt. Aus Kostengründen wurde ein Rechner aus einer Sonderaktion eines Computerherstellers beschafft. Nach der Installation zeigt sich, dass der Rechner mit zu wenig Hauptspeicher ausgerüstet ist und aufgrund von Hardwarebeschränkungen auch nicht mit viel mehr Speicher bestückt werden kann. Durch die Notwendigkeit, neue, geeignete Hardware zu beschaffen, entstehen Verzögerungen und erhebliche Mehrkosten.
- Durch fehlende Planung der Aufgabentrennung im Rahmen des Administrationskonzeptes kann ein Administrator auf alle HR-Daten eines R/3 Systems zugreifen.
- Die Zuständigkeiten und Abläufe für das Änderungsmanagement und das Notfallkonzept eines SAP Systems wurden nicht geplant. Daher haben Entwickler vollen Zugriff auf das Produktivsystem, da der Zugriff für "Notreparaturen unbedingt erforderlich ist". Ein Zugriff auf alle Konten- und Kreditkarten-Daten der Unternehmenskunden ist somit möglich.
- Besitzen Personen Entwickler-Zugriffsmöglichkeiten auf produktive SAP Systeme (diese werden über das Berechtigungsobjekt S_DEVELOP vergeben), so können diese Personen die Sicherheitsmechanismen des SAP Systems unterlaufen und unberechtigt auf Funktionen und Daten zugreifen.
- Können Transaktionen eines SAP Systems unberechtigt aufgerufen werden, so kann dies weitreichende Folgen haben. In der Regel kann dann auf Funktionen und Daten zugegriffen werden, die dem Zugreifer nicht verfügbar sein sollen. Sind administrative Transaktionen betroffen, kann die Systemsicherheit unter Umständen vollständig unterlaufen werden.
- Bestehen für einen Angreifer Zugriffsmöglichkeiten auf der Betriebssystem-Ebene eines SAP Systems, so kann der Angreifer in die Konfiguration des SAP Systems eingreifen. So ist beispielsweise der Zugriff auf die Profil-Parameter möglich, durch die unter anderem auch die Zugriffsbarrieren reduziert werden können (z. B. Kontosperr-Einstellungen). Für den Java-Stack kann auf Konfigurationsdateien zugegriffen werden, die dann modifiziert werden können. Dadurch kann die Sicherheit drastisch reduziert sein. Ist der Rechner, auf dem die Datenbank des SAP Systems läuft, betroffen, können die Datenbankinhalte auch sehr einfach durch Datei-Kopien erlangt werden. Die Sicherheitsmechanismen des SAP Systems werden damit unterlaufen.

- Standardinstallationen sind in der Regel nicht sofort auf die Sicherheitsanforderungen eines Produktivbetriebs ausgelegt. Werden Komponenten mit Standardkonfiguration dennoch produktiv betrieben, so ist die Gefahr groß, dass die System- und Datensicherheit gefährdet ist. Angriffsmöglichkeiten können durch verschiedene unkonfigurierte Schnittstellen entstehen und reichen von unberechtigtem Zugriff auf Funktionen und Daten bis hin zu Durchgriffen auf das Betriebssystem unter den Berechtigungen des SAP Systems.
- Werden die (öffentlich bekannten) Standardpasswörter wichtiger Benutzer wie "SAP*" oder "DDIC" im ABAP-Stack oder "Administrator" oder "System" im Java-Stack nicht verändert, so können Angreifer Administrator-Zugriffmöglichkeiten erlangen. Damit kann ein Angreifer auf alle Daten des SAP Systems zugreifen und administrative Funktionen ausführen.
- Wird ein SAP System ausgesondert und dessen Identität (IP, SID) nicht durch ein Ersatzsystem übernommen, so kann die unvollständige Aussonderung dazu führen, dass Angreifer ein eigenes SAP System aufsetzen, das die Identität des ausgesonderten Systems übernimmt. Zugriffe anderer SAP Systeme über bestehende Destinationen werden dann vom Angreifersystem akzeptiert. Damit können dort Daten abgerufen und auch gespeichert werden. Diese enthalten auch Authentisierungsinformationen, die für den Anmeldeprozess benötigt werden. Oft werden technische Benutzer in mehreren Systemen gleichartig verwendet, so dass dadurch auch Zugriffsmöglichkeiten auf andere Systeme bestehen können.
- Ist für ein SAP System die HTTP-basierte RFC-SOAP-Schnittstelle aktiviert (ABAP-ICF-Dienst oder JAVA-Stack-SOAP-Dienst), so können Benutzer RFC-fähige Bausteine über die HTTP-Schnittstelle aufrufen. In der Regel ist dies in Szenarien, in denen der SAP System-Zugriff über einen Browser erfolgt, nicht gewünscht. Dennoch können in diesem Fall RFC-Aufrufe durchgeführt werden, so dass je nach Berechtigungseinstellung auch unberechtigte Zugriffe auf Daten ermöglicht werden.
- Werden wichtige Systemereignisse nicht protokolliert oder die Protokolleinträge nicht ausgewertet, so können Angriffe oder Sicherheitsverletzungen nicht erkannt werden. Erfolgreichen Angriffen kann nicht begegnet oder nachgegangen werden. Daher kann unbemerkt ein unberechtigter Zugriff auf Daten oder Funktionen bestehen.

G 2.109 Fehlende oder unzureichende Planung des Speichersystems

Die Auswahl und der Einsatz von Speichersystemen und Speichernetzen erfordert sorgfältige Planung, Installation und Konfiguration, um einen störungsfreien Einsatz zu gewährleisten. Mögliche Gefährdungen aufgrund mangelnder Planung werden im Folgenden verdeutlicht.

Wachsende Anforderungen an Speicherplatz

- Der Bedarf an Speicherplatz wächst in Organisationen erfahrungsgemäß schneller als erwartet. Wenn die neu installierten Speichersysteme nicht auf den potentiellen Zuwachs eingerichtet sind, kann es innerhalb von kurzer Zeit notwendig werden, neue Systeme zu beschaffen oder gar die gesamte Speicher-Infrastruktur neu zu konzipieren.

Verfügbarkeits-anforderungen

- Die Technologie für Speichersysteme und Speichernetze bietet die Möglichkeit, eine sehr hohe Verfügbarkeit zu erreichen. Insbesondere bei hochverfügbaren Speicherumgebungen ist eine sehr ausführliche Planung notwendig, um mögliche Fehler zu vermeiden. Oft wird versucht die Verfügbargkeit von Speichersystemen mit Hilfe redundant ausgelegter Komponenten zu steigern. Wenn dabei die Funktion des Speichersystems oder Speichernetzes doch an einer Stelle von der Funktion einer einzelnen Komponente abhängt, gefährdet dies wieder die gesamte Verfügbarkeit des Systems. Komponenten mit solcher Wirkung werden SpoF genannt (single points of failure).

Einsatz ungeeigneter Technologie

- Die Anfordeungen einer Anwendung an Performance sowie Interoperabilitätsanforderungen bezüglich der vorhandenen Software und Hardware können den Einsatz von bestimmten Produkten erzwingen. Wenn diese Aspekte nicht rechtzeitig in der Planung berücksichtigt werden, kann dies teure und ineffiziente Korrekturen während der Realisierung, Verzögerungen im Einsatz oder gar erhebliche Störungen im Betrieb als Folge haben.

G 2.110 Mangelhafte Organisation bei Versionswechsel und Migration von Datenbanken

Alle organisatorischen Schritte vor und während eines Versionswechsels des Datenbankmanagementsystems (DBMS) oder einer Datenbankmigration werden in Migrations- und Versionskonzepten festgehalten. Das Fehlen solcher Konzepte kann die Aufgabenerledigung erheblich beeinträchtigen, wenn bei einer Datenbankmigration oder einem DBMS-Upgrade Probleme auftreten und das DBMS oder einzelne Datenbanken unvorhergesehen nicht zur Verfügung stehen.

Werden neben der Planung der physischen und semantischen Datenmigration keine sicheren Rückfallpositionen festgelegt, kann die Arbeitsfähigkeit der Datenbank bzw. des DBMS für Benutzer und Anwendungen gefährdet werden.

Bei einem DBMS-Versionswechsel bleiben die im DBMS abgelegten Datenbanken unverändert. Sicherheitsprobleme können hier weniger in der Datenbank selbst als im Zusammenspiel der Datenbanken mit dem neuen DBMS entstehen.

Beispiele:

- Durch ein Datenbank-Upgrade wurden Grunddefinitionen in den Typen geändert.
- Zugriffsberechtigungen für standardmäßig vom DBMS bereitgestellte Benutzergruppen sind geändert und beeinflussen damit die Rechte daraus abgeleiteter Benutzergruppen.

Bei einer Datenmigration werden Daten aus einer Datenbank in eine andere Datenbank überspielt. Dabei können die Daten in jeglicher Art konvertiert und in neue Strukturen einer Datenbank auf einem eventuell völlig anderen DBMS übertragen werden. Hier ist zu beachten, dass Datenbanken zur Sicherstellung der Datenkonsistenz unterschiedliche Konstrukte (Trigger, Constraints, etc.) benutzen können. Über solche Konstrukte werden Reihenfolgen und Abhängigkeiten innerhalb der Daten implementiert, die bei Datenmigrationen berücksichtigt und entsprechend nachgebildet werden müssen. Die Analyse und Nachbildung aller einzuhaltenden Bedingungen kann sehr aufwendig und umfangreich sein. Dadurch besteht die Gefahr, dass sich Fehler einschleichen, die die Datenkonsistenz und die Funktionalität nach der Migration gefährden.

Beispiele:

- Bei einer Datenbank-Migration von Microsoft Access auf den Microsoft SQL-Server müssen in Access vorhandene Spalten vom Typ *AutoWert* gesondert beachtet werden, da dieser Typ auf verschiedenen DBMS unterschiedlich implementiert ist.
- In der zu migrierenden Datenbank existieren die zwei Tabellen MITARBEITER und FIRMA. Um sicherzustellen, dass neue Mitarbeiter nur existierenden Firmen zugeordnet werden können, wird der Tabelle MITARBEITER ein UPDATE/INSERT-Trigger zugeordnet, der vor Neueinträgen und/oder Veränderungen in der Tabelle MITARBEITER prüft, ob es in der Tabelle FIRMA einen korrespondierenden Eintrag gibt.

Sollte es keinen entsprechenden Eintrag in der Tabelle FIRMA geben, wird die UPDATE- oder INSERT-Anweisung abgebrochen. Die in dieser DB implementierte Reihenfolge (umgangssprachlich: "Zuerst Firma, dann erst Mitarbeiter") muss bei der Migration der Datenbank beachtet werden. Sollte im Migrationslauf die Tabelle MITARBEITER vor der Tabelle FIRMA übertragen werden, so wird die Einfügung verweigert, da noch keine korrespondierenden Einträge in der Tabelle FIRMA existieren.

G 2.111 Kompromittierung von Anmeldedaten bei Dienstleisterwechsel

Bekanntgabe von Anmeldedaten

Wenn ein IT-Dienstleister gewechselt wird, müssen hierfür typischerweise diverse Anmeldedaten geändert werden. Dies führt dann zu vielfältiger Kommunikation von alten und neuen Anmeldedaten. Werden diese Daten unsicher ausgetauscht, besteht das Risiko, dass die Vertraulichkeit der Anmeldedaten und mittelbar die Integrität der IT-Umgebung beeinträchtigt wird.

Bei den vom Dienstleister verwendeten Anmeldekonten handelt es sich meistens um solche mit weitgehenden Berechtigungen im betrachteten IT-Verbund. Normalerweise sollten alle Kennwörter niemandem außer dem zugehörigen Benutzer bekannt sein. Auch alte Kennwörter gelten grundsätzlich als vertrauliche Information. In der Praxis kommt es häufig vor, dass ein aktuelles zentrales Kennwort dem neuen Dienstleister mitgeteilt wird. Bis der neue Dienstleister alle Konsolen und Applikationen mit einem neuen Kennwort versehen hat, könnte das alte Kennwort durch unbefugte Dritte missbraucht werden. Abhängig von der Konfiguration des Systems (z. B. Dienstkonten, Zertifikatsdienste) und Organisation kann es vorkommen, dass das Ändern des Kennwortes nicht in kurzer Zeit mit vertretbarem Aufwand möglich ist.

Unsichere Administration

Oft ist der Auftraggeber selbst nicht in der Lage, Benutzerkonten für externe Dienstleister auf sichere Art und Weise zu administrieren und muss dies gegebenenfalls dem neuen Dienstleister überlassen. Es kommt zu Situationen wie der gemeinsamen Nutzung von Benutzerkonten ("Account Sharing") oder den in G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten* und G 3.43 *Ungeeigneter Umgang mit Passwörtern* beschriebenen Gefährdungen.

Organisatorische Mängel

Teilweise besitzt der Auftraggeber selbst entweder keine Kenntnis mehr über Anmeldekonten mit administrativen Berechtigungen oder nur noch aufgrund einer regelmäßigen Unterrichtung durch den Dienstleister über das aktuelle Kennwort ("Account Sharing"). In jedem dieser Fälle liegen Entscheidungs- und Handlungshoheit beim Dienstleister. Der Auftraggeber verfügt über keine nur ihm bekannten Zugangsdaten mehr, mit denen er strategische Entscheidungen umsetzen kann. Diese Situation entspricht einem hohen Grad des Outsourcings. Sie stellt ein hohes Risiko für die Gefährdung der Systemsicherheit dar, wenn die Regelungen und Absicherungen für das Outsourcing nicht den Sicherheitsanforderungen entsprechen und diese nicht unmissverständlich in *Service Level Agreements* (SLA) festgehalten wurden

Insgesamt ergibt sich immer wieder die Situation, dass kritische administrative Konten sogar weniger sorgfältig gehandhabt werden als normale Benutzerkonten, weil etablierte Maßstäbe des Unternehmens oder der Behörde für den Umgang mit Benutzerkonten außer Acht gelassen werden und weil keine Verfahrensweise oder Richtlinie für den Umgang mit administrativen Konten bei Dienstleisterwechsel festgelegt wurde.

Beispiel:

Häufig wird in kleinen Unternehmen der zentrale Server von einer externen Person betreut. Diese Person hat dann auch das Kennwort für das zentrale Administratorkonto.

Oft besitzt kein anderer Benutzer innerhalb des Unternehmens ebenfalls ein administratives Konto, auch nicht der Geschäftsführer. Der gängigste Weg ist, dass der Geschäftsführer das Kennwort des zentralen administrativen Kontos in einem Tresor abgelegt hat. Kommt ein neuer Dienstleister, wird ihm dieses Kennwort mitgeteilt. Manchmal kommt es auch vor, dass kein Wartungsvertrag oder eine sonstige dauerhafte Vereinbarung über die Art des Outsourcings und der Verfahrensweisen mit irgendeiner der beteiligten externen Personen besteht. Unter Umständen hat der alte Dienstleister das Kennwort gewechselt und dann sein Engagement unerwartet und kurzfristig beendet. Das System bleibt solange nicht administrierbar, bis das Kennwort durch Nachfrage oder mit technischen Mitteln in Erfahrung gebracht wurde.

G 2.112 Unzureichende Planung von VoIP

Fehlentscheidungen, die schon in der Planungsphase getroffen werden, können später meist nur mit einem hohen Aufwand korrigiert werden. Um einen stabilen Einsatz von VoIP zu ermöglichen, müssen viele Aspekte beachtet werden.

VoIP setzt ein funktionierendes Datennetz voraus. Dieses Datennetz kann auch für weitere Dienste, wie E-Mail und WWW, genutzt werden. Durch die zusätzlichen IP-Pakete, die für VoIP erforderlich sind, kann das Datennetz schnell überlastet werden. Die Dimensionierung spielt daher für den problemlosen Betrieb eine entscheidende Rolle. Die Folgen einer Fehleinschätzung bezüglich dieses Aspekts können bis zum Ausfall aller technischen Kommunikationsmöglichkeiten reichen. Zur Kommunikation über VoIP werden Signalisierungs- und Medientransportprotokolle benötigt. Bei den Signalisierungsprotokollen, in denen hauptsächlich Steuerungsanweisungen übermittelt werden, hat sich bisher kein Standardprotokoll durchgesetzt. Neben vielen proprietären Lösungen sind die Signalisierungsprotokolle SIP und H.323 zu nennen. Viele VoIP-Geräte unterstützen nur ein Protokoll, wodurch die Planung entscheidend beeinflusst wird.

Die Auswahl eines Medientransportprotokolls ist weniger kritisch, da sich bisher nur das Realtime Transport Protocol (RTP) durchgesetzt hat. Unterstützen beide Kommunikationspartner das verschlüsselte SRTP kann die Kommunikation geschützt stattfinden.

Für die eigentliche Übertragung der Sprache wird ein Codec benötigt, der die Umwandlung von Sprache in digitale Informationen ermöglicht. Obwohl zahlreiche Codecs existieren, spielt die Auswahl bei der Planung nur eine untergeordnete Rolle. In der Regel unterstützen die Endgeräte zahlreiche Codecs. Beim Verbindungsaufbau wird deren Verwendung mit dem Kommunikationspartner ausgehandelt. Unterstützen beide Kommunikationspartner nur wenige gemeinsame Codecs, so kann es passieren, dass ein Codec gewählt wird, der für die Rahmenbedingungen nicht optimal ist. Dies kann auf der einen Seite eine hohe Auslastung des Netzes und auf der anderen Seite eine zu schlechte Sprachqualität zur Folge haben.

Neben der technischen Grundfunktionalität spielt bei der Planung und Anschaffung von VoIP-Geräten eine mögliche Verschlüsselung zwischen den Geräten eine wichtige Rolle. In einigen Anwendungsfällen kann beispielsweise ein mit IPSec oder SSL verschlüsseltes VPN genutzt werden. Die Installation eines VPN-Clienten ist aber bei dedizierten VoIP-Hardphones meist nicht möglich. Wird auch die Verschlüsselung des Medientransportsprotokolls, beispielsweise durch SRTP, nicht unterstützt, so könnte ein Angreifer diese Telefongespräche unter Umständen abhören.

G 2.113 Unzureichende Planung der Netzkapazität beim Einsatz von VoIP

Für den Einsatz von Voice over Internet Protocol (VoIP) wird ein Datennetz benötigt. Dabei können schon vorhandene Datennetze, an denen die Arbeitsplatzrechner und Server angeschlossen sind, oder hiervon unabhängige Datennetze verwendet werden. Ein Hauptargument für die Umstellung von leitungsvermittelnden Telefonlösungen zu VoIP sind aber die geringeren Wartungskosten von nur einer Kommunikationsinfrastruktur, wenn ein bestehendes Datennetz genutzt wird.

Für VoIP sind bisher nur sehr wenig Erfahrungswerte vorhanden, da es sich hierbei um eine relativ neue Technologie handelt. Wenn VoIP eine leitungsvermittelnde TK-Anlage ersetzen soll, kann in der Regel nicht auf die hier gewonnenen Erfahrungswerte zurückgegriffen werden. Dies betrifft besonders das Verhalten der VoIP-TK-Anlage bei einem großen Benutzerkreis.

Die Anbieter der VoIP-TK-Anlagen versuchen, Aussagen zu treffen, wie viele Benutzer mit ihrem Produkt verwaltet werden können. Diese Aussagen sind aber nicht sehr aussagekräftig, wenn ein bestehendes Datennetz genutzt werden soll. Treten hohe Datenmengen von den Arbeitsplatzrechner auf, kann durch die gleichzeitige Nutzung von VoIP das Netz schnell überlastet werden. Bei leitungsvermittelnden TK-Anlagen bestimmt die maximale Anzahl der Ports, an denen Telefone angeschlossen werden können, die Benutzeranzahl.

Je nach der Konfiguration der aktiven Netzkomponenten können bei einer Überlastung bestimmte IP-Pakete bevorzugt weitergeleitet werden. Werden bei einer hohen Netzlast VoIP-Pakete bevorzugt weitergeleitet, kann an den Arbeitsplatzrechnern unter Umständen nicht mehr effizient gearbeitet werden. Werden alle IP-Pakete mit einer gleich großen Priorität versendet, kann die störungsfreie Nutzung von VoIP nicht mehr garantiert werden.

Auch wenn bei der Umstellung auf VoIP das bestehende Netz für die parallele Nutzung von VoIP und regulären Informationen ausreichend dimensioniert wurde, muss dies für zukünftige Konstellationen nicht mehr genügen. Werden neue Mitarbeiter eingestellt, so müssen sie sowohl an ihren Arbeitsplatzrechnern über das Datennetz arbeiten als auch über VoIP telefonieren können. Damit steigt die Belastung des Netzes stärker an und die freien Ressourcen sind schneller aufgebraucht.

G 2.114 Uneinheitliche Windows-Server-2003-Sicherheitseinstellungen bei SMB, RPC und LDAP

Konsistente Einstellungen erforderlich

Die beiden in der Windows-Welt essentiellen Kommunikations-Protokolle SMB/CIFS und LDAP wurden vom Hersteller mit erweiterten Signierungs- und Verschlüsselungsmechanismen ausgestattet. Sie dienen der Verschlüsselung und Authentisierung dieser an sich unsicheren Protokolle. Unter Windows Server 2003 sind einige der Mechanismen schon in den Einstellungen der lokalen Sicherheitsrichtlinie vorkonfiguriert. Der Einsatz dieser Mechanismen betrifft die Kommunikation mit allen beteiligten Windows-Servern im Netz sowie viele Basisdienste von Windows und hat Auswirkungen auf den gesamten Netzbereich. Wenn diese Einstellungen nicht flächendeckend ordnungsgemäß und konsistent eingestellt werden, sind schwer nachvollziehbare Seiteneffekte bis hin zu Fehlfunktionen einzelner Windows-Server und -Clients die Folge.

Verfügbarkeit beeinträchtigt

Durch Fehlkonfiguration, falsches Vorgehen und falsche Aktivierungsreihenfolge beim Vornehmen der Signierungs- und Verschlüsselungseinstellungen zu SMB und LDAP kann die Verfügbarkeit für weite Teile des Windows-Netzes stark beeinträchtigt werden. Bei größeren Umgebungen kann das Zurückversetzen des Windows-Netzes in einen funktionstüchtigen Zustand sehr hohen Aufwand verursachen, da in einer solchen Situation viele netzbasierte Verwaltungs- und Steuerungsfunktionen gestört sind.

Insbesondere für Domänen-Controller stellen inkonsistente Einstellungen innerhalb der Domäne eine große Gefahr dar, weil sich entsprechende Symptome (Störung von Verwaltungsfunktionen wie z. B. Gruppenrichtlinien) unter Umständen erst nach einer gewissen Zeit bemerkbar machen.

Ältere Windows-Versionen sind nicht ohne weiteres kompatibel zu den erhöhten Sicherheitseinstellungen für SMB, RPC und LDAP. Zum Beispiel sind Vertrauensstellungen ohne Kerberos-Authentisierung, wie sie in großen, standortübergreifenden IT-Verbünden genutzt werden, nicht ohne weiteres zu den erhöhten Sicherheitseinstellungen kompatibel. Durch unzureichende Analyse aller betroffenen IT-Systeme und eine unzureichende Planung des Einsatzes können unerwartete Kommunikationsstörungen in allen Bereichen die Verfügbarkeit insgesamt stark einschränken. Eine unzureichende Planung kann dadurch hohe Folgekosten bei der Realisierung nach sich ziehen.

Beispiel:

In großen Umgebungen kann es zu Schwierigkeiten beim Domänenbeitritt eines Servers sowie zu Problemen mit Vertrauensstellungen kommen, wenn keine Kerberos-basierte Vertrauensstellung verwendet wird. Anmeldeversuche schlagen sporadisch fehl, obwohl das richtige Kennwort eingegeben wurde. Dies kommt durch unterschiedlich konfigurierte Domänencontroller zustande, die zufällig für Authentisierungsversuche ausgewählt werden. Auch Applikationen können in ihrer Funktionsweise beeinträchtigt werden.

G 2.115 Ungeeigneter Umgang mit den Standard-Sicherheitsgruppen von Windows Server 2003

Im Betriebssystem Windows Server 2003 sind zu den aus Windows 2000 Server bekannten eingebauten Sicherheitsgruppen weitere Standardgruppen hinzugekommen. Die Rechte dieser Gruppen können z. T. nicht eingeschränkt werden und die Berechtigungen sind vom Hersteller nicht im Einzelnen dokumentiert. Bestimmte Berechtigungen werden gar nicht angezeigt und sind nicht administrierbar, so z. B. bei der Gruppe Netzwerkkonfigurations-Operatoren.

Unkenntnis bezüglich Sicherheitsgruppen

Die Gruppen stellen nicht prinzipiell eine Gefährdung dar. Die Unkenntnis über die Funktionsweise dieser Gruppen sowie deren ungeeignete Verwendung können jedoch zu vorsätzlichem oder versehentlichem Missbrauch von Administratorrechten und zur Fehlkonfiguration des Systems führen.

Neue Gruppen sind:

- Hilfedienstgruppe

  Diese Gruppe für das Hilfe- und Supportcenter wird für die Administration und den Betrieb des Servers nicht benötigt, birgt jedoch Möglichkeiten für Missbrauch oder Fehlkonfiguration, weil der Gruppe umfangreiche Berechtigungen für Administrationswerkzeuge zugeordnet werden können.

- Netzwerkkonfigurations-Operatoren

  Mitglieder können die Parameter des TCP/IP-Stacks einstellen und manipulieren und somit den Server unerreichbar machen oder für Angriffe öffnen.

- Systemmonitorbenutzer und Leistungsprotokollbenutzer

  Systemmonitorbenutzer dürfen das Programm für den Systemmonitor (perfmon.exe) ausführen und benutzen, ohne dass sie besondere Berechtigungen benötigen. Mitglieder der Gruppe Leistungsprotokoll-benutzer können Protokolle des Systemmonitors anschauen, verwalten und die Aufzeichnung von Überwachungsdaten konfigurieren. Sie haben direkten Zugriff auf einen Teil der Windows Management Instrumentation (WMI) Datenbank. Leistungs- und Nutzungsprofile sind sicherheitskritische Informationen, genauso wie Informationen über Ausfälle und Fehlfunktionen, die Anlass für einen Angriffsversuch sein könnten. Es stellt eine Gefahr dar, wenn Benutzerkonten unabsichtlich zusätzliche Berechtigungen mittels dieser Gruppen erlangen Remote-desktopbenutzer.

  Mitglieder können sich von einem anderen Computer aus mittels Remote Desktop Protocol (RDP) auf einem Mitgliedsserver oder allein stehenden Server anmelden und mit ihm arbeiten, als würden sie direkt vor dem physikalischen System sitzen. Dies stellt ein Risiko dar, denn jeder normale Benutzer kann sich auf diese Weise anmelden, ohne dass er besondere zusätzliche Berechtigungen benötigt.

- Distributed COM-Benutzer

  Ab Windows Server 2003 mit Service Pack 1 stehen detailliertere Berechtigungsstrukturen für Distributed-COM-Objekte (DCOM) zur Verfügung, um die Ausführung von COM-Modulen und die Aktivierung von COM-Objekten besser kontrollieren zu können. Insbesondere die Remote-Ausführung von anderen Clients aus mittels Remote Procedure Calls (RPC) kann damit besser kontrolliert werden. Viele Windows-Funktionen können über COM-Objekte gesteuert werden, z. B. Windows Update, Richtlinienergebnissatz, Zertifikatsdienste und mehr. Die Berechtigungen werden in der Konsole Komponentendienste konfiguriert. Standardmäßig haben die Distributed-COM-Benutzer hier das höchste Berechtigungslimit, welches sogar über das von normalen Administratoren hinausgeht. Der falsche Umgang mit dieser Gruppe kann die verbesserten DCOM-Sicherheitsfunktionen unwirksam machen oder sogar zu einer erhöhten Angreifbarkeit des Systems führen.

- Erstellungen eingehender Gesamtstrukturvertrauensstellung

  Diese Gruppe ist neu auf Domänencontrollern. Mitglieder dieser Gruppe können eingehende unidirektionale Vertrauensstellungen zur Active-Directory-Gesamtstruktur eines IT-Verbundes erstellen. Durch Vertrauensstellungen können Rechte in der jeweils anderen Domänenumgebung ausgeübt werden, daher kann der Missbrauch bzw. fahrlässige Umgang mit dieser Gruppe Angreifern vielfältige Einflussmöglichkeiten auf den gesamten IT-Verbund verschaffen.

G 2.116 Datenverlust beim Kopieren oder Verschieben von Daten unter Windows Server 2003

Das Verschieben und Kopieren von Objekten oder ganzer Teilbäume aus oder in Verzeichnisse umfasst mehrere zum Teil versteckte Vorgänge, welche die bewegten Datenobjekte und Verzeichnisstrukturen unbrauchbar machen können. Die Gefährdung geht weniger vom einzelnen Benutzer aus, sondern eher von Administratoren, da sie zum Teil große oder systemkritische Datenbestände bewegen müssen.

Migrationsszenarien

Die klassische Gefahr, die oft bei Migrationsszenarien anzutreffen ist, stellt das Verschieben von Objekten des Dateisystems über Medien- oder Systemgrenzen hinweg dar. Vor dem Entfernen der Daten von ihrem Ursprungsort findet keine Kontrolle dieser Daten am Zielort statt. Die von der Verschiebung betroffenen Daten sind gegebenenfalls verloren.

Meta-Informationen von Objekten

Weniger offensichtlich ist das Verhalten der Meta-Informationen von Objekten, z. B. Zugriffsberechtigungen oder andere Attribute, die für mehrere Objekte gleichzeitig gelten. Oft sind komplexe Berechtigungsstrukturen mit automatischen Vererbungsmechanismen über die Verzeichnisstruktur gestülpt, die an Ursprungs- und Zielort unterschiedlich wirken. Beim Transfer von Dateien unterscheidet Microsoft Windows beispielsweise zwischen Kopieren und Verschieben einer Datei. Verschieben bewirkt die Mitnahme der vorhandenen Dateiberechtigungen zum Zielort, das Kopieren hingegen setzt die Dateiberechtigungen neu gemäß den Vorgaben am Zielort. Voraussetzung ist immer, dass Berechtigungen und andere Meta-Informationen am Zielort überhaupt korrekt interpretiert werden können. Sonst könnten gewachsene Berechtigungsstrukturen auf einen Schlag verloren gehen.

In Bezug auf die Wirkung von Kopier- und Verschiebemechanismen können Unterschiede bei einzelnen Komponenten auftreten, in Windows Server 2003 beispielsweise zwischen dem Dateisystem, den Komponentendiensten, den Internet Information Services (IIS) und dem Active Directory. Unkenntnis der Mechanismen hinter den Bedienkonzepten und mangelnde Sorgfalt können schnell zu Datenverlust und zur Fehlkonfiguration des Systems führen.

Unerwartete Effekte bei darunterliegenden Systemkomponenten

Unerwartete Effekte beim Kopieren und Verschieben sind nicht zuletzt auf darunterliegende Systemkomponenten zurückzuführen, die zur Speicherung und Erzeugung von Objekten und Verzeichnissen verwendet werden. Beispiele aus Windows Server 2003 sind Distributed File System (DFS), Active Directory oder das Encrypting File System (EFS). Beispielsweise beinhalten die Lese- und Schreibprozesse beim Kopieren/Verschieben im EFS Schritte zur Zwischenspeicherung und Kryptografie, greifen auf Zertifikatsdienste zurück und speichern öffentliche Schlüssel als Meta-Information ab. Unbedarftes Kopieren und Verschieben von Dateien und Verzeichnisbäumen kann schnell dazu führen, dass die Daten nicht mehr verfügbar oder nicht vollständig sind bzw. deren Vertraulichkeit nicht mehr gewährleistet ist.

Alternate Data Streams

Speziell beim Dateisystem NTFS können unerwartete Effekte durch Alternate Data Streams (ADS) in Dateien auftreten. ADS sind unsichtbare Bereiche innerhalb einer Datei, in denen Windows Server 2003 Zusatzinformationen abspeichern kann, z. B. Zoneninformationen oder Piktogramme. Die

Kommandozeile und der Windows Explorer weisen ein unterschiedliches Verhalten im Umgang mit ADS auf. Durch Verschiebe- und Kopiervorgänge können ADS versehentlich oder missbräuchlich verändert werden, verloren gehen oder ungewollt mit Inhalt gefüllt werden. Besteht kein ausreichender Schutz durch geeignete Dateiberechtigungen, dann können ADS zu einem potentiell sehr gefährlichen Angriffspunkt werden.

Beispiel:

Auf einem Domänencontroller wird unter Verwendung des Windows-Befehls *xcopy* der Inhalt vom Systemlaufwerk auf eine andere Festplattenpartition kopiert. Der Befehl wird mit bestimmten Parametern aufgerufen, welche auch das Kopieren der *SysVol*-Ordner bewirken. Nach dem Kopiervorgang wird die Sicherung nicht mehr benötigt und rekursiv gelöscht (z. B. mit *rd /s*). Danach sind jedoch alle Informationen, die normalerweise über den *SysVol*-Ordner repliziert werden, auf diesem Domänencontroller nicht mehr verfügbar (z. B. Gruppenrichtlinienobjekte, Anmeldeskripte). Die Ursache liegt in der Struktur der *SysVol*-Ordner, welche Verbindungspunkte (*Junction-Points*) zu DFS-Freigaben enthalten, die mit File Replication Service (FRS) erläutern repliziert werden. *Xcopy* sichert in diesem Falle nicht den gesamten Inhalt, sondern nur die Verbindungspunkte. Der spätere rekursive Löschvorgang erreicht über die kopierten Verbindungspunkte die originalen DFS-Freigaben und löscht Teile von deren Inhalt, sofern die Berechtigungen dies zulassen. Unter Umständen wird die Löschung noch auf andere Domänencontroller repliziert und somit der gesamte Domänenbetrieb gestört. Das Problem kann nun nur noch durch eine Wiederherstellung des kompletten Systemstatus aus der Datensicherung beseitigt werden.

G 2.117 Fehlende oder unzureichende Planung des WLAN-Einsatzes

Ein WLAN muss sorgfältig geplant und aufgebaut werden, damit nicht einzelne Sicherheitslücken alle hiermit vernetzten IT-Systeme beeinträchtigen kann. Dies kann sogar dazu führen, dass über ein unzureichend gesichertes WLAN ein damit gekoppeltes Behörden- oder Unternehmensnetz kompromittiert wird. Falls Sicherheitsmechanismen zwischen LAN und WLAN nicht abgestimmt sind, kann es dadurch auch zu Sicherheitslücken kommen, beispielsweise durch Mängel bei der Planung zur Trennung von Benutzergruppen.

Bei fehlender oder unzureichender Planung können sich eine Vielzahl von Problemen ergeben, wie beispielsweise die folgenden:

- Sensitive Daten könnten mitgelesen werden, wenn keine oder nur unzureichende Sicherheitsmaßnahmen im WLAN umgesetzt wurden.
- Die Leistungsfähigkeit eines Funknetzes könnte durch nicht beachtete andere WLAN-Installationen oder andere Funk-Systeme gemindert werden, wenn diese in den Nutzungsbereichs des Funknetzes hineinstrahlen.
- Falls bei der Planung eines WLANs die Gebäudedämpfung oder die Dämpfung durch absorbierende Ausbaumaterialien (beispielsweise Stahlschränke, Nasszellen, Versorgungsleitungen, Stahlbetonbauweise) nicht berücksichtigt wurde, kann dessen Leistungsfähigkeit ebenfalls reduziert werden.
- Gleichkanalstörungen aus einer benachbarten Funkzelle des eigenen WLAN sind eine weitere häufige Ursache für Störungen in einem WLAN. Hierdurch können sich zwei Teilnehmer benachbarter Zellen gegenseitig behindern, da sich deren Funkwellen im Raum überlagern und gegenseitig stören würden.
- Durch Funklöcher kann die Leistungsfähigkeit stark beeinträchtigt werden. Um Funklöcher zu vermeiden, wird bei unzureichender Planung des WLANs häufig einfach die Sendeleistung erhöht werden. Dadurch strahlt das WLAN eventuell in Bereiche hinein, in denen es nicht benötigt wird und in denen es unter Umständen abgehört werden kann.
- Eine Auswirkung mangelhafter Planung kann z. B. unzureichende Übertragungskapazität sein, durch die die Nutzung von bandbreitenintensiven Anwendungen eingeschränkt oder sogar verhindert werden kann.

Eine zusätzliche Gefährdung für das LAN entsteht dadurch, wenn nur eine unzureichende Absicherung der Verbindung zwischen den Access Points bzw. dem Distribution System und der kabelgebundenen Infrastruktur besteht. Erfolgt keine physikalische oder logische Absicherung auf der Ebene des Distribution System, so kann nach einer Kompromittierung der Absicherung der Luftschnittstelle bzw. der Sicherheitseinstellungen auf dem Access Point die gesamte Broadcast-Domäne, in der sich der Access Point befindet, abgehört werden. Die daraus gewonnenen Informationen könnten für einen Angriff auf das gesamte LAN genutzt werden.

Beispiel:

Werden für den Sicherheitsgateway am Übergabepunkt zwischen Distribution System und LAN die Filterregeln zu großzügig ausgelegt, kann ein Angreifer durch geschickte Manipulation der Kommunikationsdaten diesen Übergabepunkt durch einen Man-in-the-Middle-Angriff tunneln und somit Zugriff auf die interne LAN-Infrastruktur erlangen. Voraussetzung ist, dass entweder die Sicherheitsmechanismen auf der Luftschnittstelle kompromittiert wurden oder ein direkter Zugang zum Distribution System besteht. Außerdem könnten Schwachstellen auf Betriebssystemebene ebenfalls zur Tunnelung genutzt werden, falls diese die Systeme des Übergabepunktes nicht ausreichend gehärtet wurden.

G 2.118 Unzureichende Regelungen zum WLAN-Einsatz

Bei einem Access Point sind in der Regel in der Standard-Einstellung keine Sicherheitsmechanismen aktiviert. Werden WLAN-Komponenten wegen fehlender Vorgaben ungesichert in den Produktivbetrieb übernommen, stellt dies eine massive Gefährdung für das WLAN und daran angeschlossene IT-Systeme dar. Das ist vergleichbar mit der Gefährdung durch einen ungesicherten Internet-Anschluss. Sofern also ein Mitarbeiter, aufgrund fehlender Regelungen zum WLAN-Einsatz, einen ungenehmigten bzw. ungesicherten Access Point an ein internes Netz einer Institution anschließt, untergräbt er praktisch sämtliche im LAN ergriffenen Sicherheitsmaßnahmen, wie z. B. die Firewall zum Schutz gegen unberechtigte externe Zugriffe aus dem Internet.

Unklare Zuständigkeiten

Falls Zuständigkeiten nicht klar geregelt sind, kann es z. B. aufgrund fehlender Regelungen zur Administration der WLAN-Infrastruktur zu Fehlkonfigurationen der WLAN-Komponenten kommen. Bei fehlenden Vorgaben zum Konfigurationsmanagement kann es durch nur einen nicht gemäß vorgegebenem Standard-Profil konfigurierten Access Point oder WLAN-Client zu einer Kompromittierung des gesamten Netzes der Institution kommen.

Bei unzureichender Abstimmung der unterschiedlichen Zuständigkeiten innerhalb einer Institution sowie mit externen Dienstleistern kann es in der Praxis immer wieder zu Problemen kommen. Bezogen auf das WLAN ergeben sich Gefährdungen insbesondere dann, wenn für die Betreuung der physikalischen (passiven) Infrastruktur, der aktiven Netztechnik und der Sicherheitssysteme unterschiedliche Gruppen zuständig sind, die organisatorisch weit voneinander entfernt liegen und erst von einer entsprechend hohen Führungsebene koordiniert werden.

Probleme können sich auch ergeben, wenn keine einheitliche Regeln zur Dokumentation von Systemänderungen, wie beispielsweise Austausch von WLAN-Komponenten, Änderungen an Konfigurationen, Austausch der WLAN-Schlüsselinformationen, definiert sind.

Keine Regelungen für die Überwachung

Wurden auch zur Überwachung der WLAN-Infrastruktur keine Festlegungen getroffen und die entsprechenden finanziellen und personellen Ressourcen nicht bereitgestellt, werden Angriffe auf das WLAN eventuell nicht rechtzeitig erkannt. Hierzu zählen beispielsweise:

- Ohne regelmäßige Kontrollen wird unter Umständen übersehen, dass fremde Access Points (inklusive privater Access Points) an das Distribution System bzw. unmittelbar an das LAN angeschlossen wurden.
- Wenn die WLAN-Protokolle nicht regelmäßig ausgewertet werden, werden Sicherheitsvorfälle nicht rechtzeitig erkannt. So kann eine plötzliche Häufung fehlgeschlagener Anmeldevorgänge am Access Point auf Angriffsversuche hindeuten.

Werden dringend erforderliche Updates der Virenschutzsoftware oder sicherheitsrelevanter Patches nicht zeitgerecht eingespielt, kann es zur Kompromittierung einer WLAN-Komponente kommen. Besonders gefährdet sind hier WLAN-Komponenten mit direktem Zugriff auf das Internet oder bei der

Verwendung in öffentlichen WLANs. Je nach Art der Schadsoftware kann diese beim nächsten Verbinden mit dem Heimat-WLAN zur Kompromittierung der gesamten WLAN-Infrastruktur und darüber hinaus führen.

Fehlende Regelungen zur Reaktion auf Sicherheitsvorfälle im WLAN

Sofern es für den Betrieb eines WLANs keine Überlegungen gibt, wie im Notfall auf Vorfälle reagiert werden soll, kann dies dazu führen, dass es lange dauert, bis Sicherheitsprobleme erkannt und bereinigt werden. In der Zwischenzeit könnte es beispielsweise zu Datenabfluss oder zu Wurmattacken kommen. Sogar wenn Attacken bemerkt werden, werden eventuell aber Gegenmaßnahmen nicht zeitnah (innerhalb von Minuten) eingeleitet, wenn nicht auf entsprechend vorbereitete Maßnahmenkataloge, geregelte Abläufe und Befugnisse zu notwendigen Eingriffen zurückgegriffen werden kann.

Beispiel:

- Ein Unternehmen hatte Zugangsinformationen zu einem internen WLAN im Internet veröffentlicht, um mobilen Mitarbeitern den Zugriff von unterwegs zu vereinfachen. Jeder, der diese Informationen kennt, kann sich somit gegenüber dem WLAN authentisieren und erlangt Zugang zu eventuell schutzbedürftigen Daten. Obwohl das WLAN selber nur Informationen mit geringem Schutzbedarf enthielt, konnte über die Anbindung an ein LAN auf Produktivsysteme zugegriffen werden. Die dadurch erlangten Daten, beispielsweise geheime Konstruktionszeichnungen von einem Prototypen, wurden teilweise im Internet veröffentlicht. Andere wurden an einen Mitbewerber weitergegeben. Dieser hätte somit feststellen können, welche Neuentwicklungen geplant sind und schneller durch Eigenentwicklungen darauf reagieren können. Glücklicherweise hat er aber hierüber die Polizei informiert.

G 2.119 Ungeeignete Auswahl von WLAN-Authentikationsverfahren

Die Auswahl der zu verwendenden Authentikationsverfahren muss sich am Schutzbedarf der in einem WLAN transportierten Daten orientieren. Zunächst ist WEP als unsicher einzustufen und bietet eine Vielzahl von Angriffsmöglichkeiten, wie beispielsweise das Extrahieren der Schlüssel aus den Datenpaketen. Diese könnten dann zu einem erfolgreichen Zugriff auf ein WLAN benutzt werden.

Wird das Schlüsselmaterial, das für die Authentikation bzw. Verschlüsselung im WLAN verwendet wird, nicht sorgfältig verteilt oder ausreichend sicher gespeichert, so sind darauf aufbauende Methoden, um ein entsprechendes Sicherheitsniveau zu erreichen, eventuell vollkommen wertlos. Zu einfache Passwörter oder unzureichend geschützte Zertifikate bieten jedem Angreifer einen gültigen Zugang zu einem WLAN. Bei einem WPA-gesicherten WLAN stellen beispielsweise Pre-Shared Keys eine Sicherheitslücke dar, wenn diese nicht geeignet ausgewählt wurden, also nicht kompliziert genug sind.

Es gibt aber auch EAP-Methoden, die aufgrund einiger Schwachstellen eine Bedrohung darstellen. Beispielsweise wird bei EAP-MD5 CHAP als Authentisierungsmethode verwendet, das unter anderem die beidseitige Kenntnis eines unverschlüsselten Passworts erfordert. Weiterhin unterstützt EAP-MD5 keine Schlüsselerzeugung und kann daher nicht unmittelbar mit IEEE 802.11i benutzt werden.

Bei EAP-PEAP ist aus kryptographischer Sicht zu beanstanden, dass PEAP zur Sicherung des äußeren Tunnels nur die Identität des Servers prüft, nicht aber die des Clients.

Einige Implementationen von EAP-Methoden enthalten auch Schwachstellen. So ist das proprietäre EAP-LEAP von Cisco anfällig für sogenannte Wörterbuch-Attacken und es gibt Tools, die diese Schwachstelle bereits gezielt ausnutzen und selbst starke Passwörter wirkungslos sind.

Ebenso ist es von Nachteil, dass EAP-LEAP explizit von allen WLAN-Komponenten unterstützt werden muss und es keine Interoperabilität zwischen EAP-LEAP und anderen EAP-Methoden besteht, wie es in IEEE 802.1X gefordert ist.

G 2.120 Ungeeignete Aufstellung von sicherheitsrelevanten IT-Systemen

Werden sicherheitsrelevante IT-Systeme, auf denen Authentikationsdaten vorgehalten werden, an leicht zugänglichen Orten aufgestellt, kann dies zu einer massiven Gefährdung der Gesamtsicherheit eines Netzes führen. Zu den sicherheitsrelevanten IT-Systemen gehören z. B. Sicherheitsgateways, Directory Server, die einen Verzeichnisdienst für Benutzeridentitätsdaten bereitstellen oder IT-Systeme, auf denen Authentikationsdaten vorgehalten werden. Nicht geeignete Orte für deren Aufstellung sind beispielsweise öffentliche Besprechungsräume, Flure oder normale Büroräume. Auch kleinere, aber trotzdem sicherheitsrelevante Netzkoppelelemente wie Router, Switches oder Access Points dürfen nicht ungesichert in Durchgangswegen untergebracht werden. Ein Access Point sollte z. B. nicht ungeschützt direkt unter der Decke installiert werden. Hierdurch ist ein einfacher physischer Zugriff gegeben, durch den Zugriffsinformationen auf das zugehörige WLAN sehr einfach ausgelesen werden könnten. Falls ein direkter Zugriff auf sicherheitsrelevante IT-Systeme möglich ist, können dabei auch andere Sicherheitsmechanismen außer Kraft gesetzt werden.

Beispiel:

- Ein Access Point wird in einem öffentlichen Besprechungsraum aufgestellt, um einen drahtlosen Zugriff auf das Internet zu gewährleisten. Access Points stellen einen gewissen Wert dar, der zum Diebstahl verleiten kann. Bei einer Besprechung fällt auf, dass dieser Access Point nicht mehr vorhanden ist und es stellt sich heraus, dass er vor mehreren Wochen gestohlen wurde. Da ein Access Point in der Regel wichtige Informationen für den Zugriff auf das WLAN enthält, kann der Dieb unbehindert und unbemerkt Informationen für eine weitere Kompromittierung erlangen. Mit ihm sind z. B. wichtige Zertifikate für die Authentikation am WLAN entwendet worden. Bis zu deren Sperrung und Änderung war das Netz angreifbar.

Auch durch ungünstige Umgebungseinflüsse (z. B. Erschütterungen, unzulängliche klimatische Bedingungen oder eine hohe Staubbelastung) können Schäden an sicherheitsrelevanten IT-Systemen hervorgerufen werden.

G 2.121 Unzureichende Kontrolle von WLANs

Ein WLAN ist ein potentielles Ziel von Angriffen, sei es, um dieses unberechtigt nutzen zu können oder um dessen Verfügbarkeit zu stören (DoS-Angriffe). Diese könnten eine Kompromittierung der mit dem WLAN verbundenen Infrastruktur nach sich ziehen. Wenn keine ausreichende Kontrolle des WLANs stattfindet, werden Angriffe meistens überhaupt nicht oder nicht zeitnah erkannt.

Falsch konfigurierte Intrusion Detection Systeme

Werden bei der Planung für ein Intrusion Detection System die Kommunikationsmuster zum WLAN nicht mit betrachtet, so führt dies entweder dazu, dass Angriffe vom Intrusion Detection System nicht erkannt werden können, oder dass zulässige Kommunikation zu einem Alarm führt.

Eine akute Gefährdung kann auch bei der Protokollierung von IDS-relevanten Ereignissen entstehen:

- Wenn zu viele Informationen protokolliert bzw. zu lange gespeichert werden, besteht die Gefahr, dass die Datenbanken des Intrusion Detection Systems überlaufen.
- Werden bei der Protokollierung zu wenige oder die falschen Daten aufgezeichnet, wird eventuell ein Angriff nicht erkannt und es kann keine sinnvolle post-mortem-Analyse durchgeführt werden.

Unerlaubte Mitnutzung des WLANs

Sofern keine ausreichend starken Authentisierungsmechanismen für den Zugang zu einem WLAN implementiert sind, könnte ein Angreifer über eine WLAN-Installation beispielsweise auf das Internet zugreifen. Dadurch könnte die zur Verfügung stehende Bandbreite reduziert und die Antwortzeit für autorisierte WLAN-Nutzer erhöht werden. Ebenso könnte der so erlangte Internet-Zugang dazu verwendet werden,

- Angriffe auf andere Systeme im Internet durchzuführen,
- Spam-Mails zu verbreiten,
- strafrechtlich relevante Inhalte aus dem Internet herunterzuladen oder
- Internet-Tauschbörsen zu benutzen.

Keine Auswertung der Log-Dateien

Wenn Angreifer versuchen, sich an einem WLAN anzumelden, müssen sie zunächst die Authentisierung überwinden. Falls sie hierbei Wörterbuch- oder Brute-Force-Methoden anwenden, kommt es zu Fehlermeldungen bei den Authentisierungskomponenten, die diese in ihren Log-Dateien verzeichnen. Werden diese Protokoll-Dateien nicht regelmäßig ausgewertet, so können solche Angriffe nicht erkannt und entsprechende Gegenmaßnahmen ergriffen werden. Werden darüber hinaus erfolgreiche Anmeldungen nicht auf ihre Gültigkeit überprüft, so könnten Angreifer unbemerkt das WLAN mit gültigen ausgespähten Zugangsinformationen benutzen, sogar während die Mitarbeiter abwesend sind.

Beispiel:

Der Mitarbeiter Herr Müller ist für drei Wochen in Urlaub. Während dieser Zeit wurden seine Zugangsinformationen für das WLAN von einem Angreifer erfolgreich entschlüsselt. Dieser kann sich nun mit diesen Informationen erfolgreich und unbemerkt mit dem WLAN der Institution verbinden und auf alle Bereiche zugreifen, zu denen der Mitarbeiter zugelassen ist. Hierdurch könnten sogar sensible Daten erspäht werden. Bei einer regelmäßigen Analyse der Protokoll-Dateien des Authentisierungsservers hätte den Administratoren auffallen können, dass Herr Müller gar nicht anwesend ist und sich somit auch nicht mit dem WLAN verbinden kann. Ebenso hätte eine Urlaubssperre des WLAN-Accounts von Herrn Müller diesen Angriff verhindern können.

G 3 Gefährdungskatalog Menschliche Fehlhandlungen

G 3.57 Fehlerhafte Konfiguration des Betriebssystems für den IIS

G 3.58 Fehlerhafte Konfiguration eines IIS

G 3.59 Unzureichende Kenntnisse über Sicherheitslücken und Prüfwerkzeuge für den IIS

G 3.60 Fehlerhafte Konfiguration von Exchange 2000 Servern

G 3.61 Fehlerhafte Konfiguration von Outlook 2000 Clients

G 3.62 Fehlerhafte Konfiguration des Betriebssystems für den Apache Webserver

G 3.63 Fehlerhafte Konfiguration eines Apache Webservers

G 3.64 Fehlerhfte Konfiguration von Routern und Switchen

G 3.65 Fehlerhafte Administration von Routern und Switchen

G 3.66 Fehlerhafte Zeichensatzkonvertierung beim Einsatz von z/OS

G 3.67 Unzureichende oder fehlerhafte Konfiguration des z/OS-Betriebssystems

G 3.68 Unzureichende oder fehlerhafte Konfiguration des z/OS-Webservers

G 3.69 Fehlerhafte Konfiguration der Unix System Services unter z/OS

G 3.70 Unzureichender Dateischutz des z/OS-Systems

G 3.71 Fehlerhafte Systemzeit bei z/OS-Systemen

G 3.72 Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF

G 3.73 Fehlbedienung der z/OS-Systemfunktionen

G 3.74 Unzureichender Schutz der z/OS-Systemeinstellungen vor dynamischen Änderungen

G 3.75 Mangelhafte Kontrolle der Batch-Jobs bei z/OS

G 3.76 Fehler bei der Synchronisation mobiler Endgeräte

G 3.77 Mangelhafte Akzeptanz von IT-Sicherheitsmaßnahmen

G 3.78 Fliegende Verkabelung

G 3.79 Fehlerhafte Zuordnung von Ressourcen des SAN

G 3.80 Fehler bei der Synchronisation von Datenbanken

G 3.81 Unsachgemäßer Einsatz von Sicherheitsvorlagen für Windows Server 2003

G 3.82 Unsachgemäßer Einsatz von Sicherheitsvorlagen für Windows Server 2003

G 3.83 Fehlerhafte Konfiguration von VoIP-Komponenten

G 3.84 Fehlerhafte Konfiguration der WLAN-Infrastruktur

G 3.85 Verletzung von Brandschottungen

G 3.1 Vertraulichkeits-/Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer

Durch Fehlverhalten können IT-Benutzer den Vertraulichkeits- bzw. Integritätsverlust von Daten herbeiführen bzw. ermöglichen. Die Folgeschäden ergeben sich aus der Schutzbedürftigkeit der Daten. Beispiele für ein solches Fehlverhalten sind:

- Mitarbeiter holen versehentlich Ausdrucke mit personenbezogenen Daten nicht am Netzdrucker ab.
- Es werden Datenträger versandt, ohne dass die vorher darauf gespeicherten Daten physikalisch gelöscht wurden.
- Dokumente werden auf einem Webserver veröffentlicht, ohne dass geprüft wurde, ob diese tatsächlich zur Veröffentlichung vorgesehen und freigegeben sind.
- Aufgrund von fehlerhaft administrierten Zugriffsrechten vermag ein Mitarbeiter Daten zu ändern, ohne die Brisanz dieser Integritätsverletzung einschätzen zu können.
- Neue Software wird mit nicht anonymisierten Daten getestet. Nicht befugte Mitarbeiter erhalten somit Einblick in geschützte Dateien bzw. vertrauliche Informationen. Möglicherweise erlangen überdies auch Dritte Kenntnis von diesen Informationen, weil die Entsorgung von "Testausdrucken" nicht entsprechend geregelt ist.
- Beim Ausbau, Verleih, Einsendung zur Reparatur oder Ausmusterung von Festplatten können Daten auf zum Teil intakten Dateisystemen in unbefugte Hände gelangen.

Betreut ein Outsourcing-Dienstleister mehrere Mandanten, so können Daten einer auslagernden Organisation durch menschliches Versagen anderen Mandanten des Outsourcing-Dienstleisters zugänglich werden.

Mögliche Ursachen können beispielsweise folgende sein:

- Falsches Routing einer Druckausgabe.
- Auswahl einer falschen E-Mail-Adresse aus dem Adressbuch.
- Fehler in einer Datenbank.
- Unbedachtes "copy - paste" (z. B. von Konfigurationsdateien von Systemen verschiedener Auftraggeber).
- Postversand (z. B. von Backup-Medien, Verträgen) an die falsche Adresse.

G 3.2 Fahrlässige Zerstörung von Gerät oder Daten

Durch Fahrlässigkeit, aber auch durch ungeschulten Umgang kann es zu Zerstörungen an Geräten und Daten kommen, die den Betrieb des IT-Systems empfindlich stören können. Dies ist auch durch die unsachgemäße Verwendung von IT-Anwendungen möglich, wodurch fehlerhafte Ergebnisse entstehen oder Daten unabsichtlich verändert oder zerstört werden. Durch unachtsames Benutzen eines einzigen Löschbefehls können ganze Dateistrukturen gelöscht werden.

Beispiele:

- Benutzer, die aufgrund von Fehlermeldungen den Rechner ausschalten, statt ordnungsgemäß alle laufenden Anwendungen zu beenden bzw. einen Sachkundigen zu Rate zu ziehen, können hierdurch schwerwiegende Integritätsfehler in Datenbeständen hervorrufen.
- Durch umgestoßene Kaffeetassen oder beim Blumengießen eindringende Feuchtigkeit können in einem IT-System Kurzschlüsse hervorrufen werden.
- In einem z/OS-System verfügte ein Systemprogrammierer über die Berechtigung, das Programm *ICKDSF* zum Formatieren von Festplatten aufzurufen. Als er zur Ausübung seiner Tätigkeit dringend eine Festplatte benötigte, wählte er aus dem vorhandenen Pool eine freie Festplatte aus, gab jedoch aufgrund eines Tippfehlers eine falsche Adresse an. Den im System-Log anstehenden Reply las er nur flüchtig und beantwortete ihn sofort. Die Formatierung einer bereits belegten Festplatte wurde dadurch freigegeben und wichtige Produktionsdaten zerstört.
- Ein Benutzer, der es sich zur Gewohnheit gemacht hat, unter Unix den Löschbefehl *rm* grundsätzlich ohne den Parameter für die Sicherheitsabfragen (*-i*) durchzuführen oder gar mit *-f* die Sicherheitsabfragen grundsätzlich ausschaltet, riskiert in hohem Maße das versehentliche Löschen von Dateien. Ähnliches gilt auch für den Befehl *del* *.* unter MS-DOS.

G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen

Aufgrund von Nachlässigkeit und fehlenden Kontrollen kommt es immer wieder vor, dass Personen die ihnen empfohlenen oder angeordneten IT-Sicherheitsmaßnahmen nicht oder nicht im vollen Umfang durchführen. Es können Schäden entstehen, die sonst verhindert oder zumindest vermindert worden wären. Je nach der Funktion der Person und der Bedeutung der missachteten Maßnahme können sogar gravierende Schäden eintreten.

Vielfach werden IT-Sicherheitsmaßnahmen aus einem mangelnden Sicherheitsbewusstsein heraus nicht beachtet. Ein typisches Indiz dafür ist, dass wiederkehrende Fehlermeldungen nach einer gewissen Gewöhnungszeit ignoriert werden.

Beispiele:

- Der verschlossene Schreibtisch bietet zur Aufbewahrung von Disketten oder anderen Informationsträgern keinen hinreichenden Schutz gegen unbefugten Zugriff, wenn der Schlüssel im gleichen Büro aufbewahrt wird, z. B. auf dem Schrank oder im Zettelkasten.
- Geheimzuhaltende Passwörter werden schriftlich fixiert in der Nähe eines Terminals oder PCs aufbewahrt.
- Obwohl die schadensmindernde Eigenschaft von Datensicherungen hinreichend bekannt ist, treten immer wieder Schäden auf, wenn Daten unvorhergesehen gelöscht werden und aufgrund fehlender Datensicherung die Wiederherstellung unmöglich ist. Dies zeigen insbesondere die dem BSI gemeldeten Schäden, die z. B. aufgrund von Computer-Viren entstehen.
- Der Zutritt zu einem Rechenzentrum sollte ausschließlich durch die mit einem Zutrittskontrollsystem (z. B. Magnetstreifenleser, Chipkartenleser oder biometrische Verfahren) gesicherte Tür erfolgen. Die Fluchttür wird jedoch, obwohl sie nur im Notfall geöffnet werden darf, als zusätzlicher Ein- und Ausgang genutzt.
- In einem z/OS-System liefen täglich Batch-Jobs für die RACF-Datenbank-Sicherungen. Die korrekte Ausführung dieser Abläufe sollte täglich von den zuständigen Administratoren geprüft werden. Da die Sicherungen jedoch über mehrere Monate ohne Probleme durchgeführt wurden, kontrollierte niemand mehr den Ablauf. Erst nachdem die RACF-Datenbanken des Produktionssystems defekt waren und die Sicherungen zurückgespielt werden sollten, wurde festgestellt, dass die Batch-Jobs seit mehreren Tagen nicht mehr gelaufen waren. Dies führte dazu, dass keine aktuellen Sicherungen vorhanden waren und die Änderungen der letzten Tage von Hand nachgetragen werden mussten. Neben einem erheblichen zusätzlichen Administrationsaufwand ergab sich dadurch ein Unsicherheitsfaktor, da nicht alle Definitionen sicher rekonstruiert werden konnten.

G 3.4 Unzulässige Kabelverbindungen

Hauptursache unzulässiger Verbindungen ist neben technischen Defekten die fehlerhafte Verkabelung, z. B. bei der Belegung von Rangier- und Spleißverteilern. Ungenaue Dokumentation und unzureichende Kabelkennzeichnung führen häufig zu versehentlichen Fehlbelegungen und erschweren das Erkennen von absichtlichen Fehlbelegungen.

Durch unzulässige Verbindungen können Informationen zusätzlich oder ausschließlich zu falschen Empfängern übertragen werden. Die normale Verbindung kann gestört werden.

G 3.5 Unbeabsichtigte Leitungsbeschädigung

Je ungeschützter ein Kabel verlegt ist, desto größer ist die Gefahr einer unbeabsichtigten Beschädigung. Die Beschädigung führt nicht unbedingt sofort zu einem Ausfall von Verbindungen. Auch die zufällige Entstehung unzulässiger Verbindungen ist möglich. Typische Beispiele für solche Beschädigungen sind:

Im Innenbereich:

- Herausreißen der Geräteanschlussleitung mit dem Fuß bei "fliegender" Verlegung,
- Beschädigung unter Putz verlegter Leitungen durch Bohren oder Nageln,
- Eindringen von Wasser in Fensterbank-Kanäle,
- Eindringen von Wasser in Fußbodenkanäle bei der Gebäudereinigung,
- Beschädigung auf Putz oder Estrich verlegter Leitungen beim Transport sperriger und schwerer Gegenstände.

Im Außenbereich:

- Beschädigung bei Tiefbauarbeiten, sowohl durch Handschachtung als auch durch Bagger,
- Eindringen von Wasser in Erdtrassen/Erdkabel,

Beispiel:

In einer Fußgängerzone hatte es sich die Putzfrau eines kleinen Geschäftes zu Angewohnheit gemacht, das gebrauchte Putzwasser in den direkt vor der Ladentür befindlichen Revisionsschacht einer Post-Kabeltrasse zu schütten. Das Wasser verdunstete zwar mit der Zeit immer wieder, der Schmutz- und Seifenanteil jedoch lagerte sich auf den Kabeln ab und musste für Arbeiten daran erst mühsam und zeitaufwendig entfernt werden.

- Beschädigung von Kabeln durch Nagetiere,
- Beschädigung von Trassen und Kabeln durch Wurzeln (Baumwurzeln besitzen genug Kraft, um Kabel abzuquetschen),
- Beschädigung durch Überschreitung zulässiger Verkehrslasten (Rohre können brechen, Kabel können abscheren).

G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal

Es ist bereits nicht immer ganz einfach, eigene Mitarbeiter ausreichend zum richtigen Umgang mit IT zu schulen. Bei Betriebsfremden kann grundsätzlich nicht vorausgesetzt werden, dass sie mit der IT entsprechend den Vorgaben der besuchten Institution umgehen, vor allem, da sie diese in den seltensten Fällen kennen.

Die Gefährdung durch Besucher, Reinigungs- und Fremdpersonal erstreckt sich von der unsachgemäßen Behandlung der technischen Einrichtungen, über den Versuch des "Spielens" an IT-Systemen gegebenenfalls bis zum Diebstahl von IT-Komponenten.

Beispiele:

- Besucher können, wenn sie unbegleitet sind, Zugriff auf Unterlagen, Datenträger oder Geräte haben, diese beschädigen oder unbefugt in Kenntnis von schützenswerten Infornationen gelangen.
- Durch Reinigungspersonal kann versehentlich eine Steckverbindung gelöst werden, Wasser kann in Geräte gelangen, Unterlagen können verlegt oder sogar mit dem Abfall entfernt werden.
- In einem Rechenzentrum sollten in den Maschinenräumen Malerarbeiten durchgeführt werden. Der Maler stieß mit der Leiter versehentlich an den zentralen Notausschalter der Stromversorgung und löste diesen aus. Die gesamte Stromversorgung der z/OS-Systeme in diesem Rechenzentrum war sofort unterbrochen. Durch den Stromausfall waren mehrere Platten (DASD - Direct Access Storage Device) nicht sofort verfügbar. Der hinzugezogene Techniker benötigte mehrere Stunden, bis die Produktion wieder anlaufen konnte.

G 3.7 Ausfall der TK-Anlage durch Fehlbedienung

Neben dem technischen Versagen durch Defekt von Bauteilen, Stromausfall oder Sabotage gibt es eine Reihe weiterer Umstände, die zum Ausfall einer TK-Anlage führen können. So können z. B. durch unzureichend ausgebildetes Wartungspersonal Änderungen an der Anlagenkonfiguration vorgenommen werden, die solche Ausfälle zur Folge haben. Das nicht rechtzeitige Erkennen von Alarmsignalen oder abnormem Betriebsverhalten kann dieselbe Folge haben, ferner unsachgemäßes oder unüberlegtes Handeln bei eigentlich einfachen Routinereparaturen.

G 3.8 Fehlerhafte Nutzung des IT-Systems

Eine fehlerhafte Nutzung des IT-Systems beeinträchtigt die Sicherheit eines IT-Systems, wenn dadurch IT-Sicherheitsmaßnahmen missachtet oder umgangen werden.

Beispielsweise können zu großzügig vergebene Rechte, leicht zu erratende Passwörter, nicht ausreichend geschützte Datenträger mit Sicherungskopien oder bei vorübergehender Abwesenheit nicht gesperrte Terminals zu IT-Sicherheitsvorfällen führen.

Gleichermaßen können durch fehlerhafte Bedienung von IT-Systemen oder IT-Anwendungen Daten versehentlich gelöscht oder verändert werden.

G 3.9 Fehlerhafte Administration des IT-Systems

Eine fehlerhafte Administration beeinträchtigt die Sicherheit eines IT-Systems, wenn dadurch IT-Sicherheitsmaßnahmen missachtet oder umgangen werden.

unsichere Netzzugänge

Eine fehlerhafte Administration liegt z. B. vor, wenn Netzzugangsmöglichkeiten geschaffen oder nicht verhindert werden, die für den ordnungsgemäßen Betrieb des IT-Systems nicht notwendig sind oder auf Grund ihrer Fehleranfälligkeit eine besonders große Bedrohung darstellen.

unnötige Zugriffsrechte

Ein häufiges Problem ist, dass bei Arbeiten am System Zugangskonten verwendet werden, die mehr Zugriffsrechte besitzen, als für die Tätigkeit unbedingt nötig sind. Hierdurch erhöht sich unnötig die Gefahr von Schäden durch Viren und Trojanischen Pferden. Alle Zugangskonten, die nicht mehr benötigt werden, müssen deaktiviert werden.

mangelhafte Anpassungen

Standard-Installationen von Betriebssystemen oder Systemprogrammen weisen in den seltensten Fällen alle Merkmale einer sicheren Installation auf. Mangelnde Anpassungen an die konkreten Sicherheitsbedürfnisse können hier ein erhebliches Risiko darstellen. Die Gefahr von Fehlkonfigurationen besteht insbesondere bei komplexen Sicherheitssystemen, wie zum Beispiel RACF unter z/OS. Viele Systemfunktionen beeinflussen sich gegenseitig.

Besondere Beachtung müssen Systeme finden, deren fehlerhafte Administration Einfluss auf den Schutz anderer Systeme haben (Firewalls).

Jede Modifikation von Sicherheitseinstellungen und die Erweiterung von Zugriffsrechten stellt eine potentielle Gefährdung der Gesamtsicherheit dar.

Beispiele:

unzureichende Protokollierung

- Über das bei G 3.8 *Fehlerhafte Nutzung des IT-Systems* gesagte hinaus kann der Systemadministrator durch eine fehlerhafte Installation neuer oder vorhandener Software Gefährdungen schaffen. Eine fehlerhafte Administration liegt auch vor, wenn Protokollierungsmöglichkeiten nicht genutzt oder vorhandene Protokolldateien nicht ausgewertet werden, wenn zu großzügig Zugangsberechtigungen vergeben und diese dann nicht in gewissen Abständen kontrolliert werden, wenn Login-Namen oder UIDs mehr als einmal vergeben werden oder wenn vorhandene Sicherheitstools, wie z. B. unter Unix die Benutzung einer *shadow*-Datei für die Passwörter, nicht genutzt werden.

Alterung von Passwörtern

- Mit dem Lebensalter von Passwörtern sinkt deren Wirksamkeit. Grund dafür ist die sich stetig erhöhende Wahrscheinlichkeit eines erfolgreichen Angriffes.
- Der Administration eines Firewall-Systems gilt es besondere Aufmerksamkeit zu schenken, da dieses Voraussetzung für den Schutz einer Vielzahl anderer Systeme ist.
- In einem z/OS-System wurden die Dateien der Anwender durch RACF-Profile via *Universal Access* derart geschützt, dass niemand unkontrolliert darauf zugreifen konnte (*UACC = NONE*). Durch eine Unachtsamkeit des Administrators erlaubte ein Eintrag in der *Conditional Access List* des Profils allen IDs (* Eintrag) den Zugriff *READ*. Als Folge konnte trotz der

Definition *UACC=NONE* jeder Anwender im System über die *Conditional Access List* die Dateien einsehen.

G 3.10 Falsches Exportieren von Dateisystemen unter Unix

Exportierte Platten können von jedem Rechner, der sich mit dem in der Datei */etc/exports* bzw. */etc/dfs/dfstab* angegebenen Namen meldet, gemountet werden. Der Benutzer dieses Rechners kann jede UID und GID annehmen. Solange Verzeichnisse nicht mit der Option *root=* exportiert wurden, stellt die UID 0 (*root*) eine Ausnahme dar, die beim Zugriff auf einen NFS-Server üblicherweise auf eine andere UID (z. B. die des Benutzers *nobody* oder *anonymous*) abgebildet wird. Es lassen sich daher nur Dateien schützen, die *root* gehören.

Für die Verwendung der Protokolle NFS für den Export von Dateisystemen und die Verteilung von Systemdateien mittels NIS sind keine ausreichenden Schutzmaßnahmen in geschützten Umgebungen verfügbar. Der Einsatz stellt somit eine Gefährdung der Integrität der Systeme dar.

G 3.11 Fehlerhafte Konfiguration von sendmail

Fehler in der Konfiguration oder Software von *sendmail* haben in der Vergangenheit schon mehrmals zu Sicherheitslücken auf den betroffenen IT-Systemen geführt (Stichwort Internet-Wurm).

Beispiel:

Es ist durch verschiedene Veröffentlichungen bekannt, dass es möglich ist, die Benutzer- und Gruppenkennung, die mit den Optionen *u* und *g* eingestellt sind (normalerweise *daemon*) zu erlangen. Dazu muss im Absenderfeld (*From:*) eine Pipe angegeben werden, durch die eine fehlerhafte Mail zurückgeschickt wird, und in der Mail selber muss ein Fehler erzeugt werden. Schickt man also z. B. eine Mail mit dem Inhalt

```
cp /bin/sh /tmp/sh
chmod oug+rsx /tmp/sh
```

an einen unbekannten Empfänger und benutzt als Absender ‘ */bin/sh* ‘, so wird die Mail als unzustellbar zurückgeschickt, was in diesem Falle einer Ausführung des kurzen Shellskripts gleichkommt. Durch dieses Skript wird dann eine Shell mit gesetztem *suid*-Bit erzeugt, die die im *sendmail.cf* gesetzte Benutzer- und Gruppenkennung hat.

G 3.12 Verlust der Datenträger beim Versand

Werden Datenträger in nicht sonderlich stabilen Behältnissen (Briefumschlägen oder sonstigen Verpackungen) versandt, besteht die Gefahr, dass der Datenträger (insbesondere Disketten) bei Beschädigung der Verpackung verloren geht. Auch besteht die Gefahr des Verlustes auf dem Postweg oder durch Unachtsamkeit eines Boten. Falls beispielsweise eine Diskette zusammen mit einem Anschreiben in einem Umschlag verschickt wird, der wesentlich größer als die Diskette ist, so kann beim Empfang des Umschlages die innenliegende Diskette übersehen und zusammen mit dem scheinbar leeren Umschlag entsorgt werden.

G 3.13 Übertragung falscher oder nicht gewünschter Datensätze

Es ist denkbar, dass der für den Versand vorgesehene Datenträger bereits Daten früherer Arbeitsgänge enthält, die dem Empfänger nicht zur Kenntnis gelangen sollen. Werden diese Daten nicht gezielt physikalisch gelöscht, können diese vom Empfänger gelesen werden.

Befinden sich darüber hinaus die zu übertragenden Daten in einem Verzeichnis mit weiteren Daten, die ebenfalls schutzbedürftig sind, besteht die Gefahr, dass diese versehentlich mit auf den Datenträger übertragen werden (z. B. durch *copy* *.*) und dem Empfänger unnötig (unberechtigt) zur Kenntnis gelangen.

Sollen Datensätze nicht über das Medium "Datenträger", sondern über Datennetze direkt versandt werden (E-Mail im Internet, Modem-Verbindung, interne Firmennetze, X.400-Dienst), bieten Kommunikationsprogramme die Möglichkeit der Verwendung von Kurzbezeichnungen für komplexe Adressstrukturen und Verteilerlisten für die Mehrfachversendung. Werden solche Verteilerlisten nicht zentral geführt oder nicht in regelmäßigen Abständen aktualisiert, können Datensätze an Adressen versendet werden, die zu nicht mehr autorisierten Personen gehören.

G 3.14 Fehleinschätzung der Rechtsverbindlichkeit eines Fax

Häufig wird versucht, bei eiligen Entscheidungen den Postweg einzusparen, indem wichtige Unterlagen oder Informationen an den Geschäftspartner per Fax übermittelt werden. Dabei wird oft außer Acht gelassen, dass so übermittelte Unterlagen in einem Streitfall nicht immer als rechtsverbindlich angesehen werden. Bestellungen müssen dann nicht vom Kunden angenommen, Zusagen nicht eingehalten werden. Eine Rechtsmittelfrist kann trotz rechtzeitigen Absendens eines Fax ablaufen.

G 3.15 Fehlbedienung eines Anrufbeantworters

Grundsätzlich besteht die Gefahr der Fehlbedienung eines Anrufbeantworters. Bei einigen Geräten ist die Gefahr eines Bedienungsfehlers recht hoch, da sie beispielsweise mit Funktionstasten versehen sind, die doppelt oder zum Teil sogar dreifach belegt sind. Erschwerend kann hinzukommen, dass die Bedientasten so klein sind und so nahe nebeneinander liegen, dass Fehlgriffe kaum vermeidbar sind.

So ist es durchaus möglich, dass der Anrufbeantworter aufgrund von Fehlbedienungen einen Anruf erst gar nicht entgegennimmt. Dies geschieht zum Beispiel, wenn man versehentlich das Gerät deaktiviert oder den Ansagetext mittels Tastendruck gelöscht hat.

G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten

Zugangsrechte zu einem IT-System und Zugriffsrechte auf gespeicherte Daten und IT-Anwendungen dürfen nur in dem Umfang eingeräumt werden, wie sie für die Wahrnehmung der Aufgaben erforderlich sind. Werden diese Rechte fehlerhaft administriert, so kommt es zu Betriebsstörungen, falls erforderliche Rechte nicht zugewiesen wurden, bzw. zu Sicherheitslücken, falls über die notwendigen Rechte hinaus weitere vergeben werden.

Beispiel:

Durch eine fehlerhafte Administration der Zugriffsrechte hat ein Sachbearbeiter die Möglichkeit, auf die Protokolldaten zuzugreifen. Durch gezieltes Löschen einzelner Einträge ist es ihm daher möglich, seine Manipulationsversuche am Rechner zu verschleiern, da sie in der Protokolldatei nicht mehr erscheinen.

G 3.17 Kein ordnungsgemäßer PC-Benutzerwechsel

Arbeiten mehrere Benutzer an einem PC, so kann es aufgrund von Nachlässigkeit oder Bequemlichkeit dazu kommen, dass sich bei einem Wechsel der vorhergehende Benutzer nicht abmeldet und der neue sich nicht ordnungsgemäß anmeldet. Dies wird von den Betroffenen meist damit begründet, dass die Zeit, die das IT-System zum Neustarten benötigt, sehr lang ist und als nicht akzeptabel empfunden wird.

Dieses Fehlverhalten führt jedoch dazu, dass die Protokollierung von An- und Abmeldevorgängen und damit ein Teil der Beweissicherung unwirksam wird. Es lässt sich anhand der Protokolle nicht mehr zuverlässig feststellen, wer den Rechner zu einem bestimmten Zeitpunkt genutzt hat.

Beispiel:

- Ein PC wird abwechselnd von drei Benutzern eingesetzt, um Reisekostenabrechnungen durchzuführen. Nachdem der erste Benutzer den Anmeldevorgang durchgeführt hat, erfolgt kein ordnungsgemäßer PC-Benutzerwechsel mehr, weil die damit verbundenen Ab- und Anmeldevorgänge aus Bequemlichkeit nicht durchgeführt werden.
- Aufgrund von Unregelmäßigkeiten wird geprüft, wer welchen Vorgang am Rechner bearbeitet hat. Da nach Protokollierung nur ein Benutzer am PC gearbeitet hat, kann der Verursacher im Nachhinein nicht mehr festgestellt werden bzw. der einzige angemeldete Benutzer muss die Konsequenzen tragen.

G 3.18 Freigabe von Verzeichnissen, Druckern oder der Ablagemappe

mangelhafter Passwortschutz unter WfW

Unter Windows für Workgroups sind bei der Benutzung des Datei- oder Druckmanagers bzw. der Zwischenablage bei der Freigabe von Verzeichnissen, Druckern oder Seiten der Ablagemappe Bedienungsfehler möglich. Dies kann zur Folge haben, dass ungewollt Ressourcen freigegeben werden. Der notwendige Passwortschutz wird eventuell nicht oder nur unzureichend eingesetzt, wenn die Benutzer nicht ausreichend über die Peer-to-Peer-Funktionalität in Windows für Workgroups unterrichtet worden sind.

Zu beachten ist weiterhin, dass ein freigegebenes Verzeichnis automatisch beim nächsten Start wieder freigegeben wird, ohne dass der Benutzer es bemerkt, falls die Freigabeoption *Beim nächsten Start wieder freigeben* aktiviert ist.

Unter Windows 95 müssen bei der Freigabe explizit Zugriffsberechtigungen vergeben werden, so dass sich jeder Benutzer bewusst machen muss, dass und wem der Zugriff ermöglicht werden soll. Unter Windows NT/2000 kann nur ein Administrator bzw. Hauptbenutzer Dateien und Verzeichnisse freigeben.

unterschiedliche Protokolle unter Unix und Linux

Auf IT-Systemen unter Unix oder Linux existieren eine ganze Reihe von Möglichkeiten, anderen IT-Systemen über das Netz Ressourcen zur Verfügung zu stellen. Dies kann beispielsweise durch die Installation von SAMBA, die Einrichtung von NFS-Shares oder die Aktivierung des FTP-Daemons erfolgen. Hierzu sind in der Regel Supervisor-Rechte erforderlich, bestimmte Dienste lassen sich jedoch auch so konfigurieren, dass sie so genannte nicht-privilegierte Ports nutzen und somit auch von normalen Benutzern gestartet werden können. Dadurch besteht die Gefahr, dass ungewollt Ressourcen über das Netz zur Verfügung gestellt werden.

Missbrauch der freigegebenen Ressourcen

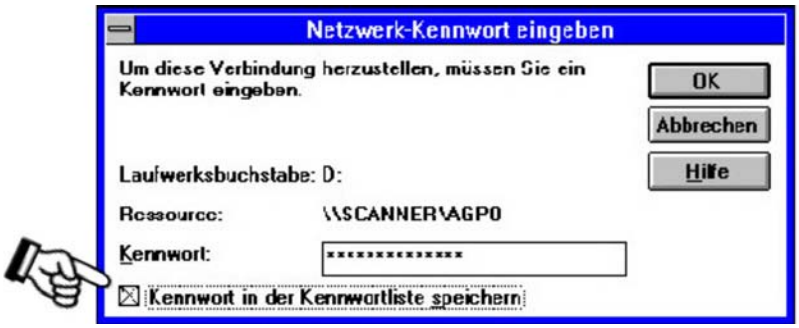
Da freigegebene Ressourcen (ausgenommen sind die Seiten der Ablagemappe) im Allgemeinen für alle Teilnehmer angezeigt werden, können andere Teilnehmer solche erkennen und ggf. missbrauchen. Unter Umständen werden vertrauliche Daten gelesen, Daten unautorisiert verändert oder gelöscht. Wurde beispielsweise ein Verzeichnis ohne Passwortschutz zum Beschreiben freigegeben, ist es möglich, in dieses solange Dateien zu speichern, bis die Kapazität der Festplatte erschöpft ist.

Beispiel:

Nach der Einführung der WfW-Benutzeroberfläche in einem servergestützten LAN, die nicht durch eine Schulung begleitet war, hatten rund 10% der Benutzer ungewollt die komplette Festplatte (Stammverzeichnis C:\) freigegeben.

G 3.19 Speichern von Passwörtern unter WfW und Windows 95

Der Zugriff auf Verzeichnisse, Drucker oder Seiten der Ablagemappen, die von anderen freigegeben wurden, wird unter WfW und Windows 95 dadurch erleichtert, dass die dazu benötigten Passwörter in der Datei [*anmeldename*].*pwl* gespeichert werden können. Dazu kann die Option "Kennwort in der Kennwortliste speichern" gewählt werden. Ist diese Option durch Voreinstellung aktiviert, kann es auch ungewollt dazu kommen, dass Passwörter gespeichert werden. Unter Windows 95 in Netware-Netzen werden die Anmeldepasswörter automatisch in der Datei [*anmeldename*].*pwl* gespeichert, die Zugriffsrechte aber grundsätzlich auf Benutzer-Ebene erteilt.



Ein Dritter, der sich Zugang zu einem WfW- oder Windows 95-Rechner verschafft, hat unmittelbaren Zugriff auf die Kennwortliste ([*anmeldename*].*pwl*). Die dort gespeicherten Passwörter für den Zugriff auf Ressourcen anderer werden durch das WfW- bzw. Windows 95-Anmeldepasswort geschützt. Ist dieses deaktiviert oder bekannt bzw. ist WfW oder Windows 95 bereits ohne Bildschirmsperre aktiv, können Unberechtigte Verbindungen zu anderen Rechnern herstellen.

Hinweis:

Mittlerweile werden im Internet Programme angeboten, die eine Entschlüsselung der PWL-Dateien unter WfW ohne Kenntnis des Anmeldepasswortes ermöglichen. Die in diesen Dateien gespeicherten Passwörter sind in vielen Fällen auch über die windows-spezifische, temporäre Auslagerungsdatei *386spart.par* im Klartext zu gewinnen. Daher muss ein entsprechender Zugangsschutz zum PC oder ein Zugriffsschutz auf Dateiebene installiert sein.

G 3.20 Ungewollte Freigabe des Leserechtes bei Schedule+

Im Lieferumfang von WfW ist das Programm *mail* und der Terminplaner *Schedule+* enthalten. Wird von mehreren Benutzern ein gemeinsames Post-Office unter *mail* genutzt, kann auch eine gemeinsame Terminplanung mit *Schedule+* erfolgen. Dort können dann Zugriffsprivilegien für den eigenen Terminkalender vergeben werden. Standardmäßig ist für jeden Teilnehmer desselben Post-Office das Zugriffsrecht "Offene/Besetzte Zeitblöcke anzeigen" für den privaten Kalender aktiviert, so dass, falls dieses Recht nicht explizit entzogen wird, das zeitliche Arrangement - nicht jedoch der Inhalt - des privaten Kalenders von anderen eingesehen werden kann. Der private Nutzer könnte jedoch in dem Glauben sein, dass seine offenen/besetzten Zeitblöcke nicht eingesehen werden können, da er keine Zugriffsrechte verteilt hat.

G 3.21 Fehlbedienung von Codeschlössern

Erfahrungsgemäß führen Fehler in der Bedienung von mechanischen Codeschlössern verhältnismäßig oft dazu, dass der Schrank nicht mehr ordnungsgemäß geöffnet werden kann. Die Fehlbedienungen treten bei der Eingabe und besonders häufig bei der Änderung des Codes auf. Um die aufbewahrten Datenträger oder informationstechnischen Geräte wieder zugänglich zu machen, muss dann ein spezialisierter Schlüsseldienst beauftragt werden, so dass neben dem Schaden, der aus der fehlenden Verfügbarkeit der Datenträger oder Geräte entsteht, auch erhebliche Reparaturkosten anfallen können. Im ungünstigsten Falle muss ein neuer Schutzschrank beschafft werden.

G 3.22 Fehlerhafte Änderung der Registrierung

Windows-Betriebssysteme ab Windows 95 bieten die Möglichkeit, die Benutzerumgebung eines PC fest bzw. benutzerindividuell einzuschränken. Dies geschieht in der Regel unter Verwendung des Systemrichtlinieneditors (unter Windows 95 *POLEDIT.EXE*) oder des Registrierungseditors (unter Windows 95 *REGEDIT.EXE*). Unter Windows NT/2000/XP werden die Registrierungseditoren *regedt32.exe*, *regedit.exe* sowie das kommandozeilenorientierte Werkzeug *reg.exe* eingesetzt, um die Registrierung zu bearbeiten.

Die Benutzung dieser Programme sollte mit Bedacht und jede Änderung der Registrierung mit äußerster Sorgfalt ausschließlich durch geschultes Personal erfolgen, weil sehr schnell ein Systemzustand eingestellt werden kann, der ein Arbeiten mit dem PC nicht mehr erlaubt. Im ungünstigsten Fall ist dann das Betriebssystem neu zu installieren oder bestimmte Hardware-Komponenten erneut zu initialisieren (durch Laden der entsprechenden Treiber).

Unter Windows NT/2000/XP sind Registrierungseinträge durch Zugriffsrechte geschützt. Die Sicherheitseinstellungen für Registrierungsschlüssel können unter Windows NT/2000 nur mit dem Registrierungseditor *regedt32.exe* festgelegt werden. Unter Windows XP kann dazu sowohl *regedt32.exe* als auch *regedit.exe* verwendet werden. Durch falsche Konfiguration der Zugriffsrechte kann ein Benutzer die Registrierung wissentlich oder unwissentlich auf unerlaubte Weise modifizieren. Unsachgemäße Änderungen können dabei zu Systemschäden führen, so dass die Sicherheit und/oder die Arbeitsfähigkeit des Arbeits-PCs bzw. im Extremfall des gesamten Netzes gefährdet ist.

G 3.23 Fehlerhafte Administration eines DBMS

Wird ein Datenbankmanagementsystem (DBMS) nachlässig oder fehlerhaft administriert, kann dies folgende Gefährdungen nach sich ziehen:

- Verlust von Daten,
- (gezielte oder unbeabsichtigte) Datenmanipulation,
- unberechtigter Zugang zu vertraulichen Daten,
- Verlust der Datenbankintegrität,
- Crash der Datenbank und
- Zerstörung der Datenbank.

Die oben aufgeführten Gefährdungen können durch zu großzügig vergebene Rechte für die Benutzer, durch eine unregelmäßige oder gar keine Datenbanküberwachung, durch mangelhafte Datensicherungen, durch ungültige, aber noch nicht gesperrte Kennungen usw. hervorgerufen werden.

G 3.24 Unbeabsichtigte Datenmanipulation

Je umfangreichere Zugriffsberechtigungen auf eine Datenbank für die Anwender bestehen, um so größer ist auch das Risiko einer unbeabsichtigten Datenmanipulation. Dies kann prinzipiell von keiner Anwendung verhindert werden. Die grundsätzlichen Ursachen für unbeabsichtigte Datenmanipulationen können z. B. sein:

- mangelhafte oder fehlende Fachkenntnisse,
- mangelhafte oder fehlende Kenntnisse der Anwendung,
- zu umfangreiche Zugriffsberechtigungen und
- Fahrlässigkeit (z. B. das Verlassen des Arbeitsplatzes ohne korrekte Beendigung der Anwendung).

G 3.25 Fahrlässiges Löschen von Objekten

Bei Novell Netware Version 4 ist es erstmalig möglich, das Objekt Admin, welches bei der Installation automatisch angelegt wurde zu löschen. Das Objekt Admin, welches den von Netware 3.x bekannten Supervisor ersetzt, wird bei der Neuinstallation eines Netware 4-Netzes angelegt und besitzt zu diesem Zeitpunk noch alle Administrationsrechte. Aus der Möglichkeit dieses Objekt zu löschen entstehen folgende Gefährdungen:

- Wird kein Ersatzadministrator (*"Ersatz-Admin")* als Objekt in der NDS zu erzeugt, besteht die Gefährdung das die NDS oder einzelne Container nicht mehr administriert werden können. Daraus resultiert dann die Notwendigkeit, die NDS neu zu installieren und alle enthaltenen Objekte neu zu erzeugen, was zu einem vollständigen Ausfall des Netware 4-Netzes führen kann.
- Bei einer dezentralen Administration eines Netware 4-Netzes werden üblicherweise Administratoren auf Organisationsebene (Containerebene) eingerichtet. Durch den IRF (Inherited Rights Filter) kann von diesen das Vererben von Rechten anderer Administratoren auf untergeordnete Organisationen eingeschränkt bzw. verhindert werden, so dass nur noch der dezentrale Administrator alle Rechte hat. Wird dieser nun in der NDS gelöscht, kann eine komplette organisatorische Einheit nicht mehr administriert werden, da die anderen Administratoren auf diesen Container keinen Zugriff mehr haben. besser: Durch die dezentrale *(Verteilung der Administrationsaufgaben)* Administration ist es nicht mehr möglich, den Container durch andere Administratoren zu verwalten.

G 3.26 Ungewollte Freigabe des Dateisystems

Novell Netware Version 4 unterscheidet zwischen Objekt- und Dateirechten. Objektrechte beinhalten die Berechtigungen zum Anlegen, Ändern, Betrachten oder Löschen von Objekten der NDS. Unter Dateirechten versteht man die Berechtigungen zum Lesen, Schreiben, Löschen etc. von Dateien oder Verzeichnissen. Das NDS Objekt "Server" stellt hierbei die einzige Schnittstelle zwischen dem Objekt- und dem Dateisystem dar.

Aus diesem Grund erhält jeder Benutzer, der als Supervisor für ein Serverobjekt eingetragen ist, somit auch Supervisor-Rechte für das komplette zugehörige Dateisystem, da das Supervisor-Attribut nicht durch einen IRF (Inherited Rights Filter) gefiltert werden kann. Dadurch bekommt er möglicherweise unbeabsichtigten Zugriff auf vertrauliche Daten, ohne dass dies bemerkt wird, bzw. beabsichtigt war.

G 3.27 Fehlerhafte Zeitsynchronisation

In Novell Netware 4.x können mehrere Server in einem Netz zusammenarbeiten. Um einen reibungslosen Ablauf der Netzdienste, wie z. B. Datums- und Zeitangaben der Dateien, Revision und Protokollierung und die zeitlichen Beschränkungen bei der Anmeldung zu gewährleisten, ist eine gleiche Uhrzeit auf allen Servern von großer Bedeutung. Auch Änderungen in einem Verzeichnisbaum werden in Novell Netware Version 4.x mit einem Zeitstempel versehen, der die Reihenfolge der Abarbeitung bei der Aktualisierung der NDS festlegt. Aus diesem Grund ist es wichtig, dass für alle Netware 4.x Server im Netz eine gemeinsame Zeit verwaltet wird.

Dabei können die folgenden Gefährdungen auftreten:

- Wird vor der Installation eines Netware 4.x Servers die interne Hardwareuhr des zugehörigen Rechners nicht überprüft und ggf. angepasst, so kann sich der neue Server u. U. nicht mit dem restlichen Netware 4.x Netz abgleichen, und es besteht die Gefahr einer Fehlfunktion der NDS.
- Kommt es in einem Netz, welches das Einzelreferenz-Verfahren zur Zeitsynchronisation nutzt, zum Ausfall der Zeitquelle, so ist keine Ersatzzeit mehr verfügbar. Dadurch können Datei- und Objektrechte unkontrolliert verändert werden.
- Veränderungen an der NDS, die aufgrund einer falschen Systemzeit einen sehr weit in der Zukunft liegenden Zeitstempel haben, werden auch erst zu diesem Zeitpunkt ausgeführt. Dies kann zu Fehlern oder Problemen führen, die nur sehr schlecht oder gar nicht nachzuvollziehen sind, da eine sehr große Zeitspanne zwischen dem Absetzen und dem Ausführen der entsprechenden Änderungen liegt.
- Wird an einem Netware 4.x Server nachträglich eine Funkuhr angeschlossen, aber die Sommer- bzw. Winterzeit-Umstellung nicht deaktiviert, so wird eine zusätzliche Stunde korrigiert.

G 3.28 Ungeeignete Konfiguration der aktiven Netzkomponenten

Durch eine ungeeignete Konfiguration der Netzkomponenten kann es zu einem Verlust der Verfügbarkeit des Netzes oder Teilen davon, zu einem Verlust der Vertraulichkeit von Informationen oder zu einem Verlust der Datenintegrität kommen. Dabei können insbesondere die folgenden Fehlkonfigurationen unterschieden werden:

- Aktive Netzkomponenten, die zur Bildung von VLANs (Virtual LANs) eingesetzt werden, segmentieren das Netz logisch. Im Fall einer Fehlkonfiguration kann ggf. die Kommunikation innerhalb eines VLANs, zwischen einzelnen oder zwischen allen VLANs zum Erliegen kommen. In Abhängigkeit der VLAN-Strategie des betreffenden Herstellers betrifft dies zum einen die Zuordnung von miteinander kommunizierenden Systemen zu den gleichen VLANs, zum anderen auch das VLAN-Routing, insofern ein solches durch die aktiven Netzkomponenten unterstützt wird.

  Beispiel: Bei VLANs, die nur über Router miteinander kommunizieren können, werden die zentralen Infrastrukturserver, die beispielsweise Datei- und Druckdienste bereitstellen, nicht gleichzeitig auch den VLANs der Arbeitsplatzsysteme zugeordnet, Router sind ebenfalls nicht vorhanden. In diesem Fall können einige Arbeitsplatzsysteme die Dienste der zentralen Infrastrukturserver nicht nutzen, da diese in einem nicht erreichbaren Teilnetz sind.

- Ein Netz kann durch den Einsatz von Routern mittels Teilnetzbildung strukturiert werden. Für eine Kommunikation zwischen den Teilnetzen ist eine entsprechende Konfiguration der Router erforderlich, die hierzu die Leitwege zwischen den verschiedenen Teilnetzen in Routing-Tabellen vorhalten müssen. Routing-Tabellen können statisch oder dynamisch verwaltet werden. In beiden Fällen ist eine Kommunikation zwischen unterschiedlichen Teilnetzen nicht möglich, wenn die Routing-Tabellen keinen Leitweg zwischen den betreffenden Teilnetzen enthalten. Zu einer Fehlkonfiguration kann es dementsprechend durch eine fehlerhafte Definition statischer Routing-Tabellen oder durch eine fehlerhafte Konfiguration der Routing-Protokolle (wie z. B. RIP oder OSPF) kommen, die zum automatischen Abgleich dynamischer Routing-Tabellen verwendet werden.

  Beispiel: Eine Router-zu-Router-Verbindung ist durch einen statischen Eintrag der entsprechenden IP-Adressen konfiguriert. Bei einer Änderung der IP-Adresse einer der Router oder durch das Zwischenschalten eines weiteren Routers ist diese Kommunikationsstrecke nicht mehr verfügbar.

- Aktive Netzkomponenten, die in der Lage sind, Protokolle oder Netzadressen zu filtern, können mit dieser Technik eine Kommunikation bestimmter Protokolle unterbinden oder eine Kommunikation zwischen Systemen mit bestimmten Netzadressen verhindern. Eine Fehlkonfiguration der betreffenden Filter kann entsprechend zu einer unerwünschten Unterbindung der Kommunikation in Abhängigkeit des fehlkonfigurierten Filters und der Art der Fehlkonfiguration führen.

Ebenso können fehlkonfigurierte Filter dazu führen, dass Verbindungen aufgebaut werden, die Eindringlingen die Möglichkeit bieten, Angriffe gegen IT-Systeme im geschützten Netz durchzuführen. Je nach Art des Angriffs kann daraus ein Verlust der Verfügbarkeit einzelner Netzkomponenten oder auch des ganzen Netzes resultieren. Weiterhin können z. B. durch die mögliche Manipulation der Verbindungswege Datenpakete umgeleitet werden oder Datenpakete verändert oder mitgelesen werden.

Beispiele:

Ein Multiport-Repeater ist so konfiguriert, dass nur Systeme mit bestimmten MAC-Adressen an bestimmte Ports angeschlossen werden können. Nach einem Austausch der Netzkarte in einem der Endgeräte und der damit verbundenen Änderung der MAC-Adresse, wird dieses System keine Verbindung mehr zum Netz bekommen (Verlust der Verfügbarkeit).

Durch eine ungeeignete Konfiguration von aktiven Netzkomponenten (insbesondere von VLANs oder Filterregeln) können Broadcast-Domänen unnötig groß werden oder es können unnötige Kommunikationsverbindungen entstehen. Dadurch kann es Unbefugten möglich sein, vertrauliche Daten zu lesen.

G 3.29 Fehlende oder ungeeignete Segmentierung

Lokale Netze können physikalisch durch aktive Netzkomponenten oder logisch durch eine entsprechende VLAN-Konfiguration segmentiert werden. Dabei werden die angeschlossenen IT-Systeme eines Netzes auf verschiedene Segmente verteilt. Dies verbessert die Lastverteilung innerhalb des Netzes und erhöht dessen Administrierbarkeit.

Dabei kann es zu folgenden konkreten Gefährdungen kommen:

- Verlust der Verfügbarkeit

  Durch eine hohe Anzahl von IT-Systemen innerhalb eines Schicht-2-Segments erhöht sich in diesem die Netzlast. Dies kann die Verfügbarkeit dieses Netzsegmentes stark beeinträchtigen oder sogar zu dessen Überlastung und Ausfall führen. Bei CSMA/CD-basierten Netzzugangsprotokollen (z. B. Ethernet) kommt es daneben häufiger zu Kollisionen, wodurch sich die verfügbare Bandbreite reduziert. Eine ungeeignete Segementierung kann auch dann vorliegen, wenn Systeme durch aktive Netzkomponenten der Schicht 2 oder 3 getrennt werden, die sehr viel miteinander kommunizieren.

- Kein ausreichender Schutz der Vertraulichkeit

  Um einen Schutz vertraulicher Daten gewährleisten zu können, sollten auch nur die unbedingt notwendigen Benutzer darauf Zugriff haben. Broadcast-Domänen sind daher auf das unbedingt notwendige Maß zu beschränken. Wurden die einzelnen Segmente jedoch ungeeignet konfiguriert, können nun auch andere Benutzer die übertragenen Nachrichten mit vertraulichen Daten mitlesen und ggf. auswerten.

Beispiele:

- Zwei IT-Systeme, die große Datenmengen austauschen, sind durch einen Router getrennt. Dies kann eine ungeeignete Segmentierung darstellen, da der Datenverkehr durch einen relativ langsamen Router geführt werden muss.
- Zwei IT-Systeme, die häufig Passwörter oder andere sensitive Informationen austauschen, sind durch eine Brücke getrennt. Dies bedingt, dass dieser Datenverkehr in beiden Segmenten abgehört werden kann. Die Begrenzung des Datenverkehrs zwischen diesen beiden IT-Systemen auf ein Segment würde einen höheren Schutz der Vertraulichkeit mit sich bringen.

G 3.30 Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners

Im häuslichen Bereich ist es einfacher, den dienstlichen Telearbeitsrechner privat zu nutzen, weil Kontrollen durch den Arbeitgeber nur bedingt möglich sind. Dadurch besteht die Gefahr, dass nicht geprüfte Software eingesetzt wird oder virenverseuchte Daten auf den Telearbeitsrechner gelangen. Diese unerlaubte Nutzung des Telearbeitsrechners kann nicht nur durch den Telearbeiter selbst, sondern auch durch Angehörige oder Besucher erfolgen. Insbesondere Kinder und Jugendliche können versucht sein, den Telearbeitsrechner für Spielzwecke zu verwenden, teilweise sogar, ohne dass der Telearbeiter dies merkt. Mögliche Schäden sind beispielsweise: gelöschte Festplatten mit Totalverlust der Daten, Reinstallationskosten oder Nacherfassungsarbeiten.

G 3.31 Unstrukturierte Datenhaltung

Durch unzureichende Vorgaben und/oder fehlende Schulung der Mitarbeiter kann es zu einer unübersichtlichen Speicherung der Daten auf den benutzten Datenträgern kommen. Dadurch kann es zu verschiedenen Probleme kommen wie:

- Speicherplatzverschwendung durch mehrfache Speicherung von Dateien,
- vorschnelle Löschung oder nicht erfolgte Löschung von Daten, da keiner mehr weiß, was in welchen Dateien gespeichert ist,
- unbefugte Zugriffe, wenn sich Dateien in Verzeichnisse oder auf Datenträgern befinden, die Dritten zugänglich gemacht werden, oder
- nicht konsistente Versionsstände in verschiedenen Verzeichnen und IT-Systemen.

Beispiel:

Es wurde unterlassen, einen neuen Mitarbeiter mit wenig IT-Erfahrung in die strukturierte Datenhaltung einzuweisen. Bereits nach kurzer Zeit traten Probleme auf, weil der Benutzer alle Dateien im Hauptverzeichnis gespeichert hatte, ohne auch nur ein Unterverzeichnis anzulegen.

G 3.32 Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von kryptographischen Verfahren

Beim Einsatz kryptographischer Produkte sind diverse gesetzliche Rahmenbedingungen zu beachten. In einigen Ländern dürfen beispielsweise kryptographische Verfahren nicht ohne Genehmigung eingesetzt werden. Dies kann dazu führen, dass bei der Übermittlung verschlüsselter Datensätze in solche Länder die Empfänger diese nicht lesen können, da sie die benötigten Kryptomodule nicht einsetzen können, oder sich vielleicht sogar strafbar machen.

Außerdem ist in sehr vielen Ländern auch der Export von Produkten mit starker Kryptographie erheblich eingeschränkt. Hier sind insbesondere die USA zu nennen. Bei Exportrestriktionen wird häufig die Stärke von an sich starken Verschlüsselungsprodukten künstlich (durch Reduzierung der Schlüsselmannigfaltigkeit) herabgesetzt. Solche künstlich geschwächten Verfahren bieten teilweise nicht einmal für mittleren Schutzbedarf ausreichenden Schutz. Dies gilt z. B. für aus den USA stammende PC-Standardsoftware wie Internet-Browser (SSL), in denen nur eine reduzierte Schlüssellänge von 40 Bit eingesetzt wird. Teilweise erfordern die Exportregelungen aber auch, dass Teile der Schlüssel hinterlegt werden, so dass die Kryptomodule zwar im Prinzip uneingeschränkt nutzbar sind, aber für die ausländischen Nachrichtendienste eine Zugriffsmöglichkeit im Bedarfsfall bleibt.

Auf der anderen Seite können solche Einschränkungen, die beim Einsatz innerhalb mancher Länder bzw. beim Export gelten, dazu verleiten, schützenswerte Daten unverschlüsselt zu lassen oder mit minderwertigen Kryptoprodukten zu schützen. Dies kann zum einen Angreifern Tür und Tor öffnen und zum anderen auch zum Verstoß gegen nationales Recht führen. So kann durch Datenschutzgesetze der Einsatz adäquater kryptographischer Verfahren zum Schutz personenbezogener Daten vorgeschrieben sein.

G 3.33 Fehlbedienung von Kryptomodulen

Die Fehlbedienung von Kryptomodulen hat in der Praxis schon öfter zu Schäden geführt. Diese Fehlbedienung kann verschiedene Auswirkungen haben:

- Daten werden unverschlüsselt übertragen, weil versehentlich der Klartext-Modus im Kryptomodul aktiviert wurde.
- Bei der Eingabe von kryptographischen Schlüsseln werden Schlüsselteile falsch eingegeben. Die Folge ist, dass weder der Sender (dem die Falscheingabe nicht aufgefallen ist) noch der Empfänger (der den wirklich verwendeten Schlüssel nicht kennen kann) die mit dem falsch eingegebenen Schlüssel chiffrierten Daten korrekt entschlüsseln können.
- Während des Verschlüsselungsvorgangs wird die Stromzufuhr des Kryptomoduls versehentlich ausgeschaltet. Dies hat zur Folge, dass nur Teile der Daten verschlüsselt vorliegen, andere Teile unverschlüsselt. In einem solchen Fall ist es möglich, dass eine Entschlüsselung nicht mehr möglich ist, weil der Vorgang unkontrolliert abgebrochen wurde.
- Bei Eingabe von Verschlüsselungsparametern werden falsche Parameter eingegeben. Dies kann zur Folge haben, dass nicht ausreichend sichere Kryptoalgorithmen oder unsichere kryptographische Schlüssel verwendet werden.
- Wird der Anwender bei der Schlüsselerzeugung beteiligt, in dem er bei der Generierung des Schlüssels zur Eingabe von zufälligen Zeichen aufgefordert wird, besteht eine Fehlbedienung auch darin, an dieser Stelle keine zufälligen Zeichen, sondern bekannte oder leicht erratbare Zeichenketten (Worte) zu verwenden.

Derlei Fehlbedienungen eines Kryptomoduls können dazu führen, dass die Vertraulichkeit, die Integrität und die Verfügbarkeit von Daten beeinträchtigt wird. Als Beispiele seien genannt:

- Daten werden nicht oder nicht mehr verschlüsselt, obwohl die Verschlüsselung zur Wahrung der Vertraulichkeit erforderlich wäre.
- Verschlüsselte Daten können nicht mehr entschlüsselt werden, weil durch die Fehlbedienung eine ordnungsgemäße Nutzung des Kryptomoduls nicht mehr möglich ist.
- Daten werden ungewollt oder absichtlich in einer Weise verschlüsselt, die nicht mehr rekonstruierbar ist, weil der notwendige kryptographische Schlüssel unbekannt ist.
- Korrekt verschlüsselte Daten werden verändert, so dass die Daten dann nicht mehr entschlüsselbar sind.

G 3.34 Ungeeignete Konfiguration des Managementsystems

Für den sicheren Einsatz eines Netz- und/oder Systemmanagementsystems ist eine konsistente Konfiguration aller beteiligten Komponenten nötig. Zwar werden die einzelnen Komponenten in der Regel von einer zentralen Instanz aus verwaltet (Managementkonsole), das Managementsystem besteht jedoch aus vielen Einzelkomponenten, die auf die zu verwaltenden Netzkomponenten verteilt sind. Eine konsistente Konfiguration eines solchen Systems lässt sich in zwei Bereiche unterteilen:

- Einerseits müssen die mit Hilfe des Managementsystems eingestellten Konfigurationen der Systemkomponenten (z. B. Rechner, Router) insgesamt konsistent sein. Ein Server sollte also so konfiguriert sein, dass alle berechtigten Client-Maschinen zugreifen können, aber auch nur diese.
- Andererseits muss auch die Managementsoftware selbst konsistent konfiguriert werden.

Wird beabsichtigt oder unbeabsichtigt die Konsistenz der Konfigurationen verletzt, so arbeiten die Komponenten nicht mehr reibungslos zusammen, was zu Sicherheitsproblemen führen kann. Beispielsweise könnte ein Server nicht mehr zugreifbar oder Zugriffsrechte zu offen gesetzt sein.

G 3.35 Server im laufenden Betrieb ausschalten

Wird ein Netz durch ein Managementsystem verwaltet, so existieren (insbesondere im Bereich Systemmanagement) Server mit Sonderaufgaben. Auf den so genannten Managementservern werden in der Regel Datenbanken mit Managementinformationen gehalten. Werden solche Server im laufenden Betrieb einfach ausgeschaltet, so werden z. B. die im Speicher des Rechners gehaltenen Daten nicht mehr auf das Dateisystem geschrieben. Dies hat zur Folge, dass beim nächsten Start der Maschine Inkonsistenzen auch in den Managementdaten existieren können. Große Managementsysteme benutzen deshalb in der Regel Datenbanken, die durch den Einsatz so genannter Transaktionsmechanismen dafür sorgen, dass die Informationen in einen (alten) konsistenten Zustand zurückversetzt werden können. Dies verringert die Gefahr, kann sie jedoch nicht vollständig beseitigen und kann sogar zum Angriff genutzt werden (Ausnutzen einer alten Konfiguration mit weniger restriktiven Zugriffsrechten).

Ausschalten von Archivsystemen

Auch bei der elektronischen Archivierung kann es zu Fehlern kommen, wenn das Archivsystem vollständig oder in Teilen im laufenden Betrieb abgeschaltet wird. Ein Abschalten kann dazu führen, dass Dokumente als archiviert gelten, tatsächlich aber nur unvollständig oder gar nicht auf das Speichermedium geschrieben worden sind und daher nicht mehr reproduziert werden können.

G 3.36 Fehlinterpretation von Ereignissen

Beim Einsatz eines Managementsystems ist es eine Aufgabe des jeweils verantwortlichen Systemadministrators, die Meldungen des Managementsystems zu analysieren und zu interpretieren, um dann geeignete Maßnahmen einzuleiten. In der Regel basieren die Meldungen des Managementsystems auf Überwachungsmechanismen, die Systemprotokolle unterschiedlichster Art automatisch nach gewissen Regeln durchsuchen. Es ist dabei nicht einfach, aus der Fülle der anfallenden Protokolldaten automatisiert Anomalien, die auf Systemfehler hindeuten, zu erkennen und entsprechende Meldungen an den Systemadministrator zu erzeugen. Darüber hinaus kann ein Fehler hier sogar unentdeckt bleiben. Die eingehenden Meldungen müssen daher immer vom Systemadministrator gesichtet und interpretiert werden, da die Meldungen (im Fehlerfall) auf Fehlersymptome und deren (automatischer) Interpretation beruhen. Ein Systemadministrator muss hier auch Fehlalarme und Falschmeldungen erkennen können. Werden Systemmeldungen vom Administrator falsch interpretiert, so führen vermeintlich korrigierende Gegenmaßnahmen u. U. zu einer Verschlimmerung der Situation.

G 3.37 Unproduktive Suchzeiten

Im Internet werden Millionen von Informationsseiten, Dokumente und Dateien angeboten. Zum Navigieren in diesem riesigen Informationsangebot wird eine durch einfachen Mausklick zu bedienende Querverweistechnik verwendet. Sie erlaubt den schnellen Wechsel auf weiterführende Informationsseiten, die ihrerseits wieder neue Querverweise auf weitere Seiten beinhalten. Das Springen über Querverweise von einer Informationsseite zu weiteren wird als "Surfen" bezeichnet und kann zu sehr langen Suchzeiten führen.

In vielen Organisationen wurden Internet-Dienste eingeführt, ohne die damit verbundenen Ziele und erwarteten Auswirkungen vorher konkret zu untersuchen. Die Schulungen und Hilfen für die Benutzer sind häufig nicht ausreichend, so dass es zu unproduktiven Suchzeiten im vielfältigen Angebot des Internets kommt. Die Kosten für diese Abfragen sind oft weder den Benutzern noch den IT-Verantwortlichen bekannt. Nach Schätzung einer Unternehmensberatung entstehen durch Surfen sowie unnötige und langatmige Recherchen im Internet vermeidbare Personal- und Kommunikationskosten in mehrstelliger Millionenhöhe je Jahr.

G 3.38 Konfigurations- und Bedienungsfehler

Konfigurationsfehler entstehen durch eine falsche oder nicht vollständige Einstellung der Parameter und Optionen, mit denen ein Programm gestartet wird. In diese Gruppe fallen z. B. falsch gesetzte Zugriffsrechte für Dateien. Bei Bedienungsfehlern sind nicht nur einzelne Einstellungen falsch, sondern es werden IT-Systeme oder IT-Anwendungen falsch behandelt. Ein Beispiel hierfür ist das Starten von Programmen, die für den Einsatzzweck des Rechners nicht notwendig sind, aber evtl. von einem Angreifer missbraucht werden können.

ungeprüfte Software

Beispiele für aktuelle Konfigurations- bzw. Bedienungsfehler sind das Speichern von Passwörtern auf einem PC, auf dem ungeprüfte Software aus dem Internet ausgeführt wird (solche Software wurde z. B. im Frühjahr 98 für das Ausspähen von T-Online-Passwörtern eingesetzt), oder das Laden und Ausführen von schadhaften ActiveX-Controls. Diese Programme, die u. a. die Aufgabe haben, WWW-Seiten durch dynamische Inhalte attraktiver zu machen, werden mit den gleichen Rechten ausgeführt, die auch der Benutzer hat - sie können also beliebig Daten löschen, verändern oder versenden.

Offenlegung von Informationen

Viele Programme, die für die ungehinderte Weitergabe von Informationen in einem offenen Umfeld gedacht waren, können bei falscher Konfiguration potentiellen Angreifern Daten zu Missbrauchszwecken liefern. So kann beispielsweise der *finger*-Dienst darüber informieren, wie lange ein Benutzer bereits am Rechner sitzt. Aber auch WWW-Browser übermitteln bei jeder Abfrage einer Datei eine Reihe von Informationen an den WWW-Server (z. B. die Version des Browsers und des verwendeten Betriebssystems, den Namen und die Internet-Adresse des PCs). In diesem Zusammenhang sind auch die Cookies zu nennen. Hierbei handelt es sich um Dateien, in denen WWW-Server-Betreiber Daten über den WWW-Nutzer auf dem Rechner des Nutzers speichern. Diese Daten können beim nächsten Besuch des Servers abgerufen und vom Server-Betreiber für eine Analyse der vom Benutzer vorher auf dem Server besuchten WWW-Seiten verwendet werden.

Der Einsatz eines Domain Name Systems (DNS), das für die Umsetzung eines Internet-Namens wie *rechner1.universitaet.de* in die zugehörige numerische Adresse zuständig ist, stellt eine weitere Gefahrenquelle dar. Zum einen ermöglicht ein falsch konfigurierter DNS-Server die Abfrage von vielen Informationen über ein lokales Netz. Zum anderen hat ein Angreifer durch die Übernahme dieses Servers die Möglichkeit, gefälschte IP-Nummern zu verschicken, so dass jeglicher Verkehr von ihm kontrolliert werden kann.

aktive Inhalte

Eine große Bedrohung geht auch von den automatisch ausführbaren Inhalten (**Executable Content**) in E-Mails oder HTML-Seiten aus. Dies ist unter dem Stichwort Content-Security-Problem bekannt. Dateien, die aus dem Internet geholt werden, können Code enthalten, der nur beim "Betrachten" und ohne Rückfrage beim Benutzer ausgeführt wird. Dies ist z. B. bei Makros in Winword-Dateien der Fall und wurde zum Erstellen von so genannten Makro-Viren ausgenutzt. Auch neue Programmiersprachen und -schnittstellen wie ActiveX, Javascript oder Java, die für Anwendungen im Internet entwickelt worden sind, besitzen bei falscher Implementierung der Kontrollfunktionen ein Schadpotential.

Fehlerhafte RACF-Datenbanken

Die Verfügbarkeit des Sicherheitssystems RACF ist bei z/OS-Betriebssystemen von zentraler Bedeutung für die Verfügbarkeit des gesamten Systems. Durch unsachgemäßen Einsatz von z/OS-Utilities bei der RACF-Datenbanksicherung oder fehlerhafte Bedienung der RACF-Kommandos kann diese eingeschränkt werden.

G 3.39 Fehlerhafte Administration des RAS-Systems

Die fehlerhafte Administration von RAS-Komponenten stellt ein nicht zu vernachlässigendes Risikopotential dar. Auch RAS-Systeme sind - ab einer gewissen Größe und Struktur - komplexe Systeme, deren korrekte und sichere Konfiguration nur von geschulten Systemadministratoren zu leisten ist. Fehler in der Administration wirken sich in der Regel sehr stark auf die Stabilität und Sicherheit aus, da ein Administrator privilegierte Rechte im System besitzt. Für RAS-Systeme sind hier u. A. folgende Probleme zu nennen:

- Sicherheitsrelevante Routineaufgaben auf dem RAS-Client werden häufig vernachlässigt. Dazu gehören z. B. die regelmäßige Datensicherung oder die Prüfung auf Computer-Viren. Insbesondere mobile RAS-Clients werden vom jeweiligen Benutzer mitgeführt und sind daher nur selten für die Systemadministration verfügbar. Zwar kann auch eine entfernte Administration während einer aufgebauten RAS-Verbindung erfolgen, je nach Nutzungsprofil sind die Verbindungszeiten jedoch zu kurz, um eine geregelte Fernwartung durchzuführen. Werden die regelmäßigen administrativen Aufgaben jedoch nicht durchgeführt, so kann es zu nicht abgestimmten Konfigurationen kommen.

Vernachlässigung sicherheitsrelevanter Routineaufgaben

- Die Fernadministration von Rechnern kann mit Hilfe von verbreiteten Software-Produkten erfolgen und wird vielfach schon in Ansätzen durch Mechanismen des Betriebssystems möglich. Die Verwendung unautorisierter Software (durch den Benutzer oder den Administrator) führt oft dazu, dass entweder nicht erlaubte Protokolle über eine RAS-Verbindung verwendet werden oder Einstellungen erfolgen, die nicht konform mit der geltenden Sicherheitsrichtlinie sind und somit Sicherheitslücken öffnen können.

unautorisierte Verwendung von Software zur entfernten Administration

- Wenn die Computer-Viren-Prüfung ausschließlich auf dem Server stattfindet, ist die Client-seitige Datenverschlüsselung problematisch. Über RAS-Verbindungen können viele Applikationsprotokolle abgewickelt werden, so dass auch der Transport von E-Mail, WWW-Inhalten oder Dateien möglich ist. Verschlüsselte Daten können in diesem Fall von Server-seitigen Computer-Viren-Schutzprogrammen nicht mehr auf Viren untersucht werden.

Verschlüsselung und Virenschutz

- Auf dem RAS-Client ist kein oder kein aktuelles Computer-Viren-Schutzprogramm installiert oder nicht aktiviert. Da RAS-Clients in vielen Fällen in unsicheren Umgebungen betrieben werden und somit beispielsweise der Austausch von Datenträgern praktisch nicht kontrolliert werden kann, stellen Computer-Viren eine besonders starke Gefährdung dar. Insbesondere besteht die Gefahr, dass Computer-Viren oder Trojanische Pferde über den RAS-Client in das LAN gelangen.

fehlender Virenschutz auf RAS-Clients

- Werden bandbreitenintensive Funktionen über RAS-Verbindungen ausgeführt, so besteht die Gefahr, dass der Benutzer die RAS-Verbindung unterbricht und neu aufbaut, weil er davon ausgeht, dass eine Störung vorliegt. In Wirklichkeit ist jedoch lediglich die Antwortzeit unakzeptabel lang, da die Bandbreite nicht ausreicht. Hierdurch können einerseits Inkonsistenzen in den Anwendungsdaten durch den nicht erwarteten Verbindungsabbruch und andererseits erhöhte Belastungen des RAS-Systems

lange Antwortzeiten durch unzureichende Bandbreite

durch die wiederholten Verbindungswünsche mit anschließendem Abbruch entstehen.

falsch konfigurierte Komponenten zur Kommunikation

- Eine generelle Gefahr bei unzureichender Administration sind inkompatibel oder fehlerhaft konfigurierte Hard- oder Software-Komponenten zur Kommunikation, da diese die RAS-Verbindungen erst ermöglichen. Hier reichen die Fehlkonfigurationen von fehlenden Sicherheitseinstellungen bis hin zu inkompatiblen Kommunikationsprotokollen. Ebenso breit gestreut sind auch die daraus resultierenden Konsequenzen, beispielsweise kommen gewünschte Verbindungen nicht zustande oder nicht autorisierte Dritte können sich erfolgreich verbinden.

Beispiele:

- Ein Außendienstmitarbeiter nutzt den Replikationsmechanismus eines Groupware-Produktes, um seine lokale Kopie einer technischen Referenzdatenbank regelmäßig auf den neuesten Stand zu bringen. Durch die Fehlkonfiguration des Replikationsmechanismus wird die Replikation auch immer nach dem RAS-Verbindungsaufbau angestoßen, so dass die Verbindung über Mobiltelefon-Modem nach erfolgreichem Aufbau scheinbar immer "stehen bleibt".
- Ein Unternehmen setzt ein Softwaremanagementsystem ein, das regelmäßig neue Software-Updates auf den einzelnen Benutzerrechnern installiert. Aufgrund eines Konfigurationsfehlers werden in dieses Verfahren auch die mobilen RAS-Clients mit einbezogen. Nach erfolgreichem Verbindungsaufbau wird dann die gesamte Bandbreite durch die Managementsoftware in Anspruch genommen, die ein größeres Update-Paket auf dem Rechner installieren will.

G 3.40 Ungeeignete Nutzung von Authentisierungsdiensten bei Remote Access

Inkonsistente RAS-Benutzerverwaltung

Die Identität der RAS-Benutzer muss beim Verbindungsaufbau festgestellt werden. Dazu werden typischerweise Authentisierungsmechanismen verwendet, die auf einer Benutzerverwaltung mit gespeicherten Authentisierungsdaten beruhen. RAS-Systeme bieten für die Speicherung der Benutzerdaten mehrere Möglichkeiten an: eine eigene Benutzerverwaltung, Nutzung der Benutzerverwaltung des Betriebssystems, Nutzung von Authentisierungsservern (mit eigener Benutzerverwaltung). Werden getrennte Benutzerverwaltungen für RAS und Betriebssystem verwendet, so kann es aufgrund von Störungen im organisatorischen Ablauf zu Inkonsistenzen in den beiden Datenbeständen kommen. Dies kann zu unerlaubten Verbindungsaufnahmen und unberechtigten Zugriffen auf Daten führen. Eine getrennte Verwaltung empfiehlt sich daher nicht.

Beispiel:

- Beim Ausscheiden eines Mitarbeiters wird das Benutzerkonto nicht in der RAS-Benutzerverwaltung gelöscht. Der ehemalige Mitarbeiter kann sich daher immer noch über den RAS-Zugang einwählen und auf allgemein zugängliche Daten zugreifen. Der Zugang kann auch dazu benutzt werden, weitere Angriffe durchzuführen.

Speichern von Authentisierungsdaten auf dem RAS-Client

Viele Client-Komponenten für den Remote Access erlauben es, die zur Authentisierung notwendigen Daten nach einmaliger Eingabe lokal zu speichern, so dass beim erneuten Verbindungsaufbau die Eingabe der Daten durch den Benutzer nicht mehr erforderlich ist. Dies birgt jedoch ein hohes Risikopotential für den Fall, dass der RAS-Client einem unberechtigten Zugriff ausgesetzt ist. Der Authentisierungsmechanismus kann dann seine Aufgabe nicht mehr erfüllen. Dadurch können Unbefugte ggf. auf die lokalen Netze zugreifen, die über eine RAS-Verbindung vom jeweiligen Client aus erreichbar sind. Die Sicherheit dieser lokalen Netze ist somit gefährdet. Ähnliche Gefährdungen ergeben sich durch das Speichern von Schlüsseln zur Datenverschlüsselung oder digitalen Signatur auf dem RAS-Client.

G 3.41 Fehlverhalten bei der Nutzung von RAS-Diensten

Ohne geeignete Schulung der Anwender kann es - wie bei jedem anderen IT-System - durch (meist unbewusstes) Fehlverhalten bei der RAS-Nutzung bzw. im Umfeld der RAS-Nutzung zu Sicherheitsproblemen (z. B. Verstoß gegen die IT-Sicherheitsrichtlinien, Fehlkonfiguration) kommen.

Weiterhin werden stationäre und mobile IT-Systeme, auf denen RAS-Client-Software installiert ist, häufig nicht nur zum Zugriff auf ein LAN benutzt. Insbesondere wenn die RAS-Verbindung über das Internet aufgebaut wird, erfolgt oft auch die Nutzung von WWW und E-Mail über diese IT-Systeme. In manchen Fällen wird auch auf fremde Netze zugegriffen, beispielsweise wenn Außendienstmitarbeiter mit mobilen RAS-Clients Verbindungen zu Kundennetzen aufbauen. Dadurch ergeben sich folgende Gefährdungen:

Aufbau nicht genehmigter RAS-Verbindungen

- Durch den Aufbau nicht genehmigter Verbindungen wird das System mindestens unnötig belastet, da jeweils eine Überprüfung auf die Zulässigkeit durchgeführt werden muss. Auf diese Weise werden unnötigerweise Systemressourcen belegt. In Kombination mit Fehlkonfigurationen kann es auch dazu kommen, dass unberechtigte Zugriffe erfolgreich durchgeführt werden.

Nutzung des RAS-Clients im Internet

- RAS-Clients können u. A. für den Internet-Zugang eingesetzt werden. Hier ergibt sich die Gefährdung dadurch, dass bei Verbindungen mit dem Internet ohne besondere Vorkehrungen (z. B. sichere Konfiguration, PC-Firewall) u. U. auch von außen auf den Client-Rechner zugegriffen werden kann. Dadurch ist der Rechner jedoch potentiellen Angriffen ausgesetzt. Ein Angreifer kann so z. B. die Datenverschlüsselung abschalten oder andere RAS-Konfigurationsdaten verändern, so dass eine gesicherte RAS-Kommunikation nicht mehr möglich ist. Ähnliche Probleme (Viren, Trojanische Pferde) ergeben sich durch Software, die aus dem Internet geladen und auf dem RAS-Client abgespeichert wurde.

Anschluss des RAS-Clients an ein fremdes Netz

- Wird ein RAS-Client an ein fremdes LAN angeschlossen (z. B. Kundennetz oder privates Heimnetz), so bestehen in diesem LAN oft weitere Übergänge zu anderen Netzen (Internet, lokale Teilnetze). Je nach Sicherheitsvorgaben der LAN-Verwaltung kann der unkontrollierte Zugriff auf den RAS-Client möglich sein (siehe auch G 5.39 *Eindringen in Rechnersysteme über Kommunikationskarten*).

Beispiele:

- Auf einer Dienstreise verbindet sich ein Mitarbeiter über Internet mit dem Firmennetz. Vor dem Verbindungsaufbau mit dem RAS-System lädt er eine ausführbare Datei von einem WWW-Server. Die Datei enthält neben der "offiziellen" Funktionalität auch noch einen "bösartigen" Programmteil, der versucht, in der RAS-Konfiguration die Sicherheitsmechanismen zu beeinflussen (z. B. Abschalten der Verschlüsselung) und auf Daten im Firmennetz zuzugreifen, wenn eine bestehende RAS-Verbindung vorgefunden wird.

- Ein Außendienstmitarbeiter verbindet seinen Laptop mit dem Netz eines Kunden. Um Daten mit dem Kunden austauschen zu können, gibt er lokale Verzeichnisse für Zugriffe aus dem Netz frei. Versehentlich wird bei dem Datenaustausch auch die Datei übertragen, in der der Außendienstmitarbeiter seine Authentisierungsdaten abgelegt hat.

G 3.42 Unsichere Konfiguration der RAS-Clients

eingeschränkte Administrationsmöglichkeiten bei RAS-Clients

Die Sicherheit des RAS-Systems hängt sowohl von der sicheren Konfiguration der RAS-Server als auch der RAS-Clients ab. Unterliegt die Konfiguration des Servers noch der vollständigen Kontrolle eines Administrators, so befinden sich RAS-Clients häufig außerhalb der Behörde bzw. des Unternehmens. Damit kann der Rechner nur noch lose in administrative Abläufe eingegliedert werden. Insbesondere beim Einsatz mobiler RAS-Clients können Benutzer auch mit gewissen administrativen Rechten ausgestattet sein, um Probleme beim RAS-Zugang durch Ändern von RAS-Konfigurationsparametern selbst oder unter telefonischer Anleitung zu beheben.

Generell ergibt sich durch die eingeschränkten Kontrollmöglichkeiten der Systemadministration die Gefahr, dass RAS-Clients unsicher konfiguriert sind. Beispiele sind:

unsichere Konfiguration des Browsers

- Browser sind häufig sehr unübersichtlich zu konfigurieren, was immer wieder zu Fehleinstellungen führt. Durch das Ausschalten von Sicherheitsmechanismen (z. B. Aktivieren von Java, JavaScript, ActiveX) kann nicht vertrauenswürdige Software auf den Client gelangen.
- Problematisch ist auch die Installation nicht zugelassener Software auf dem RAS-Client, da diese Sicherheitslücken aufweisen kann bzw. Computer-Viren oder Trojanische Pferde eingeschleppt werden können.
- Die vorhandenen Sicherheitsmechanismen für den RAS-Zugang werden vom Benutzer in vielen Fällen nicht oder nicht korrekt eingestellt (siehe auch G 5.91 *Abschalten von Sicherheitsmechanismen für den RAS-Zugang*).

Nutzung inkompatibler Authentisierungsmechanismen

- Zu weiteren Problemen kann es kommen, wenn inkompatible Authentisierungsmechanismen zwischen RAS-Client und RAS-Server benutzt werden. So ist z. B. das Authentisierungsprotokoll MS-CHAP eines Windows 3.11-RAS-Clients inkompatibel mit dem MS-CHAP-Protokoll eines Windows NT 4.0-Servers. Dies führt dazu, dass Verbindungen nicht aufgebaut werden können.

G 3.43 Ungeeigneter Umgang mit Passwörtern

Selbst die Nutzung von durchdachten Authentikationsverfahren hilft wenig, wenn die Benutzer nicht sorgfältig mit den benötigten Zugangsmitteln umgehen. Unabhängig davon, ob Passwörter, PINs oder Authentikationstoken zum Einsatz kommen, werden diese immer wieder weitergegeben oder unsicher aufbewahrt.

Weitergabe von Passwörtern oder Token

Benutzer geben oft aus Bequemlichkeit Passwörter an andere Benutzer weiter. Häufig werden Passwörter innerhalb von Arbeitsgruppen geteilt, um jedem Mitarbeiter den Zugriff auf gemeinsam zu bearbeitende Dateien zu erleichtern. Der Zwang zur Passwortbenutzung wird oft als lästig empfunden und dadurch unterlaufen, dass Passwörter nie gewechselt werden oder alle Mitarbeiter dasselbe Passwort benutzen.

Verlust eines Authentisierungs-Tokens

Wird zur Benutzer-Authentisierung ein Token-basiertes Verfahren eingesetzt (z. B. Chipkarte oder Einmalpasswortgenerator), so ergibt sich bei Verlust die Gefahr, dass das Token unberechtigt verwendet wird. Ein unberechtigter Benutzer kann mit diesem Token u. U. erfolgreich eine Remote Access-Verbindung aufbauen.

zu viele verschiedene Passwörter

Durch die Vielzahl verschiedener Passwörter und PINs können sich Benutzer diese oftmals nicht alle merken. Daher werden Passwörter immer wieder vergessen, was teilweise zu hohem Aufwand führt, um mit dem System weiterarbeiten zu können. Authentikationstoken können ebenso verloren werden. Bei sehr sicheren IT-Systemen kann der Verlust von Passwörtern oder Token sogar dazu führen, dass alle Benutzerdaten verloren sind.

Passwort unter der Tastatur

Passwörter werden oft notiert, damit sie nicht vergessen werden. Dies ist solange kein Problem, wie sie sorgfältig, also vor unbefugtem Zugriff geschützt, aufbewahrt werden. Leider ist dies nicht immer der Fall. Ein klassisches Beispiel ist die Passwortaufbewahrung unter der Tastatur oder auf einem Klebezettel am Bildschirm. Auch Authentikationstoken finden sich gerne unter der Tastatur.

zu einfache Passwörter

Ein anderer Trick, um Passwörter nicht zu vergessen, ist die "geeignete" Auswahl. Wenn Benutzer Passwörter selber auswählen können und nicht ausreichend für die Probleme hierbei sensibilisiert sind, werden in vielen Fällen Trivialpasswörter wie "4711" oder Namen von Freunden gewählt.

Beispiele:

- In einem Unternehmen wurde bei Stichproben festgestellt, dass viele Passwörter zu schlecht gewählt bzw. zu selten gewechselt wurden. Es wurde technisch erzwungen, dass die Passwörter monatlich gewechselt wurden und außerdem Zahlen oder Sonderzeichen enthalten mussten. Es stellte sich heraus, dass ein Administrator seine Passwörter wie folgt auswählte:

  januar98, februar98, maerz98, ...

- In einer Behörde zeigte sich das Phänomen, dass Benutzer, die ihre Büros zur Straßenseite hatten, häufig dasselbe Passwort hatten: den Namen des gegenüberliegenden Hotels, der in großen Leuchtbuchstaben die Aussicht dominierte.

G 3.44 Sorglosigkeit im Umgang mit Informationen

Häufig ist zu beobachten, dass zwar eine Vielzahl von organisatorischen oder technischen Sicherheitsverfahren vorhanden sind, diese jedoch durch den sorglosen Umgang mit der Technik wieder ausgehebelt werden. Ein typisches Beispiel hierfür sind die fast schon sprichwörtlichen Zettel am Monitor, auf denen alle Zugangspasswörter notiert sind. Auch andere Beispiele für Nachlässigkeit, Pflichtvergessenheit oder Leichtsinn im Umgang mit schützenswerten Informationen finden sich in großer Menge.

Beispiele:

- In der Bahn oder im Restaurant geben Mitarbeiter oft intimste Unternehmensdetails über ihr Mobiltelefon weiter. Dabei informieren sie jedoch nicht nur den Gesprächspartner, sondern auch die Umgebung. Beispiele für besonders interessante Interna sind, **Mithörer**
  - warum der Vertrag mit einer anderen Firma nicht zustande kam oder
  - wie viele Millionen der Planungsfehler in der Strategie-Abteilung gekostet hat und wie das die Aktienkurse des Unternehmens drücken könnte, wenn irgendjemand davon erführe.
- Häufig ist es bei Dienstreisen erforderlich, ein Notebook, einen Organizer oder Datenträger mitzunehmen. Gerne werden diese dann während Pausen im Besprechungsraum, im Zugabteil oder im Auto zurückgelassen. Bei mobilen IT-Systemen sind die damit erfassten Daten oftmals nicht an anderer Stelle gesichert. Wenn die IT-Systeme dann gestohlen werden, sind damit die Daten unwiederbringlich verloren. Dazu kommt, dass sich brisante Daten auch Gewinn bringend weiterveräußern lassen, wenn der Dieb mangels Verschlüsselung und Zugriffsschutz einfach darauf zugreifen kann. **Mitnehmer**
- Ein Grund, ein Notebook oder Akten auf Dienstreisen mitzunehmen, ist auch, die Fahrzeiten produktiv nutzen zu können. Hierbei bieten sich Mitreisenden oft interessante Einblicke, da es in der Bahn oder im Flugzeug kaum zu vermeiden ist, dass Sitznachbarn in den Unterlagen oder auf dem Bildschirm mitlesen können. **Mitleser**

  Öffentliche Räumlichkeiten, z. B. Hotel-Foyer, Hotel-Business-Center, Zug-Abteil, bieten in der Regel nur wenig Sichtschutz. Gibt der Benutzer Passwörter ein oder muss Veränderungen an den Konfigurationen vornehmen, so kann ein Angreifer diese Informationen erlangen und missbräuchlich nutzen.
- Immer wieder sind in der Presse Artikel zu finden über Behörden und Unternehmen, in deren Hinterhöfen sich hochbrisante Papiere im Altpapiercontainer fanden. Bekannt wurden auf diese Weise beispielsweise die Gehaltszahlen aller Mitarbeiter eines Unternehmens und die geheimen Telefonnummern von Unternehmensvorständen. **brisante Informationen im Altpapier**
- Wenn IT-Systeme Defekte aufweisen, werden diese schnell zur Reparatur gegeben. Meist besteht bei einem Defekt auch keine Möglichkeit mehr, die auf dem IT-System gespeicherten Daten zu löschen. Bei einem Schaden besteht aber häufig die erste Priorität darin, möglichst schnell wieder ein **Austausch von Komponenten bei Reparatur**

funktionierendes Gerät zur Verfügung zu haben. Daher zeigen viele Fachhändler besonderen Kundenservice, indem sie die defekten Komponenten einfach austauschen und die Kunden mit einem funktionsfähigen System nach Hause schicken.

Es hat allerdings diverse Fälle gegeben, bei denen der Kundendienst den Fehler bei einer anschließenden Überprüfung schnell beheben konnte und der nächste Kunde ebenso kulant das jetzt reparierte Gerät erhielt - inklusive aller vom ersten Kunden erfassten Daten.

G 3.45 Unzureichende Identifikationsprüfung von Kommunikationspartnern

Leichtfertige Weitergabe von Interna

Bei persönlichen Gesprächen, am Telefon oder auch bei E-Mail sind viele Personen bereit, weit mehr Details zu äußern, als sie das in schriftlicher Form oder in größerer Runde tun würden. Hierbei wird häufig vom Kommunikationspartner stillschweigend erwartet, dass die Gesprächs- oder E-Mail-Inhalte vertraulich gehandhabt werden. Darüber hinaus besteht die Neigung, die Identität des Kommunikationspartners nicht zu hinterfragen, da dies als unhöflich empfunden wird. Dies gilt auch für weitere Nachfragen zum Grund des Anrufes oder dem Auftraggeber ("Ich arbeite für die XY-Bank und benötige noch einige detaillierte Angaben zu ihren Einkommensverhältnissen."). Solche Verhaltensweisen werden auch beim "Social Engineering" ausgenutzt (siehe auch G 5.42 *Social Engineering*).

Beispiel:

Es sind viele Fälle bekannt, in denen Journalisten Prominente angerufen und sich als andere Prominente ausgegeben haben. Damit gelang es ihnen, den Prominenten Aussagen zu entlocken, die nicht für die Öffentlichkeit bestimmt waren. Dies war besonders brisant bei einigen Direktübertragungen im Radio, bei denen auch die Veröffentlichung nicht mehr rückgängig zu machen war.

G 3.46 Fehlerhafte Konfiguration eines Lotus Notes Servers

Fehlkonfigurationen eines Software-Systems sind häufig die Ursache für erfolgreiche Angriffe. Aufgrund der Komplexität eines Notes-Servers besteht auch hier die Gefahr, dass das Notes-System durch Fehlkonfiguration nicht den geforderten Sicherheitsansprüchen genügt. Durch die Fülle an Konfigurationseinstellungen und durch die sich gegenseitig beeinflussenden Parameter können auch viele Gefährdungen entstehen. Einige typische Fehlkonfigurationen werden im folgenden aufgeführt:

- **Fehlende Zugriffseinschränkungen auf einen Server**: In der Grundeinstellung ist es generell jedem erlaubt, auf einen Notes-Server zuzugreifen. Werden keine Zugriffsbeschränkungen auf einen Server definiert, so wird diese erste Hürde nicht genutzt. Insbesondere in der Kombination mit schwachen oder falschen Zugriffsberechtigungen auf weitere Dienste oder Datenbanken können so Sicherheitsprobleme entstehen.
- **Fehlerhafte Zugriffslisten (Access Control Lists, ACLs) oder unsichere Standard-ACLs**: Jede Datenbank erhält bei der Erzeugung eine (durch die jeweilige Datenbankvorlage bestimmte) Zugriffsliste mit Standardeinträgen. Je nach Vorlage bietet diese keinen ausreichenden Schutz für die Datenbank im Normalbetrieb. Dies gilt insbesondere dann, wenn die Datenbank nach der Erzeugung initialisiert oder weiter konfiguriert werden muss. Oft sind dazu zunächst umfangreiche Rechte notwendig, die für den laufenden Betrieb nicht mehr benötigt werden. Werden die Standardzugriffslisten nicht verändert, kann dies dazu führen, dass Unbefugte auf die Datenbank zugreifen können oder Benutzern zu hohe Rechte eingeräumt werden.
- **Es wird keine Verschlüsselung eingesetzt**: Die Verschlüsselung der Netzkommunikation (Port-Verschlüsselung) und die Verschlüsselung von Datenbanken oder Datenbankfeldern ist in der Regel standardmäßig nicht aktiviert. Um die Verschlüsselung zu nutzen, muss diese explizit aktiviert werden. Wird dies vergessen, so sind die Daten ungeschützt.
- **Unzureichende Berechtigungen für Server oder administrative Prozesse**: Damit eine Notes-Datenbank korrekt funktionieren kann, muss sie von einem dedizierten Server verwaltet und gewartet werden. Zu den Verwaltungs- und Wartungsaufgaben eines Servers gehört u. a. das Aktualisieren von Datenbank-Kopien (Daten, Zugriffslisten, usw.). Sind dem verantwortlichen Server keine ausreichenden Rechte eingeräumt, so schlagen die Verwaltungsaktionen fehl. Dies kann zu Sicherheitsproblemen führen, dass z. B. Veränderungen an den Zugriffsberechtigungen nicht an die Kopien einer Datenbank weitergegeben werden können.
- **Akzeptieren von Cross-Zertifikaten**: Zwischen verschiedenen Zertifikatshierarchien (ohne gemeinsame Zertifizierungsinstanz) können Vertrauensstellungen eingetragen werden, indem eine sogenannte Cross-Zertifizierung erfolgt (Anerkennen fremder Zertifikate). Cross-Zertifikate können meist automatisch erzeugt werden, wenn ein unbekanntes Zertifikat "entdeckt" wird. Dies gilt sowohl für Notes-Zertifikate, als auch für X.509-Zertifikate. Dabei können Cross-Zertifikate auch von Benutzern einfach im

persönlichen lokalen Adressbuch erzeugt werden. Das Anlegen von Cross-Zertifikaten im NAB kann dagegen nur durch einen berechtigten Administrator erfolgen. Werden Zertifikate leichtfertig als vertrauenswürdig anerkannt, so kann dies zu Sicherheitsproblemen (z. B. bei aktiven Inhalten, die mit dem nun als vertrauenswürdig geltenden Zertifikat signiert sind) führen.

Die aufgeführten Problemfelder sind Beispiele für mögliche Gefährdungen durch Fehlkonfigurationen. Abhängig vom jeweiligen Einsatzumfeld können weitere Gefährdungen hinzukommen.

Beispiel:

Ein Server ist so konfiguriert, dass anonyme Zugriffe nicht gestattet sind. An der Web-Schnittstelle sind nur SSL-Verbindungen erlaubt. Bei der Konfiguration der Datenbank-ACLs wird daher kein "Anonymous"-Eintrag erstellt. Weiterhin wird auf das Erzwingen des SSL-geschützen Web-Zugriffs verzichtet, da der Server nur SSL-Verbindungen an der Web-Schnittstelle annimmt. Die "-Default-"-Rechte aus den Datenbank-Vorlagen wurden nicht geändert, um den administrativen Aufwand bei Vorlagenänderungen zu minimieren. Durch die Einführung einer neuen Datenbank, die öffentliche Informationen enthält, wird der Server so konfiguriert, dass nun auch normale Web-Zugriffe auf diese Datenbank erlaubt sind (anonym, nicht SSL geschützt). Ab nun kann auf alle Server-Datenbanken anonym zugegriffen werden, es gelten dabei die "-Default-"-Rechte, die oft mindestens das Lesen erlauben. Dadurch besteht die Gefahr, dass Unbefugte vertrauliche Daten einsehen oder Informationen manipulieren können.

G 3.47 Fehlerhafte Konfiguration des Browser-Zugriffs auf Lotus Notes

Erlaubt ein Notes-Server auch den Web-Zugriff, so erfolgt der Zugriff mit zwei unterschiedlichen Mechanismen, die sich im benutzten Protokoll, in den Authentisierungsmechanismen und in der Steuerung der Zugriffskontrolle unterscheiden. Dadurch kann es insbesondere bei der Einführung des Web-Zugriffes auf einen Notes-Server zu Fehlkonfigurationen kommen, die einem Web-Benutzer u. U. mehr Rechte als gewünscht zuweist. Dies kann folgende typische Ursachen haben:

- **Der Web-Authentisierungsmechanismus ist zu schwach**: Dies kommt in der Regel durch eine Kombination von Problemen zustande:
  - Wenn zur Authentisierung Benutzername und Passwort, aber kein SSL zum Schutz der Authentisierungsdaten eingesetzt wird, kann dadurch das Internet-Passwort abgehört werden.
  - Es werden SSL-Client-Zertifikate eingesetzt, der Client-Rechner ist jedoch unzureichend geschützt (z. B. kein Passwort auf der Zertifikat-Datenbank). Hier besteht die Gefahr, dass die Client-Zertifikate durch unberechtigte Dritte genutzt werden, ohne dass der Zertifikatsinhaber dies bemerkt.
  - Wenn die Option "anonymer Zugriff" freigeschaltet ist, kann dies in Verbindung mit fehlerhaften Zugriffslisten (z. B. kein "Anonymous"-Eintrag und "-Default-"-Eintrag erlaubt "Manager" Rechte) zu unberechtigten Zugriffen auf Datenbanken führen.
- **Die Datenbank erzwingt nicht den SSL-geschützten Zugriff**: Obwohl eine Datenbank sensitive Daten enthält, die nur geschützt übertragen werden sollen, erzwingt die Datenbank-Konfiguration keine SSL-Verbindung. Als Folge werden die Daten u. U. ungeschützt übertragen, wenn SSL nicht auf dem Server erzwungen wird oder die Konfiguration des Servers geändert wird.
- **Unzureichende Berechtigungseinschränkungen**: Für den Web-Zugriff können zusätzliche Berechtigungseinschränkungen auf Servern und Datenbanken konfiguriert werden. Sind diese nicht konsistent eingestellt, so kann z. B. durch direkte URL-Eingaben u. a. auf Datenbanken, Datenbankmasken oder Agenten zugegriffen werden.

Die aufgeführten Problemfelder sind Beispiele für mögliche Gefährdungen eines Notes-Systems durch Fehlkonfiguration der Web-Schnittstelle.

G 3.48 Fehlerhafte Konfiguration von Windows 2000/XP/Server 2003 basierten IT-Systemen

Windows 2000/XP und Windows Server 2003 sind komplexe Betriebssysteme, deren Sicherheit im Wesentlichen durch die eingestellten Parameter bestimmt wird. Dadurch ergeben sich insbesondere durch Fehlkonfiguration einzelner oder mehrerer Komponenten Sicherheitsgefahren, die von Fehlfunktionen bis hin zur Kompromittierung eines Windows 2000/XP/Server 2003 Netzes führen können.

Migration enthält mehr Risiken als Neuinstallation

- Bei der Migration von Windows NT 4.0 zu einer neueren Windows Version bleiben die Zugriffsberechtigungen von Windows NT erhalten, die auch normalen Benutzern weitreichenden Zugriff auf Systemdateien erlauben. Damit ist die Zugriffssicherheit bei migrierten Windows Systemen im Allgemeinen niedriger als bei neu installierten Windows Systemen.
- Ist der Authentisierungsmechanismus NTLM unsicher konfiguriert, so ist es durch Abhören des Netzverkehrs möglich, Benutzerpassworte zu rekonstruieren. Dies war bisher vor allem bei der Nutzung alter NTLM-Versionen kleiner 2.0 ein Problem, aber mittlerweile ist auch die Version 2.0 des NTLM Protokolls kompromittiert.

Falsch konfigurierte Verschlüsselung schützt nicht

- Ist EFS falsch konfiguriert (etwa bei Verwendung lokaler Benutzerkonten ohne aktiviertes SYSKEY-Kennwort), kann die EFS-Verschlüsselung umgangen werden, wenn ein Angreifer physikalischen Zugriff auf den Rechner hat.

Neben der reinen Betriebssystemkonfiguration ergeben sich Sicherheitsprobleme jedoch auch durch die fehlerhafte Konfiguration systemnaher Komponenten wie DNS, WINS, DHCP, RAS oder IPSec. Gelingt es einem Angreifer, diese Komponenten mit Erfolg anzugreifen, so ist die Systemsicherheit des gesamten Netzes gefährdet.

G 3.49 Fehlerhafte Konfiguration des Active Directory

Windows 2000 und Windows Server 2003 gestatten die Delegation einzelner administrativer Rechte - auch für Teilbereiche des Active Directory - an bestimmte Benutzer. Diese Delegation erfolgt durch die Vergabe detaillierter Einzelberechtigungen im Active Directory.

falsche Zugriffsrechte

Durch die hohe Komplexität der Rechtevergabe, z. B. viele für die einzelnen Objekttypen spezifische Einzelberechtigungen, Vererbung von Berechtigungen, unzureichende Dokumentation, im Active Directory kann es geschehen, dass

- Administratoren Zugriff auf Bereiche des Active Directory haben, zu deren Administration sie nicht befugt sind, oder
- Bereiche des Active Directory nicht durch Zugriffsrechte geschützt sind, so dass jeder Benutzer auf diese Daten zugreifen kann.

Die Gefahr des unberechtigten Zugriffs bei Fehlkonfiguration der Active-Directory-Zugriffsrechte erhöht sich insbesondere dadurch, dass mehrere Zugriffsschnittstellen auf das Active Directory existieren, z. B. ADSI, LDAP.

Besondere Gefährdungen ergeben sich aus Handlungen, die die Datenbankstruktur des Active Directory ändern:

Inkompatibilitäten

- Änderungen des Active Directory Schemas können dazu führen, dass das bestehende Windows 2000 System zu anderen Softwarepaketen, die das Active Directory nutzen, inkompatibel wird. Da sich Änderungen des Schemas z. T. nicht rückgängig machen lassen, kann dies bedeuten, dass das bestehende System völlig neu aufgesetzt werden muss.

personenbezogene Daten

- Bei der Aufnahme eines personenbezogenen Attributes in den Global Catalog des Active Directory besteht die Gefahr, dass personenbezogene Daten auch jenseits des eigentlichen Adressatenkreises zugänglich sind.

Beispiel:

Innerhalb einer Firma werden die internen Telefonnummern der Mitarbeiter im Active Directory abgelegt. Wenn die Rechner der Firma nur eine Domäne im Active Directory Baum eines größeren Unternehmensverbundes bilden, würden diese internen Telefonnummern bei Aufnahme in den Global Catalog an alle Domänen des Active Directory Baumes verteilt.

G 3.50 Fehlerhafte Konfiguration von Novell eDirectory

Fehlkonfiguration von Software ist eine der häufigsten Ursachen für erfolgreiche Angriffe. Durch die hohe Komplexität und die große Zahl der verfügbaren Parameter bei eDirectory können durch unbeachtete Seiteneffekte auch zusätzliche Sicherheitsprobleme eintreten.

Mögliche Fehlkonfigurationen betreffen unter anderem

- die Erstellung und Definition der Baumstruktur an sich,
- die Konfiguration des Zertifikatsservers,
- die Einrichtung der abzubildenden Objekte,
- die Konfiguration der Zugriffsmechanismen,
- die Vergabe der Zugriffsrechte (siehe G 3.51),
- die Konfiguration des Intranet-Clientzugriffs auf den Verzeichnisdienst (siehe G 3.29),
- den LDAP-Zugriff auf eDirectory (siehe G 3.53),
- die Konfiguration der Partitionierung der Verzeichnisdatenbank,
- die Konfiguration der Replikation des eDirectory,
- die Konfiguration der aufzuzeichnenden eDirectory-Events,
- die Konfiguration des Real-time Alert-Mechanismus,
- die Konfiguration des iMonitor-Tools zur Web-basierten Fernüberwachung sowie
- die Konfiguration eines automatisierten Backup-Mechanismus.

inkonsistente Umsetzung der Sicherheitsrichtlinie

Grundsätzlich muss die Konfiguration des Systems an der Sicherheitsrichtlinie ausgerichtet werden. Bei Fehlkonfiguration besteht die Gefahr, dass diese Richtlinie inkonsistent umgesetzt wird und damit die Zielsetzungen der Sicherheitsvorgaben nicht erreicht werden.

unautorisierte Systemzugriffe

eDirectory ermöglicht die Konfiguration einer rollenbasierten Administration des Verzeichnissystems sowie die Delegation von Administrationsrechten. Bei einer Fehlkonfiguration dieser Funktionalitäten ergeben sich u. U. erhebliche Probleme durch unautorisierte Systemzugriffe. Weiterhin besteht bei fehlerhafter Konfiguration die Gefahr, dass eine geregelte Administration nicht mehr möglich ist.

Folgende Liste gibt einen Überblick über die sicherheitsrelevanten möglichen Konsequenzen einer Fehlkonfiguration des Novell eDirectory:

- Auswahl zu schwacher Authentisierungsmechanismen,
- Falsche Rechtevergabe für den Zugriff auf die Objekte des Verzeichnisdienstes,
- unautorisierte Systemzugriffe über die Administrationsschnittstelle,
- unzureichender Schutz vor Systemangriffen,
- Blockade der Administrationsmöglichkeit des Systems,
- fehlerhafte oder langsame Replikation der Daten zwischen den Verzeichnisdatenbanken sowie
- Inkonsistenzen in der Umsetzung der Sicherheitsrichtlinie.

G 3.51 Falsche Vergabe von Zugriffsrechten im Novell eDirectory

Da eDirectory eine Reihe sensitiver Daten der Systembenutzer und -Ressourcen enthält und zudem eine enge Beziehung zu dem unterliegenden Betriebssystem besteht, ist die Vergabe von Zugriffsrechten auf das eDirectory besonders wichtig.

Access Control Lists

Die Zugriffsrechte auf eDirectory-Objekte werden über so genannte Access Control Lists (ACLs) vergeben. Dabei gibt es Zugriffsrechte auf das eDirectory-Objekt an sich sowie auf einzelne Attribute eines Objekts.

Auf Objektebene sind dabei folgende Rechte (Privilegien) zu vergeben: *Browse, Create, Delete, Rename* und *Supervisor*. Auf Attributsebene sind dies: *Compare, Read, Add or Delete Self, Write, Supervisor* sowie *Inheritance Control*. *Compare* wird dabei als Teil des *Read*-Rechtes behandelt, d. h. sofern das *Read*-Recht vergeben ist, so besteht auch automatisch das Recht *Compare*.

Inherited Rights Filter

Die Access Control Lists selbst sind Attribute (Properties) zu den jeweiligen eDirectory-Objekten. Die Zugriffsrechte auf eDirectory-Objekte vererben sich standardmäßig von Vater- auf Kindobjekte innerhalb der Baumhierarchie. Um zu verhindern, dass Brüche dieses Vererbungsmechanismus durch Partitionierung des eDirectory-Verzeichnisses entstehen, wird an das Wurzelobjekt der Partition eine *inherited ACL* angehängt. Auf die Vererbung kann mit Hilfe so genannter Masken oder *Inherited Rights Filter* Einfluss genommen werden.

Die Zugriffsrechte auf Attributsebene werden standardmäßig nicht entlang der Verzeichnishierarchie weitergeleitet. Dies kann jedoch über das Attributsrecht *Inheritance Control* konfiguriert werden. Damit lässt sich auch das besonders kritische *Self*-Recht kontrollieren.

Trustee-Anweisungen

Die Zugriffsrechte werden explizit mittels so genannter *Trustee-Anweisungen* vergeben. Dabei werden die Zugriffsrechte (Privilegien) auf das Target-Objekt (Ziel) durch andere eDirectory-Objekte (Benutzer, Benutzergruppen, Services, Anwendungen, Server, etc.) direkt in die ACL des Target-Objekts eingetragen.

Security-Äquivalenzen

Weiterhin können Zugriffsrechte indirekt durch so genannte *Security-Äquivalenzen* vergeben werden. Beispiel: Target-Objekt X erhält (mindestens) die gleichen Zugriffsmöglichkeiten wie Target-Objekt Y, d. h. die Trustees von Objekt Y werden automatisch auch Trustees von Objekt X. Dies wird ebenfalls als ACL-Eintrag von Objekt X konfiguriert.

Bei einem konkreten eDirectory-Zugriff werden stets die so genannten *effektiven Rechte* berechnet, d. h. das Endresultat der oben beschriebenen Konfigurationen.

Diese Vielfalt an Konfigurationsmöglichkeiten der eDirectory-Zugriffsrechte beinhaltet die Gefahr, dass inkonsistente oder falsche Zugriffsmöglichkeiten vergeben werden. Sofern die Zugriffsrechte im eDirectory falsch vergeben werden, ist die Sicherheit des Gesamtsystems erheblich gefährdet. Dies betrifft die Vertraulichkeit und die Integrität von Daten sowie mögliche Hintertüren für weitreichende Systemangriffe.

Blockade der Administration

Ein besonders kritischer Punkt ist auch die Vergabe der Administrationsrechte. eDirectory ermöglicht die Umsetzung eines rollenbasierten Administrationskonzeptes sowie die Delegation einzelner Administrationsaufgaben durch die Vergabe entsprechender Zugriffsrechte. Bei einer falschen Vergabe dieser Rechte wird das gesamte Administrationskonzept in Frage gestellt und unter Umständen sogar die Administration des Verzeichnissystems blockiert.

G 3.52 Fehlerhafte Konfiguration des Intranet-Clientzugriffs auf Novell eDirectory

Beim Einsatz des eDirectory-Verzeichnisdienstes im Intranet einer Organisation werden für den verteilten Benutzerzugriff auf das System entsprechende Clients benötigt. Dabei gibt es für die unterschiedlichen Betriebssysteme jeweils eigene Client-Software:

- den Novell Client für Windows-Betriebssysteme,
- eine Client-Library für Linux,
- eine Client-Library für Sun Solaris.

Der Clientzugriff auf den eDirectory-Verzeichnisdienst erfolgt über das proprietäre NDAP-Protokoll (Novell Directory Access Protocol). Dieses setzt seinerseits auf dem Novell NCP-Protokoll auf, welches über IP oder IPX betrieben werden kann.

Bei einem Zugriff mit Hilfe des Novell Clients für Windows auf den eDirectory-Baum (oder ein eDirectory-Objekt) muss der Benutzername und das Passwort dem Client übermittelt werden. Der Client sucht dann beim eDirectory nach dem entsprechenden Objekt und übermittelt dessen privaten Schlüssel, welcher mit dem Benutzerpasswort verschlüsselt ist. Auf Clientseite wird mittels des Benutzerpasswortes der private Schlüssel entschlüsselt und daraus ein so genanntes *Credential* und eine Signatur berechnet. Der private Schlüssel wird anschließend aus dem Speicher des Clients gelöscht und nur das Credential und die Signatur behalten. Diese können in der Folge für weitere "Hintergrundauthentisierungen" zu anderen Objekten oder Diensten verwendet werden. Der Benutzer muss dafür nicht mehr in Interaktion treten und nutzt somit einen *Single-Sign-On*.

Aus dem Credential und der Signatur wird mittels eines so genannten *Zero-Knowledge-Verfahrens* ein Beweis (*proof*) generiert, welcher dem Zielsystem übermittelt wird. Das Zielsystem kann mit dessen Hilfe die Identität des Clients verifizieren. Der Vorteil dieser Methode ist, dass die Signatur nicht explizit über das Netz übertragen wird und somit weniger Angriffsmöglichkeiten bestehen.

Trotzdem sind gewisse Angriffsszenarien, so genannte *Man-in-the-middle-Attacks*, bekannt geworden, welche jedoch eher theoretischer Natur sind, da zu deren Ausnutzung erheblicher technischer Aufwand betrieben werden muss.

Dessen ungeachtet kann es zu ernsthaften Sicherheitsproblemen kommen, wenn

- die Authentisierungsmechanismen für den Clientzugriff mangelhaft sind,
- ein unautorisierter Zugriff auf das eDirectory-Verzeichnis und dessen Objekte möglich ist oder
- Administratorrechte für den Verzeichnisdienst missbraucht oder unberechtigt erlangt werden können.

G 3.53 Fehlerhafte Konfiguration des LDAP-Zugriffs auf Novell eDirectory

Der LDAP-Zugriff auf den Verzeichnisdienst von eDirectory eignet sich vor allem für zwei Szenarien:

- den Benutzerzugriff auf den Verzeichnisdienst über das Internet und
- den Zugriff auf den Verzeichnisdienst durch weitere Applikationen.

Prinzipiell gibt es aus Sicht des eDirectory drei Arten des Benutzerzugriffs über LDAP:

- als [Public] Objekt (*Anonymous Bind*),
- als Proxy User (*Proxy User Anonymous Bind*),
- als NDS User (*NDS User Bind*).

Übertragung der Passwörter im Klartext

Dabei ist zu beachten, dass das [Public] Objekt im eDirectory standardmäßig stets das *Browse*-Recht über den Verzeichnisbaum besitzt, sofern dieses Recht nicht explizit entzogen wurde. Weiterhin ist zu berücksichtigen, dass ohne die Konfiguration geeigneter Authentisierungsmechanismen die Gefahr besteht, dass die Benutzerpasswörter im Klartext übertragen werden. Eine Verschlüsselung der Übertragung ist nur dann gegeben, wenn die Kommunikation zwischen Client und eDirectory-Server über SSL erfolgt.

fehlerhafte SSL-Konfiguration

Bei der SSL-Konfiguration ergeben sich ebenfalls Fehlermöglichkeiten, welche zu einer Herabsetzung des Sicherheitsniveaus oder der Performance führen können.

Weiter ist zu beachten, welche LDAP-Version die Clients unterstützen und welche Konfigurationsmöglichkeiten dort bestehen. Unter Umständen kann es dabei zu Missverständnissen kommen und die Sicherheit des Betriebs beeinträchtigt werden.

Für die Anbindung von Netzapplikationen per LDAP an den eDirectory-Verzeichnisdienst ergeben sich prinzipiell die gleichen Gefährdungen wie beim Zugriff von Clients, nämlich:

- der unautorisierte Zugriff auf das Verzeichnis,
- der Verlust der Integrität und der Vertraulichkeit der im Verzeichnis gehaltenen Daten,
- die ungewollte Einrichtung einer Hintertür für das System.

G 3.54 Verwendung ungeeigneter Datenträger bei der Archivierung

Für die Speicherung von Daten werden Datenträger eingesetzt, die jeweils einen definierten Einsatzbereich und Einsatzzeitraum aufweisen. Hierbei kann es vorkommen, dass für die Speicherung dauerhaft oder temporär Datenträger verwendet werden, die den Anforderungen nicht gerecht werden.

Typische Ursachen hierfür sind beispielsweise

- Fehler bei der Beschaffung oder Bestellung der Datenträger,
- unzureichende Vorratshaltung, so dass nicht vorgesehene Datenträger eingesetzt werden müssen, um Datenverlust zu vermeiden,
- falsche Kennzeichnung der Datenträger oder
- unzureichende Kenntnisse über den Einsatzbereich des Datenträgers.

Datenverlust

Der Einsatz ungeeigneter Datenträger kann zu einem Datenverlust führen, der auch erst nach einer längeren Speicherdauer auftreten kann.

Beispiel:

Bei der routinemäßigen Beschaffung neuer Datenträger für ein Archivsystem werden anstatt einmalbeschreibbarer WORM-Medien (Write Once Read Multiple) fälschlicherweise wiederbeschreibbare Medien bestellt und geliefert. In Folge der Verwechslung werden Archivdaten überschrieben. Da die Speicherung der ursprünglichen Daten sehr lange zurückliegt, sind keine Kopien der Originaldaten mehr vorhanden. Dadurch sind die ursprünglich gespeicherten Dokumente unwiederbringlich verloren, da diese nur noch elektronisch archiviert wurden.

G 3.55 Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsystemen

Bei der Archivierung von elektronischen Dokumenten sind verschiedene rechtliche Vorgaben zu beachten, deren Nichteinhaltung zivil- oder strafrechtliche Konsequenzen haben kann. Hervorzuheben sind hier u. a.

- Mindestaufbewahrungsfristen, die sich aus steuerlichen, haushaltsrechtlichen oder sonstigen Gründen ergeben,
- Vorgaben an die Höchstaufbewahrungsdauer, die sich aus Datenschutzregelungen ableiten,
- Zugriffsrechte, die für Externe - wie z. B. Steuerbehörden - gewährt werden müssen, sowie
- die Rechtslage zur digitalen Signatur.

Einige Quellen für rechtliche Rahmenbedingungen sind in der Maßnahme M 2.245 *Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung* aufgeführt.

G 3.56 Fehlerhafte Einbindung des IIS in die Systemumgebung

Der IIS wird weltweit in unterschiedlichen Umgebungen eingesetzt. Als Einsatzumgebung wird die Netztopologie (Anordnung von weiteren Hard- und Software-Komponenten, Netzkomponenten) verstanden, in der der IIS betrieben wird. Als wesentlicher Aspekt ist dabei auch der Kommunikationsbedarf des IIS mit anderen Systemen zu berücksichtigen.

Die Absicherung eines öffentlichen, aus dem Internet erreichbaren Servers ist im Vergleich zu einem im Intranet installierten Server in der Regel mit einem viel höheren Aufwand verbunden. Von entscheidender Bedeutung ist dabei der sichere Einsatz geeigneter Trenneinrichtungen.

Eine unzureichend geplante Netzstruktur, z. B. ohne Demilitarisierte Zone (DMZ) oder eine fehlerhaft konfigurierte Trenneinrichtung (Firewall), kann für einen Angriff aus dem Internet bzw. Intranet ausgenutzt werden.

Ein weiteres Risiko entsteht durch nicht ausreichend dimensionierte Systemressourcen (Firewall, Netzanbindung). Wenn diese Systeme nicht den Anforderungen an die Verfügbarkeit und Performance des eigentlichen Web-Servers entsprechen, besteht die Gefahr eines Single-Point-of-Failure (SPOF).

Beispiel:

Mit Hilfe eines IIS und eines Datenbank-Servers wird eine E-Business-Anwendung realisiert. Befindet sich der Datenbank-Server im gleichen Segment wie der IIS, auf den aus dem Internet zugegriffen werden darf, besteht die Gefahr, dass ein Unbefugter auch auf die Datenbank zugreifen und die vorhanden Datenbestände auslesen oder manipulieren kann.

G 3.57 Fehlerhafte Konfiguration des Betriebssystems für den IIS

Voraussetzung für den sicheren Betrieb einer Applikation ist die Sicherheit des verwendeten Betriebssystems. Da der IIS sehr stark mit dem Betriebssystem verzahnt ist und z. B. die Benutzerdatenbank und Dateiberechtigungen von Windows verwendet, ist eine sichere Konfiguration von Windows NT/2000 von entscheidender Bedeutung für den sicheren Betrieb.

Einige typische Fehlkonfigurationen werden im Folgenden aufgeführt:

- **Zu viele, nicht benötigte Dienste werden angeboten:** Je mehr Dienste und Services ein Server anbietet, desto größer sind die Angriffsmöglichkeiten auf die Verfügbarkeit des Rechners und die Vertraulichkeit und Integrität der zu verarbeitenden Daten. Jeder Dienst bzw. Service kann zusätzliche Schwachstellen enthalten, die für einen Angriff ausgenutzt werden können. Insbesondere beim Netbios-Dienst besteht die Gefahr, dass ein Angreifer Informationen über vorhandene Benutzer, Freigaben usw. abfragen kann.
- **Großzügige Konfiguration der Netzeinstellungen:** Windows ermöglicht eine Vielzahl von Netzeinstellungen in der Registry, über die z. B. Zeitbeschränkungen für eine Verbindung oder die Anzahl von gleichzeitigen Verbindungen definiert werden können. Fehlerhafte Einstellungen, insbesondere von Timer-Werten, können einen DoS-Angriff auf den Server ermöglichen.
- **Unzureichende Sicherung von Kennwörtern:** Einen weiteren Angriffspunkt bilden leicht zu erratende oder nicht ausreichend geschützte Passwörter. Windows stellt verschiedene Werkzeuge zum Sichern der Passwörter bereit, die bei der Auswahl von Passwörtern die Einhaltung einer Sicherheitsrichtlinie erzwingen (z. B. *passfilt.dll*) oder den Zugriff und das Auslesen von Passwörtern erschweren (z. B. *passprop, syskey).*

Die aufgeführten Aspekte sind Beispiele für mögliche Sicherheitsprobleme durch Fehlkonfigurationen des Betriebssystems. Abhängig vom jeweiligen Einsatzumfeld können weitere potentielle Sicherheitsprobleme hinzukommen.

G 3.58 Fehlerhafte Konfiguration eines IIS

Fehlkonfigurationen eines Software-Systems sind häufig die Ursache für erfolgreiche Angriffe. Aufgrund der Komplexität eines IIS und der vielfältigen Einsatzmöglichkeiten in Verbindung mit anderen Server-Systemen besteht auch hier die Gefahr, dass das System durch Fehlkonfiguration nicht den geforderten Sicherheitsansprüchen genügt. Durch die Fülle von Konfigurationseinstellungen und durch die sich gegenseitig beeinflussenden Parameter können auch viele Sicherheitsprobleme entstehen. Einige typische Fehlkonfigurationen werden im folgenden aufgeführt:

- **Zu viele, nicht benötigte Dienste werden angeboten:** Je mehr Dienste und Services ein Server anbietet, desto größer sind die Angriffsmöglichkeiten auf die Verfügbarkeit des Rechners und die Vertraulichkeit und Integrität der zu verarbeitenden Daten. Jeder Dienst bzw. Service kann zusätzliche Schwachstellen enthalten, die für einen Angriff ausgenutzt werden können. Beispielsweise kann der FTP-Dienst zum Übertragen von Daten auf den Server ausgenutzt werden.
- **Vertrauliche Informationen sind nicht ausreichend geschützt, da sie sich z. B. in zugänglichen Verzeichnissen befinden:** In Abhängigkeit von Aufgabe und Einsatzumgebung können auch persönliche Informationen, z. B. durch die Auswertung von Formularen, auf dem Server vorhanden sein. Sind diese Daten nicht ausreichend vor einem unberechtigten Zugriff geschützt, z. B. durch ACLs (Access Control Lists), können sie ggf. von einem Angreifer ausgelesen werden.
- **Eingabeparameter werden unzureichend geprüft:** Viele Programmierer gehen bei der Entwicklung ihrer Anwendungen davon aus, dass vom Benutzer geforderte Eingaben, z. B. in einem Formularfeld oder eine URL, immer korrekt erfolgen. Die Prüfung der Benutzereingaben wird oft auf die für die weitere Verarbeitung erforderlichen Bedingungen beschränkt. Die Überprüfung der Syntax oder der verwendeten Zeichen wird oft vernachlässigt. Dabei besteht die Gefahr, dass Eingaben, die vom System nicht erwartet werden, z. B. Sonderzeichen oder Buchstaben anstelle von Zahlen, zu unnötigen Ressourcenbelastungen und Pufferüberläufen führen können und dadurch Sicherheitsfunktionen umgangen werden können.
- **Fehlerhafte Zugriffslisten (Access Control Lists, ACLs):** Der IIS ist eng mit dem Betriebssystem verzahnt und nutzt auch die Sicherheitsmechanismen von Windows für den Zugriff auf Dateien und Verzeichnisse. Oft werden die Zugriffsrechte sehr großzügig vergeben. Beispielsweise gehört das Konto *IUSR_Computername*, das bei der Installation des IIS automatisch angelegt wird, standardmäßig der Gruppe *GAST* an und besitzt somit die Rechte, auf Verzeichnisse außerhalb des Webroot-Verzeichnisses zuzugreifen. Auch innerhalb von virtuellen Verzeichnissen entstehen u. U. Risiken, wenn z. B. Scripts oder ausführbare Programme verwendet werden. Sind die Zugriffsrechte nicht restriktiv vergeben, besteht die Möglichkeit, dass diese Programme ausgelesen oder verändert werden.

G 3.59 Unzureichende Kenntnisse über aktuelle Sicherheitslücken und Prüfwerkzeuge für den IIS

Die Entwicklung in der Informationstechnik unterliegt einem stetigen Wandel. Hard- und Software-Lösungen werden immer leistungsfähiger, Anwendungen werden aktualisiert und durch neue Versionen ersetzt. Allerdings ergeben sich durch diese Veränderungen auch neue Anforderungen an die Administratoren und IT-Verantwortlichen. Sie unterliegen einer ständigen Informationspflicht, um mit dem aktuellen Stand der Technik vertraut zu sein.

Bei unzureichenden Kenntnissen des Administrators besteht zum einen die Gefahr, dass ein System fehlerhaft konfiguriert wird, zum anderen können Bedrohungen in einer Situation falsch eingeschätzt werden. Insbesondere durch die Komplexität des IIS und das Zusammenwirken mit weiteren Systemen in einer heterogenen Systemumgebung können Risiken entstehen, die vom Administrator zu bewerten sind.

Wichtige Informationsquellen für den Administrator bilden die Veröffentlichungen von aktuellen Schwachstellen (Bulletins) der eingesetzten Software. Obwohl Microsoft bei Bedarf neue Service Packs für Windows NT und Windows 2000 veröffentlicht, existieren für Windows und den IIS Schwachstellen, die aufgrund ihrer Aktualität noch nicht in die Service Packs aufgenommen worden sind. Aktuelle Schwachstellen werden von Microsoft oder anderen Arbeitsgruppen und Organisationen veröffentlicht.

Sind dem verantwortlichen Administrator die aktuellen Sicherheitslücken nicht bekannt, kann dieser natürlich nicht die erforderlichen Sicherheitsmaßnahmen ergreifen, um das System gegen entsprechende Angriffe zu schützen.

Zur Vereinfachung der Administration von Windows und des IIS bietet Microsoft eine Reihe von Prüfwerkzeugen an, die Bestandteil des *Windows NT/2000 Ressource Kit* sind oder direkt aus dem Internet heruntergeladen werden können. Beispielsweise besteht mit dem *IIS Lockdown Tool* die Möglichkeit, in sehr kurzer Zeit eine Reihe von Sicherheitseinstellungen vorzunehmen, insbesondere für die Zugriffsbeschränkung auf wichtige Dateien und Verzeichnisse. Ein weiteres Werkzeug ist das *Hotfix Check Tool*, mit dem der Patchstatus von Windows NT und Windows 2000 geprüft werden kann.

Der Nachteil vieler Tools, die in die Administration eingreifen, besteht darin, dass sie nur einen Teil der sicherheitsrelevanten Einstellungen vornehmen und dass die einzelnen Funktionen nur unzureichend dokumentiert sind.

Beispiel:

Im Juli 2001 infizierte der Wurm *Code Red* in weniger als 14 Stunden über 350.000 Computer in der ganzen Welt. Der Wurm nutzte eine Schwachstelle aus, für die seit einiger Zeit ein Patch von Microsoft verfügbar war. Selbst Monate später waren jedoch noch eine Vielzahl von Rechnern infiziert, weil keine entsprechenden Sicherheitsmaßnahmen eingeleitet wurden.

G 3.60 Fehlerhafte Konfiguration von Exchange 2000 Servern

Generell ist die Fehlkonfigurationen eines Software-Systems häufig die Ursache für erfolgreiche Angriffe. Aufgrund der Komplexität eines Exchange 2000 Servers besteht auch hier die Gefahr, dass das Exchange System durch Fehlkonfigurationen nicht den geforderten Sicherheitsansprüchen genügt. Durch die Fülle an Konfigurationseinstellungen und durch die sich gegenseitig beeinflussenden Parameter können zahlreiche Sicherheitsprobleme entstehen.

Einige typische Fehlkonfigurationen werden im folgenden aufgeführt:

Domänen-Controller

- Der Exchange 2000 Server wird auf einem Domänen-Controller und nicht als Member Server innerhalb des Netzes installiert.

  Dies hat erhebliche Konsequenzen für die Administrationsrechte auf dem Server und verhindert eine sinnvolle Rollentrennung der Administration. Der Hintergrund ist, dass Exchange als Service unter dem Account *Local System* abläuft und somit die vollständige Kontrolle über den Rechner hat, auf dem es abläuft. Würde Exchange auf einem Domänen Controller laufen, so hätte es unter anderem auch die Kontrolle über die Kerberos-Schlüssel. Weiterhin ergeben sich Nachteile bezüglich der Performance und unter dem Aspekt der Ausfallsicherheit.

- Die Zugriffsbeschränkungen auf einen Exchange 2000 Server sind unzureichend.

  Insbesondere in der Kombination mit schwachen oder falschen Zugriffsberechtigungen auf weitere Dienste oder E-Mail-Datenbanken können so Sicherheitsprobleme entstehen.

Access Control Lists

- Zugriffslisten (Access Control Lists, ACLs) sind fehlerhaft oder es werden unsichere Standard-ACLs verwendet.

  Jedes Exchange 2000 Objekt erhält bei der Erzeugung eine Zugriffsliste mit Standardeinträgen. Je nach Vorlage (Systemrichtlinie) bietet diese keinen ausreichenden Schutz für die E-Mail-Datenbank im Normalbetrieb. Dies gilt besonders dann, wenn die E-Mail-Datenbank von Exchange 5.5 nach Exchange 2000 migriert wurde. Unter Exchange 5.5 haben einige Objekte keinen *Security Identifier* (SID). Somit existiert für diese Objekte überhaupt keine ACL, bevor die SIDs nicht nachträglich konfiguriert wurden.

  Oft sind für die Erzeugung oder Initialisierung einer E-Mail-Datenbank zunächst umfangreiche Rechte notwendig, die für den laufenden Betrieb nicht mehr erforderlich sind. Werden die Standard-ACLs nicht verändert, kann dies dazu führen, dass Unbefugte auf die E-Mail-Datenbank zugreifen können oder Benutzern zu weitgehende Rechte eingeräumt werden.

keine Verschlüsselung

- Es wird keine Verschlüsselung eingesetzt.

  Die Verschlüsselung der Netzkommunikation (Port-Verschlüsselung) sowie der E-Mail-Kommunikation ist bei einer Standardinstallation nicht aktiviert.

Um die Verschlüsselung zu nutzen, muss diese explizit eingerichtet werden. Anderenfalls sind die E-Mail-Daten während des Zustellprozesses ungeschützt.

Die aufgeführten Aspekte sind Beispiele für mögliche Sicherheitsprobleme durch Fehlkonfigurationen. Abhängig vom jeweiligen Einsatzumfeld können weitere Problemfelder hinzukommen.

G 3.61 Fehlerhafte Konfiguration von Outlook 2000 Clients

Der E-Mail-Client Outlook 2000 ist ein wichtiger Teil des E-Mail-Systems. Die korrekte Konfiguration des Clients ist wichtig für die Gesamtsicherheit des Systems.

Folgende Aspekte sollten hierbei besonders erwähnt werden:

MAPI-Schnittstelle

- Die Auswahl des Kommunikationsprotokolls kann spezielle Sicherheitsprobleme nach sich ziehen. Dabei sei besonders die MAPI-Schnittstelle erwähnt, über die sich in der Vergangenheit eine Reihe von Computer-Viren und Würmern verbreitet haben.

Benutzerprofile

- Wird ein Client-PC von mehreren Benutzern in verwendet, so wird für jeden Benutzer ein eigenes Profil angelegt und gespeichert. Hierbei besteht die Gefahr, dass dieses Profil durch einen Kollegen übernommen wird. Dadurch kann unter Umständen das Benutzerkonto einer Person gegenüber dem System unbefugt übernommen sowie die Vertraulichkeit von Daten beeinträchtigt werden.

private Schlüssel

- Werden Verschlüsselung und elektronische Signatur auf E-Mail-Ebene eingesetzt, z. B. auf der Basis von S/MIME oder PGP, so kann unter Umständen der private Schlüssel kompromittiert werden, sofern dieser lokal abgespeichert wird. Mögliche Folgen sind, dass die Vertraulichkeit der Daten beeinträchtigt und Rechte von Dritten unbefugt übernommen werden.
- Wird Verschlüsselung auf Netzebene eingesetzt, z. B. durch die Nutzung von IPSec, SSL oder TLS, so besteht die Gefahr, dass diese Mechanismen bei einer fehlerhaften Konfiguration des Client-PCs unwirksam werden.

Datenverlust

- Eine fehlerhafte Konfiguration des E-Mail-Clients Outlook 2000 kann außerdem zu einem Datenverlust sowie zu einer Blockade des Client-PCs führen. Weiterhin kann es zu einem Überlauf und damit zu einer Überlastung des Exchange 2000 Servers kommen.

Viren und aktive Inhalte

- Ist im Outlook 2000 Client die automatische Ausführung gefährlicher Dateiformate nicht in geeigneter Weise deaktiviert, so besteht die Gefahr, dass Viren und schädliche aktive Inhalte eingeschleppt oder verbreitet werden.

Die Terminverwaltung und die Aufgabenliste sind weitere Bestandteile des Exchange/Outlook-Systems, die nicht direkt der Abwicklung des E-Mail-Verkehrs dienen, sondern der Unterstützung des Workflows innerhalb einer Organisation.

Diese Bereiche enthalten mitunter jedoch ebenso sensible und schützenswerte Informationen wie die elektronischen Nachrichten. Bei einer Fehlkonfiguration dieser Teilsysteme bestehen somit folgende potentielle Sicherheitsprobleme:

- Verlust der Vertraulichkeit durch unbefugten Zugriff,
- Verlust der Integrität der Informationen durch Datenmanipulation (zufällig oder vorsätzlich),

- unberechtigte Übernahme der Rolle bzw. der Identität eines anderen Benutzers oder
- Verlust von Daten und Informationen durch unsachgemäße Datenhaltung und fehlende Backup-Vorkehrungen.

G 3.62 Fehlerhafte Konfiguration des Betriebssystems für einen Apache-Webserver

Eine fehlerhafte Konfiguration des Betriebssystems für einen Apache-Webserver kann den sicheren und fehlerfreien Betrieb des Servers stören oder die Auswirkungen von Störungen verschlimmern.

Einige häufige Fehler bei der Konfiguration des Betriebssystems sind:

Fehlerhaftes Filesystem-Layout

- Wenn die Partitionen bzw. Filesysteme nicht groß genug angelegt werden, dann kann es zu Betriebsstörungen kommen, wenn die Dateisysteme "vollaufen". Sind die Filesysteme auf einer einzigen Festplatte angelegt oder schlecht auf verschiedene Festplatten verteilt, so kann dies zu einer deutlich verschlechterten Performance des Servers führen.

Zu viele Netzdienste

- Falls auf dem Serverrechner unnötige Netzdienste laufen, so kann dadurch die Sicherheit des Gesamtsystems gefährdet sein. Oft sind in Standardinstallationen von Betriebssystemen auch zu viele Benutzer eingerichtet oder Benutzer haben zu viele oder falsche Rechte.

Zu viele installierte Programme

- Sind auf dem Serverrechner Compiler oder Interpreter für Skriptsprachen installiert, so können diese von Angreifern, die sich Zugang zum Server verschafft haben, für weitere Angriffe benutzt werden. Oft erfordern bestimmte Schritte auch das Herunterladen von Dateien von Rechnern, die der Angreifer kontrolliert. Dazu benötigt der Angreifer eventuell einen Telnet-, ssh- oder ftp-Client oder Download-Tools wie *wget*, die für den normalen Serverbetrieb nicht nötig sind.

Zu großzügige Zugriffsberechtigungen

- Oft sind die betriebssystemseitigen Zugriffsberechtigungen für die Programm- und Konfigurationsdateien eines Apache-Webservers und für *.htpasswd*-Dateien so gewählt, dass zu viele lokale Benutzer Lese- oder gar Schreibzugriff auf diese Dateien haben. Dadurch können Unbefugte Informationen über die Konfiguration des Servers erlangen, die eventuell einen Angriff erleichtern oder erst ermöglichen. Haben Unbefugte Leseberechtigung auf *.htpasswd*-Dateien, so können die Passwörter für den Zugriff auf geschützte Bereiche des Webangebotes leicht über einen Brute-Force-Angriff geknackt werden.

G 3.63 Fehlerhafte Konfiguration eines Apache-Webservers

Obwohl die Default-Konfiguration der Quelltext-Distribution eines Apache-Webservers relativ sicher ist, kann es erhebliche Sicherheitslücken verursachen, wenn für den Apache-Webserver eine Default-Konfiguration einfach übernommen oder nur geringfügig abgeändert wird.

Bei der Konfiguration eines Apache-Webservers können verschiedene Fehler gemacht werden. Einige häufige Fehler werden hier kurz erläutert:

- Apache-Distributionen von Betriebssystemherstellern oder Distributoren enthalten oft zu zu viele Module, die im speziellen Einsatzszenario nicht benötigt werden. Wird ein solches nicht benötigtes Modul geladen, so kann dies die Sicherheit des Servers dadurch gefährden, dass die Administratoren nicht reagieren, wenn in einem solchen Modul eine Sicherheitslücke bekannt wird, weil sie meinen, nicht davon betroffen zu sein.
- Werden Pfade für Protokolldateien nicht angepasst, so werden diese im Unterverzeichnis *logs* des Installationsverzeichnisses abgelegt. Da Protokolldateien sehr schnell eine beachtliche Größe erreichen können, droht ein "Voll-Laufen" der entsprechenden Partition. Dies kann zu ernsthaften Störungen des Serverbetriebs führen.
- Die Apache-Konfiguration enthält Vorgabewerte für bestimmte Einstellungen, die Einfluss auf die Performance eines Apache-Webservers haben. Werden diese Einstellungen ohne genaue Kenntnis der Auswirkungen geändert, so kann dies die Performance bedeutend verschlechtern. Oft sind auch die Auswirkungen einer Änderung nicht sofort
- Werden mit der Direktive *ScriptAlias* Verzeichnisse für den Apache-Webserver als Verzeichnisse mit ausführbaren Programmen markiert, die zu viele Skripte oder Programme enthalten, die eigentlich nicht benötigt werden, so kann dies auf analoge Weise wie bei "vergessenen" Modulen zu Sicherheitslücken führen. Haben zu viele lokale Benutzer Schreibrechte auf Verzeichnisse, die mittels *ScriptAlias* als Programmverzeichnisse markiert sind, so können böswillige Benutzer dort Programme ablegen, die sie später über einen WWW-Zugriff ausführen können.
- Oft werden die "globalen" Vorgaben für Verzeichnisoptionen nicht mit einer geeigneten *Options*-Direktive auf einen restriktiven Vorgabewert gesetzt. Dies betrifft insbesondere die Option *Includes*, die die Ausführung von Programmcode in Server-Side-Includes erlaubt. Jedoch können auch andere Optionen wie *Indexes* zu Sicherheitslücken führen.
- Die Konfiguration des Zugriffsschutzes für HTTP-Zugriffe (über die Module *mod_access* und die verschiedenen *mod_auth_*-Module) kann auf viele Arten und Weisen falsch gelöst werden, so dass dadurch entweder eine Vertraulichkeitsverlust entsteht, wenn Unbefugte Zugriff auf vertrauliche Informationen erhalten, oder aber die Verfügbarkeit der Informationen für berechtigte Benutzer nicht gewährleistet ist.
- Bei der Verwendung von *mod_ssl* kann durch verschiedene Konfigurationsfehler das Serverzertifikat unzureichend geschützt sein. Oft

wird das Serverzertifikat nicht durch eine Passphrase geschützt, so dass ein Einbrecher, der sich eine Kopie der Zertifikatsdatei verschafft, einen "gefälschten" Server aufsetzen kann. Wird eine Passphrase verwendet, so kann es zu Problemen mit der Verfügbarkeit des Webservers kommen, da in diesem Fall ein automatischer unbeaufsichtiger Neustart des Servers nicht möglich ist, weil die Passphrase eingegeben werden muss.

G 3.64 Fehlerhafte Konfiguration von Routern und Switches

Die Konfiguration aktiver Netzkomponenten hängt stark vom Einsatzzweck der Geräte ab. Nachfolgend sind einige Beispiele aufgeführt, die den sicheren Einsatz der Geräte bedrohen können.

Betriebssystem

Oft werden auf Routern und Switches veraltete oder unsichere Versionen von Betriebssystemen verwendet. Für eine Vielzahl von Versionsständen für Betriebssysteme unterschiedlicher Geräte und Hersteller stehen auf einschlägigen Seiten im Internet Exploits zum Angriff auf diese Geräte zum Download bereit.

Passwortschutz

Der Zugriff auf aktive Netzkomponenten wird oft nur unzureichend durch Passwörter geschützt.

Administrationszugänge

Administrationszugänge sind in der Praxis oft frei zugänglich. Es sind beispielsweise keine Access Control Lists (ACL) eingerichtet.

Remote-Zugriff

Aktive Netzkomponenten bieten in der Regel die Möglichkeit mit Hilfe von TELNET remote zuzugreifen. Bei der Nutzung von TELNET werden Benutzername und Passwort im Klartext übertragen.

Login-Banner

Login-Banner von aktiven Netzkomponenten verraten häufig die Modell- und Versionsnummer des Geräts.

Unnötige Netzdienste

Häufig stehen auf Routern und Switches unnötige Netzdienste bereit, mit deren Hilfe Angreifer die Verfügbarkeit, Integrität oder Vertraulichkeit der Komponenten gefährden können.

Schnittstellen

Nicht genutzte Schnittstellen auf Routern sind häufig nicht deaktiviert.

VLAN

Trunk-Ports können auf alle konfigurierten VLANs zugreifen. Das heißt, dass der Zugang zu einem Trunk-Port den Zugriff auf alle VLANs ermöglicht. Häufig sind auf Switches die Trunking-Protokolle auf den Endgeräte-Ports nicht deaktiviert. Siehe auch G 5.114 *Überwindung der Grenzen zwischen VLANs*.

Routing-Protokolle

Routing-Protokolle ohne Authentisierungsverfahren können die Vertraulichkeit, Verfügbarkeit und Integrität komplexer Netze bedrohen.

G 3.65 Fehlerhafte Administration von Routern und Switches

Eine fehlerhafte Administration von Routern und Switches kann die Verfügbarkeit, Vertraulichkeit und Integrität von Netzen bedrohen. Es gibt unterschiedliche Zugriffsmöglichkeiten, um Router und Switches zu administrieren, die bei falscher Anwendung ein Sicherheitsrisiko darstellen können:

Remote-Administration

Eine Vielzahl von aktiven Netzkomponenten bieten die Möglichkeit der Remote-Administration mit Hilfe des Dienstes Telnet. Die Nutzung von Telnet bietet allerdings eine Gefahr durch die unbefugte Erlangung von Zugriffsrechten, da der Datenverkehr inklusive des Benutzernamens und Passwortes im Klartext mitgelesen werden kann.

Viele Geräte bieten die Möglichkeit, Administrationsarbeiten mit Hilfe des Dienstes HTTP durchzuführen. Auf dem Router bzw. dem Switch ist in diesem Fall ein HTTP-Server gestartet, der Zugriff erfolgt von beliebigen Clients über Web-Browser. Die Standardeinstellungen für den Zugriff auf das Web-Interface sind nicht bei allen Herstellern einheitlich. So kann der Zugriff deaktiviert sein, es ist aber auch möglich, dass dieser Dienst ungeschützt ohne Eingabe von Benutzerinformationen verwendet werden kann.

Wie bei der Nutzung des Dienstes Telnet werden auch beim HTTP der Benutzername und das Passwort im Klartext übertragen. Zudem sind eine Reihe von Exploits bekannt, die Schwachstellen der HTTP-Server unterschiedlicher Hersteller ausnutzen.

SNMP

Die Authentisierung erfolgt bei SNMPv1 und SNMPv2 lediglich mittels eines unverschlüsselten "Community Strings". Als Standardeinstellung bei nahezu allen Herstellern ist der read-Community-String auf den Wert "public" eingestellt, während der write-Community-String auf den Wert "private" gesetzt ist. Die SNMP Community Strings werden im Klartext über das Netz übertragen. Oft wird SNMP über nicht abgesicherte Netze genutzt, so dass ein Angreifer in der Lage ist, durch Mitlesen der Datenpakete (Sniffen) SNMP Community Strings zu erraten. Nach Kenntnisnahme der Community Strings kann ein Angreifer die Kontrolle über die Netzkomponenten übernehmen.

Protokollierung

Häufig werden sicherheitsrelevante Ereignisse auf Routern und Switches nur unzureichend protokolliert. Zudem kann sich eine fehlende Alarmierungskomponente negativ auf die Verfügbarkeit, Vertraulichkeit und Integrität der Systeme auswirken.

Fehlendes Backup und Dokumentation

Oft werden Konfigurationsänderungen auf Routern und Switches nicht gesichert und nicht dokumentiert. Beim Ausfall der Komponenten stehen die letzten Änderungen beim Wiederanlauf des Ersatzsystems nicht zu Verfügung.

G 3.66 Fehlerhafte Zeichensatzkonvertierung beim Einsatz von z/OS

EBCDIC *(Extended Binary Coded Decimals Interchange Code)* und ASCII *(American Standard Code for Information Interchange)* sind Kodierungstabellen, die festlegen, wie Buchstaben, Ziffern und andere Zeichen mit Hilfe von 8 bzw. 7 Bits dargestellt werden.

z/OS-Systeme arbeiten mit EBCDIC-*Code*. Lediglich HFS- und zFS-Dateisysteme (*Hierarchical File Systems*), die unter USS (*Unix System Services*) eingesetzt werden, lassen sowohl ASCII- als auch EBCDIC-Speicherung zu. Beim Datenaustausch zwischen z/OS-Systemen und Systemen, die mit ASCII-Code arbeiten (z. B. auch von USS nach MVS), besteht die Gefahr, dass Informationen verfälscht werden, wenn fehlerhafte Übersetzungstabellen (*Code Page Translation*) zum Einsatz kommen. Besonders häufig betroffen ist dabei die Übersetzung von Sonderzeichen.

Beispiele:

Probleme mit Umlauten und Sonderzeichen

- In einem Unternehmen wurden zwischen verschiedenen OS/390- und z/OS-Systemen über einen längeren Zeitraum mittels FTP-Protokoll Daten übertragen, ohne dass es zu Problemen kam. Für ein zusätzliches Unix-System wurde der gleiche FTP-Job eingesetzt und die *EBCDIC-ASCII*-Übersetzung mit der Default-Tabelle durchgeführt. Der Transfer verlief zunächst ohne Probleme, bei der weiteren Verarbeitung der Datensätze im Unix-System zeigte sich jedoch, dass bestimmte Umlaute und Sonderzeichen nicht richtig übersetzt worden waren. Erst nach der Erstellung einer speziellen *Translation Table,* die nur für diesen Transfer zum Einsatz kam, war der Fehler bereinigt.

Datenfehler möglich

- Bei der Übertragung einer Datei mittels FTP-Protokoll von einem z/OS-Betriebssystem zu einem Unix-Betriebssystem wurde die Option *Binary* verwendet. Die Daten konnten auf dem Zielsystem nicht weiterverarbeitet werden, da die Option *Binary* die Konvertierung von EBCDIC nach ASCII unterdrückt.

G 3.67 Unzureichende oder fehlerhafte Konfiguration des z/OS-Betriebssystems

falsche Definitionen

Die Konfiguration eines z/OS-Betriebssystem ist sehr komplex und erfordert an vielen Stellen den Eingriff des System-Administrators. Durch falsche oder unzureichende Definitionen entstehen schnell Schwachstellen, die zu entsprechenden Sicherheitsproblemen führen können.

Autorisierte Programme

Programme, die von einer autorisierten Bibliothek geladen werden und entsprechend gekennzeichnet sind, können hoch autorisierte Funktionen ausführen. Gelingt es Anwendern eigene Programme unberechtigt zu autorisieren, steht diesen Programmen nahezu die gleiche Funktionalität wie den System-Programmen zur Verfügung. Ein Deaktivieren von Sicherheitssperren in RACF ist so z. B. jederzeit möglich.

System-Programme

Bei der Installation des z/OS-Betriebssystems und seiner Komponenten ist es notwendig, bestimmte System-Bibliotheken (*Partitioned Datasets*) so zu definieren, dass das Betriebssystem auszuführende System-Programme über interne Tabellen schnell findet. Die Bibliotheken dieser System-Programme werden in sogenannten *Linklists* zusammengefasst und beinhalten in der Regel hoch autorisierte Programme, die im *Kernel-Mode* laufen. Durch Fehler in der Definition (oder durch Manipulation) können andere User-Bibliotheken zu diesen *Linklists* hinzugefügt werden, die nicht dafür vorgesehen sind. Die Programme dieser Bibliotheken sind dann ebenfalls hoch autorisiert und erlauben das Ausführen von Funktionen, die Sicherheitsmechanismen umgehen können.

Fehler beim Anlegen von Systembibliotheken

System-Bibliotheken, die als PDS (*Partitioned Dataset)* mit der Option *Secondary Space* angelegt wurden, können zu Problemen im Betrieb führen. Während der Initialisierungsphase legt das System für einige System-Bibliotheken die *Directory* aus Geschwindigkeitsgründen in den Hauptspeicher und greift beim Laden des Programms nur über dieses Verzeichnis auf die Bibliothek zu. Wird bei der Erweiterung einer Bibliothek im Rahmen einer Programm-Pflege ein neuer Extent (dynamische Erweiterung des Dateibereiches auf der Festplatte) angelegt, kann es passieren, dass das alte Programm statt des neuen aktiv wird, da die interne Directory noch auf die alte Ladeadresse zeigt. Ferner kann dadurch der Platzbedarf einer Datei permanent anwachsen, ohne dass eine kontrollierte Begrenzung stattfindet.

Supervisor-Calls

Probleme mit SVCs

Supervisor-Calls (SVCs) sind Aufrufe zu speziellen z/OS-Dienstprogrammen, die im hochautorisierten Kernel-Modus laufen. Programme für diesen Modus müssen besonders sicher programmiert sein (IBM gibt hierfür entsprechende Richtlinien vor). Unsichere SVC-Programme können unter Umständen benutzt werden, um z/OS-Sicherheitsmechanismen zu umgehen. Ein Angreifer befindet sich nach einer erfolgreichen Attacke im hochautorisierten Kernel-Modus. Vielfach gibt es heute noch sogenannte *Autorisierungs-SVCs* in Gebrauch, die aus wenigen Instruktionen bestehen, über *Modeset* den Kernel-

Modus an- oder ausschalten und es damit auch erlauben, unberechtigt im Kernel-Modus Funktionen auszuführen.

TSO-Kommandos

Hoch autorisierte TSO-Kommandos

Time-Sharing-Option-Kommandos (TSO) laufen normalerweise im Anwendungsmodus ab (mit normalen User-Privilegien), d. h. sie sind nicht besonders privilegiert. z/OS verfügt jedoch über Kommandos, die für die Ausführung bestimmter Funktionen (oder Teilfunktionen) eine hohe Autorisierung benötigen. Kommandos, die nicht über die Autorisierung verfügen, die sie zur Verarbeitung benötigen, können im Betrieb Fehler produzieren. Andererseits führt die unkontrollierte Freigabe von autorisierten Kommandos zu einer Schwächung der Sicherheit.

Restricted Utilities

Besondere Dienstprogramme

IBM und andere Software-Hersteller liefern, zusammen mit den Betriebssystemkomponenten zusätzliche Dienstprogramme (*Utilities*) aus. Diese Programme führen verschiedene verarbeitende Funktionen aus, wie das Kopieren von Dateien oder das Anlegen von Katalogen (z/OS Dateiverzeichnis zum Verwalten von Dateien). Die Mehrzahl dieser Utilities benötigt zur Ausführung lediglich normale User-Privilegien, einige benötigen jedoch eine hohe System-Autorisierung zur Durchführung ihrer Funktionen. Sind diese Utilities nicht korrekt definiert, dann besteht die Gefahr, dass sie nicht richtig funktionieren. Sind diese Utilities nicht hinreichend geschützt, dann besteht die Gefahr, dass sie von nicht autorisierten Mitarbeitern missbraucht werden können. In der Folge kann die Integrität des z/OS-Systems beeinträchtigt werden.

z/OS-Kommandos unter SDSF (System Display and Search Facility)

SDSF erlaubt es dem Anwender in einem JES2-System, sich die Ausgabe von Batch-Jobs, das System-Log und weitere System-Optionen anzuschauen und darüber hinaus MVS- und JES2-Kommandos einzugeben. Falls keine oder nur unzureichende Maßnahmen getroffen wurden, kann der Anwender von SDSF unter Umständen Manipulationen vornehmen, wie z. B. laufende Batch-Jobs beenden, *Initiators* stoppen oder starten oder aber Systemkonfigurationen umdefinieren. Darüber hinaus kann er ggf. alle System-Nachrichten aus dem Syslog und auch alle Job-Logs (u. U. auch Kunden-Daten) einsehen.

Enhanced MCS-Support

z/OS unterstützt über die MCS-Konsole (*Multiple Console Support*) hinaus die *Enhanced-MCS-Konsole*. Diese stellt eine Schnittstelle dar, über die Kommandos an MVS (JES2/3) übergeben und Nachrichten von MVS empfangen werden können. Die *Enhanced-MCS-Konsole* steht unter *TSO*, *NetView* und Applikationen - wie z. B. *CICS* - zur Verfügung. Wenn nicht entsprechende Schutzdefinitionen vorgenommen werden, können unter Umständen Kommandos abgesetzt werden, die die Integrität eines Systems stark beeinträchtigen können.

Beispiele:

Ein offenes System

- Auf einem OS/390-System wurde in der Vergangenheit ein *Autorisierungs-SVC* eingesetzt, um unter *TSO/ISPF* bestimmte Funktionen im autorisierten. Modus (*Kernel-Mode*) zu nutzen. Obwohl diese Schwach-

stelle seit längerem bekannt war, wurde der SVC auch in neueren z/OS-Umgebungen installiert und stand jedem Anwender zur Verfügung.

- Aus historischen Gründen wurde ein z/OS-Betriebssystem mit dem RACF-Attribut *OPERATIONS* betrieben. Viele Benutzer, deren Konto über dieses Attribut verfügte, konnten nahezu alle Dateien lesen und modifizieren. Die Integrität der Dateninhalte konnte bei diesem z/OS-System nur noch bedingt gewährleistet werden. **Zu viele Verantwortliche**

- In einem z/OS-System wurde das *SDSF* für *JES2* ohne jeden Schutz zur Verfügung gestellt. Schon nach kurzer Zeit hatten die Mitarbeiter herausgefunden, wie sie die Priorität des eigenen Benutzerkontos im System erhöhen konnten, um ihre Batch-Jobs im System schneller bearbeiten zu lassen. Eine Kontrolle und effiziente Auslastung des Systems waren nicht mehr möglich. **Keine System-Kontrolle**

G 3.68 Unzureichende oder fehlerhafte Konfiguration des z/OS-Webservers

Die Übernahme der Default-Einstellungen oder eine fehlerhafte Konfiguration des z/OS-Webservers kann zu Sicherheitsproblemen führen.

- Bei Verwendung der standardmäßig vorgegebenen Einstellungen (*httpd.conf*-Datei) und falsch eingestellten *Userid*-Regeln können durch die *MVSDS* Funktion des Webservers unter Umständen Dateien angezeigt werden, die dem Anwender normalerweise unter seiner Kennung nicht zur Verfügung stehen sollten, wie z. B. Systemdateien.
- Administrationsfehler können dazu führen, dass Prozesse des z/OS-Webservers unter der *Started-Task*-Kennung laufen. Besitzt diese Kennung hohe Rechte im System (z. B. *Superuser)*, kann dies zu Sicherheitsproblemen führen. Datei-Zugriffe und Kommandos erfolgen dann unter der Autorisierung dieser Kennung. Als Folge sind u. U. Zugriffe auf Dateien mit Kundendaten oder, wie vorher beschrieben, auf Systemdateien über die *MVS-Dataset-Display*-Funktion möglich.
- Der z/OS-Webserver unterstützt verschlüsselte Datenkommunikation über das SSL-Protokoll. Bei falscher Konfiguration der Parameter besteht dabei die Gefahr, dass die Verschlüsselung deaktiviert ist oder die Prozesse unter einer anderen RACF-Kennung laufen.

Weitere Gefährdungen werden im Baustein B 5.4 *Webserver* aufgeführt.

Beispiel:

- Die Verwendung der Standarddefinitionen eines z/OS-Webservers ermöglichte es einem externen Angreifer, sich sensitive Dateien anzeigen zu lassen. Darüber hinaus war der Webserver so eingestellt, dass der Dienst mit hohen Rechten unter der eigenen *Started-Task*-Kennung lief. Einem externen Angreifer war es dadurch aus dem Internet möglich, die Dateien *SYS1.PROCLIB* und *SYS1.PARMLIB* anzuzeigen. Aus diesen Angaben konnte der Angreifer Informationen herauslesen, die den Angriff auf das gesamte z/OS-System erleichterten.

G 3.69 Fehlerhafte Konfiguration der Unix System Services unter z/OS

Unix System Services

Unix System Services (USS) ist ein z/OS-Subsystem, das vor der Inbetriebnahme angepasst werden muss.

Bei der Anpassung der USS-Parameter gibt es eine Reihe von Problemfeldern, die beachtet werden müssen, damit es nicht zu Sicherheitsproblemen beim z/OS-System bzw. bei Teilen des z/OS-Systems kommt.

Je nach Art der Fehlkonfiguration stehen nach dem Start des z/OS-Systems bestimmte Teilfunktionen der *Unix System Services* nicht zur Verfügung bzw. das *USS-Subsystem* startet nicht:

- Fallen Teilfunktionen der USS aus, können wichtige Subsysteme, wie z. B. TCP/IP, fehlen.
- Startet das gesamte *USS-Subsystem* nicht, steht auch das z/OS-Betriebssystem nicht zur Verfügung.
- Werden *HFS-Dateien* während der Startphase nicht allokiert (*Mount*), können Applikationen, die diese Dateien benötigen, nicht betrieben werden.

Im Folgenden sind einige typische Fehler bei der Konfiguration der USS aufgeführt:

- Der komplexe Aufbau der *BPXPRMxx-Member* kann zu Administrationsfehlern führen. Dies hat während des *Initial Program Load (IPL)* einen fehlerhaften Start des Systems zufolge. Dies ist eine Frage der Reihenfolge, in der die einzelnen Member-Definitionen durchlaufen werden.
- Bestimmte Parameter im *BPXPRM00-Member* müssen auf die Kapazitätsgrenzen des Systems abgestimmt sein. Anderenfalls besteht die Gefahr, dass mehr Unix-Prozesse anlaufen, als es das System verkraften kann.
- Es können Fehler bei den *Sysplex*-Definitionen auftreten, z. B. bei der *VERSION*-Angabe.
- Es sind Fehler bei der Definition der *Mount-Policies* von HFS- und zFS-Files (Type, Mode und Mountpoint) möglich.
- Innerhalb der *BPXPRMxx-Member* können Variablen falsch verwendet worden sein.

Beispiele:

Schwellwerte nicht angemessen

- Der Aufruf eines rekursiven Unix-Kommandos erzeugte auf einem z/OS-System fortwährend neue Prozesse, bis die z/OS-Auslagerungsdateien (*Page-Platten*) nicht mehr ausreichten. Trotz vorhandener weiterer *Page-Platten*, war es nicht möglich, das System zu retten, da nur noch wenige Systemeingaben möglich waren. Das Problem konnte nur durch einen Neustart (*IPL*) des Systems gelöst werden.

Komplexe Reihenfolgen von Parametern

- Auf einem z/OS-System mit mehreren *BPXPRMxx-Membern* wurde eine Parameteränderung in einem falschen Member vorgenommen. Die Änderung wurde vom System nicht berücksichtigt, weil der Parameter während des *IPL* von einem vorhergehenden Member gelesen wurde.

G 3.70 Unzureichender Dateischutz des z/OS-Systems

Im z/OS-Betriebssystem steuert und überwacht ein Sicherheitssystem, wie RACF, den Dateizugriff. Eine fehlerhafte Administration des Dateischutzes erlaubt es unter Umständen einem Angreifer, unberechtigt auf wichtige Dateien zuzugreifen, z. B. auf Betriebssystemprogramme, auf Konfigurationsdateien oder auf Anwendungsdaten.

RACF sieht beispielsweise vor, dass Benutzerkonten mittels spezieller Attribute (z. B. *Special* oder *Operations*) mit umfassenden Rechten ausgestattet werden können.

Es sollte beachtet werden, dass Daten, auf die ein Anwender lesenden Zugriff hat, unter z/OS immer auch von ihm kopiert werden können.

In diesem Zusammenhang sollte auch die Gefährdung G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten* beachtet werden.

Beispiele:

- Die Dateien mit den Lohndaten wurden als Kopie unter der Kennung eines Mitarbeiters angelegt, dessen Benutzerkonto in RACF mit dem Attribut *Universal Access UPDATE* definiert war. Alle Mitarbeiter hatten dadurch nicht nur lesenden Zugriff, sondern konnten die Daten auch modifizieren.

Ungewollte Einsicht bzw. Manipulation

- Aufgrund eines nachlässigen Umgangs mit dem RACF-Attribut *Operations* verfügte ein Anwender über die Möglichkeit, nahezu alle System- und Kundendaten zu lesen oder zu kopieren.

Operations-Attribut

G 3.71 Fehlerhafte Systemzeit bei z/OS-Systemen

Falsche Zeit

Die Systemzeit (Datum und Uhrzeit) stellt für eine ganze Reihe von Anwendungen und Systemprogrammen eine wichtige Größe dar, von der die korrekte Ausführung einer Vielzahl von Aktionen und die verlässliche Erstellung von Ergebnissen und Daten abhängig ist.

Durch falsche Datums-/Zeitangaben können unter anderem folgende Sicherheitsprobleme und resultierende Schäden entstehen:

- Anwendungen, die Entscheidungen auf Basis des aktuellen Datums treffen, liefern fehlerhafte Ergebnisse. Die Nacharbeitung ganzer Tagesproduktionen kann die Folge sein. Dies gilt insbesondere für Online-Anwendungen und deren Transaktionsdaten. Korrekturen sind oft nicht mehr möglich, wenn z. B. Kunden online auf das System zugreifen.
- Die Analyse von Sicherheitsvorfällen, die Zeitangaben berücksichtigt, kann deutlich erschwert sein oder zu fehlerhaften Ergebnissen führen.
- Differierende Systemzeiten in miteinander verbundenen Systemen sind problematisch, wenn z. B. Log-Daten zu einer gemeinsamen Auswertung herangezogen werden.
- Anwendungen, die Daten von mehreren Einzelsystemen empfangen und in Abhängigkeit der Zeitstempel verarbeiten, liefern verfälschte Ergebnisse.

Systemzeit bei z/OS-Systemen

Werden z/OS-Systeme nicht im *Parallel-Sysplex-Cluster* betrieben, muss die Systemzeit in der Regel während des *IPL* (Initial Program Load) manuell durch den Bediener eingegeben werden. Dabei kann es leicht passieren, dass das Datums- oder Zeitfeld falsch gesetzt wird.

Die Änderung der Systemzeit ist auch während des Betriebes möglich. Hier ist die Gefahr von Fehleingaben durch Unachtsamkeit noch größer als bei einem IPL.

In dem *Member Clock00* wird die Zeitzone bzw. die Abweichung von der Greenwich-Mean-Time (GMT) eingestellt. Eine falsche Einstellung der Zeitzone führt zum gleichen Ergebnis als wäre die Systemzeit selbst falsch eingestellt worden.

Beispiele:

Fehlerhafte Zeiteingabe

- Während des Betriebs sollte die Zeiteinstellung eines z/OS-Systems um 5 Minuten korrigiert werden. Ein Tippfehler bei der Eingabe des Kommandos *SET* führte zu einer Systemzeit, die in den Abendstunden lag. Der *Job-Scheduler* startete dementsprechend die abendliche Batch-Produktion bereits während des Tages. Weil die Batch-Jobs exklusiv auf die Datenbanken der Anwendung zugriffen, war online keine Dateneingabe mehr möglich.

G 3.72 Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF

Fehlerhafte Sicherheitseinstellungen in RACF

Im z/OS-Betriebssystem ist für den Zugangs- und Zugriffsschutz auf Ressourcen ein spezielles Sicherheitssystem zuständig. Hierfür kommt häufig RACF (*Resource Access Control Facility*) zum Einsatz. Die Konfiguration von RACF im Auslieferungszustand entspricht in der Regel nicht den Sicherheitsanforderungen im jeweiligen Einsatzszenario.

Im Folgenden werden die am häufigsten vorzufindenden Problemfelder in Bezug auf die RACF-Konfiguration beschrieben.

Gültigkeitsregeln für Passwörter

SETROPTS Definitionen

Mit dem Kommando SETROPTS können in RACF systemweit gültige Sicherheitseinstellungen des z/OS-Systems, insbesondere für Passwörter, definiert werden. Zu den Parametern gehören die minimale Passwortlänge, die Anzahl der erlaubten Anmeldeversuche, die maximale Gültigkeitsdauer, die Passwort-Historie, Auditeinstellungen und die Klassenaktivierungen.

Missbrauch von Standard-Passwörter

Im Auslieferungszustand von z/OS sind für die Kennung *IBMUSER* und das RACF-Kommando *RVARY* Standard-Passwörter voreingestellt. Noch während des Betriebs sind oft die Systemmonitore mit sicherheitskritischen Funktionen über Standard-Passwörter zugänglich.

Die Kennung *IBMUSER* dient als erste Kennung zum Aufbau eines neuen Systems und besitzt *Special*- und *Operations*-Berechtigung. Da die Kennung *IBMUSER* keinem eindeutigen Anwender zugeordnet ist, lässt sich kaum herausfinden, wer diese Kennung benutzt bzw. benutzt hat.

Mit dem RACF-Kommando *RVARY* kann die RACF-Datenbank aktiviert und deaktiviert, d. h. auch gewechselt werden.

Die Standard-Passwörter sind in der Produktdokumentation aufgeführt und damit allgemein bekannt.

Warning-Modus

RACF-Ressourcen können im *Warning-Modus* geschützt werden. Dies bedeutet, dass alle Zugriffe auf die Ressource gewährt werden, auch wenn die RACF-Definitionen einen Zugriff auf die Ressource eigentlich verbieten würden. Durch den Warning-Modus werden unter Umständen sehr viel mehr Nachrichten in das Syslog geschrieben und darüber hinaus mehr SMF-Sätze (*System Management Facility*) erzeugt. Dies kann zu einer starken Erhöhung des Plattenspeicherplatzbedarfs führen.

Eine irrtümliche Freigabe von Ressourcen über den Warning-Modus kann zu einem Verlust der Vertraulichkeit von Daten führen.

Schutz von z/OS-System-Kommandos

Die z/OS-System-Kommandos werden über spezielle Klassen im RACF geschützt. Durch unzureichende Definitionen dieser Klassen ist es möglich, dass Anwender System-Befehle absetzen können, die unter Umständen den stabilen Systembetrieb beeinträchtigen. Beispiele hierfür sind das Starten oder Stoppen von *Started Tasks* oder das Online-Setzen von Plattensystemen.

Global Access Checking Table

Sind Dateien in der *Global Access Checking Table (GAC)* eingetragen, so erfolgt beim Zugriff keine Prüfung über die RACF-Datenbank. Der Anwender bekommt direkten Zugriff gemäß den in der *GAC* definierten Regeln. Werden in der *GAC* irrtümlich Dateien eingetragen, so sind diese nicht mehr über die RACF-Profile geschützt. Diese Dateien können z. B. von allen Anwendern ausgelesen werden, falls sie in der *GAC* mit *READ* eingetragen sind.

RACF-Datenbank

Die RACF-Datenbank enthält in verschlüsselter Form alle Passwörter der Benutzer und muss, wie jede andere Datei des z/OS-Betriebssystems, über entsprechende Definitionen geschützt werden. Ist der Zugriffsschutz auf die Datenbank so definiert, dass jeder Benutzer die Datei lesen (und damit auch kopieren) kann (z. B. über die Definition *Universal Access(UACC) = READ*), ist ein Brute-Force-Angriff auf die Passwörter möglich.

Beispiele:

- Über das Kommando *RVARY* kann die RACF-Datenbank gewechselt werden. Ein Systemprogrammierer fand heraus, dass das Passwort des Kommandos *RVARY* noch mit dem ausgelieferten Standardpasswort übereinstimmte. Daraufhin konnte er eine andere speziell vorbereitete RACF-Datenbank in das System bringen und aktivieren und hatte Zugriff auf Daten, die er vorher nicht einsehen konnte.

Benutzung des RVARY-Kommandos

- Nach dem Aufbau einer neuen RACF-Datenbank vergaß ein Bediener, die Kennung *IBMUSER* zu sperren. Ein Sachbearbeiter entdeckte diese Nachlässigkeit und es gelang ihm, unerlaubt Daten aus dem System zu kopieren.

Benutzung des IBMUSERs

- Die Sicherungskopie einer RACF-Datenbank war aufgrund eines Administrationsfehlers lediglich über die Definition *UACC(READ)* geschützt. Ein Angreifer nutzte dies aus, um die Datenbank auf seinen PC zu kopieren. Auf dem PC führte er mit frei verfügbaren Programmen einen Brute-Force-Angriff auf die Passwörter der RACF-Datenbank aus und war in mehreren Fällen erfolgreich. Der Angreifer nutzte die ihm bekannten Kennungen und Passwörter von anderen Anwendern aus, um Produktionsdaten zu verändern. Der Verdacht fiel zunächst auf den Besitzer der Kennung, die für den Zugriff in den Protokolldateien registriert wurde, und nicht auf den Verursacher des Schadens.

Brute-Force-Attacke auf RACF-Datenbank

G 3.73 Fehlbedienung der z/OS-Systemfunktionen

Während des Betriebs des z/OS-Systems sind von Zeit zu Zeit Eingriffe durch die Bediener (*Operators*), wie Anpassungen von RACF-Einstellungen oder anderen Systemdefinitionen, erforderlich.

Aufgrund der Komplexität des z/OS-Betriebssystems und seiner Komponenten lassen sich Fehlbedienungen durch die Bediener nicht vollständig ausschließen. Je nach Art der Fehlbedienung können in der Folge einzelne Komponenten oder das gesamte System ausfallen. Nachfolgend sind einige typische Beispiele für Fehlbedienungen aufgeführt.

Unbeabsichtigter Neustart über die Hardware Management Console (HMC)

Der Neustart eines Systems kann über die HMC angefordert werden. Zur Auswahl des Systems genügt ein einfaches Anklicken des System-Icons, danach muss nur noch die Funktion ausgewählt werden (z. B. *Initial Program Load*). Nach Bestätigung einer entsprechenden Rückfrage führt dieser Vorgang umgehend zum Neustart des ausgewählten Systems. Alle laufenden Prozesse werden unkontrolliert beendet. Eine Verwechselung der Systeme kann hierdurch schwerwiegende Folgen nach sich ziehen.

Da in der *HMC* auch Gruppen von Systemen zusammengefasst werden können, bis hin zu allen z/OS-Systemen eines Rechenzentrums, können weite Bereiche der Informationsverarbeitung betroffen sein.

Fehler beim JES3 DSI (Dynamic System Interchange)

Das *Job Entry Subsystem* JES3 gestattet den Betrieb eines Systemverbunds, der aus einem *Global*-Rechner und verschiedenen *Local*-Rechnern bestehen kann. Auf alle Rechner im Verbund (*Global* und *Local*) werden unter der Kontrolle des *Global*-Rechners vor allem Batch-Jobs automatisch verteilt und dann dort ausgeführt (ähnlich wie bei einem *Parallel-Sysplex-Cluster*, jedoch auf JES3 beschränkt). Der *Global*-Rechner übernimmt dabei die zentrale Kontrolle des gesamten Lebenszyklus des Batch-Jobs, wie z. B. Interpretation der Job Control Language, Systemzuordnung, Ressourcenkontrolle, Output-Management usw.

Zur Übernahme der Funktion des *Global*-Rechners auf einen *Local*-Rechner sind eine Reihe von Systemfragen zu beantworten. Falsche Angaben können im Extremfall zu einem IPL (*Initial Program Load*) aller Systeme des Verbunds führen.

Sperrung von z/OS-Kennungen

Kennungen mit dem Attribut *Special* erzeugen bei mehrmaliger aufeinander folgender Falscheingabe des Passwortes während der Anmeldung eine Konsol-Nachricht (*Reply*). Das Bedienpersonal (*Operator*) kann entscheiden, ob diese Kennung gesperrt werden soll. Werden im Extremfall, z. B. bei einer DoS-Attacke, alle Kennungen mit dem Attribut *Special* gesperrt (z. B. durch Automatismen), existiert auf diesem System keine Kennung mehr, die RACF bedienen kann. Das Sicherheitssystem ist dann in sich gesperrt.

Offline-Setzen von Platten

Ein versehentliches *Offline-Setzen* einer Platte kann gravierende Auswirkungen, bis hin zum Totalausfall des Systems, haben.

Löschen der Default Program Class in RACF

Wird versehentlich (z. B. durch Tippfehler) das Stern-Profil der Klasse *Program* gelöscht, kann dies zum Stillstand des Systems führen. Ein IPL hilft nicht weiter, da dadurch die Fehlerursache nicht beseitigt wird. Es muss erst die RACF-Datenbank bereinigt werden. Ein solcher Fehler kann einen stundenlangen Ausfall des kompletten Systems und einen erheblichen Aufwand für die Fehlerbeseitigung bedeuten.

Weiterleiten von fehlerhaften RACF Kommandos

Wenn ein System in eine RACF-Kommando-Synchronisierung (z. B. *RACF Remote Sharing Facility* - RRSF) eingebunden ist, kann ein fehlerhaftes RACF-Kommando alle anderen Systeme dieses Verbundes betreffen. Wird beispielsweise das Löschen der *Default Program Class* via RRSF übertragen, kann dies zum Stillstand aller Systeme im jeweiligen RRSF-Verbund führen.

Fehlbedienung vordefinierter Programm-Funktionstasten

Auch durch die Benutzung vordefinierter Programm-Funktionstasten kann es unter Umständen zu Sicherheitsproblemen kommen. Besondere Sorgfalt ist z. B. geboten, wenn Funktionstasten mit Kommandos belegt werden, die vor der Ausführung noch um bestimmte Werte ergänzt werden müssen. Hier besteht die Gefahr, dass der Operator die Funktionstaste versehentlich drückt, ohne eine Ergänzung einzugeben. Wenn das entsprechende Kommando auch ohne Ergänzung syntaktisch korrekt ist, wird es ausgeführt und bewirkt unter Umständen unerwünschte Effekte oder sogar enorme Schäden.

Falscheingaben im Allgemeinen

Generell besteht immer die Gefahr der Falscheingaben. Soll z. B. eine System-Task (oder ein Batch-Job) gestoppt werden und der Bediener vertippt sich, so kann es vorkommen, dass auf Grund von ähnlichen Jobnamen der falsche Job gestoppt wird. Das Gleiche gilt für den Gebrauch von System Kommandos.

Wird z. B. beim Inaktivieren von SNA-Knoten statt eines einzelnen Terminal-Namens versehentlich der *Cross Domain* Manager-Name eingegeben, so bedeutet dies den Verlust aller *SNA Sessions* dieser Domain. Nach dem Neustart des Knotens müssen sich die Anwender neu einloggen und die *SNA*-Verbindung zum System neu aufbauen.

Verriegelung von Ressourcen

Bei einer gegenseitigen Verriegelung von Ressourcen (*Enqueue Contention*) können Funktionen so lange nicht verfügbar sein, bis die Verriegelung wieder gelöst wird. Oft sind eine Reihe von System-Abfragen (*Displays*) und viel Betriebserfahrung notwendig, um gegenseitige Verriegelungen mit Hilfe der richtigen MVS-Kommandos wieder aufzulösen.

Unbeabsichtigte Eingabe des Befehls "Z EOD"

Wird an einer MVS-Master-Konsole während des Betriebs der Befehl *Z EOD* eingegeben, wird dieses System kontrolliert heruntergefahren. Alle Prozesse werden beendet und müssen neu aufgesetzt werden. Dieser Vorgang und der damit verbundene Betriebsausfall dauert in der Regel mindestens 30 Minuten.

G 3.74 Unzureichender Schutz der z/OS-Systemeinstellungen vor dynamischen Änderungen

Dynamische z/OS-Anpassungen

Viele z/OS-Systemeinstellungen lassen sich während des Betriebs verändern, ohne dass ein IPL durchgeführt werden muss. Nach Veränderung einer vorhandenen oder Erstellung einer neuen Parameterdatei (Member der *Parmlib*) löst ein Aktivierungskommando den Änderungsvorgang aus.

Die Sicherheit von z/OS-Systemen kann beeinträchtigt werden, wenn bestimmte Kommandos fehlerhaft bedient oder von Unbefugten missbraucht werden. Die wichtigsten kritischen Parameterdateien und Systemkommandos, durch die im laufenden Betrieb dynamisch Einstellungen geändert werden können, sind im Folgenden aufgeführt.

Erweiterung der APF-Dateien

Dateien, die über das *Authorized Program Facility* (APF) autorisiert werden müssen, können in einem *Definitions Member* festgelegt (*PROGnn*) und anschließend mit dem Kommando *SET PROG=nn* (Kommando *SET* und Parameter *PROG=m*) aktiviert werden. Alternativ lassen sich mit dem Kommando *SETPROG APF* (Kommando *SETPROG* und Parameter *APF*) einzelne Bibliotheken in den APF-Mechanismus einbinden. Sind die *Parmlib*-Definitionen oder die passenden Kommandos nicht richtig geschützt, kann es zu Sicherheitsproblemen kommen, da Dritte hierdurch unter Umständen eigene Programme mit hohen Autorisierungen versehen und während des Betriebs aktivieren können.

Erweiterung des *LINKLIST*-Mechanismus

Programme, die ohne *Steplib* oder *Joblib DD Statement* in einem Batch-Job verfügbar sein sollen, können in der *LINKLIST* definiert werden. Diese Definitionen sind in einem *PROGnn-Member* der *Parmlib* abgelegt, wobei Dateien durch das Kommando *SETPROG LNKLST* über ein neu zu definierendes Member dynamisch hinzugefügt werden können. Ist die *LINKLIST* in der Systemdefinition (*IEASYSnn*) mit *LNKAUTH=LNKLST* definiert, sind alle Programme, die über diesen Mechanismus geladen werden, automatisch APF-autorisiert. Auch hier ist die Integrität des Systems gefährdet, wenn das Kommando ungeschützt zur Verfügung steht.

Deaktivierung und Modifizierung der *User Exits*

Durch das Kommando *SETPROG EXIT* ist es möglich, *Exits* zu deaktivieren oder durch andere zu ersetzen. Ist das Kommando nur unzureichend geschützt, kann ein Angreifer unter Umständen auf dem System eigene *Exits* ausführen. Damit lässt sich z. B. das Schreiben von SMF-Sätzen (*System Management Facility*) unterbinden und die Auditierung des Systems beeinflussen (Verschleierung).

Veränderung der Message Processing Facility (MPF)

Viele Programme zur Automation von Vorgängen werten Nachrichten (*Messages*) des Systems aus. Durch Setzen anderer MPF-Versionen (*Message Processing Facility*) mit dem Kommando *T MPF=nn* kann die Automation manipuliert oder vollständig ausgeschaltet werden (*T MPF=NO*).

Austausch von Parmlibs

Parameterdateien (*Parmlibs*) sind die zentrale Stelle der z/OS-System-Definitionen. Mit Hilfe des Kommandos *SETLOAD* lassen sich vorhandene *Parmlibs* durch neue ersetzen.

Weitere kritische z/OS-Kommandos für dynamische Änderungen

Neben den oben beschriebenen Kommandos sind eine Reihe weiterer Kommandos zum Verändern von z/OS-Systemeinstellungen verfügbar, wie z. B. *SETSSI* zum Hinzufügen oder Löschen von Subsystemen oder *SETSMS* zum Verändern der SMS-Definitionen.

Von allen diesen Kommandos, die dynamisch z/OS-Definitionen ändern, können Sicherheitsprobleme ausgehen, wenn sie unkontrolliert im System zur Verfügung stehen. Durch den Missbrauch dieser Kommandos können ähnliche Probleme entstehen wie durch die Manipulation von kritischen Definitions-Dateien.

Beispiele:

- Ein Mitarbeiter eines Unternehmens konnte aufgrund eines unzureichenden Schutzes des Kommandos *SETPROG APF* eine eigene Programmdatei autorisieren. Unter Zuhilfenahme eines weiteren Programms, das von dieser Datei geladen wurde, war es ihm möglich, wichtige Finanzdaten zu verfälschen.

Unberechtigter Zugriff auf APF-Dateien

- Ein Bediener schaltete mit dem Kommando *T MPF=NO* (T ist eine Kurzform des SET-Kommandos) das *z/OS-Message-Processing* aus. Dies führte zu einer Überlastung der Konsole (Nachrichtenflut) und zur Sperrung einiger dort definierter *Exits*, so dass die Automation des Systems stark behindert wurde.

Beeinflussung der Automation

G 3.75 Mangelhafte Kontrolle der Batch-Jobs bei z/OS

z/OS-Betriebssysteme werden noch immer in hohem Maße für die Durchführung von Batch-Jobs eingesetzt. Ein Batch-Job besteht aus einem oder mehreren Einzelschritten (Job-Steps).

Die Eingabe zu einem Batch-Job sind entweder eine/mehrere Datei(en) oder entsprechende Steuerkarten, die über das *Job Entry Subsystem (JES2/3)* zugeführt werden. Die Ausgabeverwaltung erfolgt ebenfalls durch das *Job Entry Subsystem*.

Die Steuerung der Batch-Jobs besteht im wesentlichen aus *Start*, *Überwachung* des Ablaufs und der *Prüfung* des Ergebnisses (meist in Form eines *Returncodes*). Je nach *Returncode* müssen darauf häufig Folge-Batch-Jobs gestartet werden. Je höher die Anzahl der Jobs und die Komplexität der Abläufe ist, umso höher ist die Wahrscheinlichkeit eines Fehlers.

Manuelle Steuerung

Bei der manuellen Ausführung von Batch-Jobs besteht immer die Gefahr, dass durch menschliche Fehlhandlungen Probleme in den Batch-Abläufen entstehen. Betroffen sind neben dem zeitlichen Ablauf auch die Abhängigkeiten der Batch-Jobs voneinander. Bei zunehmender Zahl der zu steuernden Batch-Jobs erhöht sich deshalb die Komplexität der gesamten Batch-Kette immer drastischer und führt zu einer immer größeren Anzahl von Fehlern. Einer manuellen Steuerung sind deshalb natürliche Grenzen gesetzt.

Zeitliche Verzögerungen können sich z. B. so auswirken, dass ein nach den Batch-Jobs laufendes Online-Verfahren nicht termingerecht gestartet werden kann oder dass Dateisicherungen mit dem Online-Verfahren kollidieren.

Maschinelle Steuerung (Job-Scheduler)

Ist ein maschinelles Verfahren (*Job Scheduler*) eingesetzt, stellt dieses zwar den Ablauf sicher. Es können jedoch Fehler auftreten, wenn die Anweisungen an diesen *Job Scheduler* nicht sachgerecht getestet wurden und sich Fehler bei den Anweisungen eingeschlichen haben. Auch durch falsch definierte Automation im Ablauf der Stapelverarbeitung kann es zu fehlerhaften Reaktionen des *Job Schedulers* kommen.

Beispiel:

- Der Abbruch eines Batch-Jobs wurde während der Stapelverarbeitung nicht registriert. Erst die Online-Verarbeitung am nächsten Tag zeigte die Fehler in den Datenbeständen. Zur Korrektur musste die Online-Verarbeitung gestoppt, Datenbestände zurückgeladen und danach die Stapelverarbeitung wiederholt werden. In dieser Zeit stand die Online-Verarbeitung nicht zur Verfügung.

Beeinträchtigung des Online-Betriebes

G 3.76 Fehler bei der Synchronisation mobiler Endgeräte

Daten, die auf mobilen IT-Systemen wie Laptops, Mobiltelefone und PDAs gespeichert sind, werden häufig mit stationären IT-Systemen abgeglichen. Dies ist beispielsweise für die Termin- und Adress-Verwaltung sinnvoll.

Bei der Synchronisation können allerdings auch Daten zerstört werden. Im allgemeinen muss vor einer Synchronisation eingestellt werden, wie mit Konflikten beim Datenabgleich umzugehen ist: ob beispielsweise bei gleichlautenden Dateien die des PDA oder des anderen Endgerät ungefragt übernommen werden oder ob eine Abfrage erfolgt. Dies wird häufig bei Inbetriebnahme der Dockingstation einmal konfiguriert und gerät danach gerne in Vergessenheit. Wenn dann aber Daten in einer anderen Reihenfolge geändert werden als ursprünglich einmal gedacht, gehen dabei schnell wichtige Daten verloren. Dies kann auch ein unangenehmer Nebeneffekt sein, wenn mehrere Benutzer ihre PDAs mit demselben Endgerät synchronisieren, ohne daran zu denken, dass gleichnamige Dateien dabei überschrieben werden können.

G 3.77 Mangelhafte Akzeptanz von IT-Sicherheit

Verschiedene Umstände können dazu führen, dass in einer Institution oder auch in Teilen einer Institution keine Akzeptanz für IT-Sicherheit vorhanden ist, und damit auch keine Einsicht in die Notwendigkeit besteht, IT-Sicherheitsmaßnahmen auf- und umzusetzen. Dies kann beispielsweise bedingt sein durch

- die Behörden- oder Unternehmenskultur (nach dem Motto: "Das war schon immer so!", "Unseren Mitarbeiter können wir vertrauen, hier muss nichts weggeschlossen werden.", "Was soll hier schon passieren?", "Diese Sicherheitsmaßnahmen stören doch nur die Arbeitsabläufe."),
- fehlende Vorbilder, wenn beispielsweise die Vorgesetzten nicht mit gutem Beispiel vorangehen, oder
- ein anderes soziales Umfeld oder einen anderen kulturellen Hintergrund ("andere Länder, andere Sitten"). Typische Probleme können dadurch entstehen, dass bestimmte Benutzerrechte oder auch die Ausstattung mit Hard- oder Software als Statussymbol gesehen werden. Einschränkungen in diesen Bereichen können auf großen Widerstand stoßen.

Beispiel:

- Im militärischen Umfeld gehen Vorgesetzte häufig davon aus, dass die Umsetzung von Sicherheitsmaßnahmen befohlen werden kann. Allerdings zeigt auch hier die Erfahrung, dass Benutzer, die nicht über Sinn und Zweck von Sicherheitsmaßnahmen informiert sind, diese umgehen, wenn sie sie nur als Behinderung ihrer eigentlichen Aufgabe ansehen.
- Ein Befehl, nur sichere Passwörter zu verwenden, führte bei einem militärischen IT-System dazu, dass ein Passwort-Generator implementiert wurde. Dieser erzeugte 16-stellige zufällige Passwörter, die einmalig 10 Sekunden am Bildschirm angezeigt wurden. Diese Zeitspanne reichte aus, um die Passwörter aufzuschreiben. Da es vielen Leuten schwer fällt, sich Passwörter der Form "aN§3bGP?tz1BuH89" zu merken, wurden diese Zettel entgegen der Anweisungen nicht vernichtet, sondern häufig in der Nähe der Rechner aufbewahrt.

G 3.78 Fliegende Verkabelung

In Besprechung-, Veranstaltungs- und Schulungsräumen wechseln häufig sowohl die Benutzer als auch die Nutzungsart. Damit wird mitunter die Geräteausstattung und damit natürlich auch die Verkabelung in solchen Räumen geändert. Je nach Lage der Anschlusspunkte im Raum (Steckdosen der Stromversorgung und des Datennetzes) kann das dazu führen, dass Kabel quer durch den Raum, auch über Verkehrswege hinweg verlegt werden. Solche "fliegenden" Kabel sind nicht nur Stolperfallen für Personen. Wenn jemand daran hängen bleibt, kann das auch zu Schäden an IT-Geräten führen:

- Im einfachsten Fall wird lediglich eine Steckverbindung gelöst und die entsprechende Verbindung unterbrochen.
- Durch den plötzlichen Zug am Kabel kann aber die Steckverbindung beschädigt oder zerstört werden. Darüber hinaus kann aber auch, besonders bei verschraubten Steckern, das angeschlossene Gerät vom Tisch auf den Boden stürzen und dabei beschädigt werden.

G 3.79 Fehlerhafte Zuordnung von Ressourcen des SAN

Betriebssysteme reagieren unterschiedlich auf sichtbare Speicherressourcen. Wenn keine eindeutige und starke Zuordnung von Servern und Speicherressourcen vorgenommen wird, können unautorisierte Zugriffe auf Speicherressourcen z. B. durch andere Server das Schutzkonzept auf Ebene des Betriebssystems oder der Anwendung unterlaufen.

An dieser Stelle ist nicht nur der vorsätzliche Angriff zu betrachten, bei dem ein Angreifer versucht Lücken der Konfiguration für seine Absichten auszunutzen. Beachtlich ist auch die Eigenart mancher Betriebssysteme, alle erreichbaren Festplatten an sich zu binden und in die eigenen Hardwarekonfiguration einzubinden.

Gerade Windows Server neigen dazu, alle sichtbaren Speicherressourcen zu beanspruchen. Bei einem Speichernetz kann es so vorkommen, dass Speicherbereiche, die anderen Systemen zugeordnet sind, diesen entzogen werden oder Daten darauf verfälscht oder zerstört werden.

G 3.80 Fehler bei der Synchronisation von Datenbanken

Um die Daten einer Datenbank an verschiedenen Standorten oder auf mobilen Endgeräten zu halten, werden oft Datenbanken oder Auszüge davon gespiegelt. Damit diese Daten untereinander abgeglichen werden können, ist eine Datenbanksynchronisation erforderlich.

Bei der Synchronisation kann es zu Konflikten und damit zu einem Datenverlust kommen, wenn zwei Benutzer den gleichen Datensatz in gespiegelten Datenbanken geändert bzw. gelöscht haben. Oft helfen hier auch nicht die im System konfigurierten Regeln, welche Daten unter welchen Bedingungen überschrieben werden, da die Datenänderungen im Normalfall inhaltlich betrachtet werden müssen. Selbst wenn diese Regeln für alle Synchronisationen gelten, sind diese Regeln nicht immer allen Anwendern bekannt und führen dadurch gegebenenfalls zum falschen Ergebnis.

Synchronisationen zwischen Datenbanken an verschiedenen Standorten werden im Normalfall automatisiert durchgeführt. Konflikte werden dabei häufig erst erkannt, wenn ein Datenbank-Administrator die Datenbank öffnet bzw. die Log-Dateien analysiert. Der Datenbank-Administrator kann oft aufgrund mangelnder Befugnisse und Kenntnisse bezüglich der Dateninhalte nicht entscheiden, wie der Konflikt zu lösen ist. Dies trifft auch zu, wenn die Synchronisation manuell angestoßen wurde, aber die Synchronisations-Programme den Anwender nicht über auftretende Konflikte informieren.

Mobile Endgeräte werden meist manuell synchronisiert. Dabei bieten einige Datenbanken die Möglichkeit, die Benutzer über Konflikte zu informieren. Dennoch kann ein Benutzer nicht immer über die Synchronisation der Daten entscheiden, wenn ihm nicht alle Umstände der Datenänderungen bekannt sind.

G 3.81 Unsachgemäßer Einsatz von Sicherheitsvorlagen für Windows Server 2003

Windows Server 2003 ermöglicht die Übernahme von Einstellungen aus Vorlagen direkt in die Systemkonfiguration. Dafür existieren drei Vorlagentypen:

- Dateien mit der Erweiterung *.inf*, in Windows Server 2003 *Sicherheitsvorlagen* genannt, werden im Sicherheitskonfigurations-Editor (SCE) bearbeitet.
- XML-Vorlagen, ab Windows Server 2003 mit Service Pack 1 als *Sicherheitsrichtlinien* bezeichnet, werden mit dem Sicherheitskonfigurations-Assistenten (SCW) bearbeitet.
- Dateien mit der Erweiterung *.pol* (Windows NT 4.0-Vorlagen) können ebenfalls auf Windows Server 2003 angewendet werden.

Einsatz von Sicherheitsvorlagen verändert die Systemkonfiguration

Alle genannten Typen werden nachfolgend Sicherheitsvorlagen genannt. Sie verändern die Systemkonfiguration, sobald sie angewendet werden.

Wenn Sicherheitsvorlagen auf einem Server eingespielt und aktiviert werden, dann besteht die Gefahr, dass bestimmte Funktionen oder der ganze Server nicht mehr verfügbar sind. Werden Sie mit Hilfe von Gruppenrichtlinien oder Skripten automatisch auf mehrere Server ausgerollt, kann der Betrieb im betrachteten IT-Verbund gestört werden und sogar vollständig ausfallen.

Hohes Gefährdungspotential bei unsachgemäßem Umgang

Durch unsachgemäßen Umgang mit Sicherheitsvorlagen ergibt sich daher ein hohes Gefährdungspotential.

Mögliche Gefährdungen können ihre Ursache bereits in einem fehlerhaften Verhalten bei der Erstellung von Sicherheitsvorlagen haben. Der Erstellung geht meist die Analyse von Anforderungen voraus. Anschließend wird ein Referenzsystem manuell vom Administrator oder automatisch durch den SCW analysiert. Die Analyseprozesse umfassen viele Komponenten des Servers und betreffen Einstellungen, die tief in das Betriebssystem eingreifen. Die Analyseprozesse können unvollständig bleiben oder unbemerkt aus technischen Gründen fehlschlagen. Die zugrunde liegenden Sicherheitsdatenbanken und Sicherheitskataloge können korrupt oder nicht aktuell sein. Außerdem können Programme von Drittherstellern oder eine spezielle Systemkonfiguration unvorhergesehenen Einfluss auf den Analysevorgang haben.

Unverträglichkeiten von Vorlagentypen

Der SCW kann Sicherheitsvorlagen des SCE umwandeln und in seine *Sicherheitsrichtlinien*-Dateien mit einbinden. Hieraus können sich Konflikte von bestimmten Parametern ergeben. Sicherheitsvorlagen insgesamt können zwar von den Verteilungsmechanismen von Active Directory und Gruppenrichtlinien profitieren, allerdings müssen dazu alle Vorlagentypen in Gruppenrichtlinienobjekte umgewandelt oder - im Falle von *.pol*-Dateien aus Windows NT 4.0 - migriert werden. Dabei können ebenfalls Konflikte oder Kompatibilitätsprobleme auftreten.

Wechselwirkung zwischen Sicherheitsvorlagen und Programmen möglich

Der Ausroll-Vorgang von Sicherheitsvorlagen auf einen Server kann fehlschlagen, wenn der Server nicht den Voraussetzungen für die jeweilige Vorlage entspricht. Alte Applikationen, die nicht für Windows 2000/2003 entwickelt wurden, führen häufig zu unerwarteten Effekten. Außerdem

können Berechtigungseinstellungen, die in der Vorlage auf *Verweigern* gesetzt sind, unerwartetes Verhalten verursachen, das sehr schwer zu beheben ist.

Bei allen beschriebenen Punkten besteht die Gefahr, dass eine Vorlage nicht die geplante Wirkung erzielt und das System in einen unvorhergesehenen Zustand versetzt wird.

Fehlende Tests, nicht repräsentative Referenzsysteme

Die Gefahren verschärfen sich erheblich, wenn beim Entwickeln und Ausrollen von Sicherheitsvorlagen auf Tests verzichtet wird oder wenn die im Test verwendeten Referenzsysteme nicht repräsentativ sind.

Konformitätsprobleme

Schließlich kann auch eine unzureichende technische und organisatorische Durchsetzung und Kontrolle der Verteilungsmechanismen von Sicherheitsvorlagen den IT-Verbund gefährden. Wenn Ausrollvorgänge unbemerkt fehlschlagen, ergeben sich Inkonsistenzen zwischen Servern. Die erwartete Konfiguration und somit die erwartete Sicherheit ist nicht flächendeckend gegeben. Beim Entwickeln und inkrementellen Ausrollen weiterer Vorlagen entsprechen einige Zielsysteme dann auch nicht mehr den erwarteten Voraussetzungen. Dieser Zusammenhang wird auch als fehlende Richtlinien-Konformität bezeichnet.

Sicherheitsvorlagen aus Windows NT 4.0 (*.pol*-Dateien) bergen verstärkt das Risiko von Konformitätsproblemen und Inkompatibilitäten mit anderen Vorlagentypen. Für *.pol*-Dateien werden in Windows Server 2003 keine Werkzeuge mehr mitgeliefert und es gibt keine Herstellerunterstützung.

G 3.82 Fehlerhafte Konfiguration der VoIP-Middleware

Eine VoIP-basierte Telefonanlage kann in ähnlicher Weise von Fehlkonfigurationen betroffen sein wie eine leitungsvermittelnde Telefonlösung. Dies reicht von falschen Zuordnungen von Telefonbenutzern zu Telefonnummern bis hin zu einem Verlust der Verfügbarkeit der Telefoninfrastruktur. Auch eher unkritische Fehler, wie ein falsch geschriebener Name im Telefonbuch, sind natürlich nicht auszuschließen.

Weiterhin können über die Telefonanlage bestimmten Benutzern Privilegien beim Telefonieren zugeordnet oder entzogen werden. Beispiele sind Telefonverbindungen ins Ausland oder der Anruf kostenpflichtiger Service-Rufnummern. Eine Fehleinstellung kann hier einen Missbrauch ermöglichen, wenn beispielsweise ein allgemein zugängliches Telefon Auslandsberechtigung erhält.

Beim Einsatz von VoIP sind in der Regel mehrere Systeme integriert. Wird SIP als Initialisierungsprotokoll eingesetzt, werden meist Systeme wie Registrare, SIP-Proxy-Server und Location-Server für die Kommunikation benötigt. Bei Veränderungen müssen alle Systeme angepasst werden, wodurch Konfigurationsfehler entstehen können. Auch wenn sich alle Dienste auf einem Rechnersystem befinden, müssen häufig alle einzeln konfiguriert werden. Wird eine Änderung nur auf einem System nicht korrekt durchgeführt, kann die gesamte Telefoninfrastruktur möglicherweise nicht mehr genutzt werden.

Bei VoIP wird in der Regel kein klassischer Anrufbeantworter eingesetzt, sondern es wird im Falle der Abwesenheit oder Nichtverfügbarkeit des Benutzers eine Voice-Mail versendet. Dies ist oft eine E-Mail, an die eine Sprachmitteilung als Audio-Datei angefügt ist. Passiert während der Konfiguration ein Tippfehler bei der E-Mail-Adresse, erhält der eigentliche Empfänger die eingegangenen Nachrichten nicht. Es kann sogar passieren, dass sie stattdessen an einen falschen Empfänger zugestellt werden.

Neben den eigentlichen VoIP-Vermittlungssystemen müssen auch die Router und Switches, die auf tieferen Netzschichten operieren, konfiguriert werden. Um Verzögerungen bei der Vermittlung zu vermeiden, kann bei vielen Geräten eingestellt werden, dass VoIP-Nachrichten bevorzugt weitergeleitet werden. Fehler bei der Konfiguration können hier im schlimmsten Fall zu einem Komplettausfall des Netzes führen.

G 3.83 Fehlerhafte Konfiguration von VoIP-Komponenten

Unabhängig davon, ob es sich bei VoIP-Komponenten um dedizierte Hardware (Appliances) oder softwarebasierte Systeme handelt, spielt die Konfiguration eine entscheidende Rolle. Neben den Einstellungen zur Signalisierung, die im Verlauf der Planung festgelegt wurden, spielt das Übertragungsverfahren für die Medienströme eine wichtige Rolle. Durch ein Kompressionsverfahren kann die Größe der IP-Pakete mit den Sprachinformationen verkleinert werden.

Sehr oft führt der Einsatz eines ungeeigneten Verfahrens, das die Sprachinformationen zu stark komprimiert, zu einer Verschlechterung der Sprachqualität. Wird hingegen ein Verfahren gewählt, das eine zu geringe Kompression vornimmt, wird der Nachrichtenstrom nicht ausreichend vermindert und das IP-Netz kann überlastet werden.

Um die Vertraulichkeit der Telefongespräche zu schützen, kann bei einigen wenigen Protokollen zur Medienübertragung, wie SRTP, eine Verschlüsselung genutzt werden. Um der Protokollierung an eventuell benötigten Vermittlungssystemen entgegenzuwirken, kann bei vielen verschlüsselten Protokollen die Verschlüsselung direkt zwischen den Endgeräten erfolgen. Eine Fehlkonfiguration kann dabei zu einer unverschlüsselten Übertragung führen, möglicherweise sogar ohne dass dies von den Benutzern bemerkt wird. Werden zu schwache Verschlüsselungsverfahren oder zu kurze Schlüssellängen gewählt, kann ein Angreifer die Kommunikation unter Umständen trotz Verschlüsselung mithören.

Nicht nur das Abhören von Gesprächen kann für einen Angreifer interessant sein. Auch die Informationen, die bei der Signalisierung übertragen werden, können von einem Angreifer missbraucht werden. Wird durch eine fehlerhafte Einstellung im Endgerät das Passwort bei der Anmeldung im Klartext übertragen, könnte der Angreifer sich beispielsweise für einen anderen Benutzer ausgeben, obwohl alle beteiligten VoIP-Komponenten sicherere (Challenge-Response-) Verfahren unterstützen. Durch diesen Identitätsdiebstahl könnte der Angreifer auf Kosten des Opfers telefonieren oder weitere Dienste, wie das Abhören vom Anrufbeantworter, missbrauchen.

Sehr oft werden Applikationen, wie Softphones oder softwarebasierte Telefonanlagen, auf einem Standard-PC betrieben. Hierfür muss ein handelsübliches Betriebssystem installiert sein, auf dem die Programme ausgeführt werden. Fehler in der Administration und Konfiguration des Betriebssystems können große Auswirkungen auf den Betrieb und die Sicherheit der VoIP-Applikationen haben.

Unabhängig davon, ob auf dem IT-System ein Endgerät (Softphone) oder eine Vermittlungsanlage (Software-TK-Anlage) betrieben wird, können durch eine fehlerhafte Verteilung von Zugriffsrechten auf der einen Seite bestimmte Funktionalitäten nicht genutzt oder auf der anderen Seite fälschlich vergebene Zugriffsrechte missbraucht werden.

G 3.84 Fehlerhafte Konfiguration der WLAN-Infrastruktur

Access Points und andere WLAN-Komponenten bieten eine Vielzahl von Konfigurationseinstellungen, die insbesondere auch die Nutzung von Sicherheitsfunktionen betreffen. Werden hier falsche Einstellungen vorgenommen, dann kann es passieren, dass entweder keine Kommunikation über den Access Point möglich ist oder die Kommunikation unzureichend geschützt erfolgt, obwohl die Benutzer von einem vorhandenen Schutz ausgehen. Durch fehlerhafte Konfiguration von WLAN-Komponenten können diverse Sicherheitsprobleme entstehen, beispielsweise:

- Falls ein Access Point ungenügend gegen unbefugten Zugriff abgesichert ist, könnte jemand hieran Konfigurationsänderungen vornehmen, die zu weiteren Sicherheitslücken führen.
- Durch eine uneinheitliche Konfiguration der WLAN-Sicherheitsmechanismen auf den Access Points, können sich Verfügbarkeitsprobleme oder Sicherheitslücken ergeben.
- Sofern über ein WLAN auf das Internet zugegriffen werden kann, ist ohne weitere Filtermechanismen eine Internet-Nutzung durch jeden möglich, der sich mit dem WLAN verbinden kann.
- Eine zu freizügige Freigabe von Verzeichnissen oder anderen Systemressourcen bei einem WLAN-Client kann einem Angreifer einen unbemerkten Zugriff auf den Client ermöglichen.
- Bei einer nicht korrekt konfigurierter oder durch den Benutzer ausgeschalteten Personal Firewall eines WLAN-Clients ist dieser unter Umständen Angriffen auf Betriebssystem-Ebene ausgesetzt. Dies ist besonders in fremden Umgebungen und Hotspots problematisch.

Sicherheitsprobleme bereiten auch immer wieder Remote-Support-Zugänge auf WLANs, wenn sie nicht ausreichend abgesichert sind und über unsichere Netze genutzt werden. Sofern hier Fehlkonfigurationen vorgenommen wurden, kann dies beispielsweise dazu führen, dass es ein WLAN-Client kompromittiert wird und ein Angreifer hierbei Informationen über den Zugriff auf das WLAN erlangt. Diese Informationen können anschließend zum Angriff auf das komplette WLAN und ein eventuell damit verbundenes LAN verwendet werden.

G 3.85 Verletzung von Brandschottungen

Jedes Gebäude, in dem IT betrieben wird, ist von einer Vielzahl von Leitungen und Kabeln durchzogen. Frisch- und Abwasserleitungen, Heizungsrohre, Energieversorgung und Datenübertragung seien als Beispiele genannt. Es ist dabei unvermeidlich, dass solche Rohr- und Kabel-Trassen Brandschutzwände und Geschossdecken queren müssen. Um den Brandschutz sicher zu stellen, sind an solchen Stellen geeignete Brandschottungen einzubauen (siehe M 1.9 *Brandabschottung von Trassen*).

Im Laufe der Gebäudenutzung ist es meist unumgänglich, Arbeiten an solchen Trassen durchzuführen oder neue Trassen zu verlegen, sei es zu Reparaturzwecken oder um Platz für zusätzlich erforderlich gewordene Leitungen zu schaffen.

Änderung von Brandlasten

Bei solchen Arbeiten müssen unter Umständen Brandschottungen teilweise oder ganz entfernt werden. Zusätzliche Kabel verändern außerdem die Brandlast der Kabeltrasse. Folge daraus ist, dass während und nach den Arbeiten der baulich vorbeugende Brandschutz mitunter massiv beeinträchtigt sein kann.

Leider zeigt die Erfahrung, dass die mit solchen Arbeiten betrauten Personen (in der Planung, in der Ausführung und in der Abnahme) die Tragweite ihrer Arbeiten für den Brandschutz häufig nicht richtig einschätzen und entsprechend handeln:

- Ersatzmaßnahmen für entfernte Brandschottungen werden weder geplant noch realisiert.
- Beschädigte Brandschottungen werden nicht umgehend ordnungsgemäß wiederhergestellt.
- Brandschutzmaßnahmen werden den neuen Gegebenheiten nicht angepasst.

Folge dieser Fehlhandlungen ist ein erhöhtes Risiko der Brandentstehung und der Ausbreitung von Feuer und Rauch. Sofern notwendige Flure, Flucht- und Rettungswege betroffen sind, wird dadurch nicht nur die IT, sondern auch die Gesundheit und das Leben von Personen gefährdet, was massive Haftungsfolgen haben kann.

G 4 Gefährdungskatalog Technisches Versagen

G 4.1	Ausfall der Stromversorgung	
G 4.2	Ausfall interner Versorgungsnetze	
G 4.3	Ausfall vorhandener Sicherungseinrichtungen	
G 4.4	Leitungsbeeinträchtigung durch Umfeldfaktoren	
G 4.5	Übersprechen	
G 4.6	Spannungsschwankungen/Überspannung/ Unterspannung	
G 4.7	Defekte Datenträger	
G 4.8	Bekanntwerden von Softwareschwachstellen	
G 4.9	Ausfall der internen Stromversorgung	
G 4.10	Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen	
G 4.11	Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client	
G 4.12	Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client	
G 4.13	Verlust gespeicherter Daten	
G 4.14	Verblassen spezieller Faxpapiere	
G 4.15	Fehlerhafte Faxübertragung	
G 4.16	Übertragungsfehler bei Faxversand	**entfallen**
G 4.17	Technischer Defekt des Faxgerätes	**entfallen**
G 4.18	Entladene oder überalterte Notstromversorgung im Anrufbeantworter	
G 4.19	Informationsverlust bei erschöpftem Speichermedium	
G 4.20	Datenverlust bei erschöpftem Speichermedium	
G 4.21	Ausgleichsströme auf Schirmungen	
G 4.22	Software-Schwachstellen oder -Fehler	
G 4.23	Automatische CD-ROM-Erkennung	
G 4.24	Dateinamenkonvertierung bei Datensicherungen unter Windows 95	
G 4.25	Nicht getrennte Verbindungen	
G 4.26	Ausfall einer Datenbank	
G 4.27	Unterlaufen von Zugriffskontrollen über ODBC	
G 4.28	Verlust von Daten einer Datenbank	
G 4.29	Datenverlust einer Datenbank bei erschöpftem Speichermedium	

G 4.60 Unkontrollierte Ausbreitung der Funkwellen

G 4.61 Unzuverlässige oder fehlende WLAN-Sicherheitsmechanismen

G 4.62 Verwendung unzureichender Steckdosenleisten

G 4.63 Verstaubte Lüfter

G 4.1 Ausfall der Stromversorgung

Trotz hoher Versorgungssicherheit kommt es immer wieder zu Unterbrechungen der Stromversorgung seitens der Verteilungsnetzbetreiber (VNB) bzw. Energieversorgungsunternehmen (EVU). Die größte Zahl dieser Störungen ist mit Zeiten unter einer Sekunde so kurz, dass der Mensch sie nicht bemerkt. Aber schon Unterbrechungen von mehr als 10 ms sind geeignet, den IT-Betrieb zu stören. Bei einer Messung mit ca. 60 Messstellen wurden 1983 in Deutschland rund 100 solcher Netzeinbrüche registriert. Davon dauerten fünf Ausfälle bis zu einer Stunde und einer länger als eine Stunde. Diese Unterbrechungen beruhten einzig auf Störungen im Versorgungsnetz. Dazu kommen Unterbrechungen durch Abschaltungen bei nicht angekündigten Arbeiten oder durch Kabelbeschädigungen bei Tiefbauarbeiten.

Von der Stromversorgung sind nicht nur die offensichtlichen, direkten Stromverbraucher (PC, Beleuchtung usw.) abhängig. Alle Infrastruktureinrichtungen sind heute direkt oder indirekt vom Strom abhängig, z. B. Aufzüge, Rohrpostanlagen, Klimatechnik, Gefahrenmeldeanlagen, Sprinkleranlagen, Telefonnebenstellenanlagen. Selbst die Wasserversorgung in Hochhäusern ist wegen der zur Druckerzeugung in den oberen Etagen erforderlichen Pumpen stromabhängig.

Die Liberalisierung des Strommarktes führte in einigen Industrieländern zu einer Verschlechterung des Versorgungsniveaus. Auch in Deutschland könnte daher die Gefahr wachsen, dass Probleme durch Ausfälle der Stromversorgung oder durch Schaltvorgänge an nationalen Versorgungsübergängen entstehen.

Beispiele:

- In einem großen süddeutschen Industriebetrieb war die gesamte Stromversorgung für mehrere Stunden unterbrochen, da technische Probleme beim Stromversorgungsunternehmen aufgetreten waren. Infolgedessen fielen sowohl die Produktion als auch sämtliche Rechner der Entwicklungsabteilungen aus, die über keine Ersatz-Stromversorgung verfügten.
- Durch einen Fehler in der USV eines Rechenzentrums schaltete diese nach einem kurzen Stromausfall nicht auf Normalbetrieb zurück. Nach Entladung der Batterien nach etwa 40 Minuten fielen alle Rechner im betroffenen Server-Saal aus.
- Anfang 2001 gab es über 40 Tage einen Strom-Notstand in Kalifornien. Die Stromversorgungslage war dort so angespannt, dass die Kalifornische Netzüberwachungsbehörde rotierende Stromabschaltungen anordnete. Von diesen Stromabschaltungen, die bis zu 90 Minuten andauerten, waren nicht nur Haushalte, sondern auch die High-Tech-Industrie betroffen. Weil mit dem Stromausfall auch Alarmanlagen und Überwachungskameras ausgeschaltet wurden, hielten die Energieversorger ihre Abschaltpläne geheim.

G 4.2 Ausfall interner Versorgungsnetze

Es gibt in einem Gebäude eine Vielzahl von Netzen, die der Ver- und Entsorgung und somit als Basis für die IT dienen. Der Ausfall von Versorgungsnetzen wie:

- Strom,
- Telefon und
- Klima/Lüftung

kann zu einer sofortigen Störung des IT-Betriebs führen. Demgegenüber kann es bei Ausfall in den Bereichen:

- Heizung,
- Wasser,
- Löschwasserspeisungen,
- Abwasser,
- Rohrpost,
- Gas,
- Melde- und Steueranlagen (Einbruch, Brand, Hausleittechnik) und
- Sprechanlagen

unter Umständen zu zeitverzögerten Störungen kommen.

Die Netze sind in unterschiedlich starker Weise voneinander abhängig, so dass sich Betriebsstörungen in jedem einzelnen Netz auch auf andere auswirken können.

Beispiele:

- Der Ausfall der Stromversorgung wirkt nicht nur auf die IT direkt, sondern auch auf alle anderen Netze, die mit elektrisch betriebener Steuer- und Regeltechnik ausgestattet sind. Selbst in Abwasserleitungen sind u. U. elektrische Hebepumpen vorhanden.
- Mit modernen TK-Anlagen (ISDN-Technik) ist es möglich, LANs aufzubauen. Störungen im TK-Netz wirken sich automatisch auf das dort realisierte LAN aus.
- Der Ausfall der Wasserversorgung beeinträchtigt evtl. die Funktion von Klimaanlagen.
- Der Ausfall der Klimaanlage kann die Nutzung des Gebäudes durch zu starke Erwärmung bzw. Abkühlung oder wegen mangelhaftem Luftaustausch beeinträchtigen.

G 4.3 Ausfall vorhandener Sicherungseinrichtungen

Durch technische Defekte oder äußere Einflüsse (z. B. aufgrund von Alterung, Fehlbedienung, mangelhafter Wartung, Manipulation, Stromausfall) kann es zum Ausfall von Sicherungseinrichtungen kommen, so dass ihre Schutzwirkung stark herabgesetzt ist oder gänzlich ausfällt. Weiterhin kommt es vor, dass in Problembereichen, z. B. durch starke Umwelteinflüsse oder besonders hohe Nutzungsfrequenzen, Kontrollen und Wartungsintervalle nicht entsprechend angepasst werden. Auch hierdurch können Sicherungseinrichtungen ausfallen.

Beispiele:

- Türschlösser können durch Alterung oder Fehlbedienung beschädigt werden.
- Feuerlöscher, die nicht ordnungsgemäß gewartet werden, funktionieren u. U. unzureichend.
- Verschmutzte Brandmelder erkennen u. U. Brände nicht ordnungsgemäß oder geben Fehlalarm.
- Schlüssel oder Ausweiskarten können durch unsachgemäße Aufbewahrung oder durch Abnutzung beschädigt werden.
- Riegelkontakte in Türen können festgeklemmt sein.
- Standbilder in Überwachungsmonitoren können sich einbrennen.
- Brandschutztüren werden oft unzulässigerweise durch Holzkeile aufgehalten.
- Es kommt vor, dass Rauchmelder in Nichtraucherzonen manipuliert werden.

G 4.4 Leitungsbeeinträchtigung durch Umfeldfaktoren

Die Übertragungseigenschaften von Kabeln mit elektrischer Signalübertragung können durch elektrische und magnetische Felder negativ beeinflusst werden. Ob dies zu einer tatsächlichen Störung der Signalübertragung führt, hängt im wesentlichen von drei Faktoren ab:

- Frequenzbereich, Stärke und Dauer der Einwirkung,
- Abschirmung des Kabels und
- Schutzmaßnahmen bei der Datenübertragung (Redundanz, Fehlerkorrektur).

Viele Beeinträchtigungen lassen sich im Vorfeld erkennen:

- Entlang von Starkstromtrassen und im Bereich großer Motoren entstehen starke induktive Felder (Eisenbahn, Produktionsbetrieb, Aufzug).
- Im Bereich von Sendeeinrichtungen existieren starke elektromagnetische Felder (Rundfunk, Polizei- bzw. Feuerwehrfunk, Betriebsfunk, Personensuchanlagen, Funknetze).
- Mobiltelefone überschreiten durch ihre Sendeleistung (2 bis 4 Watt) die Störempfindlichkeit vieler IT-Systeme,
- Kabel beeinflussen sich gegenseitig durch wechselseitige Induktion.

Unabhängig von den rein elektrischen oder magnetischen Einflüssen können weitere Umfeldfaktoren auf ein Kabel wirken:

- hohe Temperaturen (in der Prozesssteuerung),
- aggressive Gase und
- hohe mechanische Belastungen (z. B. bei provisorischer Verlegung auf dem Fußboden oder Leitungen zu beweglichen Geräten).

G 4.5 Übersprechen

Übersprechen ist eine spezielle Form der Leitungsbeeinträchtigung. Dabei wird die Störung nicht allgemein im Umfeld, sondern durch Ströme und Spannungen von Signalen erzeugt, die auf eine benachbarte Leitung übertragen werden. Die Stärke dieses Effektes ist vom Kabelaufbau (Abschirmung, Kabelkapazität, Isolationsgüte) und von den elektrischen Parametern bei der Informationsübertragung (Strom, Spannung, Frequenz) abhängig.

Nicht jede Leitung, die durch Übersprechen beeinflusst wird, muss ihrerseits auch andere beeinflussen. Bekannt ist dies aus dem Telefonnetz. Dort sind Gespräche anderer Netzteilnehmer zu hören. Diese reagieren aber auf die Aufforderung "aus der Leitung zu gehen" oft deswegen nicht, weil das Übersprechen nur in eine Richtung geschieht. Das Prüfen eigener Leitungen auf eingekoppelte Fremdsignale gibt keine Auskunft darüber, ob die eigenen Signale auf andere Leitungen übersprechen und somit dort abhörbar sind.

Der wesentliche Unterschied zu anderen Leitungsstörungen ist der, dass neben der Störung der Signalübertragung auf benachbarten Leitungen durch Übersprechen auswertbare Informationen auf fremden Leitungen zur Verfügung stehen können.

G 4.6 Spannungsschwankungen/Überspannung/ Unterspannung

Durch Schwankungen der Versorgungsspannung kann es zu Funktionsstörungen und Beschädigungen der IT kommen. Die Schwankungen reichen von extrem kurzen und kleinen Ereignissen, die sich kaum oder gar nicht auf die IT auswirken, bis zu Totalausfällen oder zerstörerischen Überspannungen. Die Ursache dafür kann in allen Bereichen des Stromversorgungsnetzes entstehen, vom Netz des Energieversorgungsunternehmens bis zum Stromkreis, an dem die jeweiligen Geräte angeschlossen sind.

Außerhalb des Energieversorgungsnetzes ist auch auf allen anderen elektrisch leitenden Netzen (wie Telefonanbindung, Gebäudeleittechnik, Wasser- oder Gasleitungen etc.) mit Einkopplungen von Überspannungen zu rechnen.

G 4.7 Defekte Datenträger

Der Ausfall bzw. der Defekt einzelner Datenträger durch technische Mängel oder Beschädigung ist kein Einzelfall. Betroffen sind Massenspeicher wie Festplatten, Bänder oder Kassettensysteme. Festplatten können durch den "Headcrash" des Schreib-/Lesekopfes, Bänder oder Kassetten durch direkte mechanische Einwirkung zerstört werden. Auch CD-ROMs können durch Verkratzen der Oberfläche unbrauchbar werden. Vor allem aber Disketten sind von Ausfällen betroffen. Häufig stellt man fest, dass diese nicht mehr beschreibbar oder lesbar sind.

Beispiele:

- In einem mittelständischen Unternehmen kam es aufgrund von Bauarbeiten zur Staubentwicklung. Die Staubpartikel gelangten auf die Magnetplatte des im Unternehmen eingesetzten Rechners und führten zu einem "Headcrash", in dessen Folge Daten zerstört wurden. **Staubpartikel**
- Beim Laptop eines Außendienstmitarbeiters kam es zu unerklärlichen Ausfallerscheinungen, obwohl der Laptop immer sorgfältig verpackt transportiert wurde. Es stellte sich heraus, dass die Festplatte des Laptops durch einen Magneten beschädigt worden war, der zur Befestigung eines Klapptisches im Zug diente. **Magnete**
- Während der Datensicherung eines Multimedia-PCs wurden ZIP-Disketten auf dessen Lautsprecher zwischengestapelt. Durch die Magnete in den Lautsprechern wurden Teile der Datenträger gelöscht.
- Aufgrund von Bit-Fehlern auf Archivdatenträgern konnten verschlüsselte Dokumente nicht mehr entschlüsselt werden. Ebenso konnten elektronische Signaturen nicht mehr verifiziert werden. **Bit-Fehler**

G 4.8 Bekanntwerden von Softwareschwachstellen

Unter Softwareschwachstellen sollen unbeabsichtigte Programmfehler verstanden werden, die dem Anwender nicht oder noch nicht bekannt sind und ein Sicherheitsrisiko für das IT-System darstellen. Es werden ständig neue Sicherheitslücken in vorhandener, auch in weit verbreiteter oder ganz neuer Software gefunden.

Beispiele:

Bekannte Beispiele für Softwareschwachstellen waren:

- Ein *Sendmail Bug* unter Unix, durch den es für jeden Benutzer möglich war, unter der UID und GID von *sendmail* Programme auszuführen und Dateien zu verändern.
- Die Routine *gets* unter Unix. Diese wurde vom Programm *fingerd* zum Einlesen einer Zeile benutzt, ohne dass eine Überprüfung der Variablengrenzen vorgenommen wurde. So konnte durch einen Überlauf der Stack so verändert werden, dass eine neue Shell gestartet werden konnte.
- cgi-scripte, die mit WWW-Servern mitgeliefert wurden. Entfernte Anwender konnten sensible Informationen über den WWW-Server erlangen.
- Ein Bug in der DNS-Software ermöglichte das Fälschen zwischengespeicherter DNS-Daten.
- Fehlerhafte Implementationen des TCP/IP-Stacks. Diese ermöglichten das Lahmlegen ganzer Netze mittels übergroßer oder anders manipulierter Pakete.

G 4.9 Ausfall der internen Stromversorgung

Der Einsatz eines mobilen IT-Systems, z. B. eines Laptop, setzt voraus, dass das System über eine vom Versorgungsnetz unabhängige Stromversorgung verfügt. Diese meist mit wiederaufladbaren Batterien konzipierte Stromversorgung reicht üblicherweise für eine mehrstündige Betriebsdauer. Nach dieser Zeit ist die ausreichende Stromversorgung nicht mehr gesichert, so dass das IT-System außer Betrieb genommen bzw. an das Stromnetz angeschlossen werden muss. Die überwiegende Zahl der mobilen Systeme überprüft kontinuierlich die Versorgungsspannung und zeigt einen kritischen Spannungsabfall an. Wird diese Anzeige ignoriert, kann es passieren, dass das System plötzlich seinen Dienst versagt und die letzten Arbeitsergebnisse im Hauptspeicher verloren gehen.

G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen

Im Gegensatz zu Stand-alone-Systemen, bei denen im wesentlichen der Login-Prozess für die Zugangskontrolle verantwortlich ist und die somit nur durch schlechte oder fehlende Passwörter korrumpiert werden können, gibt es auf Netzrechnern sehr viele komplexe Prozesse, die die verschiedensten Arten von Zugängen erlauben. So ermöglicht z. B. unter Unix der *sendmail*-Daemon das Einbringen von Texten (E-Mails) in den Netzrechner, der *FTP*-Daemon einen, wenn auch etwas eingeschränkten, Login, der u. U. (*anonymous FTP*) nicht einmal durch ein Passwort geschützt ist, der *telnet*-Daemon einen kompletten Login.

Server-Systeme wie Windows NT oder Novell Netware vermeiden aus Sicherheitsgründen die Übertragung von Klartext-Passwörtern. Dieser Schutzmechanismus wird jedoch durch den Einsatz von Diensten wie FTP oder Telnet unterlaufen, da hier wieder Klartext-Passwörter Verwendung finden.

Abgesehen davon, dass alle diese Prozesse durch eine falsche oder fehlerhafte Konfiguration eine Sicherheitslücke darstellen können, ist auf Grund ihres Umfanges natürlich auch die Wahrscheinlichkeit, dass in einem dieser Prozesse ein sicherheitsrelevanten Programmierfehler ist, wesentlich größer.

Es gibt zahlreiche verschiedene Möglichkeiten, ein z/OS-System an interne und öffentliche Netze anzubinden. Es sind Zugriffe über SNA und TCP/IP, z. B. FTP, TELNET oder Browser, möglich. Viele der von Unix-Installationen bekannten Netzfunktionen können unter den *Unix System Services* von z/OS verwendet werden. Diese Vielfalt der Anschlussmöglichkeiten macht eine sichere Netzkonfiguration der z/OS-Systeme sehr komplex.

Beispiel:

Nichtautorisierter Datenzugriff über FTP

- Einem externen Angreifer gelang es, die Benutzerkennung und das Passwort für eine hochautorisierte Anwendung unter z/OS zu ermitteln. Obwohl die Kennung über kein *TSO-Segment* verfügte, konnte der Angreifer einen Batch-Job über FTP direkt in das *JES2* einbringen und ausführen lassen. Da der Job-Output ebenfalls über FTP ausgelesen werden konnte, war dadurch der Zugriff auf vertrauliche Daten möglich.

G 4.11 Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client

Kennt man den NIS-Domain-Namen, lässt sich jeder Rechner als Client anmelden, und es lassen sich alle NIS-Maps, insbesondere also auch die *passwd*-Map, abrufen.

Ist es möglich, Administrationsrechte auf einem Rechner zu bekommen, lässt sich auf diesem ein NIS-Server-Prozess (*ypserv*) an einem privilegierten Port starten. Startet man nun den Client-Prozess *ypbind* auf dem zu infiltrierenden Rechner neu und sorgt dafür, dass der eigene Server-Prozess vor dem korrekten NIS-Server antwortet, lässt sich jede beliebige Information an den Client überspielen.

G 4.12 Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client

Für das X-Window-System gilt im besonderen Maße, dass es ohne geeignete Sicherheitsmechanismen, wie z. B. "Magic Cookies" oder Verwendung von Secure Shell, nur in einer vertrauenswürdigen Umgebung eingesetzt werden sollte. Ohne Sicherheitsfunktionen besteht für alle beteiligten Benutzer die Möglichkeit, sowohl den X-Client als auch den X-Server zu korrumpieren. Der X-Server-Prozess, der auf einem Rechner für die Ein- und Ausgabe zuständig ist, kann nicht erkennen, wem der X-Client-Prozess gehört, der mit ihm kommuniziert. Alle X-Clients können also auf alle Daten, die auf einem X-Server eingegeben werden, zugreifen, und der X-Server hat keine Möglichkeit festzustellen, von welchem X-Client er Daten erhält. So simuliert z. B. das Programm *meltdown* das optische "Schmelzen" des Bildschirms eines beliebigen X-Servers. Genauso ist es möglich, Daten von einem *xterm*-Client zu lesen oder ihm eigene Daten zu schicken, also z. B. Bildschirmabzüge von einem anderen, mit X-Windows arbeitenden Rechner zu machen.

Beispiele:

- Mit dem Tool *xspy* lassen sich automatisiert Tastatureingaben auf einem Xterm remote protokollieren.
- Fenster, die von einem Angreifer auf einem X-Server dargestellt werden, sind optisch nicht von denen des eigentlich gewünschten X-Clients zu unterscheiden. Ein Angreifer kann auf diese Weise falsche Informationen einschleusen oder mit Hilfe von gefälschten Fenstern die Eingabe von sensitiven Informationen provozieren.

G 4.13 Verlust gespeicherter Daten

Der Verlust gespeicherter Daten kann erhebliche Auswirkungen auf den IT-Einsatz haben. Sind die Anwendungsdaten oder die Kundenstammdaten verloren oder verfälscht, so können privatwirtschaftliche Betriebe in ihrer Existenz bedroht sein. Der Verlust oder die Verfälschung wichtiger Dateien kann in Behörden Verwaltungs- und Fachaufgaben verzögern oder sogar ausschließen.

Dabei können die Gründe für den Verlust gespeicherter Daten vielfältiger Art sein:

- Entmagnetisierung von magnetischen Datenträgern durch Alterung oder durch ungeeignete Umfeldbedingungen (Temperatur, Luftfeuchte),
- Störung magnetischer Datenträger durch äußere Magnetfelder,
- Zerstörung von Datenträgern durch höhere Gewalt wie Feuer oder Wasser,
- versehentliches Löschen oder Überschreiben von Dateien,
- vorsätzliches oder versehentliches Setzen von Löschmarkierungen in Archivsystemen (siehe auch G 5.106 *Unberechtigtes Überschreiben oder Löschen von Archivmedien*),
- technisches Versagen von Peripheriespeichern (Headcrash),
- fehlerhafte Datenträger,
- unkontrollierte Veränderungen gespeicherter Daten (Integritätsverlust) und
- vorsätzliche Datenzerstörung durch Computer-Viren usw.

G 4.14 Verblassen spezieller Faxpapiere

Bei Faxgeräten, die im Thermodruckverfahren arbeiten, muss Spezialpapier eingesetzt werden, auf dem oft bereits nach relativ kurzer Zeit die Schrift bis zur Unlesbarkeit verblasst oder durch Schwärzung des Papieres unlesbar wird. Außerdem können sich diese Papiere bei Kontakt mit Textmarkern oder Klebstoffen so verfärben, dass der Text nicht mehr lesbar ist.

G 4.15 Fehlerhafte Faxübertragung

Störungen auf dem Übertragungsweg

Beim Faxversand können Störungen auf dem Übertragungsweg oder an den beteiligten Geräten auftreten. Dadurch können Faxsendungen unvollständig, unlesbar oder gar nicht beim Empfänger ankommen. Entscheidungen, die von diesen Informationen abhängig sind, können fehlerhaft sein und somit Schäden verursachen.

Zustellung an einen falschen Empfänger

Weiterhin besteht die Gefahr, dass ein Fax an einen falschen Empfänger übermittelt wird. Ursache kann eine Fehlschaltung im öffentlichen Telekommunikationsnetz sein. Ebenso ist denkbar, dass bei herkömmlichen Faxgeräten Rufnummern falsch gewählt oder Zielwahltasten falsch programmiert werden. Bei der Verwendung von Faxservern kann eine Empfänger-Rufnummer falsch eingegeben oder im Adressbuch falsch abgespeichert werden. Dadurch können unter Umständen vertrauliche Informationen unbefugten Personen bekannt werden. Der mögliche Schaden ist von der Vertraulichkeit der Informationen abhängig. Darüber hinaus wird der Absender im Glauben bleiben, dass das Fax ordnungsgemäß an den gewünschten Adressaten übermittelt wurde. Hierdurch auftretende Zeitverzögerungen können zu Schäden führen.

Beispiel:

Eine bekannte deutsche Firma verlor einen Großauftrag, weil das Angebot versehentlich an einen falschen Empfänger versandt wurde.

G 4.16 Übertragungsfehler bei Faxversand

Die Gefährdung G 4.16 *Übertragungsfehler bei Faxversand* und wurde in die Gefährdung G 4.15 *Fehlerhafte Faxübertragung* integriert.

G 4.17 Technischer Defekt des Faxgerätes

Die Gefährdung G 4.17 *Technischer Defekt des Faxgerätes* wurde in die Gefährdung G 4.15 *Fehlerhafte Faxübertragung* integriert.

G 4.18 Entladene oder überalterte Notstromversorgung im Anrufbeantworter

Bei Anrufbeantwortern mit einem digitalen Speicher wird der Ausfall der Netzenergieversorgung durch Batterie oder Akkumulator überbrückt, um so den Speicherinhalt zu erhalten. Ist die Kapazität von Batterie oder Akkumulator vor Ende der Netzunterbrechung erschöpft, werden in der Regel der Ansagetext und zusätzlich bei digitaler Anrufaufzeichnung auch die bereits aufgesprochenen Nachrichten gelöscht.

G 4.19 Informationsverlust bei erschöpftem Speichermedium

Ist das Speichermedium (digitaler Speicher oder Audiokassette) des Anrufbeantworters mit aufgezeichneten Anrufen erschöpft, so ist eine weitere Aufzeichnung entweder nicht mehr möglich oder vorher aufgesprochene Nachrichten werden durch neue Anrufe überschrieben. In beiden Fällen entsteht ein Informationsverlust.

G 4.20 Datenverlust bei erschöpftem Speichermedium

Jedes Speichermedium kann nur begrenzt viele Daten aufnehmen. Wenn diese Grenze erreicht ist, kann das zu Datenverlusten führen, aber auch dazu, dass Dienste nicht mehr verfügbar sind, wie z. B. dass

- Benutzer keine Daten mehr abspeichern können,
- eingehende E-Mail abgewiesen wird und eventuell außerdem keine E-Mail mehr versandt werden kann,
- eingehende und gegebenenfalls ausgehende Faxsendungen abgewiesen werden,
- keine Protokollierung mehr möglich ist bzw. noch nicht ausgewertete Protokolldaten überschrieben werden oder
- Dokumente nicht mehr elektronisch archiviert werden können.

Die Kapazität des Speichermediums kann aus verschiedenen Gründen plötzlich erschöpft sein, z. B. durch Fehler in Anwendungsprogrammen, erhöhten Speicherbedarf der Benutzer oder auch durch einen gezielten Angriff, bei dem vorsätzlich der vorhandene Speicherplatz reduziert wird, um eine Protokollierung zu verhindern.

große Datenmengen bei der Archivierung

Bei der elektronischen Archivierung sind meist große Datenmengen zu sichern. Die Datenmengen entstehen einerseits durch die große Anzahl von Dokumenten, die bei bestimmten Vorgängen zu archivieren sind. Hinzu kommt andererseits, dass jede neu erstellte Version eines Dokuments unter Vergabe einer neuen Versionsnummer neu gespeichert wird.

G 4.21 Ausgleichsströme auf Schirmungen

Werden IT-Geräte, die über ein TN-C-Netz elektrisch versorgt werden, durch Datenleitungen mit beidseitig aufgelegtem Schirm miteinander verbunden, kann es zu Ausgleichsströmen auf dem Schirm kommen (eine erläuternde Zeichnung findet man in M 1.39 *Verhinderung von Ausgleichsströmen auf Schirmungen*).

Ursache dafür ist die Eigenart des TN-C-Netzes, dass bei ihm Schutz- (PE-) und Neutral- (N-) Leiter bis zu den einzelnen Verteilungen gemeinsam als PEN-Leiter geführt werden. Erst in der Verteilung erfolgt die Aufteilung in N-Leiter und PE-Leiter. Diese Installation ist gemäß VDE 0100 zulässig!

Werden die mit PE verbundenen Schnittstellen-Schirmungen von Geräten, die an verschiedenen Verteilungen angeschlossen sind, durch geschirmte Datenleitungen miteinander verbunden, kommt es zu einer Parallelschaltung des PEN-Leiters zwischen den Verteilungen und der Schirmung zwischen den Schnittstellen. Der dadurch über die Schirmung fließende Ausgleichsstrom kann zu Schäden an den Schnittstellen und zu Personengefährdungen bei Arbeiten an den Datenleitungen führen.

Zwischen Geräten, die in einem TN-C-Netz an der gleichen Verteilung oder zwischen Geräten, die in einem TN-S-Netz - auch an verschiedenen Verteilungen - angeschlossen sind, fließen keine Ausgleichsströme über die Schirmung von Datenleitungen.

Bei TN-CS-Netzen sind einige Teilbereiche als TN-C-Netz, andere als TN-S-Netz ausgeführt. Solange Datenleitungen mit beidseitig aufgelegtem Schirm nur jeweils innerhalb gleichartiger Teilbereiche geführt werden, gelten dort die gleichen Verhältnisse wie in den jeweiligen Netzen. Werden jedoch IT-Geräte aus unterschiedlichen Bereichen über Datenleitungen mit beidseitig aufgelegter Schirmung verbunden, können auch im TN-S-Bereich Ausgleichsströme fließen!

G 4.22 Software-Schwachstellen oder -Fehler

Wie für jede Software gilt auch für Standardsoftware: je komplexer sie ist, desto häufiger treten Programmierfehler auf. Es ist zu beobachten, dass hohe Erwartungen der Anwender und zeitlich zu knapp bemessene Erscheinungstermine bei Standardsoftwareprodukten auch dazu führen, dass die Hersteller ihre Produkte teilweise unausgereift oder nicht fehlerfrei anbieten. Werden diese Softwarefehler nicht erkannt, können die bei der Anwendung entstehenden Fehler zu weitreichenden Folgen führen.

Beispiele:

- Ein Software-Fehler in der Sicherheits-Software RACF des z/OS-Betriebssystems kann bedeuten, dass nicht nur RACF den Dienst einstellt, sondern dadurch das ganze System nicht mehr funktionsfähig ist und neu gestartet werden muss.
- Die Stärke der in Standardsoftware implementierten Sicherheitsfunktionalitäten (wie Passwörter oder Verschlüsselungsalgorithmen) wird vom Anwender häufig zu hoch eingeschätzt. Häufig können diese Sicherheitsfunktionalitäten einem sachkundigen Angriff nicht dauerhaft standhalten. Dies gilt z. B. für die Verschlüsselungsfunktionen, die in vielen Textverarbeitungsprogrammen integriert sind. Für fast alle davon gibt es im Internet zahlreiche Tools, um diese Verschlüsselung zu überwinden.
- Nachweislich führte das Auftreten eines bestimmten Wortes in der Rechtschreibprüfung eines Textverarbeitungsprogrammes immer zu dessen Absturz.
- Vielfach enthält Standardsoftware nicht dokumentierte Funktionen, wie sog. "Ostereier" oder "Gagscreens", mit denen sich die Entwickler des Produktes verewigt haben. Zum einen werden hierdurch zusätzliche IT-Ressourcen verbraucht, zum anderen wird dadurch auch deutlich, dass im Softwaretest die gesamte Funktionalität des Produktes nicht bis ins letzte geklärt werden kann.
- Die meisten Warnmeldungen der Computer Emergency Response Teams in den letzten Jahren bezogen sich auf sicherheitsrelevante Programmierfehler. Dies sind Fehler, die bei der Erstellung von Software entstehen und dazu führen, dass diese Software von Angreifern missbraucht werden kann. Der größte Teil dieser Fehler wurde durch Speicherüberläufe (Buffer Overflow) hervorgerufen. Hierbei handelt es um Fehler, bei denen eine Routine zum Einlesen von Zeichen nicht prüft, ob die Länge der eingegebenen Zeichenkette mit der Länge des dafür vorgesehenen Speicherbereiches übereinstimmt. Dadurch ist es Angreifern möglich, eine überlange Zeichenfolge zu übertragen, so dass hinter dem für die Eingabe reservierten Speicherbereich zusätzliche Befehle gespeichert werden können, die zur Ausführung gebracht werden. Diese Befehle können z. B. beliebige Programme sein.
- Eine weitere große Anzahl von Warnmeldungen wurde durch **Verfügbarkeitsangriffe** (Denial of Service, DoS) verursacht, bei denen durch Fehler in einzelnen Routinen, die für die Netzdatenverarbeitung eingesetzt werden, der gesamte Rechner zum Absturz gebracht werden kann (siehe

z. B. CERT Advisory 97.28 zu IP Denial-of-Service Attacks: Teardrop and Land-Attack).

G 4.23 Automatische CD-ROM-Erkennung

Bei Windows-Betriebssystemen wie unter Windows 95 oder Windows NT können CD-ROMs, aber auch andere auswechselbare Datenträger automatisch erkannt und bearbeitet werden. Bei eingeschalteter CD-ROM-Erkennung werden CD-ROMs automatisch erkannt und die Datei *AUTORUN.INF* automatisch ausgeführt, wenn diese sich im Wurzelverzeichnis der CD-ROM befindet. Diese Datei kann beliebige auf der CD-ROM gespeicherte Programme (z. B. mit Schadfunktion) automatisch ausführen.

Ob diese Option eingeschaltet ist, erkennt man zum Beispiel unter Windows 95 daran, dass der Explorer vor dem CD-ROM-Laufwerksbuchstaben den Namen der CD-ROM automatisch einblendet. Ein Nebeneffekt hierbei ist, dass Energiespar-Funktionen in der Regel nicht mehr aktiviert werden.

G 4.24 Dateinamenkonvertierung bei Datensicherungen unter Windows 95

Werden zur Datensicherung unter Windows 95 Programme benutzt, die lange Dateinamen nicht unterstützen, so sind alle langen Dateinamen vor der Datensicherung mit dem zum Lieferumfang von Windows 95 gehörenden Programm LFNBK.EXE und der Option /B in die 8.3er-Konvention zu konvertieren. Anschließend ist das Datensicherungsprogramm aufzurufen. Schließlich sind die ursprünglichen Dateinamen mit LFNBK.EXE /R wieder herzustellen.

Dieses Verfahren ist jedoch mit Vorsicht anzuwenden, da zum einen bei der Namenskonvertierung Informationen verloren gehen können, zum anderen sich Dateien nicht mehr herstellen lassen, sobald sich die Verzeichnisstruktur nach der Datensicherung auf diesem PC geändert hat. Dies kann dann einen Datenverlust zur Folge haben.

G 4.25 Nicht getrennte Verbindungen

Bei der Verwendung von ISDN-Kommunikationskarten kann es vorkommen, dass eine über die Kommunikationssoftware ausgelöste Verbindung nicht tatsächlich durch die ISDN-Karte getrennt wird. Besteht der Verdacht eines solchen Defekts, lässt sich dieser durch einen Anrufversuch bei der betreffenden ISDN-Rufnummer leicht verifizieren.

Beispiel:

Ein Netzadministrator hat vor seinem 14-tägigen Urlaub eine ISDN-Datenverbindung zu seinem Internet-Provider aufgebaut. Bei Beendigung der Sitzung wurde die ISDN-Verbindung nicht korrekt ausgelöst. Nach Beendigung des Urlaubs wunderte sich der Administrator über die recht hohe Rechnung für Verbindungsentgelte von Seiten des ISDN-Carriers.

G 4.26 Ausfall einer Datenbank

Der Ausfall einer Datenbank zeigt sich dem Benutzer zumeist durch fehlende Reaktion des Datenbankmanagementsystems (DBMS), welches die Daten der Datenbank darstellen soll. Der Ausfall kann durch geplante Ereignisse, wie z. B. Wartungsarbeiten, ausgelöst woden sein oder auf unvorhersehbare Ereignisse zurückgeführt werden. Zum letzteren Bereich gehören z. B. Hardware-, Software- oder Netzprobleme. Produktfehler, höhere Gewalt, Fahrlässigkeit oder Sabotage können beispielsweise Ursachen für solche Datenbankausfälle sein.

Steht eine Datenbank für einen Benutzer oder eine Anwendung nicht mehr zur Verfügung, kann dies je nach Einsatzzweck und Bedeutung der Datenbank weitreichende Folgen haben. Sämtliche Anwendungen, die auf die Daten der Datenbank angewiesen sind, können nur noch eingeschränkt oder gar nicht mehr benutzt werden. Die Benutzer solcher Anwendungen können ihre Aufgaben nur noch teilweise oder gar nicht mehr wahrnehmen, falls sie diese nicht mit anderen Mitteln erfüllen können. Je nach Art der Aufgaben, die nur mittels IT-Unterstützung unter Benutzung der Datenbank ausgeführt werden können, sind unter anderem folgende Konsequenzen möglich:

- wirtschaftlicher Schaden,
- gesundheitlicher Schaden,
- Vertrauensverlust bei Kunden oder Partnern durch die Nichterbringung vereinbarter Leistungen oder
- eingeschränkte oder vollständige Handlungsunfähigkeit.

Beispiele:

- Elektronische Archive basieren auf einer Datenbank, in der alle archivierten Dokumente indiziert sind. Bei einem Ausfall dieser Index-Datenbank können archivierte Dokumente nicht wiedergefunden bzw. nicht gesucht werden. Dadurch ist, wenn überhaupt, nur ein stark eingeschränkter Betrieb des Archivs möglich.
- Die Inhalte sowie alle Zusatzinformationen einer regelmäßig erscheinenden Publikation wurden vollständig in eine Datenbank verlagert. Da für alle Arbeiten im zuständigen Referat zumindest ein lesender Zugriff auf diese Datenbank erforderlich ist, sind ohne das korrekte Funktionieren dieser Datenbank keine inhaltlichen Arbeiten mehr möglich. Nachdem die Datenbank aufgrund von planmäßigen Wartungsarbeiten heruntergefahren wurde, kam es im weiteren Verlauf zu unvorhergesehenen Verzögerungen, wodurch die Datenbank länger als geplant nicht zur Verfügung stand. Das Referat konnte, da keine Ersatzdatenbank existierte, insgesamt eine Woche inhaltlich nur sehr eingeschränkt arbeiten.
- Eine öffentlich zur Verfügung stehende Datenbank wird durch eine immense Menge zeitgleich eintreffender Anfragen so überlastet, dass ein geregelter Zugriff auf die Datenbank fast unmöglich wird.

G 4.27 Unterlaufen von Zugriffskontrollen über ODBC

Datenbankschnittstellen stellen dem Benutzer eine Verbindung (Application Programming Interface, API) von Anwendungsprogrammen zu anderen Datenbanken in Form von Treibern zur Verfügung.

Beispiele für Datenbankschnittstellen sind:

- ODBC: Open Database Connectivity
- IDAPI: Integrated Database Application Programming Interface
- JDBC: Java Database Connectivity

Dabei werden die Anweisungen des Anwendungsprogramms durch die Datenbankschnittstelle in für die jeweilige Datenbank spezifische Befehle übersetzt, der Datenbank übermittelt und die Ergebnisse an das Anwendungsprogramm zurück übertragen.

Bestandteil der Kommunikation über die Schnittstelle zwischen Anwendungsprogramm und Datenbank ist die Identifizierung der Anwendung als registrierter Datenbanknutzer.

Existierende Zugangs- oder Zugriffskontrollen einer Datenbank können unterlaufen werden, wenn auf die Datenbank über Datenbankschnittstellen zugegriffen wird und bei der Installation, Konfiguration oder Nutzung der zugehörigen Treiber Fehler gemacht wurden. In diesem Fall kann ein Schutz vertraulicher Daten nicht gewährleistet werden und die Manipulation von Daten ist möglich.

Beispiel:

Eine ODBC-Datenquelle kann in Microsoft Excel oder Word genutzt werden, um Informationen aus einer Datenbank in ein Dokument einzubinden. Um auch später wieder einfach auf diese Informationen zugreifen zu können, ist es möglich, zu der Abfrage auch den Benutzernamen und das Passwort zu speichern. Benutzername und Passwort werden dabei im Klartext in der Datei gespeichert. Wird das betroffene Excel- oder Word-Dokument nun an einen Dritten weitergegeben, kann dieser mit einem Editor den Benutzernamen und das Passwort lesen und so möglicherweise Zugriff auf die Datenbank erhalten.

G 4.28 Verlust von Daten einer Datenbank

Ein Verlust von Daten einer Datenbank kann auf vielfältige Art und Weise verursacht werden. Dies kann sich von ungewollten Datenmanipulationen (z. B. durch das versehentliche Löschen von Daten) über einen Verlust durch einen Zusammenbruch der Datenbank, z. B. als Ergebnis der Erschöpfung eines Speichermediums, bis hin zu gezielten Angriffen erstrecken.

Jedes Speichermedium kann nur begrenzt viele Daten aufnehmen. Dies gilt auch für eine Datenbank, die für die dauerhafte Speicherung ihrer Daten auf ein physikalisches Speichermedium zurückgreifen muss. Ist dieses erschöpft, kann es zu einem Zusammenbruch der Datenbank und einem Verlust von Daten kommen.

Die Kapazität des Speichermediums kann aus verschiedenen Gründen erschöpft sein. Beispiele hierfür sind Fehler in Anwendungsprogrammen, erhöhter Speicherbedarf der Benutzer oder auch gezielte Angriffe, bei denen vorsätzlich der vorhandene Speicherplatz reduziert wird, um z. B. eine Protokollierung zu verhindern.

Unabhängig von der Ursache ist als Folge die Verfügbarkeit und die Vollständigkeit der Daten nicht mehr gewährleistet, und es kann zu folgenden Konsequenzen kommen:

- Bestimmte Anwendungen, die auf die Daten der Datenbank angewiesen sind, können gegebenenfalls nicht oder nicht mehr in vollem Umfang ausgeführt werden.
- Der Informationsgehalt der Daten in ihrer Gesamtheit geht verloren.
- Es entsteht ein hoher Aufwand, um zerstörte Daten wiederzubeschaffen.

Je nach Ursache des Datenverlustes kann es schwer bis unmöglich sein festzustellen, welche Daten nicht mehr vorhanden sind. Dies kann weitere wirtschaftliche Schäden oder Sicherheitsrisiken nach sich ziehen.

Beispiel:

Bei Änderungen des Datenmodells müssen im Rahmen eines Migrationskonzeptes unter anderem zunächst die alten Tabellen und Strukturen gesichert werden und können erst danach gelöscht werden. Anschließend werden die neuen Tabellen angelegt. Danach müssen die alten Datenbestände konvertiert und in die geänderten Tabellen eingespielt werden. Durch Fehler bei diesen Abläufen kann es schnell passieren, dass Daten verloren gehen oder sich nicht mehr einspielen lassen.

G 4.29 Datenverlust einer Datenbank bei erschöpftem Speichermedium

Diese Gefährdung ist mit der Version 2006 entfallen. Alle relevanten Inhalte werden G 4.28 *Verlust von Daten einer Datenbank* integriert.

G 4.30 Verlust der Datenbankintegrität/-konsistenz

Ein Verlust der Datenbankintegrität/-konsistenz bedeutet, dass die Daten in der Datenbank zwar noch vorhanden sind, sich aber in einem fehlerhaften Zustand befinden. Dadurch kann auf die Daten nicht mehr korrekt zugegriffen werden oder die Daten können im Weiteren nicht mehr korrekt verarbeitet werden. Eine Datenbankinkonsistenz kann auf vielfältige Art und Weise verursacht werden, von ungewollten Datenmanipulationen (z. B. durch das unbeabsichtigte Ändern von Daten) über eine fehlerhafte Synchronisationskontrolle der Transaktionen bis hin zu gezielten Angriffen.

Dadurch kann es unter anderem zu folgenden Konsequenzen kommen:

- Bestimmte Aufgaben, die auf die korrekten Daten der Datenbank angewiesen sind, können nicht oder nicht mehr in vollem Umfang durchgeführt werden.
- Der Informationsgehalt der Daten in ihrer Gesamtheit wird verfälscht.
- Es entsteht ein hoher Aufwand, um Datenintegrität und Datenkonsistenz der Datenbank wiederherzustellen.

Je nach Ursache der Verletzung der Datenbankintegrität/-konsistenz kann es schwer bis unmöglich sein festzustellen, welche Daten verändert wurden (siehe auch G 2.22 *Fehlende Auswertung von Protokolldaten*). Dies kann weitere wirtschaftliche Schäden oder Sicherheitsrisiken nach sich ziehen.

Beispiele:

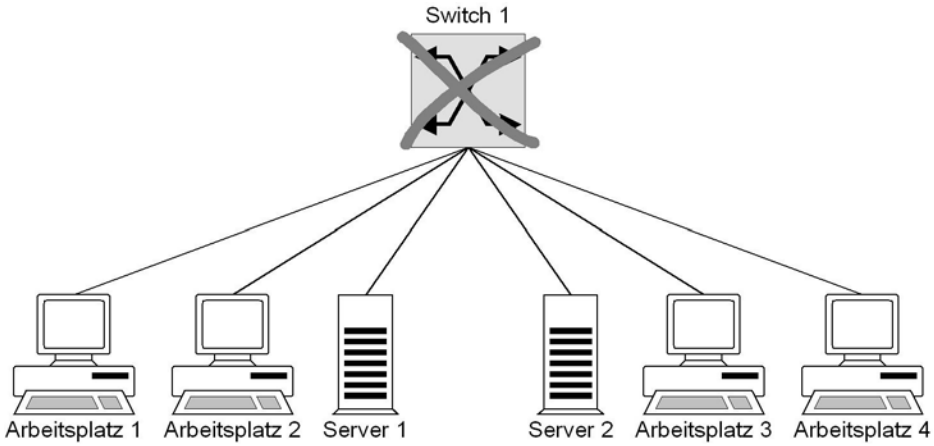
- Aus Platzmangel und Zeitdruck wurde auf einem Unix-Server eine Datei einer Datenbank im */tmp*-Dateisystem angelegt. Dieses Dateisystem wurde über Nacht automatisch gelöscht, so dass daraufhin die gesamte Datenbank nicht mehr nutzbar war.
- Elektronische Archive basieren auf einer Datenbank, in der alle archivierten Dokumente indiziert sind. Bei Verlust der Indizierung oder der Referenz auf einzelne Dokumente können diese unter Umständen nicht mehr mit vertretbarem Aufwand gefunden werden. Aus einem solchen Verlust der Datenbankintegrität kann zu einem späteren Zeitpunkt ein erheblicher wirtschaftlicher oder juristischer Schaden entstehen.

G 4.31 Ausfall oder Störung von Netzkomponenten

Durch einen Ausfall oder eine Störung von aktiven Netzkomponenten kommt es zu einem Verlust der Verfügbarkeit des Netzes oder von Teilbereichen davon. Hier können 3 Varianten unterschieden werden:

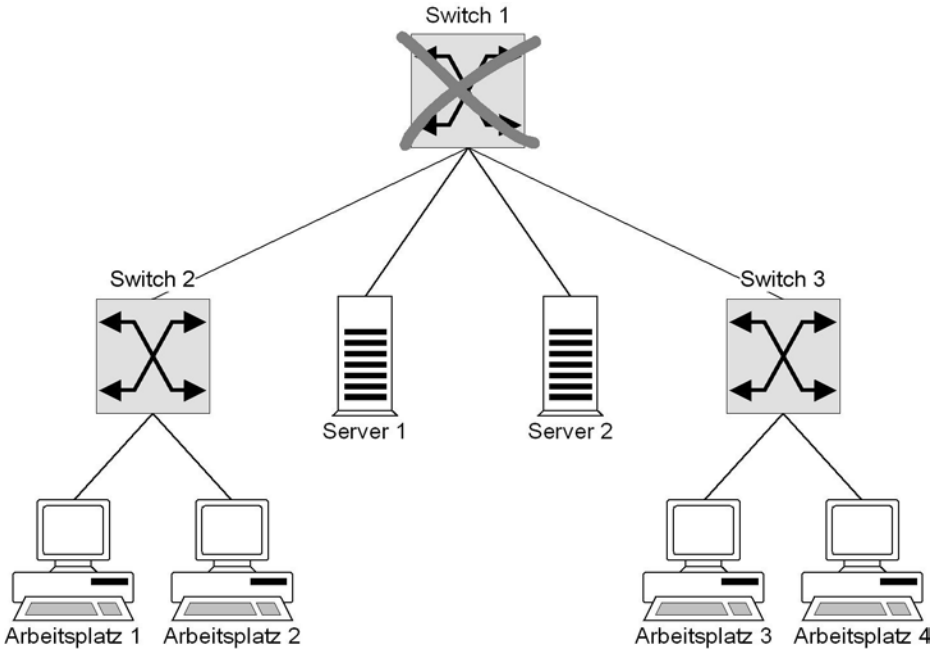
- Bei Ausfall oder Störung der kompletten Netzkomponente ist das gesamte Netz für alle angeschlossenen Endgeräte nicht mehr verfügbar. Beim Ausfall oder Störung nur eines Ports ist nur für das dort angeschlossene Endgerät das Netz nicht mehr verfügbar.

  Beispiel: Fällt, wie in der folgenden Abbildung dargestellt, der zentrale Switch 1 völlig aus, ist keinerlei Kommunikation zwischen den angeschlossenen Endgeräten mehr möglich.



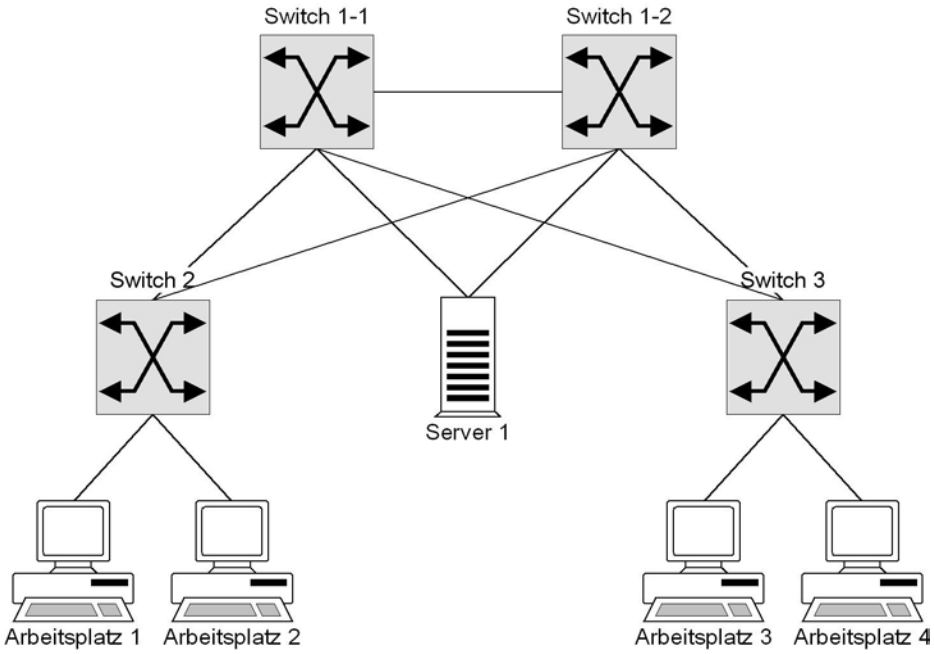
- Es handelt sich um aktive Netzkomponenten, die zwar nicht direkt an den Netzsegmenten von miteinander kommunizierenden Arbeitsplatz- und Serversystemen angeschlossen sind, jedoch im Signalpfad zwischen Arbeitsplatz- und Serversystemen liegen. Falls keine redundanten Signalpfade zwischen den betreffenden Arbeitsplatz- und Serversystemen zur Verfügung stehen, kann bei Ausfall oder Störung einer oder mehrerer dieser Komponenten keine oder nur eingeschränkte Kommunikation zwischen Arbeitsplatz- und Serversystemen mehr stattfinden.

Beispiel: Fällt, wie in der folgenden Abbildung dargestellt, Switch 1 völlig aus, ist von den Arbeitsplätzen 3 und 4 weder eine Kommunikation mit den beiden Servern noch mit den anderen Arbeitplätzen möglich.



- Es handelt sich um aktive Netzkomponenten, die nicht notwendigerweise im Signalpfad zwischen Arbeitsplatz- und Serversystemen liegen, da ein zweiter, redundanter Signalpfad existiert. Dies können z. B. aktive Netzkomponenten sein, die aus Redundanzgründen oder zum Load-Balancing installiert sind. Bei Ausfall oder Störung einer oder mehrerer dieser Komponenten ist eine Kommunikation zwischen Arbeitsplatz- und Serversystemen weiter möglich, es tritt jedoch dennoch ein Bandbreitenverlust im Netz ein, da redundante Signalpfade ggf. nicht mehr vorhanden sind oder eine Lastverteilung im Netz nicht mehr im vollen Umfang möglich ist.

Beispiel: Fällt, wie in der folgenden Abbildung dargestellt, einer der redundanten Switches 1-1 oder 1-2 aus, kann dies einen Bandbreitenverlust in der Kommunikation zwischen den Arbeitsplätzen und dem Server zur Folge haben.

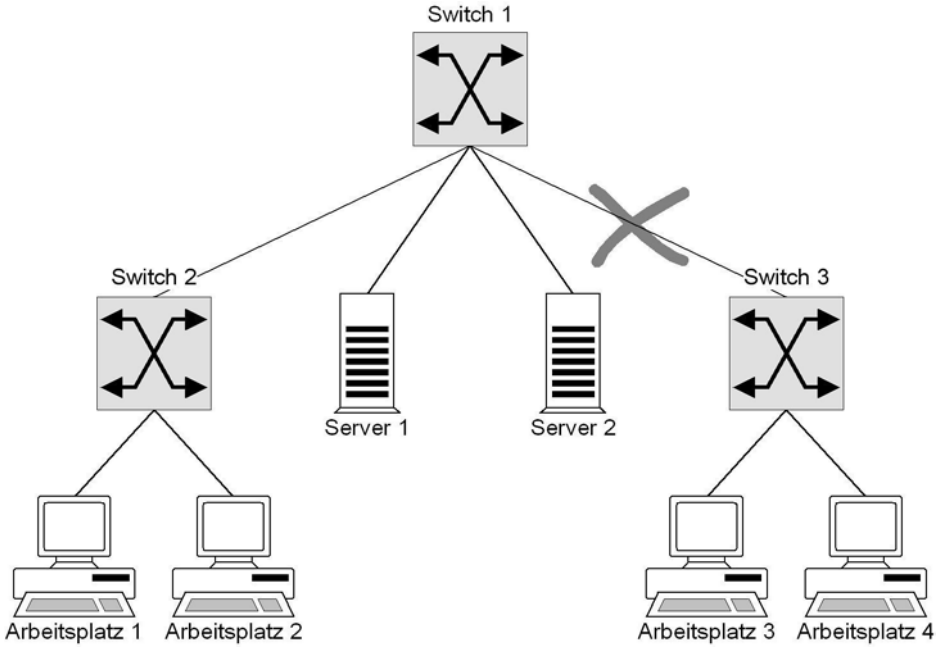


Zur Beurteilung des Ausfallrisikos können die herstellerseitig angegebenen MTBFs (Mean Time Between Failure) der Komponenten herangezogen werden.

Bei Hubs können prinzipiell zwei Techniken unterschieden werden, wie die Verbindung zwischen den einzelnen Modulen und damit den angeschlossenen Segmenten erfolgt. Bei Produkten mit passiver Backplane, dem Element, welches die Verbindung zwischen Modulen herstellt, stellt diese lediglich die elektrische Verbindung zwischen den Modulen her. Die eigentliche Steuerungselektronik ist auf den einzelnen Modulen untergebracht. Bei Produkten mit aktiver Backplane stellt diese zusätzliche Funktionalität bereit, wie konfigurierbare Kommunikation zwischen den Modulen, Signalverstärkung usw. Generell sollte berücksichtigt werden, dass aktive Netzkomponenten mit aktiver Backplane störanfälliger sind, als aktive Netzkomponenten mit passiver Backplane. Durch den Ausfall einer aktiven Backplane fällt die gesamte Kommunikation innerhalb der entsprechenden Netzkomponente aus. Eine passive Backplane kann aufgrund ihrer Bauweise dagegen nur durch mechanische Gewalteinwirkung oder durch höhere Gewalt (z. B. Blitzschlag) zerstört werden. Weiterhin stellt das Netzteil der Komponenten eine häufige Störungsursache dar, da alle aktiven Netzkomponenten auf eine stabile Stromversorgung angewiesen sind. Viele Komponenten lassen sich deshalb mit redundanten Netzteilen ausrüsten oder sind hiermit bereits ausgestattet. Im gleichen Maße kann der Ausfall einer passiven Netzkomponente den Verlust der Verfügbarkeit eines Netzes bedingen. Dies trifft beispielsweise für Kabel und Steckverbinder zu, die Segmente miteinander verbinden. Diese

Gefährdung kann z. B. bei nicht sachgemäßer Installation der Kabel (z. B. Nichtbeachtung des maximalen Biegeradiuses), fehlerhafter Konfektion der Kabel mit Steckverbindern (insbesondere bei LWL) oder Störungen durch elektromagnetische Unverträglichkeit eintreten.

Beispiel: Fällt, wie in der folgenden Abbildung dargestellt, die Verbindung zwischen Switch 3 und Switch 1 durch ein defektes Kabel oder einen defekten Steckverbinder aus, können die Arbeitsplätze 3 und 4 weder mit den Servern, noch mit den Arbeitsplätzen 1 und 2 kommunizieren. Eine Kommunikation zwischen den Arbeitsplätzen 3 und 4 ist jedoch weiterhin möglich.



G 4.32 Nichtzustellung einer Nachricht

Der Datenaustausch über E-Mail ist schnell und komfortabel, aber nicht immer sehr zuverlässig. Aufgrund von Hardware- oder Softwarefehlern bei den beteiligten IT-Systemen oder durch Störungen auf dem Übertragungsweg kommt es immer wieder zum Nachrichtenverlust. Die technischen Probleme können vielfältige Ursachen haben, z. B. können Leitungen beschädigt sein, Netzkopplungselemente ausfallen oder die Kommunikationssoftware falsch konfiguriert sein. E-Mails können auch verloren gehen, weil die Empfängeradresse nicht korrekt angegeben war. Dabei ist das größte Problem, dass die Benutzer häufig nicht über die unterbliebene Zustellung der E-Mail informiert werden. Auf eine automatisierte Unterrichtung bei einer unterbliebenen Zustellung kann nicht vertraut werden.

Viele E-Mailprogramme bieten Optionen wie "Zustellung bestätigen" oder "Empfang bestätigen". Entsprechende Rückmeldungen sollten aber nicht überbewertet werden. Zum einen werden die Zustellbestätigungen häufig nicht durch die Ankunft einer E-Mail am Bildschirmarbeitsplatz des Empfängers ausgelöst wird, sondern durch die Ankunft bei einem Mailserver. Ob der Mailserver die E-Mail erfolgreich an den Adressaten weitergeleitet hat, wird dann nicht mehr mitgeteilt. Zum anderen erfolgt auch häufig keine Zustellbestätigung, obwohl die E-Mail korrekt übertragen wurde, wenn diese Option durch die Empfängerseite nicht unterstützt wird.

G 4.33 Schlechte oder fehlende Authentikation

Authentikationsmechanismen können zur Authentikation von Benutzern oder Komponenten oder zur Bestimmung des Datenursprungs eingesetzt werden. Wenn Authentikationsmechanismen fehlen oder zu schlecht sind, besteht die Gefahr, dass

- Unbefugte auf IT-Systeme oder Daten Zugriff nehmen können,
- die Verursacher von Problemen nicht identifiziert werden können oder
- die Herkunft von Daten nicht bestimmt werden kann.

Sicherheitslücken entstehen

- bei der Benutzerauthentikation, wenn z. B. Benutzer Passwörter wählen, die einfach zu erraten sind, oder wenn sie die Passwörter nie wechseln,
- bei der Komponentenauthentikation, wenn z. B. nach Inbetriebnahme eines IT-Systems Default-Passwörter nicht durch individuell gewählte ersetzt werden, wenn die Passwörter, die bei vielen IT-Systemen fest eingegeben werden, nie wieder geändert werden oder wenn die Passwörter nicht sicher hinterlegt werden und sich nach einem Systemabsturz herausstellt, dass das jetzt dringend benötigte Passwort vergessen wurde,
- bei der Wahl der Verfahren, wenn diese z. B. völlig untauglich sind oder Sicherheitslücken bekannt werden, auf die im laufenden Betrieb aber nicht reagiert wird.

G 4.34 Ausfall eines Kryptomoduls

Wird ein Kryptomodul zur Sicherung der Vertraulichkeit schützenswerter Daten eingesetzt, kommt dem fehlerfreien Funktionieren des Kryptomoduls eine besondere Bedeutung zu. Der Ausfall eines solchen im Einsatz befindlichen Kryptomoduls kann auf verschiedene Ursachen zurückzuführen sein:

- technischer Defekt, der die Funktionsfähigkeit beeinträchtigt,
- Stromausfall, in dessen Folge die flüchtig gespeicherten kryptographischen Schlüssel gelöscht werden, so dass das Kryptomodul infolgedessen nicht mehr ordnungsgemäß verschlüsseln kann,
- unabsichtliche oder absichtliche Zerstörung durch mechanische Einwirkung, Fehlbedienung oder ähnliches.

Die Folgeschäden aufgrund des Ausfalls eines Kryptomoduls können ebenfalls vielseitig sein. Hier sind insbesondere zu nennen:

- Die kryptographische Absicherung einer Datenübertragungsstrecke ist nicht mehr möglich, so dass die Vertraulichkeit temporär nicht mehr gewahrt werden kann. Dies ist insbesondere dann kritisch, wenn der Ausfall nicht bemerkt wird und durch die Fehlfunktion keine Verschlüsselung mehr stattfindet, obwohl die Anwender auf die Sicherstellung der Vertraulichkeit der Daten durch das Kryptomodul bauen.
- Verschlüsselte Daten können nicht mehr entschlüsselt werden, solange das erforderliche Kryptomodul nicht mehr verfügbar ist. Daraus können sich Verfügbarkeitsprobleme für IT-Anwendungen ergeben, die die entschlüsselten Daten weiterverarbeiten.
- Arbeitet das Kryptomodul fehlerhaft, ohne dass ein vollständiger Ausfall eintritt, werden Daten unvollständig oder inkorrekt verschlüsselt. In beiden Fällen kann es bedeuten, dass im Falle der Datenübertragung der Empfänger der Daten bzw. bei lokaler Speicherung der Daten der Anwender die Daten nicht mehr korrekt entschlüsseln kann. Ohne entsprechende Datensicherungen bedeutet dies ggf. einen Totalverlust der Daten.

G 4.35 Unsichere kryptographische Algorithmen

Der Sicherheitszugewinn durch Einsatz kryptographischer Verfahren ist grundsätzlich von zwei Parametern abhängig: es müssen sichere kryptographische Algorithmen eingesetzt werden und die geheimen Schlüssel müssen vertraulich gehandhabt werden (zur Kompromittierung kryptographischer Schlüssel siehe G 5.83 *Kompromittierung kryptographischer Schlüssel*).

Unsichere kryptographische Algorithmen sind dadurch gekennzeichnet, dass es einem potentiellen Angreifer mit vertretbaren Ressourcen gelingt, das eingesetzte kryptographische Verfahren zu brechen. Bei Verschlüsselungsalgorithmen bedeutet dies, dass es gelingt, aus dem verschlüsselten Text den ursprünglichen Klartext zu ermitteln, ohne dass zusätzliche Informationen bekannt sind. Dabei sind als relevante Ressourcen auf Angreiferseite z. B. die verfügbare Rechenleistung, Hilfsmittel wie Analysetools, vorhandene Kenntnisse, verfügbare Arbeitszeit, Kenntnisse über Schwachstellen etc. zu berücksichtigen. Werden also unsichere kryptographische Algorithmen eingesetzt, besteht für Angreifer die Möglichkeit, den kryptographischen Schutz zu unterlaufen.

Ob jedoch ein kryptographischer Algorithmus unsicher ist, muss jeweils im Einzelfall untersucht werden. Es gibt jedoch einige Kriterien, die auf Unsicherheiten schließen lassen:

- Werden bei symmetrischen Verschlüsselungsverfahren geheime Schlüssel benutzt, deren effektive Länge geringer als 60 Bit ist, so können sie heute mit moderatem Rechnereinsatz durch Ausprobieren aller potentiell möglichen Schlüssel gebrochen werden. Mit steigender Rechnerleistung ist anzunehmen, dass diese Grenze in Zukunft über 100 Bit steigen wird.
- Werden bei asymmetrischer Verschlüsselungs- und Signaturverfahren Algorithmen eingesetzt, deren Sicherheit auf dem Problem des Faktorisierens großer Zahlen basiert, so wird heute angenommen, dass Schlüssellängen von weniger als 1024 Bit als unsicher zu betrachten sind. Dies begründet sich in den Fortschritten bei der Entwicklung effizienter Faktorisierungsalgorithmen, die heute unter massivem Rechnereinsatz Faktorisierungen von Zahlen mit rund 500 Bit erlauben. Daneben ist die mögliche Entwicklung von opto-elektronischen Beschleunigern für einen wesentlichen Teil-Rechenschritt bei diesen Verfahren in Betracht zu ziehen, was diese wesentlich beschleunigen würde.
- Hashfunktionen, die eine beliebig lange Zeichenkette auf einen Hashwert mit konstanter Bitlänge abbilden, können als unsicher betrachtet werden, wenn die konstante Länge des Hashwertes geringer ist als 128 Bit, da sonst zwei Zeichenketten ermittelt werden können, die den gleichen Hashwert ergeben.
- Kryptographische Algorithmen, die von unerfahrenen Entwicklern entworfen wurden und nicht in der wissenschaftlichen Szene untersucht wurden, sollten als potentiell unsicher betrachtet werden, da die Entwicklung sicherer kryptographischer Algorithmen langjährige Erfahrung voraussetzt.

- Nicht veröffentlichte kryptographische Algorithmen, die auffällig schnell in Software ablaufen, sollten ebenfalls als potentiell unsicher betrachtet werden. Die Erfahrung zeigt, dass sichere Algorithmen meist auf komplexen mathematischen Funktionen beruhen müssen.
- Bei der Anwendung kryptographischer Verfahren werden häufig Zufallszahlen benötigt. Schlechte Zufallszahlengeneratoren können dazu führen, dass die damit erzeugten Werte vorhersagbar sind. Dadurch können z. B. kryptographische Checksummen, die die Nachrichtenintegrität sicherstellen sollen, wertlos werden.

Von diesen Kriterien betroffen ist beispielsweise der weltweit sehr häufig eingesetzte DES-Algorithmus zur symmetrischen Verschlüsselung. Dieser benutzt eine effektive Schlüssellänge von 56 Bit. Der so genannte Triple-DES-Algorithmus als dreifache Hintereinanderausführung mit zwei Schlüsseln hat eine effektive Schlüssellänge von 112 Bit und kann zurzeit noch als ausreichend sicher betrachtet werden. Auch betroffen ist der RSA-Algorithmus, der als asymmetrisches Verfahren auf dem Faktorisierungsproblem basiert. Wird RSA mit einer Schlüssellänge unter 768 Bit betrieben, muss davon ausgegangen werden, dass dies keine ausreichende Sicherheit bietet. Für die nächsten Jahre kann eine Schlüssellänge von mindestens 1024 Bit noch als ausreichend sicher angesehen werden.

Ein häufiges Beispiel unsicherer, aber sehr schneller Algorithmen ist die so genannte XOR-Funktion, bei der konstante Werte mit dem ursprünglichen Klartext auf einfache Weise verknüpft werden. Dies ist ein hochperformanter Algorithmus, der jedoch sehr schnell gebrochen werden kann. Die XOR-Funktion kann andererseits aber der sicherste Verschlüsselungsalgorithmus überhaupt sein, wenn die zu verschlüsselnden Daten mit nicht vorhersagbaren Zufallswerten XOR-iert werden (One-Time-Pad).

Für den Laien ist es praktisch unmöglich, festzustellen, ob ein kryptographischer Algorithmus ausreichend sicher ist. Daher sollten nur solche Algorithmen eingesetzt werden, die bekanntermaßen von Experten entwickelt wurden oder die einer langjährigen Untersuchung durch die wissenschaftliche Szene unterzogen wurden.

G 4.36 Fehler in verschlüsselten Daten

Liegen Daten in verschlüsselter Form vor und werden diese verändert, kann es bei der Entschlüsselung der Daten dazu kommen, dass die Daten nicht mehr korrekt entschlüsselt werden können. Je nach Betriebsart der Verschlüsselungsroutinen kann dies bedeuten, dass nur wenige Bytes falsch entschlüsselt werden oder dass sämtliche Daten ab dem Fehler falsch entschlüsselt werden. Gibt es keine Datensicherung, kann dies einen Totalverlust der Daten bedeuten.

Die genannten Fehler in den verschlüsselten Daten können auf verschiedene Weise entstehen:

- Bei der Datenübertragung der verschlüsselten Daten kommt es zu einem Übertragungsfehler, der nicht behoben werden kann.
- Auf dem Speichermedium (Diskette, Festplatte) kommt es zu einem irreparablen Fehler.
- Ein Computer-Virus führt an den Daten Manipulationen durch.
- Ein Dritter führt absichtlich Manipulationen an den Daten durch, beispielsweise indem die verschlüsselten Daten mit einem Editorprogramm an wenigen Stellen manipuliert werden.

In ungünstigen Fällen, wenn z. B. ein Bitverlust auftritt oder zu große Datenmengen verändert werden und eine Fehlerfortpflanzung stattfindet, können die Daten selbst bei Kenntnis des kryptographischen Verfahrens und der zur Verschlüsselung benutzten Schlüssel nicht mehr rekonstruiert werden.

Noch kritischer kann sich ein Fehler in den verwendeten kryptographischen Schlüsseln auswirken. Schon die Änderung eines einzigen Bits eines kryptographischen Schlüssels führt dazu, dass sämtliche damit verschlüsselten Daten nicht mehr entschlüsselt werden können. Ohne eine Datensicherung des kryptographischen Schlüssels sind diese Daten verloren.

G 4.37 Mangelnde Authentizität und Vertraulichkeit von E-Mail

E-Mails ersetzen an vielen Stellen die herkömmliche Kommunikation per Post. Dabei wird jedoch häufig nicht beachtet, dass "normale" E-Mail ohne zusätzliche Sicherungsmaßnahmen keine Gewähr für die Authentizität und Vertraulichkeit von Nachrichten bietet.

Bei unverschlüsselten E-Mails können alle Informationen auf jedem IT-System gelesen werden, auf dem die Nachricht auf ihrem Weg durchs Netz bearbeitet wird. Da der genaue Transportweg im Allgemeinen nicht vorhersagbar ist und das zugrunde liegende Protokoll SMTP (*Simple Mail Transfer Protocol*) keine Mechanismen anbietet, einen bestimmten Weg vorzugeben, kann eine E-Mail sehr viele verschiedene Systeme passieren.

Informationen, die nicht durch digitale Signaturen geschützt sind, können auch auf jedem beteiligten System verändert oder gelöscht werden, ohne dass dies vom Empfänger bemerkt werden kann. Abgesehen von Veränderungen am Text oder an etwaigen Dateianhängen einer E-Mail können auch Informationen wie Absende- und Weiterleitungsdaten oder die Absenderadresse selbst verändert werden, siehe auch G 5.73 *Vortäuschen eines falschen Absenders*.

Daher ist es falsch, E-Mails mit klassischen Briefen zu vergleichen. Ein Vergleich mit Postkarten wäre zutreffender.

Beispiele:

- Ein Angestellter verschickte mit der Absenderangabe seines Chefs E-Mails mit Arbeitsaufträgen an verschiedene Kollegen.
- Praktisch alle der vielen Spam-E-Mails, die täglich die E-Mail-Postfächer füllen tragen eine gefälschte Absenderadresse.
- Als Absendedatum einer E-Mail wird meist die lokale Systemzeit auf dem Rechner des Absenders eingetragen. Da diese oft selbst von normalen Anwendern verstellt werden kann, stellt ein bestimmtes Absendedatum in einer E-Mail keinen Beweis dafür dar, dass diese wirklich zu einem bestimmten Zeitpunkt verschickt wurde.

G 4.38 Ausfall von Komponenten eines Netz- und Systemmanagementsystems

Bei einem Netz- und Systemmanagementsystem kann es zu einem Ausfall verschiedener Komponenten kommen. Einige der dadurch entstehenden Probleme und Gefährdungen sind im folgenden beschrieben.

Ausfall von verwalteten Komponenten

Fallen beim Einsatz eines Netz- und Systemmanagementsystems damit verwaltete Komponenten aus, so kann es je nach Managementsystem vorkommen, dass die Managementinformationen nicht automatisch aufgrund dieses Ereignisses aktualisiert werden. In der Regel wird dem Systemadministrator z. B. bei Netzmanagement-Systemen nur das Ausfallen der Komponente angezeigt. Wird z. B. der Ausfall der Komponente von einem Angreifer beobachtet oder bewusst herbeigeführt, so kann dieser u. U. außerhalb des LANs einen eigenen Rechner in das System einbringen und als die ausgefallene Komponente ausgeben (IP-Spoofing). Dieser Rechner kann dann zu weiteren Angriffen genutzt werden, bei denen er dann mit den Rechten eines internen Rechners ausgestattet ist (z. B. Einbringen falscher Managementinformationen).

Ausfall von Überwachungskomponenten

Fallen beim Einsatz eines Managementsystems Teile des Systems (auch unbemerkt) aus, so sind die durch die Komponente überwachten oder verwalteten Systemkomponenten nicht mehr an das Managementsystem angeschlossen. Neue eingehende Managementanweisungen werden dadurch nicht mehr auf diesen Rechnern umgesetzt. Dies hat zur Folge, dass inkonsistente Systemkonfigurationen entstehen, die wiederum zu Sicherheitsproblemen führen können.

Nicht-Verfügbarkeit der zentralen Managementstation

Fällt in einem durch ein Managementsystem verwalteten Netz die zentrale Managementstation aus, so kann das System nicht mehr zentral verwaltet werden. Dauert die Nicht-Verfügbarkeit länger an, weil z. B. die Hardware aufgrund fehlender Wartungsverträge nicht kurzfristig ersetzt werden kann, so werden unter Umständen Routinefunktionen wie etwa Datensicherungen nicht mehr angestoßen. Werden nun "von Hand" Änderungen an den einzelnen verwalteten Systemen unkoordiniert durchgeführt, so entstehen Inkonsistenzen und möglicherweise Sicherheitsprobleme.

Ausfall von Netzkoppelelementen während der Übertragung von Managementinformationen

Beim Einsatz eines Managementsystems zur Verwaltung eines Rechnernetzes ist der Austausch von so genannter Managementinformation zwischen den einzelnen Komponenten des Managementsystems nötig. Die Information wird über das lokale Netz übertragen. Lokale Netze bestehen in der Regel (je nach verwendeter Netztechnik) aus mehreren Teilnetzen, die über Netzkoppelelemente wie Router miteinander verbunden sind. Die Netzkoppelelemente reichen dabei Daten aus einem Teilnetz in ein anderes Teilnetz weiter. Fallen die Koppelelemente aus, so ist dies gleichbedeutend mit der physikalischen

Trennung der betroffenen Teilnetze. Managementinformationen können dann nicht mehr ausgetauscht werden. Dabei existiert in der Regel ein Teilnetz, das noch von der jeweiligen Managementstation verwaltet werden kann, und ein Teilnetz, das nicht mehr verwaltet werden kann. Je nach Dauer der Nicht-erreichbarkeit führt dies zu Inkonsistenzen und Sicherheitsproblemen.

G 4.39 Software-Konzeptionsfehler

Bei der Planung von Programmen und Protokollen können sicherheitsrelevante Konzeptionsfehler entstehen. Häufig sind diese Fehler historisch gesehen durchaus verständlich. So ist sicherlich keiner der Entwickler der im Internet verwendeten Protokolle Ende der 60er-Jahre davon ausgegangen, dass diese Protokolle einmal die Grundlage für ein weltumspannendes und kommerziell höchst bedeutendes Computer-Netz werden würden.

Beispiele:

- Beispiele für Konzeptionsfehler sind die offene Übertragung der Daten im Internet, so dass Daten (z. B. Passwörter) mitgelesen oder verändert werden können, oder die Möglichkeit, Pakete mit Internet-Adressen zu versenden, die einem anderen Rechner zugeteilt worden sind. Ein Spezialfall hiervon ist die so genannte FTP-Bounce-Attacke, bei der ausgenutzt wird, dass die Verbindung, die beim FTP-Protokoll für die Datenübertragung eingesetzt wird, zu einem beliebigen Rechner aufgebaut werden kann. Im ungünstigen Fall können auf diese Weise sogar Firewalls mit dynamischen Paketfiltern überwunden werden (siehe CERT Advisory 97-27). Weitere Fehler in den Internet-Protokollen sind sicherlich vorhanden und werden zukünftig publiziert werden.
- Ein weiteres Beispiel für einen Konzeptionsfehler ist das so genannte DNS-Spoofing (siehe auch G 5.78 *DNS-Spoofing*). Das Domain Name System ist der zentrale Auskunftsdienst im Internet, der die Übersetzung der leicht merkbaren Rechnernamen wie www.preiswert.de in die zugehörige Internet-Adresse ermöglicht. Bei DNS-Spoofing versucht ein Angreifer, einem Rechnernamen einen falschen Rechner zuzuweisen, so dass Auskunftsuchende fehlgeleitet werden.
- Ein weiteres Beispiel für einen Konzeptionsfehler ist die Möglichkeit, anonym sehr viele Werbe-E-Mails zu versenden (Mail-Spamming). Hierbei werden häufig fremde Mailserver als so genannte Remailer eingesetzt, so dass Gegenaktionen durch den Empfänger ins Leere laufen. Die Ursache für diese Angriffe liegt eindeutig in den mangelhaften Authentisierungsmöglichkeiten, die das Internet zur Zeit bietet.

G 4.40 Ungeeignete Ausrüstung der Betriebsumgebung des RAS-Clients

Die Aufnahme von RAS-Verbindungen wird häufig durch die Inkompatibilität der technischen Ausstattung verhindert. Aber auch bei kompatibler Technik kann die Verbindungsaufnahme scheitern, wenn Einwahlpunkte der entsprechenden Dienstleister fehlen oder nicht erreichbar sind. Die Gefährdungen aus diesem Bereich sind u. A.:

- Die Stromparameter zwischen RAS-Client und entferntem Standort sind inkompatibel (220V/110V).
- Die Modemanschlüsse zwischen RAS-Client und entferntem Standort sind inkompatibel.
- Das üblicherweise genutzte Vermittlungsnetz (Telekommunikationsdienstleister, Internetdienstleister) ist am entfernten Standort nicht verfügbar.
- Die Übertragung der entfernten Telefonnummer zum RAS-Server ist fehlerhaft oder inkompatibel (bei Authentisierung mittels CLIP - Calling Line Identification Protocol).

Alle möglichen technischen Probleme für beliebige Betriebsumgebungen bei der Planung des RAS-Systems zu berücksichtigen, ist zudem kaum möglich.

G 4.41 Nicht-Verfügbarkeit des Mobilfunknetzes

Die Verfügbarkeit von Mobilfunknetzen ist deutlich geringer als die von Festnetzen. Wie alle Systeme, die keine hundertprozentige Verfügbarkeit gewährleisten, stehen auch Mobilfunknetze häufig nicht an den Orten und Zeiten zur Verfügung, zu denen sie am dringendsten benötigt werden. Es sind auch nicht alle Mobilfunknetze darauf ausgelegt, flächendeckende Anbindungen zu gewährleisten.

Die häufigste Ursache für eine fehlende Mobilfunkversorgung sind sicherlich Funklöcher, also Bereiche, die von keinem Netzbetreiber versorgt werden. Bei einer sehr großen Nachfrage kann es aber auch zu einer Überlastung von Teilen des Netzes kommen. Dies kann dazu führen, dass das Empfangen oder Senden von Nachrichten verhindert wird.

Weiterhin kann es Störsender geben, die in einem räumlich abgegrenzten Bereich den Funkbetrieb derart stören, dass dort kein Mobilfunkempfang möglich ist. Es gibt auch Geräte, die genau für diesen Zweck verkauft werden. Allerdings ist der Betrieb solcher Geräte in Deutschland nicht zulässig.

Beispiel:

Die Funkkapazität einer Sendestation reicht nicht, wenn nach einem großen Unfall sehr viele Personen gleichzeitig ein Mobiltelefonat führen wollen, um Rettungsdienste zu benachrichtigen oder ihre Angehörigen zu informieren.

G 4.42 Ausfall des Mobiltelefons oder des PDAs

Die Benutzung eines Mobiltelefons oder eines PDAs kann durch verschiedene Faktoren negativ beeinträchtigt werden:

- Der Akku kann leer sein, weil vergessen wurde, ihn aufzuladen.
- Der Akku kann seine Fähigkeit, Energie zu speichern, verloren haben.
- Der Benutzer kann das Zugangspasswort bzw. die PIN vergessen haben und kann deswegen das Gerät nicht mehr benutzen.
- Komponenten wie Display, Tasten oder SIM-Karte können defekt sein.

Wenn ein Mobiltelefon oder PDA schädigenden Umwelteinflüssen ausgesetzt wird, kann seine Funktionsfähigkeit beeinträchtigt werden. Mobiltelefone und PDAs können sowohl unter zu hohen als auch zu niedrigen Temperaturen leiden, ebenso unter Staub oder Feuchtigkeit.

Beispiele:

- Für eine längere Dienstreise hat ein Mitarbeiter ein Mobiltelefon samt Zubehör aus einem Mobiltelefon-Pool mitgenommen. Unterwegs stellte sich dann heraus, dass er leider das falsche Ladegerät eingesteckt hatte. Da er damit das Mobiltelefon nicht wieder aufladen konnte, konnte er es die restliche Zeit nicht mehr benutzen.
- Das Mobiltelefon oder der PDA werden in einem geparkten Auto zurückgelassen. Dies erhöht nicht nur die Diebstahlgefahr, sondern es wird auch eventuell schädigenden Umwelteinflüssen ausgesetzt. Durch direkte Sonneneinstrahlung können im Sommer hinter einer Glasscheibe Temperaturen von über 60°C entstehen. Ein analoges Problem besteht im Winter, wo im geparkten Auto Temperaturen deutlich unter dem Gefrierpunkt herrschen können. Durch solche extremen Temperaturen kann der Akku oder auch das Display beschädigt werden.
- Auf einer Dienstreise ist dem PDA zwischendurch der Strom ausgegangen, weil die Ersatzbatterien zu spät eingesetzt wurden. Nach dem Wiedereinschalten sind allerdings viele Konfigurationseinstellungen verloren gegangen, da diese vom Betriebssystem nicht automatisch gesichert wurden. Dadurch laufen anschließend einige Anwendungen wie E-Mail und Internetzugriff nicht mehr korrekt.

G 4.43 Undokumentierte Funktionen

Viele Anwendungsprogramme enthalten undokumentierte Funktionen, also Funktionen, die nicht in der Dokumentation beschrieben sind und die den Benutzern nicht bekannt sind. Bei einigen Betriebssystemen bzw. Anwendungsprogrammen gibt es mittlerweile Bücher, die einen Großteil der bekannt gewordenen, bis dato undokumentierten Funktionen beschreiben und die im Allgemeinen dicker sind als die mitgelieferten Handbücher. Undokumentierte Funktionen müssen sich allerdings nicht nur auf Hilfsmittel mit nützlichen Effekten beschränken. Solange diese Funktionen nicht offen gelegt sind, kann nicht ausgeschlossen werden, dass mit ihnen auch viel Schaden angerichtet werden kann.

Dies ist insbesondere dann problematisch, wenn die undokumentierten Funktionen Sicherheitsmechanismen des Produktes betreffen, beispielsweise den Zugriffsschutz. Solche Funktionen dienen oft als "Hintertüren" während der Entwicklung oder der Verteilung von Anwendungsprogrammen.

Beispiele:

- Bei verschiedenen IT-Systemen fanden sich von den Entwicklern eingebaute (und vergessene) Hintertüren, um die Wartung zu erleichtern, die es allerdings auch ermöglichten, mit einem trivialen Passwort Administratorrechte zu erlangen.
- Viele Programme können (oder müssen sogar) online beim Hersteller registriert werden. Bei einigen dieser Programme wurden bei der Online-Registrierung der Software gleichzeitig ein Überblick über alle auf der Festplatte gespeicherten Programme mitgeliefert.

G 4.44 Ausfall von Novell eDirectory

Durch technisches Versagen aufgrund von Hardware- oder Software-Problemen kann es zum Ausfall eines eDirectory-Systems oder Teilen davon kommen. Als Konsequenz davon können die im Verzeichnis gehaltenen Daten temporär nicht mehr zugänglich sein, und zwar weder für eDirectory-Benutzer noch für etwaige Netzapplikationen, die auf das eDirectory zugreifen. Im Extremfall kann es auch zu Datenverlusten kommen.

Dadurch können Geschäftsprozesse gestört und der interne Workflow behindert werden, durch die vielfältigen Funktionen von eDirectory und die starke Einbindung in die Organisation kann es damit auch zu Produktivitätsausfällen kommen.

Sind Repliken der ausgefallenen Systemteile funktionsfähig vorhanden, so ist der Zugriff zwar weiterhin möglich, jedoch unter Umständen - abhängig von der Netztopologie - mit reduzierter Performance.

G 4.45 Verzögerte Archivauskunft

Verzögerungen bei der Wiederbeschaffung archivierter Dokumente können Geschäftsprozesse, in deren Kontext eine Archivanfrage erfolgt, stören oder behindern. Für derartige Verzögerungen kommen viele Ursachen in Betracht, beispielsweise:

- veraltete Archivserver-Software,
- ungünstige Wahl von Index- und Suchkriterien bei Ablage oder Suche von archivierten Daten,
- überlastete Hardware des Archivservers oder beteiligter Datenbankserver,
- Verzögerungen im Netz sowie
- unausgewogenes Verhältnis von Speichermedien zu Laufwerken.

Bei dem letztgenannten Punkt sind zwei Fälle zu unterscheiden:

ein großes Medium

- Wird für die Archivierung ein Laufwerk mit einem einzelnen Speichermedium genutzt, das eine sehr große Kapazität hat, können die Antwortzeiten sehr groß werden, da nur jeweils ein Benutzer gleichzeitig auf das Archiv zugreifen kann. Alle anderen Anfragen werden zwischengespeichert und dann der Reihe nach abgearbeitet.

viele kleine Medien

- Bei einer großen Anzahl kleiner Speichermedien sind im Verhältnis dazu nur wenige Laufwerke verfügbar. Daher müssen die Datenträger bei Anfragen entsprechend oft gewechselt werden, was zu längeren Antwortzeiten führt. Kleine Speichermedien sind darüber hinaus schneller in ihrem Speicherplatz erschöpft (siehe G 4.20 *Datenverlust bei erschöpftem Speichermedium*).

Verzögerungen können sich auch bei der Einstellung von Dokumenten ins Archiv ergeben, etwa wenn die Bestätigung des Archivierungsvorgangs durch lange Übertragungszeiten im LAN verzögert wird.

G 4.46 Fehlerhafte Synchronisierung von Indexdaten bei der Archivierung

Index des Archivsystems ...

Bei der Archivierung werden sehr große Datenvolumen gespeichert. Auf alle archivierten Daten muss zu einem späteren Zeitpunkt in annehmbarer Zeit jederzeit kontrolliert und eindeutig zugegriffen werden können. Diese Funktionalität wird durch das Archivsystem gewährleistet, das hierzu einen Index der gespeicherten Dateien erzeugt.

Archivsysteme realisieren jedoch meist nur einfache Dateizugriffe. Um mehr Komfort beim Zugriff zu erreichen, wird daher sehr oft ein übergeordnetes Dokumentenmanagementsystem (DMS) eingesetzt, über das der Zugriff auf das Archiv gesteuert und weitergehende Funktionalitäten, z. B. komplexe Suchanfragen, realisiert werden.

... und des Dokumenten-managementsystems

Das DMS erzeugt bei der Archivierung die Referenzierung der Daten, kontrolliert deren Version und legt gegebenenfalls einen Volltextindex an, so dass alle auf dem Speichermedium archivierten Daten zu einem späteren Zeitpunkt eindeutig identifiziert werden können.

Letztlich gibt es daher zwei Indexdatenbanken (im Archivsystem und im DMS), die beide synchronisiert werden müssen. Kommt es einseitig zu Veränderungen in den im DMS gespeicherten Indexdaten oder zu Fehlern auf dem Speichermedium, ohne dass die Veränderungen im anderen Teil berücksichtigt werden, können archivierte Daten nicht mehr den Referenzen im DMS zugeordnet werden.

G 4.47 Veralten von Kryptoverfahren

Die Zuverlässigkeit von Kryptosystemen ist direkt mit der fortschreitenden Entwicklung der Rechenleistung von IT-Systemen, der Entwicklung neuerer Algorithmen sowie der Forschung auf dem Gebiet der Kryptoanalyse verknüpft. Durch die Steigerung der Leistungsfähigkeit von IT-Systemen können als sicher geltende Kryptoalgorithmen bzw. Schlüssellängen zukünftig möglicherweise kompromittiert werden.

Hierdurch besteht die Gefahr, dass im Falle der Kompromittierung von Kryptoverfahren oder Kryptoschlüsseln

- verschlüsselte Daten unbefugt entschlüsselt werden können,
- von Unbefugten Dokumente mit einer technisch gültigen Signatur versehen werden können, so dass dann
- authentische, signierte Dokumente nicht mehr von gefälschten unterschieden werden können.

Beispiel:

DES mit 40 Bit langen Schlüsseln

Krankenhäuser müssen die Akten ihrer Patienten auch nach Abschluss der Behandlung für einen langen Zeitraum sicher aufbewahren. Ein deutsches Krankenhaus hat dementsprechend 1980 angefangen, die elektronisch gespeicherten Krankendaten zu verschlüsseln. Das dazu verwendete Verfahren basierte auf DES mit 40 Bit langen Schlüsseln. Da sich im Krankenhaus niemand mit Verschlüsselung auskannte, wurde dieses Verfahren auch im Jahr 2001 noch eingesetzt, obwohl mittlerweile bereits im Internet Programme verfügbar waren, um die damit verschlüsselten Daten auszulesen. Dies fiel erst bei einer Datenschutzkontrolle auf.

G 4.48 Ausfall der Systeme eines Outsourcing-Dienstleisters

Bei einem Outsourcing-Dienstleisters können die IT-Systeme teilweise oder ganz ausfallen, wodurch auch der Auftraggeber betroffen ist.

Auch wenn der IT-Ausfall nur einige Systeme oder Applikationen betrifft, kann dies dazu führen, dass die Datenverarbeitung inkonsistent oder fehlerhaft ausgeführt wird.

fehlende Mandantenfähigkeit

Außerdem ist zu berücksichtigen, dass bei unzureichender Strukturierung oder Isolation der IT-Systeme des Dienstleisters bereits der Ausfall eines Systems, das nicht dem Auftraggeber zugeordnet ist, trotzdem dazu führen kann, dass der IT-Betrieb des Auftraggebers beeinträchtigt wird. Dies kann immer dann ein Problem sein, wenn einzelne IT-Komponenten (z. B. Host-Rechner, Firewalls) für verschiedene Auftraggeber des Dienstleisters gemeinsam genutzt werden. Dann kann unter Umständen ein Fehler im Datenbestand eines beliebigen Kunden des Outsourcing-Dienstleisters dazu führen, dass beispielsweise bei der Host-Verarbeitung die Batch-Verarbeitung mehrerer Kunden eingestellt werden muss, wenn diese schlecht oder fehlerhaft konfiguriert ist.

Ähnliche Probleme ergeben sich, wenn die Anbindung zwischen auslagernder Organisation und Outsourcing-Dienstleister ausfällt.

G 4.49 Unsichere Default-Einstellungen auf Routern und Switches

Aktive Netzkomponenten werden von Herstellern oft mit unsicheren Default-Konfigurationen ausgeliefert, die den sicheren Einsatz gefährden. Bei einigen Geräten zeigen außerdem die Systembefehle zur Anzeige einer Konfiguration nicht alle Parameter an.

Folgende Aspekte sind häufig problematisch:

Betriebssystem

Aktive Netzkomponenten werden oft mit einem veralteten Versionsstand des Betriebssystems ausgeliefert.

Hostname

Werkmäßig eingestellte Hostnamen verraten oft den Hersteller der Geräte.

Dienste

Werkseitig werden Geräte mit Standardkonfigurationen ausgeliefert, auf denen eine Vielzahl von Diensten aktiviert sind. Beispielsweise können dies HTTP, Telnet, FINGER oder sonstige Dienste sein.

Benutzerkonten und Passworte

Werksmäßig eingerichtete Benutzerkonten haben dokumentierte und damit allgemein bekannte Standardnamen und -Passworte. Auf einschlägigen Internet-Seiten stehen Listen mit herstellerspezifischen Standard-Accounts und Passworten zum Download bereit.

Unsichere SNMP-Versionen

Die Authentisierung erfolgt bei SNMPv1 und SNMPv2 lediglich mittels eines unverschlüsselten sogenannten Community Strings. Als Standardeinstellung bei nahezu allen Herstellern ist der Read-Community-String auf den Wert "public" eingestellt, während der Write-Community-String auf den Wert "private" gesetzt ist. Wenn die unsicheren SNMP-Versionen genutzt werden und für die Administration kein eigenes Administrationsnetz eingerichtet wurde, kann ein Angreifer leicht die Kontrolle über Netzkomponenten erlangen, wenn diese Default-Einstellungen beibehalten werden.

Routing-Protokolle

Auf Routern und Switches verschiedener Hersteller sind standardmäßig Routing-Protokolle aktiviert.

Login-Banner

Werksmäßig verraten Login-Banner unterschiedlicher Geräte beispielsweise die Modell- und Versionsnummer des Gerätes. Diese Angaben können für die gezielte Auswahl bekannter Exploits verwendet werden und erleichtern Angreifern so die Durchführung von Angriffen.

G 4.50 Überlastung des z/OS-Betriebssystems

Auch wenn durch den *Workload Manager* ein z/OS-Betriebssystem so verwaltet wird, dass eine Überlastung eigentlich nicht vorkommen sollte, gibt es eine Reihe von Gefährdungen, die zu einer Überlastung führen können. Eine Überlastung muss nicht zwangsläufig zu einem kompletten System-Stillstand führen. Es können auch nur verschiedene System-Ressourcen nicht mehr verfügbar sein, obwohl das System selbst noch reagiert. Die nachfolgenden Situationen sind typisch, aber nicht die einzigen Gefährdungen dieser Art.

***Spool-Full*-Situation**

Die Spool-Datei eines *Job Entry Subsystem* (JESx) ist nur für eine bestimmte Menge von Ausgabedaten vorgesehen. Es kann vorkommen, dass z. B. durch eine Programmschleife unbegrenzt Daten auf die Spool-Datei des JESx geschrieben werden. Dies kann zu einer *Spool-Full*-Situation führen, neue Batch-Jobs können nicht mehr gestartet werden. Nur die laufenden Online-Verfahren sind u. U. noch aktiv, sofern keine Ausgabedateien auf die Spool-Datei geschrieben werden. Da viele JES-Kommandos bei der Ausführung eine benutzbare Spool-Datei voraussetzen, kann dies bedeuten, dass umfangreiche (und zeitintensive) Recovery-Maßnahmen notwendig sind, um dieses Problem zu bereinigen.

Vollständiger System-Stillstand

Unix-Prozesse im USS-Subsystem (*Unix System Services*) werden in z/OS auf Adressräume abgebildet. Steht nicht mehr genügend Hauptspeicher zur Verfügung, müssen diese Adressräume über den *Auxiliary Storage Manager* (ASM) auf die Page-Platten ausgelagert werden. Reichen auch diese nicht aus, kann kein Adressraum mehr angelegt werden.

Wenn die Anzahl der Unix-Prozesse im USS nicht beschränkt ist und nicht genügend Platz auf den Page-Platten zur Verfügung steht, können sich deshalb Sicherheitsprobleme durch den Start von zu vielen Unix-Prozessen ergeben. Ursache kann beispielsweise eine rekursive Funktion sein, die unentwegt neue Unix-Prozesse startet. Als Folge kann es passieren, dass das System praktisch stillsteht.

Von diesem Problem ist z/OS (mit 64 Bit-Adressierung) im Vergleich zu seinem Vorgänger OS/390 (mit 31 Bit-Adressierung) durch die höhere Adressierbarkeit deutlich weniger betroffen. Durch die höhere Adressierbarkeit kann dem z/OS-System ein größerer Hauptspeicher zur Verfügung gestellt werden. Dies hat zur Folge, dass die Page-Platten erst viel später benötigt werden.

Generell können Kommandos oder Programmteile, die ständig neue Prozesse starten, sehr schnell das System überlasten. Dies kann letztendlich einen IPL (*Initial Program Load*) erforderlich machen.

Systemüberlastung durch zu viele JESx Initiators

Über die Anzahl der gestarteten *Initiators* steuert der Administrator die Batch-Verarbeitung und deren Prioritäten. Sind zu wenig *Initiators* gestartet, können Staus bei der Batch-Verarbeitung entstehen. Sind zu viele *Initiators* gestartet, kann dies zur Überlastung von Ressourcen führen.

Werden zu viele Batch-Jobs gestartet, so besteht die Gefahr, dass die *Page Datasets* nicht ausreichen. Dies erfordert ein manuelles Eingreifen in die Systemsteuerung durch das Bedienpersonal.

Ist das *Job Entry Subsystem* mit einer sehr großen Anzahl von *Initiators* definiert worden, die jedoch nicht sofort aktiviert werden, kann es vorkommen, dass bei der Eingabe des JES2-Kommandos *$SI* (statt z. B. *$SI1-10*) alle möglichen *Initiators* gestartet werden. Dadurch laufen unter Umständen mehr Batch-Jobs an als geplant. Dies führt zwar in der Regel nicht zu einem System-Stillstand, die Antwortzeiten können sich jedoch erheblich verlängern.

Verzögerte Bandverarbeitung

Wenn gleichzeitig mehr Bandeinheiten angefordert werden, als Stationen vorhanden sind, verzögert sich die Sicherung der Daten auf Bänder. Die Sicherungs-Jobs gehen in den *Wait*-Status und warten auf freie Bandstationen.

Beispiele

Zu viele Batch-Jobs

- In einer z/OS-Installation wurden zu viele *Initiators* gestartet. Dies hatte zur Folge, dass während der Batch-Verarbeitung zu viele Batch-Jobs gleichzeitig aktiviert wurden, wodurch die CPU des Systems stark belastet wurde. Obwohl das System die Last bewältigt hat, führte die Situation zu langen Antwortzeiten bei der *Time Sharing Option* (TSO).

Zu große USS-Basisdefinitionen

- Bei der USS-Basisdefinition eines z/OS-Betriebssystems wurden die Werte von *MAXPROCSYS* und *MAXFILEPROC* auf sehr hohe Werte gesetzt. Als ein Mitarbeiter einen rekursiven Funktionsaufruf, den er auf einer Unix-Schulung kennen gelernt hatte, unter *Unix System Services* ausprobierte, blieb das System nach kurzer Zeit wegen *Auxiliary Storage Shortage* stehen.

G 4.51 Unzureichende Sicherheitsmechanismen bei PDAs

Ein IT-System, das sich im mobilen Einsatz befindet, kann über ein VPN an ein LAN angeschlossen sein, so dass die Kommunikationsverbindung sehr gut geschützt ist. Wenn allerdings dieses IT-System selber ungenügend gegen unbefugten Zugriff geschützt ist, besteht die Gefahr, dass ein Unbefugter dieses als "Gateway" missbraucht, um auf das interne Netz zuzugreifen.

Typische Endgeräte für den mobilen Einsatz sind Handys oder PDAs, bei denen meistens keine Benutzertrennung möglich ist. Dadurch kann jeder, der Zugriff auf das IT-System hat, auf alle Daten und Programme zugreifen, auch auf interne Daten der Organisation oder sehr persönliche Daten des Eigentümers.

Andere leider sehr typische Schwachstellen bei mobilen Komponenten wie PDAs sind:

- unzureichende Zugriffschutz- und Authentisierungsmechanismen
- keine oder unzureichende Möglichkeiten zur Verschlüsselung von Daten
- ungesicherte Synchronisation
- keine oder unzureichende Protokollierungsmöglichkeiten

Es gibt eine Vielzahl verschiedener PDA-Modelle mit den unterschiedlichsten Betriebssystemen. Die Sicherheitseigenschaften der verschiedenen PDA-Plattformen sind unterschiedlich, einen sicheren Schutz gegen Manipulationen bietet aber derzeit keines der kommerziell gebräuchlichen Systeme.

Beispiel:

Bei Palm OS 3.5.2 und allen Vorgängerversionen kann über eine Tastenkombination wahlweise in den sogenannten "Console Mode" oder den "Debug Mode" gewechselt werden. Beide Modi erlauben, an allen Sicherheitsmechanismen des Betriebssystems vorbei, den direkten Zugriff auf Systemdaten. Dabei ist es völlig gleichgültig, ob der PDA-Zugriff über ein Passwort geschützt ist oder nicht: beide Modi können unter Umgehung des Zugriffsschutzes aktiviert werden.

G 4.52 Datenverlust bei mobilem Einsatz

Ein mobiles Endgerät ist im Vergleich mit einem stationären wesentlich mehr Risiken ausgesetzt, die zu einem Datenverlust führen können. Ein Datenverlust kann aus Diebstahl oder Geräteverlust resultieren, aber auch durch technische Probleme oder schlichten Strommangel entstehen.

Beispiele:

- Der nagelneue PDA fällt aus der Hemdtasche und zerschellt auf den Fliesen, ein Handheld wird statt der Zeitung vom Hund apportiert, leider mit Folgen. Vor allem Transportschäden führen häufig zu Datenverlusten und Geräte- oder Komponentenausfällen. Staub, Verschmutzung, Feuchtigkeit und Stürze, kurz "unsachgemäße Behandlung", sind die Ursachen von vielen Totalverlusten der Daten mobiler Endgeräte.
- Die Daten können temporär nicht verfügbar sein, weil der Akku leer ist, da vergessen wurde, ihn aufzuladen. Sie können aber auch vollständig vernichtet sein, wenn neben dem Akku auch die Sicherungsbatterie leer ist und damit alle nicht bereits synchronisierten Daten verloren sind.
- Auch bei der Synchronisation können Daten zerstört werden. Im allgemeinen muss vor einer Synchronisation eingestellt werden, wie mit Konflikten beim Datenabgleich umzugehen ist: ob beispielsweise bei gleichlautenden Dateien die des mobilen oder des stationären Endgeräts ungefragt übernommen werden oder ob eine Abfrage erfolgt. Dies wird häufig bei Inbetriebnahme der Dockingstation einmal konfiguriert und gerät danach gerne in Vergessenheit. Wenn dann aber Daten in einer anderen Reihenfolge geändert werden, als ursprünglich einmal gedacht, gehen dabei schnell wichtige Daten verloren. Dies kann auch ein unangenehmer Nebeneffekt sein, wenn beispielsweise mehrere Benutzer ihre PDAs mit demselben Endgerät synchronisieren, ohne daran zu denken, dass gleichnamige Dateien dabei überschrieben werden können.

Fehlende Aktualität

Mobile Systeme sind naturgemäß nicht immer online. Daher befinden sich die auf diesen gespeicherten Daten nicht immer auf dem aktuellsten Stand. Dies betrifft sowohl Kalendereinträge als auch allgemeine Informationen, kann aber unter Umständen auch sicherheitsrelevante Auswirkungen haben. Während der Zeit, in der keine Verbindung zu den organisationseigenen IT-Systemen und Informationsquellen besteht, können auch keine Informationen über aktuelle Sicherheitsprobleme eingeholt werden, der Virenscanner nicht aktualisiert werden etc.

G 4.53 Unsichere Default-Einstellungen bei Speicherkomponenten

Speicherkomponenten werden von Herstellern oft mit unsicheren Default-Konfigurationen ausgeliefert, die den sicheren Einsatz gefährden.

Folgende Aspekte sind häufig problematisch:

Betriebssystem

Speichersysteme werden oft mit einem veralteten Versionsstand des Betriebssystems ausgeliefert. Dieser entspricht oft nicht dem aktuellen Sicherheitsstand.

Hostname

Voreingestellte Hostnamen verraten oft den Hersteller der Geräte. Dadurch könnten gezielte Angriffe auf bekannte Sicherhetslücken dieser Geräte gestartet werden.

Dienste

Werkseitig werden Geräte mit Standardkonfigurationen ausgeliefert, auf denen eine Vielzahl von Diensten aktiviert sind. Beispielsweise können dies HTTP, Telnet, FINGER oder sonstige Dienste sein, die aus Sicherheitsgründen bei Speichersystemen nicht aktiviert sein sollten.

Benutzerkonten und Passwörter

Vom Hersteller eingerichtete Benutzerkonten haben oft dokumentierte und damit allgemein bekannte Standardnamen und -Passwörter. Auf einschlägigen Internet-Seiten stehen Listen mit herstellerspezifischen Standard-Accounts und Passwörtern zum Download bereit, so dass hierüber ein einfacher Zugriff auf die Systeme für Unbefugte möglich ist.

Unsichere SNMP-Versionen

Die Authentisierung erfolgt bei SNMPv1 und SNMPv2 lediglich mittels eines unverschlüsselten sogenannten Community Strings. Als Standardeinstellung bei nahezu allen Herstellern ist der Read-Community-String auf den Wert "public" eingestellt, während der Write-Community-String auf den Wert "private" gesetzt ist. Wenn die unsicheren SNMP-Versionen genutzt werden und für die Administration kein eigenes Administrationsnetz eingerichtet wurde, kann ein Angreifer leicht die Kontrolle über Netzkomponenten erlangen, wenn diese Default-Einstellungen beibehalten werden.

G 4.54 Verlust des Schutzes durch verschlüsselnde Dateisystem EFS

Das verschlüsselnde Dateisystem (*Encrypting File System,* EFS) von Windows Server 2003/XP ist ein für Benutzer einfach zu bedienendes Mittel, um ein aus Anwendungssicht transparentes Arbeiten mit verschlüsselten Dateien zu ermöglichen. Es eignet sich am besten für einzelne Benutzer und exponierte Client-Computer, die zeitweise außerhalb der geschützten IT-Umgebung zum Einsatz kommen. Die Hauptintention ist das Herstellen von Vertraulichkeit für dedizierte lokale Daten.

Fahrlässiger Umgang aufgrund vermeintlicher Sicherheit

Die in G 2.19 *Unzureichendes Schlüsselmanagement bei Verschlüsselung* genannten Gefährdungen können in vielfältiger Art und Weise dazu führen, dass EFS-Zertifikate, welches zur Ver- und Entschlüsselung verwendet werden, offen gelegt werden oder abhanden kommen. Auf einem Dateiserver, wären dann große Datenmengen nicht mehr vertraulich oder nicht mehr verfügbar, was im Vergleich zu einem einzelnen Client fatal sein kann. Auf einem Server spielt auch G 2.116 *Datenverlust beim Kopieren oder Verschieben von Daten unter Windows Server 2003* eine erhebliche Rolle und kann zum Verlust oder zur Beschädigung größerer Datenmengen führen. Wenn Administratoren sich solcher Effekte und den komplexen Anforderungen nicht ausreichend bewusst sind, kann die durch Aktivierung des EFS beabsichtigte höhere Sicherheit leicht verloren gehen. Kommt aufgrund der vermeintlichen Sicherheit noch eine gewisse Fahrlässigkeit bei Benutzern und Administratoren hinzu, sind kritische Daten sogar stärker bedroht als vor der Aktivierung des EFS. Im Folgenden werden einige Teilaspekte genauer erläutert.

Zugriff des Administrators

Mit EFS ist es nicht möglich, die Vertraulichkeit von verschlüsselten Daten auf Remote-Servern gegenüber Administratoren zu garantieren. Der Administrator kann sich jederzeit die Möglichkeit verschaffen, mittels Berechtigungen und dem integrierten Wiederherstellungsverfahren auf verschlüsselte Daten zuzugreifen.

Kein Schutz vor Schadsoftware oder Administrationsfehlern

EFS ist vollständig transparent für den Benutzer und die Anwendungen. Das bedeutet, dass jeder Prozess und jede Anwendung, die im Kontext des Benutzers ausgeführt wird, Zugriff auf die verschlüsselten Dateien hat. EFS stellt somit keinen Schutz vor Schadsoftware wie Trojanischen Pferden und Viren dar. EFS ersetzt nicht die sorgfältige Administration der Zugriffsberechtigungen (*Access Control Lists*, ACL) des NTFS. Verschlüsselte Dateien können von Benutzern oder Anwendungen unabhängig vom Schutz durch EFS gelöscht werden, wenn sie über dafür ausreichende NTFS-Berechtigungen verfügen.

Unbemerkte Entschlüsselung beim Speichern in andere Dateisysteme

Die Transparenz geht soweit, dass Benutzer im Allgemeinen nicht mitbekommen, ob Daten ver- oder entschlüsselt sind. Eine Verschlüsselung liegt aber tatsächlich nur auf NTFS-formatierten Datenträgern vor. Beim Kopieren/Verschieben auf Speichermedien mit anderen Dateisystemen werden die Dateien unverschlüsselt abgespeichert.

Fehlende Kontrolle über EFS-Zertifikate

Fehlen eines zentralen Schlüsselmanagements

EFS erfordert ein definiertes zentrales Schlüsselmanagement. Ohne den Einsatz einer *Public Key Infrastructure* (PKI) werden selbstsignierte

Zertifikate des lokalen Computers (Client oder Server) benutzt. Damit stellt EFS ein nicht unerhebliches Risiko dar, durch Schlüsselverlust den Zugriff auf die verschlüsselten Dateien zu verlieren.

Werden von einem Client aus Daten mittels EFS auf einem Server verschlüsselt, der Mitglied in einer Domäne ist, muss dieser Server im Namen des Client-Benutzers ein EFS-Zertifikat anfordern. Das ist nur möglich, wenn dem Domänenkonto des Servers erweiterte Berechtigungen eingeräumt werden. So wird dem Serverobjekt innerhalb der Domäne für Delegierungszwecke vertraut. Diese "Stellvertretung" und das "Vertrauen" lassen sich mit dem Kerberos-Protokoll realisieren, designbedingt wird dadurch allerdings die Sicherheit der Kerberos-Umgebung verringert. Im Falle einer Kompromittierung des vertrauten Servers kann der Angreifer Einfluss auf benutzerspezifische Daten nehmen. Sind die Einstellungen zum Vertrauen nicht korrekt konfiguriert und auf EFS-relevante Dienste beschränkt, ergeben sich auch Manipulationsmöglichkeiten in anderen Bereichen des Servers oder der Domäne.

Außerdem erschwert das Prinzip der Erzeugung von EFS-Zertifikaten auf dem Remote-Server bzw. im Active Directory das Verwalten und Schützen des Schlüsselmaterials.

Nutzung des EFS-API

Fehlende Unterstützung für EFS-API

Greift eine Anwendung auf verschlüsselte Dateien zu, welche für mehrere Benutzer verschlüsselt wurden, muss die Anwendung das entsprechende Application Programming Interface (API) von Windows Server 2003/Windows XP unterstützen. Anderenfalls werden die Schlüssel der zusätzlichen Benutzer von den Dateien entfernt. Kein Benutzer außer dem ursprünglichen Erzeuger hat dann noch Zugriff auf die jeweilige Datei. Microsoft Office XP oder höher benutzt das korrekte API. Sicherungs-, Archiv- und Synchronisierungs-Tools von Drittherstellern bergen ähnliche Risiken, sobald sie zur Verarbeitung verschlüsselter Dateien zum Einsatz kommen.

G 4.55 Datenverlust beim Zurücksetzen des Kennworts in Windows Server 2003/XP

Sicherungskopie für private Schlüssel nötig.

Windows Server 2003 schützt wie Windows XP die privaten Schlüssel lokaler Benutzerkonten vor der Verwendung durch Administratoren. "Lokales Benutzerkonto" bedeutet, dass Benutzername und Kennwort des Kontos nur auf dem jeweiligen Computer existieren und verwendet werden können. In früheren Windows-Versionen konnte ein Administrator das Kennwort eines lokalen Benutzerkontos zurücksetzen und anschließend die privaten Schlüssel des Benutzers verwenden und exportieren. Ab Windows Server 2003/XP löscht das Krypto-API alle für ein solches Benutzerkonto gespeicherten privaten Schlüssel, sobald das Kennwort durch einen Administrator zurückgesetzt wird. Durch dieses Verhalten ist es möglich, höchstvertrauliche Informationen selbst vor Administratoren zu verbergen. Jedoch sind nach dem Zurücksetzen durch einen Administrator alle privaten Schlüssel verloren, wenn keine Sicherungskopie erstellt wurde. Verschlüsselte Daten in E-Mails und Dateien sind dann nicht mehr verfügbar.

Wiederherstellungs-agent

Dieses Verhalten kann auf Windows-Server-2003-Systemen zum Verlust des privaten Schlüssels des Wiederherstellungsagenten für das Encrypting File System (EFS) führen, wenn der Wiederherstellungsagent einem lokalen Benutzerkonto zugewiesen wurde. In diesem Fall ist ein Wiederherstellungsagent konfiguriert. Da aber kein Zugang zu seinen Schlüsseln möglich ist, kommt dieses Szenario einem nicht vorhandenen Wiederherstellungsagenten gleich. Die Daten der Benutzer, die ihren eigenen Schlüssel nicht mehr nutzen können, wären in diesem Fall verloren.

G 4.56 Ausfall der VoIP-Architektur

VoIP kann als Alternative zu einer leitungsvermittelnden TK-Anlage eingesetzt werden. Alle Gespräche, also alle eingehenden, ausgehenden und internen Telefonate, können vollständig über VoIP abgewickelt werden. Es kann sowohl das bestehende, als auch ein hierfür separat betriebenes Datennetz für die Kommunikation genutzt werden.

Kein LAN, kein Telefon

Ein IP-Netz besteht aus aktiver und passiver Netztechnik. Unter passiver Netztechnik wird in erster Linie die strukturierte Verkabelung verstanden. Zur aktiven Netztechnik gehören beispielsweise Hubs, Bridges, Switches und Router. Ein Ausfall einer oder mehrerer Komponenten der aktiven Netztechnik kann zum kompletten Stillstand des gesamten IT-Netzes führen. In einem solchen Fall ist die VoIP-Architektur ebenfalls nicht mehr nutzbar, wenn sie über dasselbe IT-Netz abgewickelt wird.

Angriffe auf tiefere Netz-Schichten

Hat ein Angreifer direkten Zugang zum LAN, beispielsweise durch Anschluss an einen Switch oder über ein drahtloses Netz, kann er unter Umständen bestehende Verbindungen beenden. Ein Beispiel hierfür ist eine mit dem Session Initiation Protocol (SIP) oder H.323 initiierte TCP-Verbindung, die mit einem IP-Paket mit gesetztem RST-Flag beendet wird.

Durch Techniken wie Flooding könnte ein Angreifer das Datennetz überlasten. Dies betrifft jedoch nicht nur VoIP-Architekturen. Praktisch jeder Nachrichtenstrom kann auf diese Weise gestört werden.

Middleware

Der Betrieb der VoIP-Architektur erfordert in der Regel den Einsatz von Komponenten für die Vermittlung der Telefonate. Beispiele hierfür sind H.323-Gatekeeper und SIP-Registrare. Diese VoIP-Middleware kann auf separaten IT-Systemen oder dedizierten Hardware-Elementen betrieben werden. Die Integration dieser Geräte in IT-Netze führt zu neuen Bedrohungen, verglichen mit leitungsvermittelnden TK-Anlagen, die eine eigene Kabelinfrastruktur voraussetzen. So könnten VoIP-Komponenten über das IP-Netz beispielsweise durch Würmer kompromittiert werden und dadurch ausfallen.

Um VoIP nutzen zu können, müssen sich die Benutzer in der Regel an einem entsprechenden System, beispielsweise einem Registrar bei SIP oder einem Gatekeeper bei H.323, anmelden. Ohne entsprechende Sicherheitsmechanismen kann ein Angreifer einen Benutzer durch gefälschte Pakete wieder abmelden (De-Registration). Dies hat zur Folge, dass dieser Benutzer nicht mehr telefonisch erreichbar ist.

Die Vermittlungseinheiten sind ein besonders attraktives Ziel für Angriffe, da beim Ausfall eines solchen Systems zahlreiche Benutzer nicht mehr telefonieren können. Hat ein Angreifer beispielsweise physischen Zugriff auf eine Vermittlungseinheit, kann er diese zentrale Architektur manipulieren, beschädigen oder einfach ausschalten. Aber auch durch logische Angriffe auf Vermittlungseinheiten, zum Beispiel durch Zurücksetzen von Netzverbindungen oder Löschen wichtiger Systemdateien, können unter Umständen hohe Schäden entstehen.

Endgeräte

Diese erhöhte Gefährdungslage gilt auch für VoIP-Endgeräte. Für Angriffe auf vernetzte IT-Systeme, deren Gefährdungslage den VoIP-Geräten ähnlich ist, wurden viele Werkzeuge entwickelt. Diese Programme können häufig

auch von weniger erfahrenen Angreifern eingesetzt werden. Durch eine Auswertung verschiedener Netzparameter, wie die Antwort auf bestimmte IP-Pakete, kann bei einigen Geräten die genaue Typbezeichnung des Endgeräts ermittelt werden. Diese Informationen können für zielgerichtete Angriffe verwendet werden.

Sowohl die VoIP-Endgeräte als auch die Middleware besitzen einen hohen Software-Anteil. Es besteht daher das Risiko, dass diese Software Schwachstellen besitzt, die von Angreifern ausgenutzt werden können. VoIP-Geräte können deshalb auch anfällig für Schadsoftware, beispielsweise für Computer-Viren oder -Würmer, sein.

Ausfall der Stromversorgung

Die Verfügbarkeit kann außerdem durch unvorhergesehene Ereignisse beeinträchtigt werden. Telefone für leitungsvermittelnde Netze erhalten ihre Betriebsspannung häufig direkt über das Telefonnetz. Wird eine TK-Anlage für leitungsvermittelnde Netze mit einer lokalen USV bei einem Stromausfall versorgt, können die Endgeräte weiterhin ihre Betriebsspannung hierüber beziehen. VoIP-Endgeräte beziehen ihre Stromversorgung hingegen in der Regel nicht vom IT-Netz, sondern separat. Auch wenn die VoIP-Anlage über eine USV versorgt wird, können die Endgeräte bei einem Stromausfall nicht verwendet werden. Hinzu kommt, dass auch ein Ausfall der aktiven Netztechnik dazu führt, dass das Datennetz nicht funktionsbereit ist und somit keine VoIP-Telefonate mehr möglich sind.

G 4.57 Störungen beim Einsatz von VoIP über VPNs

Für ein Telefonat über VoIP werden sowohl die Signalisierungsinformationen als auch der eigentliche Medienstrom über ein Datennetz gesendet. Für die Transportsicherung dieser Daten auf Protokollebene gibt es Schutzmechanismen, die jedoch nicht von allen Herstellern und Geräten unterstützt werden. Das Verfahren zum Schutz der eigentlichen Sprachkommunikation wird in der Regel von den Endgeräten ausgehandelt. Hierfür kann beispielsweise das Secure Realtime Transport Protocol (SRTP) verwendet werden.

Unterstützen nicht alle Geräte verschlüsselte Protokolle und sollen Gespräche über unsichere Netze übertragen werden, können Virtual Private Networks (VPNs) diesen Schutz gewährleisten. VPNs werden in der Praxis zur Einbindung von einzelnen Mitarbeitern oder zum Zusammenschluss ganzer Netze über ein öffentliches Netz genutzt. Beim Einsatz von VPNs werden ausgewählte oder alle Pakete von einem VPN-Gateway verschlüsselt und je nach Routingtabelle an ein entferntes VPN-Gateway übermittelt. Dieses entschlüsselt das Paket und übermittelt es an den Empfänger. Dadurch wird außerdem erreicht, dass sich Sender und Empfänger im gleichen Subnetz befinden, obwohl sie mehrere hundert Kilometer voneinander entfernt sein können.

Durch den Einsatz eines VPNs können sowohl der Signalisierungs- und Medienstrom von VoIP als auch alle weiteren Informationen, wie beispielsweise E-Mails, geschützt werden. Einige Hardphones unterstützen VPNs direkt. Wird ein verschlüsseltes Medientransportprotokoll, wie zum Beispiel SRTP, verwendet, ist es ausreichend, wenn nur der Signalisierungsstrom durch das VPN geschützt wird.

Der Einsatz von VPNs in Verbindung mit VoIP führt jedoch häufig zu Problemen.

Priorisierung von VoIP

Bei Netzen, die neben VoIP-Daten auch andere Informationen übertragen, werden an den Routern und Switches oft VoIP-Nachrichten bevorzugt weitergeleitet. Durch dieses Vorgehen sollen Qualitätsstörungen, wie Aussetzer oder Jitter, vermieden werden. Obwohl hierfür bei IPv4 ein eigenes Feld im IP-Header vorgesehen ist (Type of Service), wird es in der Praxis häufig nicht verwendet. Stattdessen priorisieren die Router die Pakete an Hand ihres Inhalts. Bei einer Verschlüsselung des Inhalts ist dies aber nicht mehr möglich. Als Folge kann es bei der Übertragung von VoIP über VPNs vermehrt zu Störungen der Übertragungsqualität kommen, wenn das Netz zu stark ausgelastet ist.

NAT

Die Verwendung von Hiding NAT (Network Adress Translation oder Masquerading) kann ebenfalls zu Problemen führen. Im Gegensatz zu statischen NAT wird nicht jeder internen IP-Adresse genau eine öffentliche IP-Adresse zugeordnet, sondern mehrere interne Adressen können eine öffentliche IP-Adresse parallel nutzen. Für dieses Verfahren müssen nicht nur die internen IP-Adressen, sondern auch die Portnummern im IP-Paket durch das NAT-Gateway geändert werden. Diese Änderungen führen dazu, dass die vom VPN-Gateway erzeugte Prüfsumme nicht mehr zu dem neuen Paket passt. Wird die gesamte IP-Nutzlast verschlüsselt, kann dies auch zu Problemen führen.

Pakete, die zur Übermittlung von VoIP-Inhalten genutzt werden, sind meist sehr klein. Würde mit der Übermittlung gewartet werden, bis sich eine bestimmte Anzahl von Bytes angesammelt haben, könnte eine zu große Verzögerung bei der Übertragung entstehen. So ist die eigentliche Nutzlast der IP-Pakete in der Regel zwischen 10 und 40 Bytes groß. Sollen die IP-Pakete durch ein VPN geschützt werden, kommt zusätzlich ein VPN-Header hinzu. Bei IP-Paketen mit einem geringen Umfang stellen die hinzukommenden VPN-Informationen einen signifikanten Overhead dar. Als Folge ergibt sich durch die Aktivierung der VPN-Absicherung eine deutliche Erhöhung des VoIP-Datenaufkommens. Dies kann zu einer Überlastung des LANs oder des WANs führen.

Auch die Ver- und Entschlüsselung der übertragenen Informationen benötigen Ressourcen. Ist das System, dass die Ver- oder Entschlüsselung vornimmt, schwach dimensioniert, kann an dieser Stelle ebenfalls eine Verzögerung in der Übertragung auftreten. Eine solche Erhöhung der Latenzzeit kann zu Aussetzern oder anderen Qualitätsproblemen führen.

Viele Verschlüsselungsarchitekturen für VPN nutzen X.509-Zertifikate oder Preshared Secrets. Besonders für die zertifikatsbasierte Lösung setzen viele Hersteller derzeit auf proprietäre Ansätze, die untereinander nicht kompatibel sind. Wenn VoIP-Verbindungen zu externen Partnern aufgebaut werden sollen, kann mit diesen daher nicht oder nicht verschlüsselt telefoniert werden.

G 4.58 Schwachstellen beim Einsatz von VoIP-Endgeräten

Bei VoIP-Endgeräten werden zwei Arten unterschieden: Hardphones und Softphones. Hardphones sind eigenständige Geräte mit meistens proprietären Betriebssystemen, die direkt an das IP-Netz angeschlossen werden. Einige Hardphones laden ihre aktuelle Konfiguration über das TFTP-Protokoll.

Softphones sind auf dem Computer installierte Anwendungsprogramme, deren Funktionalität der eines Hardphones entspricht. Für den Zugang zum IP-Netz benutzen Softphones die Schnittstelle des Computers, die sie mit anderen installierten Anwendungen teilen.

Alle VoIP-Endgeräte bieten im Wesentlichen ähnliche Funktionen an, die von Programmen mit Schadensfunktionen beeinträchtigt werden können. Das Bedrohungsspektrum erstreckt sich dabei von der partiellen Beeinträchtigung des Normalbetriebs bis zu einer vollständigen Übernahme der Kontrolle über das Gerät durch den Angreifer.

Bei mangelhaften Sicherheitsvorkehrungen kann es zur Ausbreitung von Schadsoftware, wie Trojanischen Pferden, kommen. Trojanische Pferde könnten bei der VoIP-Nutzung beispielsweise benutzt werden, um private Informationen eines Teilnehmers oder Gesprächsinhalte während des Gesprächs an einen Angreifer zu übermitteln.

Schadprogramme könnten auch versuchen, Anrufe ohne Wissen des Anwenders zu initiieren oder Informationen über die geführten Telefonate sowie private Telefonnummern aus dem Adressbuch zu ermitteln und weiterzuleiten.

Wird ein Anruf vom Anwender initiiert, so bauen Geräte die Verbindung gemäß der eingestellten Konfiguration und der gewählten Telefonnummer auf. Manipulationen an der Konfiguration oder Firmware des Geräts können zur Störung des Anwahlprozesses oder sogar zur Umleitung des Gesprächs über die Angreiferinfrastruktur führen. Damit kann der Angreifer das darauf folgende Gespräch unter Umständen auch abhören.

Beendet der Anrufer das Gespräch, so könnte ein infiziertes Gerät die Signalisierung des Gesprächsendes vortäuschen, während die Verbindung im Hintergrund aufrecht erhalten wird. Diese Verbindung könnte zum Abhören des Benutzers genutzt werden. Ist ein Gerät von Schadsoftware befallen, so könnte diese möglicherweise auch die Signalisierung von ankommenden Anrufen unterdrücken, ohne dass der Angerufene es merkt. Dies hätte zur Folge, dass der Benutzer nicht mehr angerufen werden kann.

Eine weitere potentielle Angriffsvariante durch Schadsoftware besteht darin, das Mikrofon eines VoIP-Endgerätes unbemerkt zu aktivieren, um die Gespräche im Raum aufzuzeichnen und per VoIP an den Angreifer zu übermitteln. Der Aufwand zur Programmierung einer entsprechenden Schadsoftware mit einer solchen Funktionalität ist dabei relativ gering, weil die benötigte VoIP-Funktionalität (Codec, VoIP-Protokolle) bereits auf den Endgeräten implementiert ist und von der Schadsoftware genutzt werden kann.

In welchem Maße die beschriebenen Risiken tatsächlich bei einem Gerät auftreten, hängt von mehreren Faktoren ab, wie z. B. Art und Einstellungen des Betriebssystems, Verwendung von gemeinsamen Ressourcen mit anderen

Anwendungen (z. B. bei Softphones), und implementierten Schutzmechanismen.

Generell lässt sich sagen, dass Softphones für Angriffe von Programmen mit Schadensfunktionen anfälliger sind als Hardphones, weil Softphones meist auf weit verbreiteten Betriebssystemen basieren und Ressourcen mit anderen installierten Anwendungen teilen, die eigene Sicherheitslücken haben können. Dagegen haben Hardphones eine eigene Netzschnittstelle und basieren meist auf proprietären Betriebssystemen, deren Einstellungen auf die geforderte Funktionalität zugeschnitten sind. Somit können sie in der Regel nur den Angriffen von schädlichen Programmen ausgesetzt werden, die speziell für solche Betriebssysteme entwickelt worden sind.

G 4.59 Nicht-Erreichbarkeit bei VoIP durch NAT

Über seine IP-Adresse kann ein Rechner im Internet eindeutig angesprochen werden. Bei dem zur Zeit hauptsächlich verwendeten Internet Protocol in der Version 4 (IPv4) setzt sich die IP-Adresse aus vier Zahlen zwischen 0 und 255 zusammen, also zum Beispiel 194.95.176.226. Bei dem neueren Internet Protocol in der Version 6 (IPv6) besteht eine IP-Adresse aus acht vierstelligen hexadezimalen Zahlen, wie FEDC:BA98:7654:3210:FEDC:BA98:7654:3210. Ein großer Nachteil der Version 4 gegenüber der Version 6, die sich bisher noch nicht durchgesetzt hat, ist die geringe Anzahl von verfügbaren öffentlichen IP-Adressen. Nur sehr wenige Institutionen erhalten genug IP-Adressen, um jedem Arbeitsplatzrechner eine eigene, statische IP-Adresse zuweisen zu können. Durch Network Address Translation (NAT) kann dieses Problem behoben werden. Dabei benötigt nur das System, das sich zwischen dem öffentlichen und dem privaten Netz befindet, eine oder wenige öffentliche IP-Adressen. Die eigentlichen Arbeitsplatzrechner erhalten interne IP-Adressen, wobei von einer aktiven Netzkomponente (meistens ein NAT-Gateway) bei der Weiterleitung eines Paketes die interne in eine externe IP-Adresse umgewandelt wird.

Für den Medienstrom, der für die Übertragung der Sprachinformation benötigt wird, muss eine neue UDP- bzw. TCP-Verbindung aufgebaut werden. Die hierfür benötigten IP-Adressen und Portnummern werden in den Signalisierungsnachrichten übertragen. Durch NAT werden im UDP- bzw. TCP-Header des Medienstroms die Quell-IP-Adresse im IP-Header und die Quellportnummer modifiziert. Die Angaben über die Quell-IP-Adresse und die Portnummer im Nachrichtenteil der Signalisierungsnachricht bleiben unverändert.

In Folge können keine Medienströme an das VoIP-Telefon, das sich hinter einem NAT-Gateway befindet, gesendet werden. VoIP-Geräte, die sich im Internet befinden, können keinen Medienstrom zu einem hinter einem NAT-Gateway befindlichen VoIP-Telefon senden, da die private IP-Adresse nicht im Internet geroutet wird. Eine Sprachkommunikation ist somit zu VoIP-Geräten, die sich hinter einem NAT-Gateway befinden, weil eine sicherheitskritische Konfiguration erreicht werden soll, nicht möglich, obwohl bei der Signalisierung keine Fehler aufgetreten sind.

Eine Ausnahme bilden Protokolle wie beispielsweise IAX (InterAsterisk eXchange) oder Skype. Bei diesen Protokollen findet sowohl die Signalisierung als auch der Medientransport über eine bestehende Verbindung statt. Da keine zusätzlichen Verbindungen zu den Rechnern im privaten Netz aufgebaut werden müssen, treten die beschriebenen Probleme mit NAT bei dem Einsatz dieser Protokolle nicht auf. Da hiermit aber auch keine Kontrolle am Netzübergang mehr stattfindet, können dadurch andere Sicherheitsprobleme entstehen.

Um eine VoIP-Kommunikation über ein NAT-Gateway hinweg zu ermöglichen, kann der Medienstrom des NAT-Gateways zu den VoIP-Geräten statisch weitergeleitet werden. Dieser Lösungsansatz ist oft bei der Anbindung privater Kunden an SIP-Providern zu finden. Dies kann allerdings zu Problemen führen. Hier baut der Sender, der sich außerhalb des LANs befindet, eine Verbindung zu dem NAT-Gateway über eine reservierte Portnummer auf. Das NAT-Gateway leitet diese zu einem Endgerät, das der Portnummer zugeordnet

ist, weiter. Dies setzt voraus, dass die Gesprächsteilnehmer die reservierten Portnummern kennen. Gravierender ist der Nachteil, dass auf die weitergeleiteten Ports der VoIP-Systeme hinter dem NAT-Gateway aus dem öffentlichen Datennetz zugegriffen werden kann.

G 4.60 Unkontrollierte Ausbreitung der Funkwellen

Funknetze bzw. die ausgesendeten Funkwellen überschreiten nicht selten die Grenzen der selbstgenutzten Räumlichkeiten, so dass Daten auch noch in Bereiche übertragen werden, die nicht vom Benutzer oder einer Institution kontrolliert und gesichert werden können. Eine Aufzeichnung ist somit ohne viel Aufwand möglich und die Entdeckung solcher Lauschangriffe wird nur bei einem Bruchteil der Fälle erfolgen. Ziel solcher Angriffe kann es sein, sensitive Informationen zu erlangen oder zu manipulieren. Selbst wenn die Daten verschlüsselt übertragen werden, reicht es durch den unzureichenden Schutz vieler drahtloser Netze häufig aus, eine Zeitlang den Funkverkehr aufzuzeichnen und auszuwerten, um anschließend mit den gesammelten Daten die kryptographischen Schlüssel berechnen zu können und so die übertragenen Daten zu entschlüsseln. Durch den Einsatz von Richtantennen könnten zudem auch außerhalb der eigentlichen Nutzreichweite des Funknetzes Daten empfangen und abgehört werden.

Beispiel:

Ein Laptop mit WLAN-Karte zusammen mit einigen frei verfügbaren WLAN-Applikationen reicht aus, um nach schlecht gesicherten WLANs zu suchen. Beim Wardriving wird beispielsweise mit einem WLAN-Client eine bestimmte Region, ein Stadtviertel oder typische Büroumgebung abgefahren und dabei aufgezeichnet, wo sich welche WLANs melden und wie schlecht diese gesichert sind. Dabei können diese Daten auch direkt mit GPS-Daten verknüpft werden, um die geographische Position der gefundenen WLANs festhalten zu können. Anschließend können schlecht gesicherte WLANs gezielt angegriffen werden, z. B. um darüber kostenlos auf das Internet zugreifen zu können.

G 4.61 Unzuverlässige oder fehlende WLAN-Sicherheitsmechanismen

Im Auslieferungszustand sind die WLAN-Komponenten häufig so konfiguriert, dass keine oder nur einige Sicherheitsmechanismen aktiviert sind. Einige der Mechanismen sind darüber hinaus unzuverlässig und bieten keinen ausreichenden Schutz. Auch heute noch sind diverse WLAN-Komponenten im Einsatz bzw. als Neugeräte am Markt verfügbar, die lediglich unzureichende Sicherheitsmechanismen wie z. B. WEP unterstützen. Teilweise können diese Geräte nicht einmal auf stärkere Sicherheitsmechanismen aufgerüstet werden.

Können keine oder nur schwache Mechanismen genutzt werden, mit denen sich die Funkschnittstelle bzw. die über das WLAN genutzten Dienste angemessen absichern lassen, ist keine sichere Kommunikation im WLAN möglich. Hierdurch ergeben sich weitere Gefahren für alle damit gekoppelten Komponenten, also z. B. alle auf einem WLAN-Client gespeicherten Daten oder ein LAN, was die gesamte IT-Infrastruktur einer Behörde oder eines Unternehmens beeinträchtigen kann. Im Folgenden werden mögliche Sicherheitsprobleme exemplarisch aufgeführt.

WEP

Wird die Funkübertragung im WLAN gar nicht oder nur mit WEP geschützt, kann ein Angreifer leicht die gesamte WLAN-Kommunikation abhören und damit nicht selten in den Besitz vertraulicher Informationen gelangen. Beim Einsatz einiger Geräte wie WLAN-fähigen Druckern wird vielfach nicht wahrgenommen, dass hiermit ein WLAN aufgebaut wird und dieses somit auch nicht adäquat abgesichert. Ein Angreifer könnte aber eventuell nicht nur die gedruckten Daten abhören, sondern über die WLAN-Komponente auf Hintergrundsysteme zugreifen.

SSID Broadcast

Bei der Übergabe zwischen zwei benachbarten Funkzellen dient die SSID (Service Set Identifier oder Netzname) dazu, den nächsten Access Point zu finden. Einige Access Points bieten die Möglichkeit, das Senden der SSID im Broadcast zu unterbinden, um das WLAN vor Unbefugten zu verstecken (so genanntes "Closed System"). Allerdings kann mittels WLAN-Analysatoren auch in diesem Falle die SSID aus anderen Management- und Steuersignalen ermittelt werden.

Manipulierbare MAC-Adressen

Jede Netzkarte verfügt über eine eindeutige Hardware-Adresse, die sogenannte MAC-Adresse (Media Access Control-Adresse). Die MAC-Adressen der WLAN-Clients können relativ einfach abgehört und manipuliert werden, somit sind die in den Access Points zum Zweck des Zugriffsschutzes häufig eingebauten MAC-Adressfilter überwindbar.

Fehlendes Schlüsselmanagement

Kryptographische Schlüssel müssen in vielen WLANs manuell verteilt werden, d. h. in jedem WLAN-Client und Access Point muss der gleiche statische Schlüssel eingetragen werden. Dies erfordert physischen Zugriff auf die Komponenten. Diese Art des Schlüsselmanagements führt in der Praxis oft dazu,

dass die kryptographischen Schlüssel sehr selten oder überhaupt nicht gewechselt werden. Wenn dann ein WLAN-Schlüssel offengelegt wird, wird das gesamte WLAN kompromittiert.

Schwachstellen beim administrativen Zugriff auf Access Points

Viele Access Points bieten unterschiedliche Schnittstellen und Protokolle zur Administration an und erlauben es, diese sowohl über die LAN-, als auch über die Funkschnittstelle zu verwenden. Erfolgt die Administration über die Funkschnittstelle über Klartext-Protokolle, wie Telnet, HTTP oder SNMP, können die über das WLAN übertragenen Administrationspasswörter mitgelesen werden. Angreifer könnten diese Informationen zum Umkonfigurieren des Access Points nutzen.

Verschlüsselte Varianten der genannten Zugriffsprotokolle werden häufig auf der Access-Point-Seite nicht unterstützt bzw. nicht erzwungen.

G 4.62 Verwendung unzureichender Steckdosenleisten

Oft reicht die Zahl fest installierter Steckdosen für die Menge der zu betreibenden Geräte nicht aus. Um diesen Mangel auszugleichen, werden dann typischerweise Steckdosenleisten verwendet. Solche Steckdosenleisten stellen, wenn sie von unzureichender Qualität sind, auf Grund

- mangelhafter Kontaktierung
- zu schwacher Kontaktfedern
- fehlender Zugentlastung
- zu geringen Leitungsquerschnitts
- von Überlastung

eine gefährliche Zündquelle und damit große Brandgefahr dar.

Werden zusätzlich mehrere kleinere Steckdosenleisten hintereinander geschaltet, um ausreichende Steckplätze für alle Geräte bereitzustellen, steigt die Gefahr durch zu geringen Leitungsquerschnitt und Überlastung weiter an.

Liegen Steckdosenleisten im Fußraum von Arbeitsplätzen, sind sie häufigen mechanischen Belastungen durch Gegentreten, Staubsaugen etc. ausgesetzt. Dadurch können fehlende Zugentlastungen und schwache Kontakte rasch zu Übergangswiderständen, Überhitzungen und schließlich zum Brand führen. Darüber hinaus sind solche frei ausliegenden Steckdosenleisten gefährliche Fußangeln.

G 4.63 Verstaubte Lüfter

IT-Geräte sollen, wie alle anderen elektrischen Geräte auch, nur innerhalb einer vom Hersteller festgelegten Temperaturspanne betrieben werden. Die Einhaltung der Minimaltemperatur stellt in der Regel keine besonderen Anforderungen. Hingegen müssen meist zusätzliche Einrichtungen betrieben werden, um die Maximaltemperatur einhalten zu können. Den meisten dieser Einrichtungen ist gemeinsam, dass die überschüssige Wärme mittels Lüftern abgeführt wird.

Es befindet sich immer ein gewisser Staubanteil in der Umgebungsluft, auch in der Raumluft von normalen Büroräumen oder Serverräumen. Da sich dieser zum Teil an Lüftern absetzt, bilden sich dort mit der Zeit meist ansehnliche Staubpolster. Diese Staubansammlungen können

- den Luftdurchsatz und damit die Kühlwirkung der Lüfter so weit reduzieren, dass Geräte überhitzen und ausfallen oder (vornehmlich bei Netzteilen) sich entzünden.
- den freien Lauf des Lüfters bremsen oder komplett unterbinden, wodurch der nun blockierte Lüftermotor selbst überhitzt und zur Zündquelle wird.

G 5 Gefährdungskatalog Vorsätzliche Handlungen

G 5.1 Manipulation/Zerstörung von IT-Geräten oder Zubehör

unterschiedliche Motive

Außentäter, aber auch Innentäter, können aus unterschiedlichen Beweggründen (Rache, Böswilligkeit, Frust) heraus versuchen, IT-Geräte, Zubehör, Schriftstücke oder ähnliches zu manipulieren oder zu zerstören. Die Manipulationen können dabei umso wirkungsvoller sein, je später sie entdeckt werden, je umfassender die Kenntnisse des Täters sind und je tief greifender die Auswirkungen auf einen Arbeitsvorgang sind. Die Auswirkungen reichen von der unerlaubten Einsichtnahme in schützenswerte Daten bis hin zur Zerstörung von Datenträgern oder IT-Systemen, die erhebliche Ausfallzeiten nach sich ziehen können.

Beispiel:

- In einem Unternehmen nutzte ein Innentäter seine Kenntnis darüber, dass ein wichtiger Server empfindlich auf zu hohe Betriebstemperaturen reagiert, und blockierte die Lüftungsschlitze für den Netzteillüfter mit einem hinter dem Server aufgestellten Gegenstand. Zwei Tage später erlitt die Festplatte im Server einen temperaturbedingten Defekt und der Server fiel für mehrere Tage aus. Hinterher behauptete der Angreifer, dass es sich um ein Versehen handelte.
- Ein Mitarbeiter hat sich über das erneute Abstürzen des Systems so stark geärgert, dass er seine Wut an seinem Arbeitsplatzrechner ausließ. Hierbei wurde durch Fußtritte gegen den Rechner die Festplatte so stark beschädigt, dass sie unbrauchbar wurde. Die hier gespeicherten Daten konnten nur teilweise wieder durch ein entsprechendes Backup vom Vortag rekonstruiert werden.

G 5.2 Manipulation an Daten oder Software

Daten oder Software können auf vielfältige Weise manipuliert werden: durch falsches Erfassen von Daten, Änderungen von Zugriffsrechten, inhaltliche Änderung von Abrechnungsdaten oder von Schriftverkehr, Änderungen in der Betriebssystemsoftware und vieles mehr. Ein Täter kann allerdings nur die Daten und Software manipulieren, auf die er Zugriff hat. Je mehr Zugriffsrechte eine Person besitzt, desto schwerwiegendere Manipulationen kann sie vornehmen. Falls die Manipulationen nicht frühzeitig erkannt werden, kann der reibungslose IT-Einsatz empfindlich gestört werden.

unterschiedliche Motive

Manipulationen an Daten oder Software können aus Rachegefühlen, um einen Schaden mutwillig zu erzeugen, zur Verschaffung persönlicher Vorteile oder zur Bereicherung vorgenommen werden.

Beispiele:

- 1993 wurde in einem schweizer Finanzunternehmen durch einen Mitarbeiter die Einsatzsoftware für bestimmte Finanzdienstleistungen manipuliert. Damit war es ihm möglich, sich illegal größere Geldbeträge zu verschaffen.
- Sehr häufig werden Kundendatenbanken von Mitarbeitern beim Verlassen der Firma kopiert. Auch das mutwillige Zerstören von Datenbanken oder die Erpressung mit der Zerstörung stellen ein Risiko dar.
- Archivierte Dokumente stellen meist besonders schützenswerte Daten dar. Die Manipulation solcher Dokumente ist besonders schwerwiegend, da sie unter Umständen erst nach Jahren bemerkt wird und eine Überprüfung dann oft nicht mehr möglich ist.
- Eine Mitarbeiterin hat sich über die Höhergruppierung ihrer Zimmergenossin in der Buchhaltung dermaßen geärgert, dass sie sich während einer kurzen Abwesenheit der Kollegin aus dem Zimmer Zugang zu deren Rechner verschafft hat. Hier hat sie durch einige Zahlenänderungen in der Monatsbilanz enormen negativen Einfluss auf das Jahresergebnis des Unternehmens nehmen können.

G 5.3 Unbefugtes Eindringen in ein Gebäude

Das unbefugte Eindringen in ein Gebäude geht verschiedenen Gefährdungen der IT wie Diebstahl oder Manipulation voraus. Maßnahmen, die dagegen gerichtet sind, wirken dadurch auch gegen die entsprechenden Folgegefährdungen. Bei qualifizierten Angriffen versierter Täter ist die Zeitdauer entscheidend, in der die Täter ungestört ihr Ziel verfolgen können. Ziel eines Einbruchs kann der Diebstahl von IT-Komponenten oder anderer leicht veräußerbarer Ware sein, aber auch das Kopieren oder die Manipulation von Daten oder IT-Systemen. Dabei können nicht offensichtliche Manipulationen weit höhere Schäden als direkte Zerstörungsakte verursachen.

Schon durch das unbefugte Eindringen können Sachschäden entstehen. Fenster und Türen werden gewaltsam geöffnet und dabei beschädigt, sie müssen repariert oder ersetzt werden.

Beispiele:

- Bei einem nächtlichen Einbruch in ein Bürogebäude konnten die Täter keine lohnende Beute machen. Aus Frustration darüber leerten sie die Pulverlöscher in die Büroräume. Der Einbruchschaden war gering, der Vandalismusschaden dagegen durch die Reinigungskosten und Arbeitsunterbrechungen unverhältnismäßig hoch. **Vandalismus**
- Bei einem Einbruch in ein Unternehmen an einem Wochenende wurde nur Bagatellschaden durch Aufhebeln eines Fensters angerichtet, lediglich eine Kaffeekasse und kleinere Einrichtungsgegenstände wurden entwendet. Bei einer Routinekontrolle wurde jedoch später festgestellt, dass ein zentraler Server genau zum Zeitpunkt des Einbruchs geschickt manipuliert wurde. **Manipulationen**

G 5.4 Diebstahl

Durch den Diebstahl von IT-Geräten, Zubehör, Software oder Daten entstehen einerseits Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen Zustandes, andererseits Verluste aufgrund mangelnder Verfügbarkeit. Darüber hinaus können Schäden durch einen Vertraulichkeitsverlust und daraus resultierenden Konsequenzen entstehen.

Von Diebstählen sind neben teuren IT-Systemen auch mobile IT-Systeme, die unauffällig und leicht zu transportieren sind, häufig betroffen.

Beispiele:

- Im Frühjahr 2000 verschwand ein Notebook aus dem amerikanischen Außenministerium. In einer offiziellen Stellungnahme wurde nicht ausgeschlossen, dass das Gerät vertrauliche Informationen enthalten könnte. Ebenso wenig war bekannt, ob das Gerät kryptographisch oder durch andere Maßnahmen gegen unbefugten Zugriff gesichert war. Bei Sicherheitsuntersuchungen war bereits vor ungenügenden Sicherheitskontrollen gewarnt worden.
- In einem deutschen Bundesamt wurde mehrfach durch die gleichen ungesicherten Fenster eingebrochen. Neben anderen Wertsachen verschwanden auch mobile IT-Systeme. Ob Akten kopiert oder manipuliert wurden, konnte nicht festgestellt werden.

G 5.5 Vandalismus

Vandalismus ist dem Anschlag sehr verwandt, nur dass er nicht wie dieser gezielt eingesetzt wird, sondern meist Ausdruck blinder Zerstörungswut ist.

Sowohl Außentäter (z. B. enttäuschte Einbrecher, außer Kontrolle geratene Demonstrationen) als auch Innentäter (z. B. frustrierte oder alkoholisierte Mitarbeiter) kommen in Betracht. Die tatsächliche Gefährdung durch Vandalismus ist schwerer abschätzbar als die eines Anschlages, da ihm in der Regel keine zielgerichtete Motivation zugrunde liegt. Persönliche Probleme oder ein schlechtes Betriebsklima können dabei Ursachen sein.

G 5.6 Anschlag

Die technischen Möglichkeiten, einen Anschlag zu verüben, sind vielfältig: geworfene Ziegelsteine, Explosion durch Sprengstoff, Schusswaffengebrauch, Brandstiftung. Ob und in welchem Umfang ein IT-Betreiber der Gefahr eines Anschlages ausgesetzt ist, hängt neben der Lage und dem Umfeld des Gebäudes stark von seinen Aufgaben und vom politisch-sozialen Klima ab. IT-Betreiber in politisch kontrovers diskutierten Bereichen sind stärker bedroht als andere. IT-Betreiber in der Nähe üblicher Demonstrationsaufmarschgebiete sind stärker gefährdet als solche in abgelegenen Randbereichen. Für die Einschätzung der Gefährdung durch politisch motivierte Anschläge können die Landeskriminalämter oder das Bundeskriminalamt beratend hinzugezogen werden.

viele Dokumente auf kleinem Raum

Für elektronische Archive ist bei dieser Einschätzung als besonderer Umstand zu berücksichtigen, dass darin eine große Anzahl von Dokumenten auf vergleichsweise kleinem Raum gespeichert wird. Dies können z. B. Krankendaten, Verträge, Urkunden, Testamente privater Personen sowie Dokumente und Verträge von Unternehmen, Behörden und anderen staatlichen Einrichtungen sein. Deren Vernichtung kann weitreichende Auswirkungen haben, nicht nur auf die speichernde Stelle, sondern auch auf eine Vielzahl anderer Benutzer. Anschläge auf elektronische Archive können daher erhebliche Schäden verursachen.

Beispiele:

- In den 80er-Jahren wurde ein Sprengstoffanschlag auf das Rechenzentrum einer großen Bundesbehörde in Köln verübt.
- Ein Finanzamt im rheinischen Raum wurde praktisch jährlich durch Bombendrohungen für einige Stunden lahm gelegt.
- Ende der 80er-Jahre wurde von einem versuchten Anschlag der RAF auf das Rechenzentrum einer großen deutschen Bank berichtet.

G 5.7 Abhören von Leitungen

Wegen des geringen Entdeckungsrisikos ist das Abhören von Leitungen eine nicht zu vernachlässigende Gefährdung der IT-Sicherheit. Grundsätzlich gibt es keine abhörsicheren Kabel. Lediglich der erforderliche Aufwand zum Abhören unterscheidet die Kabel. Ob eine Leitung tatsächlich abgehört wird, ist nur mit hohem messtechnischen Aufwand feststellbar.

Möglichkeiten und Interessen des Angreifers

Der Entschluss, eine Leitung abzuhören, wird im wesentlichen durch die Frage bestimmt, ob die Informationen den technischen bzw. den finanziellen Aufwand und das Risiko der Entdeckung wert sind. Die Beantwortung dieser Frage ist sehr von den individuellen Möglichkeiten und Interessen des Angreifers abhängig. Somit ist eine sichere Festlegung, welche Informationen und damit Leitungen ggf. abgehört werden, nicht möglich.

Der Aufwand zum Abhören von Leitungen kann sehr gering sein. Bei manchen Arten von LAN-Verkabelung kann der Zugang zu einer LAN-Dose ausreichen, um den gesamten Netzverkehr des lokalen Netzes abzuhören. Noch einfacher ist das Abhören des Netzverkehrs bei drahtlosen Netzen (Wireless LAN / Funk-LAN, IEEE 802.11). Beim Abhören drahtloser Netze ist zudem das Risiko der Entdeckung praktisch gleich null.

automatische Analyse von Verbindungen bei Klartextprotokollen

Besonders kritisch ist die ungeschützte Übertragung von Authentisierungsdaten bei Klartextprotokollen wie HTTP, ftp oder telnet, da sich hier die Position der vom Nutzer eingegebenen Daten in den übertragenen Paketen durch die einfache Struktur der Protokolle leicht bestimmen lässt (siehe auch G 2.87 *Verwendung unsicherer Protokolle in öffentlichen Netzen*). Eine automatische Analyse solcher Verbindungen lässt sich somit mit geringem Aufwand realisieren.

Mittels Password-Sniffings können in einem ersten Schritt Passwörter bei der Übertragung zu einem System abgefangen werden. Dies erlaubt dem Angreifer anschließend auf dieses IT-System zu gelangen, um dann weitere Angriffe lokal auf dem Rechner durchzuführen.

Beispiele:

- So ist es z. B. falsch anzunehmen, dass per E-Mail versandte Nachrichten mit klassischen Briefen vergleichbar sind. Da E-Mails während ihres gesamten Weges durch das Netz gelesen werden können, ist ein Vergleich mit Postkarten sehr viel realistischer.
- Einige Hersteller liefern Programme (Sniffer), die zum Debuggen der Netze dienen, aber auch zum Abhören benutzt werden können, schon zusammen mit ihren Betriebssystemen aus.

G 5.8 Manipulation an Leitungen

Neben dem Abhören von Leitungen (siehe G 5.7 *Abhören von Leitungen*) kann eine Manipulation an Leitungen noch andere Ziele haben:

- Frustrierte Mitarbeiter manipulieren Leitungen so, dass es zu unzulässigen Verbindungen innerhalb und außerhalb der eigenen IT kommt. Dabei geht es oft nur darum, den IT-Betrieb zu stören.

unzulässige Verbindungen

- Leitungen können so manipuliert werden, dass eine private Nutzung zu Lasten des Netzbetreibers erfolgen kann. Neben den dadurch entstehenden Kosten bei der Nutzung gebührenpflichtiger Verbindungen werden Leitungen und Ressourcen durch die private Nutzung blockiert.

private Nutzung

- Durch die Manipulation von Leitungen kann es möglich werden, darauf übertragene Daten zum Vorteil des Täters zu verändern. Insbesondere bei kassenwirksamen Verfahren, in der Lohnbuchhaltung und bei allen IT-Anwendungen, die sich direkt oder indirekt mit der Verwaltung von Sachwerten befassen, können sich durch Manipulationen hohe Schäden ergeben.

Manipulation übertragener Daten

G 5.9 Unberechtigte IT-Nutzung

Ohne Mechanismen zur Identifikation und Authentisierung von Benutzern ist die Kontrolle über unberechtigte IT-Nutzung praktisch nicht möglich. Selbst bei IT-Systemen mit einer Identifikations- und Authentisierungsfunktion in Form von Benutzer-ID- und Passwort-Prüfung ist eine unberechtigte Nutzung denkbar, wenn Passwort und zugehörige Benutzer-ID ausgespäht werden.

Um das geheim gehaltene Passwort zu erraten, können Unbefugte innerhalb der Login-Funktion ein mögliches Passwort eingeben. Die Reaktion des IT-Systems gibt anschließend Aufschluss darüber, ob das Passwort korrekt war oder nicht. Auf diese Weise können Passwörter durch Ausprobieren erraten werden.

Viel Erfolg versprechender ist jedoch die Attacke, ein sinnvolles Wort als Passwort anzunehmen und alle Benutzereinträge durchzuprobieren. Bei entsprechend großer Benutzeranzahl wird damit oft eine gültige Kombination gefunden.

Falls die Identifikations- und Authentisierungsfunktion missbräuchlich nutzbar ist, so können sogar automatisch Versuche gestartet werden, indem ein Programm erstellt wird, das systematisch alle möglichen Passwörter testet.

Beispiel:

- 1988 nutzte ein Internet-Wurm eine Schwachstelle der betroffenen Unix-Betriebssysteme aus, um gültige Passwörter zu finden, obwohl die gültigen Passwörter verschlüsselt gespeichert waren. Dazu probierte ein Programm sämtliche Eintragungen eines Wörterbuches aus, indem es sie mit der zur Verfügung stehenden Chiffrierfunktion verschlüsselte und mit den abgespeicherten verschlüsselten Passwörtern verglich. Sobald eine Übereinstimmung gefunden war, war auch ein gültiges Passwort erkannt.

G 5.10 Missbrauch von Fernwartungszugängen

Bei unzureichend gesicherten Fernwartungszugängen ist es denkbar, dass Hacker Zugang erlangen, z. B. zum Administrierungsport des IT-Systems. Sie können somit nach Überwindung des Anlagenpasswortes bzw. anderer Authentisierungsmechanismen gegebenenfalls alle Administrationstätigkeiten ausüben. Hierdurch können je nach Absicht und Kenntnissen eines Angreifers eine Vielzahl von Schäden entstehen. Bei einem vollständigen Anlagenausfall, schweren Betriebsstörungen, verfälschten Daten oder auch dem Verlust der Vertraulichkeit aller auf dem betroffenen IT-System gespeicherten Daten können unter Umständen größte finanzielle Schäden entstehen.

Beispiele:

- Zur Weitergabe von Systemfehlern an den Hersteller wird bei Großrechnern mit dem Betriebssystem z/OS in der Regel das *Remote Support Facility (RSF)* eingesetzt. RSF kann auch verwendet werden, um seitens des Herstellers Patches am sogenannten Microcode vorzunehmen. Ein Missbrauch des RSF-Zugangs von z/OS-Systemen stellt deshalb eine erhebliche Gefahr dar.
- Auch bei Plattenherstellern für z/OS-Systeme ist es inzwischen üblich, Probleme über Fernwartungszugänge zu lösen.

G 5.11 Vertraulichkeitsverlust in TK-Anlagen gespeicherter Daten

In TK-Anlagen werden personenbezogene und interne Daten für längere Zeit auf Festplatten gespeichert. Personenbezogene Daten sind hierbei beispielsweise Gebührendaten, Konfigurationsdaten, Berechtigungen und gegebenenfalls Daten für die elektronischen Telefonbücher, Passwörter und Verrechnungsnummern.

Beim Betrieb von VoIP-TK-Anlagen können auch Sprachinformationen sehr effizient protokolliert werden, da sie schon digital vorliegen. Auf diese Weise können beispielsweise auch alle geführten Telefongespräche vollständig auf Festplatten gespeichert und zur Auswertung auf ein anderes System kopiert werden. Es besteht das Risiko, dass eine solche Protokollierung der Telefonate unzulässigerweise aktiviert und für Angriffe auf die Vertraulichkeit missbraucht wird.

Die gespeicherten Daten könnten durch das TK-Administrationspersonal eingesehen und verändert werden. Art und Umfang dieser Eingriffe sind vom Anlagentyp und, falls vorgesehen, von der Rechtevergabe abhängig. Das Administrationspersonal hat diese Möglichkeit sowohl vor Ort als auch über Fernwartung. Bei einer externen Fernwartung hat der damit Beauftragte (im Regelfall der Hersteller oder ein entsprechender Dienstleister) jederzeit diese Möglichkeit.

Bei älteren TK-Anlagen müssen für eine Aktualisierung der Anlagensoftware die Festplatten oft zu den TK-Anlagen-Herstellern gebracht werden. Personenbezogene Daten könnten dann vom Hersteller ausgelesen werden. Bei aktuellen TK-Anlagen kann eine Aktualisierung dagegen meist direkt durch den zuständigen TK-Administrator erfolgen.

G 5.12 Abhören von Telefongesprächen und Datenübertragungen

Wenn Telefongespräche unverschlüsselt übertragen werden, besteht die Gefahr, dass Angreifer alle Informationen mithören. Ein Angreifer könnte beispielsweise direkt die Telefonkabel anzapfen oder an einer zwischen den Gesprächsteilnehmern vermittelnden TK-Anlage lauschen.

Beim Einsatz von VoIP ist das sind das Abhören von Telefongesprächen und Datenübertragungen wesentlicher einfacher. Alle Sprachinformationen werden hierbei innerhalb eines IP-Medienstroms, beispielsweise mit dem *Realtime Transport Protocol* (RTP) übertragen. Durch Techniken wie *Spoofing* und *Sniffing* stehen alle Möglichkeiten von Angriffen in IP-Datennetzen zur Verfügung.

Bei vielen TK-Anlagen können Anrufer einem Empfänger Nachrichten hinterlassen, wenn dieser zu dem Zeitpunkt telefonisch nicht erreichbar ist. Einige Anrufbeantworter, vor allem bei VoIP-Anlagen, verschicken diese Informationen als Audio-Datei innerhalb einer VoiceMail. Der Inhalt dieser Mail könnte, wie ein VoIP-Medienstrom, direkt von einem Angreifer abgefangen und angehört werden.

Sowohl bei VoIP als auch bei den leitungsvermittelnden TK-System können auch durch eine missbräuchliche Verwendung von Leistungsmerkmalen unter Umständen Gespräche im Kollegenkreis mitgehört werden. Als Beispiel hierfür kann die Dreierkonferenz genannt werden. Erhält der Teilnehmer A einen Anruf für den Teilnehmer B, so könnte er, anstatt den Anruf zu übergeben, versuchen, heimlich eine Dreierkonferenz herzustellen. Besitzt Teilnehmer B ein Telefon ohne Display, würde er diese Tatsache nicht bemerken.

Des Weiteren könnten bei VoIP und bei leitungsvermittelnden TK-Systemen Gespräche durch das Aktivieren von gesperrten, in Deutschland zum Teil unzulässigen Leistungsmerkmalen von Dritten mitgehört werden. Als ein Beispiel sei hier nur die Zeugenschaltung erwähnt. Eine derartige Aktivierung erfordert genauere Systemkenntnisse.

G 5.13 Abhören von Räumen

Grundsätzlich müssen zwei Varianten des unbefugten Abhörens von Räumen unterschieden werden. Bei der ersten Variante geht die Bedrohung ausschließlich von einem Endgerät aus. Hier sind intelligente Endgeräte mit eingebauten Mikrofonen wie Multimedia-PCs, PDAs, Mobiltelefone, aber auch Anrufbeantworter oder ISDN-Karten zu nennen. Solche Endgeräte können, wenn entsprechende Funktionalitäten implementiert sind, aus der Ferne, d. h. aus dem öffentlichen Netz, dazu veranlasst werden, die eingebauten Mikrofone freizuschalten. Ein bekanntes Beispiel hierfür ist die so genannte "Baby-Watch-Funktion" von Anrufbeantwortern (siehe Baustein B 3.403 *Anrufbeantworter*).

Die zweite Variante ist die Ausnutzung der Funktionalität der TK-Anlage selbst in Verbindung mit entsprechend ausgerüsteten Endgeräten. Diese Gefährdung entsteht durch die missbräuchliche Verwendung des Leistungsmerkmals "direktes Ansprechen" in Kombination mit der Option "Freisprechen". Die auf diese Weise realisierbare Funktion einer Wechselsprechanlage kann unter gewissen Umständen auch zum Abhören eines Raumes ausgenutzt werden.

Bei der Nutzung von VoIP-Softphones ergibt sich ein weiteres Gefährdungsszenario. Diese Applikationen ermöglichen die Verwendung eines Multimedia-PCs als Telefon-Endgerät. Der Multimedia-PC wird in der Regel auch für weitere Aufgaben genutzt, beispielsweise zum Surfen im Internet. Da ein Mikrofon für die Sprachübermittlung benötigt wird, könnte es unter Umständen durch Schadsoftware aktiviert werden und das Abhören ermöglichen. Die Ausnutzung der entsprechenden Funktionalität der TK-Anlage, wie sie oben beschrieben wird, ist zusätzlich möglich.

G 5.14 Gebührenbetrug

In letzter Zeit waren vermehrt Meldungen über Gebührenbetrug an TK-Anlagen durch Hacker in der Presse zu lesen. Solche Manipulationen sind auf verschiedene Weisen durchführbar. Zum einen kann versucht werden, vorhandene Leistungsmerkmale einer TK-Anlage für diese Zwecke zu missbrauchen. Geeignet hierfür sind beispielsweise aus der Ferne umprogrammierbare Rufumleitungen oder Dial-In-Optionen. Zum anderen können die Berechtigungen so vergeben werden, dass kommende "Amtsleitungen" abgehende "Amtsleitungen" belegen können. Auf diese Weise kann bei Anwahl einer bestimmten Rufnummer von außen der Anrufer automatisch wieder mit dem "Amt" verbunden werden, wobei dies allerdings auf Kosten des TK-Anlagenbetreibers geschieht.

Eine weitere Art des Gebührenbetruges ist der durch den Benutzer selbst. Auf unterschiedliche Arten, wie z. B. durch das Telefonieren von fremden Apparaten, Auslesen fremder Berechtigungscodes (Passwort) oder Verändern der persönlichen Berechtigungen kann versucht werden, auf Kosten des Arbeitgebers oder der anderen Beschäftigten zu telefonieren.

G 5.15 "Neugierige" Mitarbeiter

Moderne TK-Anlagen verfügen in der Regel über eine Vielzahl von Leistungsmerkmalen, um den Benutzern größtmögliche Bequemlichkeit bei der Kommunikation und eine möglichst weitgehende Anpassung an die jeweilige Arbeitsumgebung zu bieten.

Einige dieser Leistungsmerkmale von TK-Anlagen können jedoch u. U. durch "neugierige" Mitarbeiter missbraucht werden. Beispielsweise könnten Mitarbeiter versuchen,

- unerlaubt Anrufe für Kollegen auf ihren eigenen Telefonapparat umzuleiten,
- unerlaubt Anrufe für andere anzunehmen,
- unerlaubt fremde Anruf- und Wahlwiederholspeicher auszulesen und
- unerlaubt Telefongespräche Dritter mitzuhören.

Hierdurch besteht die Gefahr, dass "neugierige" Mitarbeiter unerlaubt Kenntnis von Informationen erlangen, die nicht für sie bestimmt oder sogar vertraulich sind.

Beispiel:

- Mit Hilfe der Funktion "Anruf heranholen" kann ein Benutzer einen Anruf, der gerade auf dem Apparat eines Kollegen ankommt, aber noch nicht angenommen ist, auf den eigenen Telefonapparat umleiten. Ein Mitarbeiter eines Unternehmens verwendete diese Funktion, um Anrufe für einen abwesenden Kollegen entgegenzunehmen. Angeblich um Zeit zu sparen, meldete er sich nur mit einem kurzen "Hallo?" und gab dadurch seine Identität nicht preis. Einige der Anrufer gingen daher fälschlicherweise davon aus, dass sie tatsächlich mit der gewünschten Person sprachen und berichteten über vertrauliche Angelegenheiten. Auf dieses Weise erhielt der "neugierige" Mitarbeiter unerlaubt Einblick in Projekte und Privatangelegenheiten seines Kollegen.

G 5.16 Gefährdung bei Wartungs-/Administrierungsarbeiten durch internes Personal

Zum eigenen Vorteil oder aus Gefälligkeit für Kollegen könnte bei Wartungs- oder Administrationsarbeiten durch internes Personal versucht werden, Berechtigungen (z. B. Auslandsberechtigung für Telefongespräche oder Zugriff auf Internetdienste) zu ändern oder Leistungsmerkmale zu aktivieren. Dabei können durch Unkenntnis Systemabstürze verursacht werden oder weitere Sicherheitslücken durch Konfigurationsfehler eröffnet werden. Ferner können durch unsachgemäße Handhabung der Hardwarekomponenten diese u. U. zerstört werden. Zusätzlich hat das Wartungspersonal vollen oder eingeschränkten Zugriff auf die gespeicherten Daten (lesend und schreibend) und könnte diese unbefugt weitergeben oder manipulieren.

Auch die eigenhändige Steuerung oder zeitweilige Deaktivierung von Regel- oder Alarmtechnik birgt ein hohes Gefährdungspotential. Dies betrifft auch Gefahrenmeldeanlagen und Leitsysteme.

Beispiele:

- Eine kurzfristig eingestellte Aushilfe, die die Aufgabe hatte, nicht mehr genutzte Accounts zu sperren, nutzt ihre umfassende Berechtigung, um sich urheberrechtlich geschützte Software vom zentralen Applikationsserver für private Zwecke herunterzuladen. Um das Programm auch gleich an Freunde verteilen zu können, nutzt er dienstliche CD-ROM-Brenner und Datenträger.
- Damit eine Kollegin auch während der Dienstzeit ihre privaten Homebanking-Transaktionen ausführen kann, wird ihr aus Gefälligkeit ein exklusiver Zugang zu ihrem Internet-Provider via ISDN zugänglich gemacht. Als sie sich zu Ostern einen Bildschirmschoner aus dem Internet herunterlädt, infiziert sie ihren PC mit einem Virus. Da der Rechner mit dem Hausnetz verbunden ist, verbreitet sich der Virus sehr schnell. Das Unternehmensnetz ist bis zur Behebung des Problems für mehrere Stunden nicht nutzbar.
- Einbruchmeldeanlagen haben in vielen Fällen einen integrierten Protokollierungsdrucker. Es kommt immer wieder vor, dass die Einbruchmeldeanlage zum Auswechseln der hierzu erforderlichen Papierrolle "vorsorglich" abgeschaltet wird. Beim anschließenden Wiedereinschalten besteht die Gefahr, dass das System unsachgemäß gestartet wird und sich dadurch Fehlfunktionen ergeben.

G 5.17 Gefährdung bei Wartungsarbeiten durch externes Personal

Ein IT-System kann bei Wartungsarbeiten auf jedwede Weise manipuliert werden. Die Gefahr besteht in erster Linie darin, dass der Eigentümer oft nicht in der Lage ist, die vorgenommenen Modifikationen nachzuvollziehen. Darüber hinaus hat der externe Wartungstechniker genau wie der interne auch üblicherweise Zugriff auf alle auf der Anlage gespeicherten Daten.

G 5.18 Systematisches Ausprobieren von Passwörtern

Zu einfache Passwörter lassen sich durch systematisches Ausprobieren herausfinden. Dabei ist zwischen dem simplen Ausprobieren aller möglichen Zeichenkombinationen bis zu einer bestimmten Länge (sogenannter Brute-Force-Angriff) und dem Ausprobieren anhand einer Liste mit Zeichenkombinationen (sogenannter *Wörterbuch-Angriff*) zu unterscheiden. Beide Ansätze lassen sich auch kombinieren.

Die meisten Betriebssysteme verfügen über eine Datei oder Datenbank (z. B. *passwd*- bzw. *shadow-Datei* bei Unix oder RACF-Datenbank bei z/OS) mit den Kennungen und Passwörtern der Benutzer. Allerdings werden zumindest die Passwörter bei vielen Betriebssystemen nicht im Klartext gespeichert, sondern es kommen kryptographische Mechanismen zum Einsatz. Ist die Datei nur unzureichend gegen unbefugten Zugriff geschützt, kann ein Angreifer diese Datei möglicherweise kopieren und mit Hilfe leistungsfähigerer Rechner und ohne Einschränkungen hinsichtlich der Zugriffszeit einem Brute-Force-Angriff aussetzen.

Die Zeit, die bei einem Brute-Force-Angriff zum Herausfinden eines Passworts benötigt wird, hängt ab von

- der Dauer einer einzelnen Passwortprüfung,
- der Länge des Passworts und
- der Zeichenzusammensetzung des Passworts (z. B. Buchstaben/Zahlen).

Die Dauer einer einzelnen Passwortprüfung hängt stark vom jeweiligen System und dessen Verarbeitungs- bzw. Übertragungsgeschwindigkeit ab. Im Falle eines Angriffs spielen auch die Methode und die Technik des Angreifers eine Rolle.

Länge und Zeichenzusammensetzung des Passworts lassen sich dagegen durch organisatorische Vorgaben oder sogar durch technische Maßnahmen beeinflussen.

Beispiel:

- Mit einem gut ausgestatteten PC lassen sich derzeit bei der Standard-Passwort-Verschlüsselung von Unix bzw. Linux etwa 400.000 Passwortprüfungen pro Sekunde durchführen. Bei der Standard-Passwort-Verschlüsselung von Windows NT/2000/XP sind es sogar über 6.000.000 Prüfungen pro Sekunde (Quelle: Der Hamburgische Datenschutzbeauftragte, 2003).

  Bei einem Zeichenvorrat von 26 Zeichen dauert es somit etwa 6 Tage, um ein 8 Zeichen langes Passwort unter Unix bzw. Linux zu ermitteln (Standard-Passwort-Verschlüsselung). Die gleiche Aufgabe dauert unter Windows sogar nur etwa 9 Stunden.

G 5.19 Missbrauch von Benutzerrechten

Eine missbräuchliche Nutzung liegt vor, wenn man vorsätzlich recht- oder unrechtmäßig erworbene Möglichkeiten ausnutzt, um dem System oder dessen Benutzern zu schaden.

In nicht wenigen Fällen verfügen Anwender aus systemtechnischen Gründen über höhere oder umfangreichere Zugriffsrechte, als sie für ihre Tätigkeit benötigen. Diese Rechte können zum Ausspähen von Daten verwendet werden, auch wenn Arbeitsanweisungen den Zugriff verbieten.

Beispiel:

- Auf vielen Unix-Systemen ist die Datei */etc/passwd* für jeden Benutzer lesbar, so dass er sich Informationen über dort eingetragene persönliche Daten verschaffen kann. Außerdem kann er mit Wörterbuchattacken (siehe G 5.18 *Systematisches Ausprobieren von Passwörtern*) versuchen, die verschlüsselten Passwörter zu erraten. Bei zu großzügiger Vergabe von Gruppenrechten, insbesondere bei den Systemgruppen wie z. B. *root, bin, adm, news* oder *daemon*, ist ein Missbrauch wie z. B. das Verändern oder Löschen fremder Dateien leicht möglich.
- Ein für die Verwaltung der Festplatten in z/OS-Systemen zuständiger Storage-Administrator konnte dank des Attributes *Operations*, das er für die Ausführung seiner Tätigkeit von der RACF-Administration erhalten hatte, Kundendateien einsehen. Er nutzte dieses Zugriffsrecht aus, um unerlaubt Kopien zu erstellen.

G 5.20 Missbrauch von Administratorrechten

Eine missbräuchliche Administration liegt vor, wenn man vorsätzlich recht- oder unrechtmäßig erworbene Super-User- (*root*-) Privilegien ausnutzt, um dem System oder dessen Benutzern zu schaden.

Beispiele:

- Da *root* auf Unix-Anlagen keinerlei Beschränkungen unterliegt, kann der Administrator unabhängig von Zugriffsrechten jede Datei lesen, verändern oder löschen. Außerdem kann er die Identität jedes Benutzers seines Systems annehmen, ohne dass dies von einem anderen Benutzer bemerkt wird, es ist ihm also z. B. möglich unter fremden Namen Mails zu verschicken oder fremde Mails zu lesen und zu löschen. **keine Beschränkungen für root**
- Es gibt verschiedene Möglichkeiten, missbräuchlich Super-User-Privilegien auszunutzen. Dazu gehören der Missbrauch von falsch administrierten Super-User-Dateien (Dateien mit Eigentümer *root* und gesetztem s-Bit) und des Befehls *su*. **Super-User-Dateien**
- Die Gefährdung kann auch durch automatisches Mounten von austauschbaren Datenträgern entstehen: Sobald das Medium in das Laufwerk gelegt wird, wird es gemountet. Dann hat jeder Zugriff auf die dortigen Dateien. Mit sich auf dem gemounteten Laufwerk befindenden s-Bit-Programmen kann jeder Benutzer Super-User-Rechte erlangen. **automatisches Mounten**
- In Abhängigkeit von der Unix-Variante und der zugrunde liegenden Hardware kann bei Zugangsmöglichkeit zur Konsole der Monitor-Modus aktiviert oder in den Single-User-Modus gebootet werden. Das ermöglicht die Manipulation der Konfiguration. **Zugang zur Konsole**
- Durch Softwarefehler kann es möglich sein, dass eine Anwendung nur eine begrenzt große Menge an Daten verarbeiten kann. Werden dieser Anwendung übergroße Datenmengen oder Parameter übergeben, können Bereiche im Hauptspeicher mit fremden Code überschrieben werden. Dadurch können Befehle mit den Rechten der Anwendung ausgeführt werden. Dies war u. a mit dem Befehl *eject* unter SunOS 5.5 möglich, der mit SetUID-Rechten ausgestattet ist, also bei der Ausführung Super-User-Rechte besitzt. **Softwarefehler**

G 5.21 Trojanische Pferde

Anwenderprogramme, Command Tables und Scriptsprachen

Ein Trojanisches Pferd, oft auch (eigentlich fälschlicherweise) kurz *Trojaner* genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Der Benutzer kann daher auf die Ausführung dieser Funktion keinen Einfluss nehmen - insoweit besteht eine gewisse Verwandtschaft mit Computer-Viren. Es ist jedoch keine Selbstreproduktion vorhanden. Als Träger für Trojanische Pferde lassen sich alle möglichen Anwenderprogramme benutzen. Aber auch Scriptsprachen, wie Batch-Dateien, ANSI-Steuersequenzen, *REXX Execs* und *ISPF Command Tables* bei z/OS-Betriebssystemen, Postscript und Ähnliches, die vom jeweiligen Betriebssystem oder Anwenderprogramm interpretiert werden, können für Trojanische Pferde missbraucht werden.

Die Schadwirkung eines Trojanischen Pferdes ist um so wirkungsvoller, je mehr Rechte sein Trägerprogramm besitzt.

Beispiele:

geänderte Login-Programme

- Ein geändertes Login-Programm kann ein Trojanisches Pferd enthalten, das Namen und Passwort des Benutzers über das Netz an den Angreifer übermittelt und dann an das eigentliche Login-Programm weitergibt. Solche Trojanischen Pferde sind z. B. bei Online-Diensten wie AOL oder T-Online aufgetreten.

Bildschirmschoner

- Auch Bildschirmschoner, besonders solche, die aus dem Internet herunter geladen werden, können eine versteckte Funktion enthalten, mit der die eingegebenen Passwörter des angemeldeten Benutzers protokolliert und an einen Angreifer übermittelt.

Back Orifice und NetBUS

- Bei dem Programm *Back Orifice* handelt es sich um eine Client-Server-Anwendung, die es dem Client erlaubt, einen Windows-PC über das Netz fernzuwarten. Insbesondere können Daten gelesen und geschrieben sowie Programme ausgeführt werden. Eine Gefährdung entsteht dadurch, dass dieses Programm in ein anderes Anwendungsprogramm integriert und somit als Trojanisches Pferd verwendet werden kann. Wird das Trojanische Pferd gestartet und besteht eine Netzverbindung, so kann ein Angreifer die Fernwartungsfunktion von *Back Orifice* für den Benutzer unbemerkt benutzen. In diesem Zusammenhang ist auch das Programm NetBUS zu erwähnen, das ähnliche Funktionen bietet.

manipulierte Programme und Bibliotheken

- Mit Hilfe von Root-Kits für verschiedene Unix-Varianten, die manipulierte Versionen von Systemprogrammen wie *ps*, *who*, *netstat* etc. enthalten, ist es möglich, längere Zeit unbemerkt Hintertüren (so genannte *Backdoors*) offen zu halten, die einen unbemerkten Einbruch in das System ermöglichen und dabei die Angriffsspuren verstecken. Häufig werden u. a. die Dateien */sbin/in.telnetd, /bin/login, /bin/ps, /bin/who, /bin/netstat* und die C-Libraries ausgetauscht.

aktuelles Verzeichnis im Suchpfad

- Eine weitere Gefahrenquelle bei Unix-Systemen ist der "." in der Umgebungsvariable *$PATH*. Wenn das jeweils aktuelle Arbeitsverzeichnis (.) als Pfad in der Variable *PATH* enthalten ist, werden zunächst die dort befindlichen Programme ausgeführt. So könnte beim Auflisten des Inhaltes eines

Verzeichnisses vom Superuser unbeabsichtigt ein darin enthaltenes modifiziertes "*ls*"-Programm mit root-Rechten ausgeführt werden.

- Eine Möglichkeit, sich im z/OS-Betriebssystem höhere Rechte zu erschleichen, bietet sich dann, wenn für den Angreifer ein *Update*-Zugriff auf Dateien existiert, die entweder beim Logon-Vorgang durchlaufen (z. B. eine *REXX EXEC*) oder während der Verarbeitung allgemein benutzt werden (z. B. *ISPF Command Tables*). Der Angreifer kann dann den vorhandenen Code durch eigene Programmteile ersetzen.

Einschleusen von Programmcode

G 5.22 Diebstahl bei mobiler Nutzung des IT-Systems

Wird ein IT-System mobil genutzt, so ergeben sich neue Gefährdungen, die stationäre IT-Systeme in dem Maße nicht berühren. Mobile Systeme wie Laptops werden üblicherweise nicht in einem durch Schutzvorkehrungen gesicherten Raum eingesetzt. Sie werden in PKW oder öffentlichen Verkehrsmitteln transportiert, in fremden Büroräumen in Pausen hinterlassen oder in Hotelzimmern unbewacht aufgestellt.

Aufgrund dieser Umfeldbedingungen sind solche mobil eingesetzten IT-Systeme naturgemäß einem höheren Diebstahlrisiko ausgesetzt. Der im Kofferraum eines PKW eingeschlossene Laptop kann gestohlen werden, ohne dass dies das originäre Ziel des Diebstahl ist, denn mit dem gestohlenen Wagen würde auch der Laptop in die falschen Hände geraten.

Beispiel:

Dem Geschäftsführer einer größeren Firma wurde auf einer Geschäftsreise der Laptop gestohlen. Der materielle Verlust war vernachlässigbar, innerhalb eines Tages konnte ein neuer Laptop beschaft werden. Schmerzlicher war der Verlust von wichtigen Kundendaten, die auf dem Laptop gespeichert waren. Von diesen Informationen gab es keine Datensicherung, da sie erst im Verlauf der Geschäftsreise erfasst worden sind.

G 5.23 Computer-Viren

Computer-Viren gehören zu den Programmen mit Schadensfunktionen. Als Schaden ist hier insbesondere der Verlust oder die Verfälschung von Daten oder Programmen sicherlich von größter Tragweite. Solche Funktionen von Programmen können sowohl unbeabsichtigt als auch bewusst gesteuert auftreten.

Die Definition eines Computer-Virus bezieht sich nicht unmittelbar auf eine möglicherweise programmierte Schadensfunktion:

Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.)

Die Eigenschaft der Reproduktion führte in Analogie zum biologischen Vorbild zu der Bezeichnung "Virus". Die Möglichkeiten der Manipulation sind sehr vielfältig. Besonders häufig sind das Überschreiben oder das Anlagern des Virus-Codes an andere Programme und Bereiche des Betriebssystems.

Computer-Viren können im Prinzip bei allen Betriebssystemen auftreten. Die größte Bedrohung ist jedoch im Bereich der IBM-kompatiblen Personalcomputer (PC) vorhanden. Bei den hier am meisten verbreiteten Betriebssystemen (MS-DOS, PC-DOS, DR DOS, NOVELL DOS etc.) werden derzeit weltweit rund 20.000 Viren (einschließlich Varianten) gezählt.

Spezielle Computer-Viren für die Betriebssysteme Windows 3.x, Windows NT, Windows 95, OS/2 und Unix spielen in der Praxis eine untergeordnete Rolle. Bei PC-typischer Hardware können jedoch die Festplatten dieser Rechner von DOS-Boot-Viren infiziert werden, wenn die Boot-Reihenfolge zuerst ein Booten von Diskette vorsieht.

Für Apple-Computer sind ca. 100 spezielle Computer-Viren bekannt, für die es auch entsprechende Suchprogramme gibt.

Arten von Computer-Viren

Es werden drei Grundtypen von Computer-Viren unterschieden:

- Boot-Viren
- Datei-Viren
- Makro-Viren

Es sind auch Misch- und Sonderformen dieser drei Typen bekannt. Weitere Unterteilungsmerkmale sind die Tarnmechanismen, mit denen die Viren oft gegen die Erkennung durch Benutzer und Suchprogramme geschützt sind.

Boot-Viren

Als "Booten" bezeichnet man das Laden des Betriebssystems. Hierbei werden u. a. Programmteile ausgeführt, die zwar eigenständig sind, sich aber in sonst

nicht zugänglichen und im Inhaltsverzeichnis der Disketten und Festplatten nicht sichtbaren Sektoren befinden. Boot-Viren überschreiben diese mit ihrem Programm. Der originale Inhalt wird an eine andere Stelle auf dem Datenträger verlagert und dann beim Start des Computers anschließend an den Virus-Code ausgeführt. Dadurch startet der Computer scheinbar wie gewohnt. Der Boot-Virus gelangt jedoch bereits vor dem Laden des Betriebssystems in den Arbeitsspeicher des Computers und verbleibt dort während der gesamten Betriebszeit. Er kann deshalb den Boot-Sektor jeder nicht schreibgeschützten Diskette infizieren, die während des Rechnerbetriebs benutzt wird. Boot-Viren können sich nur durch Booten oder einen Boot-Versuch mit einer infizierten Diskette auf andere Computer übertragen.

Datei-Viren

Die meisten Datei-Viren (auch File-Viren genannt) lagern sich an Programmdateien an. Dies geschieht jedoch so, dass beim Aufruf auch hier der Virus-Code zuerst ausgeführt wird und erst anschließend das originale Programm. Dadurch läuft das Programm anschließend scheinbar wie gewohnt und der Virus wird nicht so schnell entdeckt. Es sind jedoch auch primitivere, überschreibende Viren bekannt, die sich so an den Anfang des Wirtsprogramms setzen, so dass dieses nicht mehr fehlerfrei läuft. Datei-Viren verbreiten sich durch Aufruf eines infizierten Programms.

Bei den Mischformen von Boot- und Datei-Viren haben so genannte multipartite Viren eine größere Bedeutung erlangt. Sie können sich sowohl durch Aufruf eines infizierten Programms als auch durch Booten (oder einen Boot-Versuch) von einer infizierten Diskette verbreiten.

Makro-Viren

Auch Makro-Viren sind in Dateien enthalten, diese infizieren jedoch nicht die Anwendungsprogramme, sondern die damit erzeugten Dateien. Betroffen sind alle Anwendungsprogramme, bei denen in die erzeugten Dateien nicht nur einzelne Steuerzeichen, sondern auch Programme und andere Objekte eingebettet werden können. Davon sind insbesondere Microsoft Word- und Excel-Dateien betroffen. Bei diesen steht eine leistungsfähige Programmiersprache für Makros zur Verfügung, die auch von weniger geschulten Benutzern leicht zur Programmierung von Viren missbraucht werden kann (siehe auch G 5.43 *Makro-Viren*).

Makros sind Programme, mit deren Hilfe das Anwenderprogramm um zusätzliche Funktionen erweitert werden kann, die auf den Anwendungsfall zugeschnitten sind (z. B. Erzeugen einer Reinschrift aus dem Entwurf eines Textes). Diese Makros laufen erst mit dem jeweiligen Anwendungsprogramm (Microsoft Word, Excel etc.) bei der Bearbeitung des Dokuments ab, indem der Benutzer das Makro aktiviert oder das Makro automatisch gestartet wird. Wird z. B. eine Word-Datei über einen WWW-Browser empfangen, der das Dokument automatisch mit Microsoft Word öffnet, kann hierdurch ein enthaltenes Makro aktiviert werden. Da Datendateien auch häufiger als herkömmliche Programmdateien über Datenträger und vernetzte IT-Systeme verteilt werden, ist die Gefährdung durch Makro-Viren inzwischen größer als durch Boot- und Datei-Viren.

Beispiele für Schadensfunktionen von Computer-Viren

- Der Boot-Virus Michelangelo überschreibt an jedem 6. März die ersten Spuren der Festplatte mit stochastischem Inhalt und macht sie dadurch unbrauchbar.
- Der multipartite Virus Onehalf verschlüsselt maximal die Hälfte des Inhalts der Festplatte. Wird der Virus entfernt, sind die verschlüsselten Daten nicht mehr verfügbar.
- Der Microsoft Word-Makro-Virus WAZZU fügt bei den befallenen Dokumenten an zufälligen Stellen das Wort "Wazzu" ein.
- Der Microsoft Word-Makro-Virus Melissa erschien am 26.3.1999 und verbreitete sich über das Wochenende weltweit. Er ist in einer Datei von Word 97 oder Word 2000 enthalten, die von einem befallenen Computer mittels Microsoft Outlook an bis zu 50 gespeicherte Einträge aus jedem Adressbuch verschickt wird. Dies hat bei einigen größeren Organisationen das Mail-System überlastet.
- W32.Mypics.Worm ist ein in Visual Basic geschriebener Computerwurm, der sich automatisch auf Windows 95/98 und Windows NT Rechnern verbreitet. Er enthält eine zerstörerische Schadenswirkung, die aktiv wird, sobald die Jahreszahl 2000 ist. Dann wird u. a. das BIOS des Rechners verändert, so dass der Rechner nicht mehr korrekt bootet.

G 5.24 Wiedereinspielen von Nachrichten

Angreifer zeichnen bei diesem Angriff eine Nachricht auf und spielen diese Information zu einem späteren Zeitpunkt unverändert wieder ein.

Beispiele:

- Ein Angreifer zeichnet die Authentisierungsdaten (z. B. Benutzer-ID und Passwort) während des Anmeldevorgangs eines Benutzers auf und benutzt diese Informationen, um sich unter Vortäuschen einer falschen Identität Zugang zu einem System zu verschaffen (siehe auch G 5.21 *Trojanische Pferde*).
- Um finanziellen Schaden beim Arbeitgeber (Unternehmen oder Behörde) zu verursachen, gibt ein Mitarbeiter eine genehmigte Bestellung mehrmals auf.

G 5.25 Maskerade

Manipulation des Absenderfeldes oder der Kartenadresse

Die Maskerade benutzt ein Angreifer um eine falsche Identität vorzutäuschen. Eine falsche Identität erlangt er z. B. durch das Ausspähen von Benutzer-ID und Passwort (siehe auch G 5.9 *Unberechtigte IT-Nutzung*), die Manipulation des Absenderfeldes einer Nachricht oder durch die Manipulation einer Adresse (siehe beispielsweise auch G 5.48 *IP-Spoofing* oder G 5.87 *Web-Spoofing*) im Netz. Weiterhin kann eine falsche Identität durch die Manipulation der Rufnummernanzeige (Calling Line Identification Presentation) im ISDN oder durch die Manipulation der Absenderkennung eines Faxabsenders (CSID - Call Subscriber ID) erlangt werden.

Ein Benutzer, der über die Identität seines Kommunikationspartners getäuscht wurde, kann leicht dazu gebracht werden, schutzbedürftige Informationen zu offenbaren.

Aufschalten auf eine bestehende Verbindung

Ein Angreifer kann durch eine Maskerade auch versuchen, sich in eine bereits bestehende Verbindung einzuhängen, ohne sich selber authentisieren zu müssen, da dieser Schritt bereits von den originären Kommunikationsteilnehmern durchlaufen wurde. (siehe dazu auch G 5.89 *Hijacking von Netz-Verbindungen*)

G 5.26 Analyse des Nachrichtenflusses

Über eine Verkehrsflussanalyse versucht ein Angreifer Auskunft darüber zu erhalten, wer wann welche Datenmengen an wen gesendet hat und wie oft. Sogar wenn der Lauscher die Nachrichteninhalte nicht lesen kann, können hierdurch Rückschlüsse auf das Benutzerverhalten gezogen werden. Die Informationen über Datum und Uhrzeit der Erstellung einer Nachricht können zu einem Persönlichkeitsprofil des Absenders ausgewertet werden. Daneben forschen Adresssammler für Adressverlage nach E-Mail- und Post-Adressen, um unaufgefordert Werbung zuzuschicken.

Innerhalb des ISDN (Integrated Services Digital Network) wäre der D-Kanal einer Kommunikationsverbindung, welcher der Signalisierung zwischen Endgerät und Vermittlungsstelle dient, ein geeigneter Angriffspunkt. Die Analyse der dort übertragenen Signalisierung mittels eines Protokollanalysators lässt nicht nur die o. a. Rückschlüsse auf das Benutzerverhalten zu (z. B. wer telefoniert wann mit wem wie lange?), sondern kann auch der Vorbereitung komplexerer Angriffe über den D-Kanal dienen.

G 5.27 Nichtanerkennung einer Nachricht

Bei jeder Art von Kommunikation kann ein Kommunikationsteilnehmer den Nachrichtenempfang ableugnen (Repudiation of Receipt). Dies ist insbesondere bei finanziellen Transaktionen von Bedeutung. Ein Nachrichtenempfang kann beim Postversand ebenso abgeleugnet werden wie bei Fax- oder E-Mail-Nutzung.

Beispiel:

Ein dringend benötigtes Ersatzteil wurde elektronisch bestellt. Nach einer Woche Arbeitsausfall wurde das Fehlen reklamiert. Der Lieferant leugnet, je eine Bestellung erhalten zu haben.

Ebenso kann es passieren, dass ein Kommunikationsteilnehmer den Nachrichtenversand ableugnet, z. B. also eine getätigte Bestellung abstreitet (Repudiation of Origin).

G 5.28 Verhinderung von Diensten

Ein solcher Angriff, auch "Denial of Service" genannt, zielt darauf ab, die IT-Benutzer daran zu hindern, Funktionen oder Geräte zu benutzen, die ihnen normalerweise zur Verfügung stehen. Dieser Angriff steht häufig im Zusammenhang mit verteilten Ressourcen, indem ein Angreifer diese Ressourcen so stark in Anspruch nimmt, dass andere Benutzer an der Arbeit gehindert werden. Es können z. B. die folgenden Ressourcen künstlich verknappt werden: Prozesse, CPU-Zeit, Plattenplatz, Inodes, Verzeichnisse.

Dies kann z. B. geschehen durch

- das Starten von beliebig vielen Programmen gleichzeitig,
- das mehrfache Starten von Programmen, die viel CPU-Zeit verbrauchen,
- das Belegen aller freien Inodes in einem Unix-System, so dass keine neuen Dateien mehr angelegt werden können,
- unkoordiniertes Belegen von Bandstationen in z/OS-Systemen, so dass Anwendungen auf freie Bandstationen warten müssen und die Online-Verarbeitung eingeschränkt ist,

Sperren von Bandstationen am z/OS-System

- bewusste Falscheingabe von Passwörtern (auch Skript-gesteuert) mit dem Ziel der Sperrung aller Kennungen eines z/OS-Systems,

DoS-Attacke auf z/OS Kennungen

- das Anlegen sehr vieler kleiner Dateien in einem Verzeichnis auf einem DOS-PC, so dass in diesem Verzeichnis keine neuen Dateien mehr angelegt werden können,
- die gezielte Überlastung des Netzes,
- das Kappen von Netzverbindungen.

G 5.29 Unberechtigtes Kopieren der Datenträger

Werden Datenträger ausgetauscht oder transportiert, so bedeutet dies unter Umständen, dass die zu übermittelnden Informationen aus einer gesicherten Umgebung heraus über einen unsicheren Transportweg in eine ggf. unsichere Umgebung beim Empfänger übertragen werden. Unbefugte können sich in solchen Fällen diese Informationen dort durch Kopieren einfacher beschaffen, als es in der ursprünglichen Umgebung der Fall war.

Wegen der großen Konzentration schützenswerter Informationen auf Datenträgern elektronischer Archive (z. B. personenbezogene oder firmenvertrauliche Daten) stellen diese ein besonderes Angriffsziel für Diebstahl oder Kopie durch Unbefugte dar.

Beispiel:

Vertrauliche Entwicklungsergebnisse sollen vom Entwicklungslabor in X-Stadt zur Produktion nach Y-Stadt transportiert werden. Werden die entsprechenden Datenträger unkontrolliert über den Postweg versandt, kann nicht ausgeschlossen werden, dass diese unberechtigterweise kopiert und ggf. an die Konkurrenz verkauft werden, ohne dass die Bloßstellung der Informationen bemerkt wird.

G 5.30 Unbefugte Nutzung eines Faxgerätes oder eines Faxservers

Der unberechtigte Zugang zu einem Faxgerät oder unberechtigte Zugriff auf einen Faxserver kann für manipulative Zwecke ausgenutzt werden. Dabei können neben den Kosten für die Faxübertragung (Gebühren und Material) auch Schäden dadurch entstehen, dass ein Unbefugter vorgibt, das Gerät als Berechtigter zu nutzen (Schreiben mit Firmenkopf vom entsprechenden Fax-Anschluss).

Es muss zudem vermieden werden, dass Unbefugte Zugriff auf eingehende Faxsendungen haben.

Beispiele:

- Ein Faxgerät ist im Flur aufgestellt, so dass jeder im Vorbeigehen unkontrolliert Faxe lesen oder an sich nehmen kann.
- Bei einem Faxserver sind die Berechtigungen auf die gespeicherten Faxdaten falsch gesetzt, so dass Unbefugte fremde Faxe lesen können.

G 5.31 Unbefugtes Lesen von Faxsendungen

Beim Einsatz von Faxgeräten besteht dann die Gefahr des unbefugten Lesens eingegangener Faxsendungen, wenn die Geräte in frei zugänglichen Bereichen aufgestellt werden. Zudem können Unbefugte Kenntnis vom Inhalt vertraulicher Faxsendungen erlangen, wenn die Verteilung innerhalb der Organisation fehlerhaft ist.

zu weitgehende Zugriffsrechte

Beim Einsatz von Faxservern ist eine unbefugte Kenntnisnahme ein- und ausgehender Faxsendungen u. U. möglich, sofern die Zugriffsrechte auf dem Faxserver nicht sorgfältig vergeben werden.

manipulierte Adressbücher

Faxserver verfügen zudem über so genannte Adressbücher. Die Adressbücher erleichtern die Versendung von Faxen, da die Benutzer nur den jeweiligen Empfänger auswählen und nicht bei jedem Fax die Empfängerrufnummer erneut eingeben müssen. Sofern in einem Adressbuch eine falsche Empfängerrufnummer eingetragen ist, wird bei Benutzung dieses Eintrages das Fax an den falschen Empfänger gesendet. Häufig bieten Adressbücher auch die Möglichkeit, mehrere Adressaten zu einer Gruppe zusammenzufassen. Der Benutzer, der ein Fax an die Mitglieder einer solchen Gruppe senden will, braucht als Empfänger nur die Gruppe und nicht jedes Gruppenmitglied anzugeben. Sofern sich in solch einer Gruppe unbefugte Adressaten befinden, können diese Kenntnis von allen Faxsendungen erhalten, die über diese Gruppendefinition versandt werden. Die falsche Zuordnung kann durch Unachtsamkeit oder aufgrund einer gezielten Manipulation erfolgen.

Auf einem Faxserver eingegangene Faxsendungen müssen an die Empfänger verteilt werden. Dies kann entweder dadurch erfolgen, dass Eingangs-Faxsendungen ausgedruckt und manuell an die Empfänger weitergeleitet werden oder dass der Faxserver die Verteilung automatisch über das Netz vornimmt.

unbefugte Kenntnisnahme am Drucker

Eine unbefugte Kenntnisnahme von eingegangenen Faxsendungen ist u. U. bei der manuellen Verteilung möglich, wenn der Drucker, auf dem der Ausdruck erfolgt, in einem allgemein zugänglichen Bereich aufgestellt wurde oder die Verteilung innerhalb der Organisation fehlerhaft ist.

manipulierte Zuordnungstabellen

Bei der automatischen Weiterleitung von Faxsendungen benötigt der Faxserver eine Zuordnungstabelle, in der festgelegt wird, an welchen Benutzer bzw. an welche Benutzergruppe Eingangs-Faxsendungen, die z. B. von einem bestimmten Absender stammen oder über eine bestimmte Rufnummer gesendet wurden, weitergeleitet werden sollen. Sofern ein Unbefugter in einer solchen Zuordnungstabelle - sei es durch Unachtsamkeit oder aufgrund einer gezielten Manipulation - aufgenommen wird, erhält er Faxsendungen, die nicht für ihn bestimmt sind.

G 5.32 Auswertung von Restinformationen in Faxgeräten und Faxservern

Faxgeräte

Abhängig vom technischen Verfahren, mit denen Faxgeräte Informationen speichern, weiterverarbeiten oder drucken, können sich nach dem Faxempfang Restinformationen unterschiedlichen Umfanges im Faxgerät befinden. Sie können wiederhergestellt werden, wenn man in den Besitz des Gerätes oder der entsprechenden Bauteile kommt.

Thermotransferdruck

Bei Faxgeräten, die mittels des Thermotransferverfahrens drucken, werden eingehende Faxsendungen zunächst auf eine Zwischenträgerfolie geschrieben, mit deren Hilfe sie dann ausgedruckt werden. Diese Folie ist Verbrauchsmaterial und muss regelmäßig ausgetauscht werden, das Entfernen der Folie ist daher leicht möglich. Gelangt ein Unbefugter in den Besitz dieser Folie (durch Diebstahl oder bei der Entsorgung), kann er den Inhalt mit einfachen technischen Mitteln reproduzieren. Dabei können ihm die Informationen von mehreren hundert Faxseiten bekannt werden.

Zwischenspeicher im Faxgerät

Die meisten Faxgeräte verfügen über einen Zwischenspeicher (Dokumentenspeicher, Puffer), in den ausgehende Faxe bis zur erfolgreichen Übertragung eingelesen bzw. eingehende Faxe vor dem Ausdrucken zwischengespeichert werden können. Dieser Speicher kann je nach Faxgerät eine größere Anzahl Faxseiten enthalten und kann im Allgemeinen von jedem, der Zugang zum Faxgerät hat, ausgedruckt werden.

Faxserver

Restinformationen auf Festplatten

Faxserver sind Applikationen, die auf IT-Systemen installiert sind, die in aller Regel mit mindestens einer Festplatte ausgestattet sind oder über das Netz auf ein Laufwerk zugreifen können. Hierauf werden Faxsendungen solange gespeichert, bis sie an einen Empfänger zugestellt werden können. Weiterhin arbeiten moderne Betriebssysteme mit Auslagerungsdateien, die auch Restinformationen enthalten können. Hier besteht die Gefahr, dass diese Informationen bei Zugriff auf diesen Faxserver unerlaubt ausgewertet werden. Fällt z. B. eine Festplatte während der Garantiezeit aus, muss diese zur Geltendmachung von Garantieansprüchen an den Händler oder an den Hersteller eingesandt werden. Problematisch ist dabei, dass sich noch Daten auf der Festplatte befinden können, von denen Unbefugte auf diesem Weg Kenntnis erlangen können. Bei defekten Festplatten ist eine Löschung der Daten mit Softwaretools häufig nicht möglich.

unzureichender Schutz des Arbeitsspeichers

Ein unbefugter Zugriff auf Faxdaten im Faxclient ist dann möglich, wenn ein Arbeitsplatzrechner bzw. die dort installierte Fax-Software nicht ausreichend gesichert ist. Auch beim Zugriff auf die Festplatte des Arbeitsplatzrechners können Informationen von Unbefugten ausgelesen werden.

G 5.33 Vortäuschen eines falschen Absenders bei Faxsendungen

So wie man einen Brief unter falschem Namen und mit falschem Briefkopf schreiben kann, kann man auch ein entsprechend gefälschtes Fax versenden. Dadurch können Schäden entstehen, wenn der Empfänger die darin enthaltenen Informationen als authentisch und ggf. als rechtsverbindlich ansieht (siehe G 3.14 *Fehleinschätzung der Rechtsverbindlichkeit eines Fax*).

Beispiele:

- Unterschriften können von anderen Schriftstücken eingescannt und auf die Faxvorlage ausgedruckt bzw. beim Einsatz eines Faxservers als Grafikdatei in das Schriftstück einkopiert werden. Auf dem empfangenen Fax ist kein Unterschied zwischen einer so reproduzierten und einer authentischen handschriftlichen Unterschrift erkennbar.
- Bei der Übertragung wird in der Regel die Rufnummer des sendenden Faxanschlusses übermittelt. Es ist jedoch möglich, eine andere Rufnummer vorzutäuschen. Daher ist auch die Auswertung des Empfangsprotokolls keine verlässliche Bestätigung des Absenders.

G 5.34 Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes

Um häufig wiederkehrende Empfänger-Faxnummern nicht ständig neu eingeben zu müssen, bieten einige Faxgeräte programmierbare Zielnummerntasten an. Häufig werden die Empfängernummern beim Versenden des Fax nicht einmal mehr kontrolliert. Kann ein Unbefugter die Programmierung der Zieltasten ändern und veranlasst er dann noch, dass die bei der neuen Zieladresse eingehenden Faxsendungen möglichst unverzüglich zum berechtigten Empfänger weitergeleitet werden, kann er bequem den Fax-Verkehr zu diesem Empfänger mitverfolgen, ggf. ohne jemals entdeckt zu werden.

G 5.35 Überlastung durch Faxsendungen

Eine Überlastung durch eingehende Faxsendungen kann entstehen, wenn nicht genügend Faxanschlüsse oder nicht genügend Telekommunikations-Leitungen bzw. Kanäle vorhanden sind. Darüber hinaus kann ein Faxanschluss absichtlich blockiert werden, indem

- andauernd umfangreiche Faxe (ggf. mit sinnlosem Inhalt) zugesandt werden oder
- absichtlich solange Faxe zugesandt werden, bis der Papiervorrat eines Faxgerätes und der Pufferspeicher aufgebraucht sind.

Überlastung durch eingehende Faxsendungen

Ein Faxserver kann ebenfalls überlastet werden, wenn solange Faxe zugesendet werden, bis der zur Verfügung stehende Platz auf der Festplatte ausgeschöpft ist. Zu beachten ist aber, dass eine gefaxte Seite DIN A 4 etwa 70 kb groß ist. Bei heute üblichen Festplattengrößen müssen dazu sehr viele Faxsendungen dieser Art eingehen. Zudem muss berücksichtigt werden, dass nur eine begrenzte Zahl an Leitungen bzw. Kanälen zur Verfügung steht und jede Faxsendung auch für die Abwicklung des Faxprotokolls Zeit benötigt. Eine Überlastung des Faxservers in diesem Sinne kann nur dann auftreten, wenn eine zu klein dimensionierte Festplatte gewählt wurde oder Faxsendungen auf dem Faxserver archiviert werden.

Überlastung durch ausgehende Faxsendungen

Im Gegensatz zu herkömmlichen Faxgeräten ist die Überlastung eines Faxservers durch ausgehende Faxsendungen durchaus möglich. So kann durch eine sehr große Anzahl von Serien-Faxsendungen ein Faxserver völlig ausgelastet werden und damit auch keine eingehenden Faxsendungen mehr empfangen.

G 5.36 Absichtliche Überlastung des Anrufbeantworters

Es besteht die Möglichkeit für einen Angreifer, das begrenzte Speichermedium (digitaler Speicher oder Audiokassette) während eines Anrufs (z. B. mit unsinnigen Informationen) zu füllen, so dass weitere Aufzeichnungen entweder nicht mehr möglich sind oder schon aufgezeichnete Nachrichten verloren gehen (siehe dazu auch G 4.19 *Informationsverlust bei erschöpftem Speichermedium*).

G 5.37 Ermitteln des Sicherungscodes

Nahezu alle modernen Anrufbeantworter verfügen über die Anrufaufzeichnung hinaus noch über eine Reihe zusätzlicher Funktionen. Typische Beispiele sind Fernabfrage, Umleitung eines Anrufes, Raumüberwachung oder Fernwirkung auf angeschlossene elektrische Geräte. Diese Funktionen lassen sich über Telefon während eines Anrufes am Anrufbeantworter fernsteuern (bei Impulswahlverfahren über einen zusätzlichen Fernabfragesender, bei Tonwahlverfahren direkt über die Telefontastatur). Die Nutzung dieser Fernabfrage- und Fernsteuerungsmöglichkeit wird i. allg. durch einen Sicherungscode (Geheimzahl, PIN) geschützt. Dieser Sicherungscode wird ebenfalls mittels des Fernabfragesenders durch Töne unterschiedlicher Frequenz an den Anrufbeantworter übermittelt.

Wenn ein Dritter diesen Sicherungscode in Erfahrung gebracht hat, ist es ihm möglich, über die Fernsteuerung auf den Anfrufbeantworter Einfluss zu nehmen, genauso als wäre der Anrufbeantworter in seinem Besitz. Der entstehende Schaden hängt davon ab, ob der Dritte schutzbedürftige Nachrichten abhört oder andere Leistungsmerkmale missbraucht.

Beispiel:

Es wurde berichtet, dass in letzter Zeit vermehrt die Sicherungscodes einiger Anrufbeantworter ermittelt wurden, indem ein normaler Personalcomputer mit Modem eingesetzt wurde, um innerhalb von kurzer Zeit sämtliche nur möglichen Zahlenkombinationen durchzuprobieren.

G 5.38 Missbrauch der Fernabfrage

Ist einem Dritten der Sicherungscode eines Anrufbeantworters bekannt geworden, kann er über die Fernabfrage einen Großteil der im Anrufbeantworter implementierten Funktionen missbrauchen. Nachfolgend werden die kritischsten Funktionen, die über die Fernabfrage angesprochen und damit missbraucht werden können, dargestellt:

- **Raumüberwachung**

  Die Funktion Raumüberwachung aktiviert das Mikrofon des Anrufbeantworters und erlaubt so das Abhören des Raumes. Bemerkenswert hierbei ist, dass die wenigsten Geräte dieses Abhören durch einen Aufmerksamkeitston kenntlich machen - lediglich eine Anzeige mittels Leuchtdiode ist Standard.

  Wird diese Funktion missbräuchlich bei Abwesenheit des Angerufenen aktiviert, fällt die eingeschaltete Raumüberwachung nach Rückkehr dem Angerufenen nicht auf. Seine Gespräche innerhalb des Raumes können dann unbemerkt abgehört werden.

- **Abhören oder Löschen gespeicherter Gespräche**

  Es können eingegangene Anrufe abgehört und auch gelöscht werden. Der Schaden ist abhängig vom Schutzbedarf der aufgezeichneten Informationen.

- **Ändern oder Löschen des gespeicherten Ansagetextes**

  Bei einigen Geräten kann durch Fernabfrage eine Löschung des Ansagetextes vorgenommen und damit Anrufbeantworter außer Betrieb gesetzt werden. Durch gezielte Falschinformationen können Anrufer eventuell verwirrt werden.

- **Änderung gespeicherter Rufnummern der Anrufmeldung oder Anrufweiterschaltung**

  Das Leistungsmerkmal Anrufmeldung bewirkt, dass der Anrufbeantworter nach Eingang eines Anrufes selbständig eine vorher eingespeicherte Telefonnummer anwählt. Meldet sich der angerufene Teilnehmer, wird ein bestimmtes Tonsignal bzw. ein Erinnerungstext durch den Anrufbeantworter gesendet und damit signalisiert, dass ein Anruf aufgezeichnet wurde. Bei einzelnen Geräten werden die gespeicherten Nachrichten ohne weitere Mitwirkung abgespielt. In der Regel jedoch muss die Wiedergabe der aufgenommenen Anrufe durch Eingabe des Sicherungscodes aktiviert werden. Das Leistungsmerkmal der Anrufweiterschaltung bewirkt, dass ein Anrufer zu einer vorher eingespeicherten Telefonnummer weiterverbunden wird.

  Durch Abschaltung der Anrufmeldung oder Anrufweiterschaltung werden die Funktionen nicht mehr ausgeführt und der Benutzer wird von wichtigen Anrufen nicht mehr in Kenntnis gesetzt bzw. ist nicht mehr erreichbar. Ein Umprogrammieren dieser Funktionen gestattet es, Anrufe gezielt umzuleiten, beispielsweise zu einem kostenpflichtigen Telefonansagedienst.

- **Vor- und Rückspulen eines Aufzeichnungsbandes**

  Einige analog aufzeichnende Anrufbeantworter erlauben das ferngesteuerte Vor- und Rückspulen des Aufzeichnungsbandes. Durch Vorspulen bis ans Bandende sind weitere Aufzeichnungen ausgeschlossen. Nach dem Zurückspulen des Bandes werden bereits aufgesprochene Texte durch den nächsten Anruf überspielt.

- **Fernwirkmöglichkeiten**

  Einige Geräte gestatten es, aus der Ferne über den Anrufbeantworter elektrische Geräte zu steuern (Ein- und Ausschalten). Je nach Funktion und Bedeutung der angeschlossenen Geräte kann dies beliebig hohen Schaden nach sich ziehen.

- **Abschalten des Gerätes**

  Einige Geräte können ferngesteuert abgeschaltet werden, so dass die Funktion des Anrufbeantworters nicht mehr zur Verfügung steht.

G 5.39 Eindringen in Rechnersysteme über Kommunikationskarten

Eine Kommunikationskarte (z. B. eine ISDN-Karte oder ein internes Modem, aber auch ein externes Modem) kann eingehende Anrufe automatisch entgegennehmen. Abhängig von der eingesetzten Kommunikationssoftware und deren Konfiguration besteht dann die Möglichkeit, dass ein Anrufer unbemerkt Zugriff auf das angeschlossene IT-System nehmen kann.

Über eine Kommunikationskarte kann ein externer Rechner als Terminal an einen Server angeschlossen werden. Falls der Benutzer sich nach einer Terminalsitzung abmeldet, aber die Leitung ansonsten bestehen bleibt, ist vom externen Rechner ein Zugang wie über ein lokales Terminal möglich. Damit haben Dritte, die Zugang zu diesem Rechner haben, die Möglichkeit, Benutzer-Kennungen und Passwörter zu testen. Wesentlich gefährlicher ist der Fall, dass die Verbindung unterbrochen wird, aber der Benutzer nicht automatisch am entfernten System ausgeloggt wird. Dann kann der nächste Anrufer unter dieser Benutzer-Kennung weiterarbeiten, ohne sich anmelden zu müssen. Er hat somit vollen Zugriff auf das IT-System, ohne sich identifiziert und authentisiert zu haben.

G 5.40 Abhören von Räumen mittels Rechner mit Mikrofon

Viele IT-Systeme werden mittlerweile mit Mikrofon ausgeliefert. Das Mikrofon eines vernetzten Rechners kann von denjenigen benutzt werden, die über Zugriffsrechte auf die entsprechende Gerätedateien verfügen (unter Unix ist das zum Beispiel */dev/audio*, unter Windows NT ist es ein Eintrag in der Registrierung). Wenn diese Rechte nicht sorgfältig vergeben sind und dadurch auch andere als die vorgesehenen Benutzer Zugriff haben, kann das Mikrofon zum Abhören missbraucht werden.

Beispiel:

- Im März 2001 hat ein TV-Wirtschaftsmagazin gezeigt, wie über das Mikrofon eines Laptops ein Raum abgehört werden kann, wenn der Rechner mit einer ISDN-Telefonleitung verbunden ist. Dies wurde mit dem Laptop einer deutschen Politikerin demonstriert. Zunächst wurde sie in einer gefälschten Virenwarnung per E-Mail aufgefordert, ein als Anlage mitgeschicktes Schutzprogramm zu öffnen. Dieses Programm enthielt aber ein Trojanisches Pferd, das später über die ISDN-Leitung eine Verbindung nach außen herstellte und die Telefonnummer übermittelte.

  Danach konnte der Rechner von außen angerufen werden, ohne dass der Benutzer darüber optisch oder akustisch informiert wurde. Anschließend wurde über die offene Verbindung das eingebaute Mikrofon im Laptop aktiviert und die Geräusche aus dem Büro nach außen übertragen.

G 5.41 Mißbräuchliche Nutzung eines Unix-Systems mit Hilfe von uucp

Das Programmpaket UUCP (Unix-to-Unix Copy) erlaubt den Austausch von ASCII- und Binärdateien zwischen IT-Systemen und die Ausführung von Kommandos auf entfernten IT-Systemen. UUCP war ursprünglich auf Unix-Systeme beschränkt, ist aber mittlerweile auch für viele andere Betriebssysteme verfügbar. Bei der Kommunikation über UUCP werden IT-Benutzern auf entfernten Rechnern Rechte auf dem lokalen Rechner eingeräumt. Wenn diese Rechte nicht sorgfältig und auf das Notwendige beschränkt vergeben werden, besteht die Gefahr der missbräuchlichen Nutzung des lokalen Systems. Denkbar ist auch eine Maskerade über UUCP, indem z. B. ein Host - bei Kenntnis des Passworts - vorgetäuscht wird.

G 5.42 Social Engineering

Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch "Aushorchen" zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln. Ein typischer Fall von Angriffen mit Hilfe von Social Engineering ist das Manipulieren von Mitarbeitern per Telefonanruf, bei dem sich der Angreifer z. B. ausgibt als:

- Vorzimmerkraft, deren Vorgesetzter schnell noch etwas erledigen will, aber sein Passwort vergessen hat und es jetzt dringend braucht,
- Administrator, der wegen eines Systemfehlers anruft, da er zur Fehlerbehebung noch das Passwort des Benutzers benötigt,
- Telefonentstörer, der einige technische Details wissen will, z. B. unter welcher Rufnummer ein Modem angeschlossen ist und welche Einstellungen es hat,
- Externer, der gerne Herrn X sprechen möchte, der aber nicht erreichbar ist. Die Information, dass Herr X drei Tage abwesend ist, sagt ihm auch gleichzeitig, dass der Account von Herrn X in dieser Zeit nicht benutzt wird, also unbeobachtet ist.

Wenn kritische Rückfragen kommen, ist der Neugierige angeblich "nur eine Aushilfe" oder eine "wichtige" Persönlichkeit.

Eine weitere Strategie beim systematischen Social Engineering ist der Aufbau einer längeren Beziehung zum Opfer. Durch viele unwichtige Telefonate im Vorfeld kann der Angreifer Wissen sammeln und Vertrauen aufbauen, das er später ausnutzen kann.

Solche Angriffe können auch mehrstufig sein, indem in weiteren Schritten auf Wissen und Techniken aufgebaut wird, die in vorhergehenden Stufen erworben wurden.

Beispiel:

- Ein Angreifer hat leichteres Spiel, wenn er das Opfer dazu bringt, ihn von sich aus zu kontaktieren. Beispielsweise kann der Angreifer die Telefonanlage der Ziel-Organisation so manipulieren, dass alle Anrufe an den Administrator an ihn weitergeleitet werden. Dies kann zum Beispiel nach einem erfolgreichen Social-Engineering-Angriff auf den Telefontechniker oder einer erfolgreichen Kompromittierung einer unsicher konfigurierten Telefonanlage von außen geschehen. Gelingt es dem Angreifer dann beispielsweise, einen Denial-of-Service-Angriff durchzuführen, wird das Opfer des Angriffes den Administrator verständigen. Durch die Manipulation der Telefonanlage erreicht das Opfer aber nur den Angreifer. Dass dieser kein "echter" Administrator ist, wird aber normalerweise niemand im normalen Tagesgeschäft hinterfragen.

Viele Anwender wissen, dass sie Passwörter an niemanden weitergeben dürfen. Social Engineers wissen dies und müssen daher über andere Wege an das gewünschte Ziel gelangen. Beispiele hierfür sind:

- Ein Angreifer kann das Opfer bitten, ihm unbekannte Befehle oder Applikationen auszuführen, z. B. weil dies bei einem IT-Problem helfen soll. Dies kann eine versteckte Anweisung für eine Änderung von Zugriffsrechten sein. So kann der Angreifer an sensible Informationen gelangen.
- Viele Benutzer verwenden zwar starke Passwörter, aber dafür werden diese für mehrere Konten genutzt. Wenn ein Angreifer einen nützlichen Netzdienst (wie ein E-Mail-Adressensystem) betreibt, an dem die Anwender sich authentisieren müssen, kann er an die gewünschten Passwörter und Logins gelangen. Viele Benutzer werden die Anmeldedaten, die sie für diesen Dienst benutzen, auch bei anderen Diensten verwenden.

Beim Social Engineering tritt der Angreifer nicht immer sichtbar auf, es gibt auch diverse Varianten, bei denen er im Hintergrund bleibt. Oft erfährt das Opfer niemals, dass es ausgenutzt wurde. Ist dies erfolgreich, muss der Angreifer nicht mit einer Strafverfolgung rechnen und besitzt außerdem eine Quelle, um später an weitere Informationen zu gelangen.

Phishing

Die Nutzung von E-Mail und Internet-Diensten bietet viele Möglichkeiten, unter Vorspiegelung falscher Tatsachen an Informationen zu gelangen. Hierzu gehört beispielsweise das sogenannte "Phishing".

Phishing ist ein Kunstwort aus "Passwort" und "Fishing" und bezeichnet Methoden, bei denen IT-Benutzern Passwörter, Kreditkartendaten oder andere vertrauliche Informationen entlockt werden. Hierzu senden die Angreifer zum Beispiel geschickt formulierte E-Mails an die Benutzer.

Beispiel:

- Viele Online-Banking-Benutzer erhielten E-Mails, die scheinbar von der Service-Abteilung ihrer Bank kamen. Darin wurden sie informiert, dass sie sich aufgrund von Service-Änderungen auf der angegebenen Webseite mit ihrem Standard-Banking-Passwort anmelden und die neuen Dienstleistungen mit einer TAN freischalten sollten. Die Webseite sah zwar authentisch aus, hatte aber mit der genannten Bank nichts zu tun und diente ausschließlich dem Zweck, die Zugangsdaten zu fremden Konten zu erlangen.

  Ähnliche Angriffe gab es auch auf Nutzer beliebter E-Commerce- und Auktions-Webseiten.

G 5.43 Makro-Viren

Mit dem Austausch von Dateien (z. B. per Datenträger oder E-Mail) besteht die Gefahr, dass neben der eigentlichen Datei (Textdatei, Tabelle etc.) weitere, mit dem Dokument verbundene Makros bzw. eingebettete Editorkommandos übersandt werden. Diese Makros laufen erst mit dem jeweiligen Anwendungsprogramm (Winword, Excel etc.) bei der Bearbeitung des Dokuments ab, indem der Benutzer das Makro aktiviert bzw. das Makro automatisch gestartet wird. Wird ein Dokument über einen WWW-Browser empfangen, der das Dokument automatisch öffnet, kann hierdurch ein (Auto-) Makro aktiviert werden.

Da die Makrosprachen über einen sehr umfangreichen Befehlssatz verfügen, besteht auch die Gefahr, dass einem Dokument ein Makro beigefügt wird, das eine Schadfunktion enthält (z. B. einen Virus).

In der Praxis hat diese Gefährdung insbesondere bei den Dateien der Programme Word für Windows und Excel der Firma Microsoft weltweit beträchtlich zugenommen. Für den Benutzer ist dabei nicht transparent, dass Dateien für Word-Vorlagen (*.DOT), in denen Makros enthalten sein können, durch Umbenennen in *.DOC-Dateien scheinbar zu Datendateien werden, die keine Makros enthalten. Von Microsoft Word werden solche Dateien jedoch ohne Hinweis auf diese Tatsache in nahezu gleicher Weise verarbeitet (Ausnahme: Winword ab Version 7.0a).

Die Word-Makro-Viren haben inzwischen die Spitzenstellung bei gemeldeten Infektionen eingenommen. Hervorzuheben ist, dass Makro-Viren auf verschiedenen Betriebssystem-Plattformen auftreten können, nämlich auf allen, auf denen Winword läuft (Windows Versionen 3.1 und 3.11, Windows 95, Windows NT, Apple-Computer).

Beispiel:

- Der Winword-Makro-Virus "Winword.Nuclear" wurde im Internet über die Datei WW6ALERT.ZIP verbreitet. Der Makro-Virus bewirkt einerseits, dass an Ausdrucken der Text "STOP ALL FRENCH NUCLEAR TESTIN IN PACIFIC!" angehängt wird, andererseits aber auch den Versuch, Systemdateien zu löschen.

G 5.44 Missbrauch von Remote-Zugängen für Managementfunktionen von TK-Anlagen

TK-Anlagen verfügen über Remote-Zugänge für Managementfunktionen. Über diese Zugänge können alle Administrations- und Wartungstätigkeiten sowie sonstige Managementfunktionalitäten wie z. B. Alarmsignalisierung und -bearbeitung abgewickelt werden.

Solche Remote-Zugänge sind besonders in TK-Anlagen-Verbünden (Corporate Networks) nützlich und teilweise unverzichtbar. Bei der Art des Remote Zuganges lässt sich zwischen

- "Modem"-Zugang über dedizierte Managementports und
- direkte Einwahl über DISA (Direct Inward System Access)

unterscheiden. Desweiteren sind in neueren Protokollierungsverfahren wie QSig und einigen anderen proprietären Protokollen Managementfunktionen bereits im Signalisierungsspektrum enthalten. Hieraus ergeben sich potentielle Missbrauchsmöglichkeiten.

Bei unzureichend gesicherten Fernwartungszugängen ist es denkbar, dass Hacker Zugang zu den Managementprogrammen des TK-Systems erlangen. Sie können somit nach Überwindung des Anlagenpasswortes ggf. **alle** Administrationstätigkeiten ausüben. Der entstehende Schaden kann sich vom vollständigen Anlagenausfall, über schwerste Betriebsstörungen, den Verlust der Vertraulichkeit aller auf der Anlage vorhandenen Daten bis hin zum großen direkten finanziellen Schaden z. B. durch Gebührenbetrug erstrecken.

G 5.45 Ausprobieren von Passwörtern unter WfW und Windows 95

In einem Peer-to-Peer-Netz unter WfW und Windows 95 werden Zugriffsrechte zu Verzeichnissen durch die Vergabe von Passwörtern realisiert. Es findet keine Unterscheidung einzelner Benutzer statt. Der Zugriff auf ein freigegebenes Verzeichnis und die darin gespeicherten Dateien wird lediglich bei der Eingabe eines korrekten Passwortes erlaubt. Dies gilt nicht beim Einsatz von Windows 95 in Netware-Netzen. Unter WfW und Windows 95 ist es daher prinzipiell möglich, die Zugriffspaßwörter zu freigegebenen Verzeichnissen durch Ausprobieren zu ermitteln. Da keine Beschränkung der Anzahl von Fehlversuchen bei der Passworteingabe existiert, kann dies mittels einer gewissen Systematik Erfolg versprechend sein.

G 5.46 Maskerade unter WfW

Da jeder Benutzer eines WfW-Rechners den Rechner- und Anmeldenamen ändern kann, ist WfW nicht in der Lage, Benutzer zuverlässig zu identifizieren. Maskerade ist daher leicht möglich. Damit kann ein potentieller Angreifer unter falschem Namen auf seinem Rechner ein Verzeichnis für alle am Netz unter WfW arbeitenden Mitarbeiter freigeben, in dem sich Schadprogramme befinden. Er kann auch versuchen, sich unberechtigt Zugriff auf Verzeichnisse anderer zu verschaffen. Der Geschädigte wird über den wahren Verursacher getäuscht. Ebenso kann ein Angreifer Kommunikation in WfW (z. B. über die Telefonfunktion) in einfacher Weise unter falschem Namen führen und den Empfänger über die Identität des tatsächlichen Absenders täuschen. Auch ist es möglich, die Anmeldung eines bestimmten Rechners unter WfW zu verhindern, indem man sich unter dessen Namen zeitlich vor diesem unter WfW anmeldet.

G 5.47 Löschen des Post-Office unter WfW

Wird von mehreren Benutzern unter dem WfW-Programm *mail* ein gemeinsames Post-Office genutzt, kann dieses unter Umgehung aller WfW-Sicherheitsfunktionen unberechtigt gelöscht werden, wenn zu einem dem Post-Office bekannten Rechner kein ausreichender Zugangsschutz (z. B. über ein BIOS-Passwort) gewährleistet ist.

G 5.48 IP-Spoofing

IP-Spoofing ist eine Angriffsmethode, bei der falsche IP-Nummern verwendet werden, um dem angegriffenen IT-System eine falsche Identität vorzuspielen.

Bei vielen Protokollen der TCP/IP-Familie erfolgt die Authentisierung der kommunizierenden IT-Systeme nur über die IP-Adresse, die aber leicht gefälscht werden kann. Nutzt man darüber hinaus noch aus, dass die von den Rechnern zur Synchronisation beim Aufbau einer TCP/IP-Verbindung benutzten Sequenznummern leicht zu erraten sind, ist es möglich, Pakete mit jeder beliebigen Absenderadresse zu verschicken. Damit können entsprechend konfigurierte Dienste wie *rlogin* benutzt werden. Allerdings muss ein Angreifer dabei u. U. in Kauf nehmen, dass er kein Antwortpaket von dem missbräuchlich benutzten Rechner erhält.

Weitere Dienste, die durch IP-Spoofing bedroht werden, sind *rsh, rexec,* X-Windows*,* RPC-basierende Dienste wie NFS und der TCP-Wrapper, der ansonsten ein sehr sinnvoller Dienst zur Einrichtung einer Zugangskontrolle für TCP/IP-vernetzte Systeme ist. Leider sind auch die in Schicht 2 des OSI-Modells eingesetzten Adressen wie Ethernet- oder Hardware-Adressen leicht zu fälschen und bieten somit für eine Authentisierung keine zuverlässige Grundlage.

In LANs, in denen das Address Resolution Protocol (ARP) eingesetzt wird, sind sehr viel wirkungsvollere Spoofing-Angriffe möglich. ARP dient dazu, zu einer 32-Bit großen IP-Adresse die zugehörige 48-Bit große Hardware- oder Ethernet-Adresse zu finden. Falls in einer internen Tabelle des Rechners kein entsprechender Eintrag gefunden wird, wird ein ARP-Broadcast-Paket mit der unbekannten IP-Nummer ausgesandt. Der Rechner mit dieser IP-Nummer sendet dann ein ARP-Antwort-Paket mit seiner Hardware-Adresse zurück. Da die ARP-Antwort-Pakete nicht manipulationssicher sind, reicht es dann meist schon, die Kontrolle über einen der Rechner im LAN zu bekommen, um das gesamte Netz zu kompromittieren.

G 5.49 Missbrauch des Source-Routing

Der Missbrauch des Routing-Mechanismus und -Protokolls ist eine sehr einfache protokoll-basierte Angriffsmöglichkeit. In einem IP-Paket lässt sich der Weg, auf dem das Paket sein Ziel erreichen soll oder den die Antwortpakete nehmen sollen, vorschreiben. Die Wegbeschreibung kann aber während der Übertragung manipuliert werden, so dass nicht die durch die Routing Einträge vorgesehenen sicheren Wege benutzt werden (z. B. über die Firewall), sondern andere unkontrollierte Wege.

G 5.50 Missbrauch des ICMP-Protokolls

Das Internet Control Message Protocol (ICMP) hat als Protokoll der Transportschicht die Aufgabe, Fehler- und Diagnoseinformationen zu transportieren. Durch Missbrauch von ICMP-Nachrichten kann ein Angreifer sowohl den Netzbetrieb stören als auch Informationen über das interne Netz herausfinden, die ihm bei der Planung eines Angriffs nützen:

- Durch ICMP-*Redirect* Nachrichten können die Routing-Tabellen von Rechnern manipuliert werden.
- ICMP-*Unreachable* Nachrichten können dazu benutzt werden, bestehende Verbindungen zu stören oder ganz zu unterbrechen.
- Die verschiedenen ICMP-*Request* Nachrichtentypen (*Echo Request, Information Request, Timestamp Request, Address Mask Request*) können auf einfache Weise dazu benutzt werden, das interne Netz einer Organisation zu "kartographieren" (*ICMP Sweeps*).
- Auch gefälschte ICMP-*Reply* Nachrichten können dazu benutzt werden, um Informationen über das interne Netz herauszufinden, indem sie die Zielrechner dazu bewegen, auf diese mit einer Fehlermeldung zu antworten.
- Verschiedene Betriebssysteme unterscheiden sich in der Art und Weise, wie sie auf bestimmte ICMP-Nachrichten reagieren. Neben der Information darüber, dass eine bestimmte Adresse aktiv ist können ICMP-Antworten daher auch verraten, unter welchem Betriebssystem der betreffende Rechner läuft (*Fingerprinting*).
- Fehlerhafte Implementierungen von ICMP in einigen Betriebssystemen haben in der Vergangenheit zu Sicherheitsproblemen geführt:
  - Rechner mit Windows 95 konnten durch bestimmte ICMP-Echo Pakete ("Ping of Death") zum Absturz gebracht werden.
  - In ICMP-Antwortpaketen verschiedener Betriebssysteme konnten Ausschnitte aus dem Arbeitsspeicher des betreffenden Rechners enthalten sein. Im Extremfall könnten auf diese Weise Passwörter oder kryptographische Schlüssel an einen externen Rechner übermittelt werden.
- Jede Art von ICMP-Nachrichten kann auch dafür benutzt werden, einen verdeckten Informationskanal zu schaffen, auf dem Daten aus dem internen Netz nach draußen zu transportiert werden können.

G 5.51 Missbrauch der Routing-Protokolle

Routing Protokolle wie RIP (Routing Information Protocol) oder OSPF (Open Shortest Path First) dienen dazu, Veränderungen der Routen zwischen zwei vernetzten Systemen an die beteiligten Systeme weiterzuleiten und so eine dynamische Änderung der Routing-Tabellen zu ermöglichen. Es ist leicht möglich, falsche RIP-Pakete zu erzeugen und somit unerwünschte Routen zu konfigurieren.

Der Einsatz von dynamischem Routing ermöglicht es, Routing-Informationen an einen Rechner zu schicken, die dieser in der Regel ungeprüft zum Aufbau seiner Routing-Tabellen benutzt. Dies kann ein Angreifer ausnutzen, um gezielt den Übertragungsweg zu verändern.

G 5.52 Missbrauch von Administratorrechten im Windows NT/2000/XP/Server 2003 System

Eine missbräuchliche Administration liegt vor, wenn vorsätzlich recht- oder unrechtmäßig erworbene Administratorberechtigungen und -rechte ausgenutzt werden, um dem System oder dessen Benutzer zu schaden.

Beispiel:

- **Besitzübernahme beliebiger Dateien**
  Durch missbräuchliche Nutzung des Rechtes zur Besitzübernahme beliebiger Dateien kann sich ein Administrator unter Windows NT/2000/XP/Server 2003 Zugriff auf beliebige Dateien verschaffen, obwohl deren Eigentümer ihm diesen Zugriff explizit durch entsprechende Zugriffskontrollen verwehrt haben. Eine Zugriffsübernahme kann allerdings vom ursprünglichen Eigentümer der Dateien erkannt werden, da der Administrator sich hierbei zum Besitzer der betreffenden Dateien machen muss. Unter Windows NT/2000/XP/Server 2003 ist keine Funktion verfügbar, um diese Änderung wieder rückgängig zu machen. Dagegen bietet Windows Server 2003 die Möglichkeit, die Besitzübernahme zu verschleiern und den Besitz an einen beliebigen Benutzer zurückzugeben. Ein Administrator kann auch ohne Besitzübernahme unbemerkt auf Benutzerdateien zugreifen, in dem er sich z. B. in die Gruppe Sicherungs-Operatoren einträgt und ein Backup der Dateien durchführt, die er lesen will.

- **Fälschung von Protokolldaten**
  Es gibt verschiedene Möglichkeiten, missbräuchlich Administratorrechte auszunutzen. Dazu gehören unzulässige Zugriffe auf Dateien, Veränderungen der Protokollierungseinstellungen und der Vorgaben für Benutzerkonten. Andere Möglichkeiten des Missbrauchs bestehen in der Fälschung von Protokollinformationen durch Verstellen der Systemzeit oder in der detaillierten Verfolgung der Tätigkeiten einzelner Benutzer.

- **Booten von Fremdmedien**
  In Abhängigkeit von der zugrunde liegenden Hardware kann bei Zugangsmöglichkeit zur Konsole bzw. zum Systemgehäuse das System gebootet werden. Dies ermöglicht gegebenenfalls die Manipulation der Konfiguration, wenn hierbei von einem Fremdmedium gebootet oder ein anderes Betriebssystem ausgewählt werden kann.

G 5.53 Bewusste Fehlbedienung von Schutzschränken aus Bequemlichkeit

Eine häufig festzustellende Form der absichtlichen Fehlbedienung von Schutzschränken mit mechanischen Codeschlössern besteht darin, nach Schließen eines Schutzschrankes den Code nicht zu verwerfen, um den Code beim Öffnen nicht wieder eingeben zu müssen. Dieses Fehlverhalten reduziert den Schutzwert des Schrankes gegen unbefugten Zugriff, da hierdurch einem Dritten das Öffnen des Schutzschrankes ohne Kenntnis des Codes ermöglicht wird.

Ebenso häufig anzutreffen ist der Umstand, dass Schutzschränke bei kurzfristigem Verlassen des Raumes nicht verschlossen werden, um sich das Öffnen des Schrankes nach Rückkehr zu ersparen. Dies reduziert ebenfalls den Schutzwert gegen unbefugten Zugriff.

G 5.54 Vorsätzliches Herbeiführen eines Abnormal End

Ein Netware ABEND (Abnormal End) wird hervorgerufen, wenn das Netware Betriebssystem aufgrund von Hard- und/oder Softwareproblemen nicht mehr in der Lage ist, Netzprozesse ordnungsgemäß weiterzuführen bzw. zu steuern. Der Fileserver wird in diesen Fällen gestoppt und muss neu gestartet werden.

Hat ein Angreifer Zugriff auf die Konsole des Novell Netware Servers, so kann ein Netware ABEND durch die Eingabe bestimmter Parameter vorsätzlich herbeigeführt werden.

Der ABEND eines Novell Netware Servers kann sogar von jedem, der Zugriff auf das Netz hat, herbeigeführt werden, ohne das ein autorisiertes Login auf dem Novell Netware Server erfolgen muss. Durch den Aufruf des Programms *SYS:\PUBLIC\RENDIR.EXE* mit zusätzlichen Parametern kann jede Workstation im Status "Attached" den ABEND eines Novell Netware Servers provozieren.

G 5.55 Login Bypass

Die Login-Scripts (System-Login-Script, User-Login-Script) eines Novell Netware Servers erstellen, nach erfolgter Anmeldung am Novell Netware Server, die persönliche Netzumgebung für den Benutzer.

Durch die Verwendung von Optionen beim Ausführen von *LOGIN.EXE* unter Novell Netware werden weder das System-Login-Script noch das User-Login-Script des ausgewählten Novell Netware Servers ausgeführt. Sicherheitseinstellungen die in die Login-Scripts implemetiert wurden werden somit umgangen. Hierdurch ist es dem Benutzer nach dem autorisierten Login möglich, sich mit Hilfe des Map Kommandos unabhängig von den in den Login-Scripts (System-Login-Script, User-Login-Script) festgelegten Parametern auf dem Novell Netware Server zu "bewegen". In Verbindung mit einer unzureichenden Rechtevergabe kann dies dazu führen, dass Informationen, die nicht für den Benutzer zugänglich sein sollen, diesem zugänglich werden.

G 5.56 Temporär frei zugängliche Accounts

Bei der Einrichtung eines neuen User-Accounts wird dieser standardmäßig ohne Passwort eingerichtet. Von Seiten des Netzbetriebssystems besteht hierbei keinerlei Zwang, ein Passwort zu vergeben, obwohl dieses in den Standardeinstellungen ("Default Account Balance/Restrictions") eingestellt werden kann. Diese neu eingerichteten Accounts sind somit für jederman frei zugänglich, ohne dass eine Passwortabfrage erfolgt. Die Gefährdung des sogenannten "race on new accounts" ist hierbei umso höher einzuschätzen, je privilegierter der neue Account auf dem Novell Netware Server ist.

In diesem Zusammenhang wird darauf hingewiesen, dass verschiedene Versionen (z. B. Vers. 3.75, Vers. 3.76) des Netware Utilities *SYS:\PUBLIC\SYSCON.EXE* bei der Vergabe eines neuen Passwortes durch einen Systemverwalter dieses Passwort unverschlüsselt über das Netz übertragen.

G 5.57 Netzanalyse-Tools

Werden die im Netzsegment übertragenen Informationen nicht verschlüsselt, so können diese Informationen mit Hilfe von Netzanalyse-Tools, den sogenannten "Sniffern", im Klartext ausgelesen werden. Hierbei ist auch zu beachten, dass diese "Sniffer" keineswegs immer als "Hackingsoftware" betrachtet werden können, da viele Produkte, die dem Management des Netzes dienen, eine derartige Funktion beinhalten.

Trace-Funktionen des z/OS-Betriebssystems

Trace-Funktionen unter z/OS

Unter z/OS stehen dem Bediener sogenannte Trace-Funktionen zur Verfügung. Mit Hilfe der *Generalized Trace Facility (GTF)* lassen sich in SNA- oder TCP/IP-Netzen unter anderem Terminal-Sessions überwachen. Wird die Trace-Funktion auf die Session des RACF-Administrators angewandt, kann unter Umständen dessen Passwort ermittelt werden, wenn die Inhalte der Session nicht verschlüsselt sind. Eine ähnliche Trace-Funktion ist in der *Network Logical Data Manager*-Komponente (*NLDM)* des Produktes *NetView* enthalten.

G 5.58 "Hacking Novell Netware"

"Hacking Novell Netware" kann prinzipiell auf zwei Arten durchgeführt werden.

Zum einen kann, ausgehend von einer Workstation, eine gezielte Attacke gegen einen User Account erfolgen, um dessen Passwort in Erfahrung zu bringen.

Die gezielte Attacke gegen einen User Account kann hierbei über einen sogenannten Brute Force Angriff erfolgen, bei dem eine Workstation (Status: Attached) Login-Versuche unter einem zuvor festgelegten User Account durchführt und hierbei mit Hilfe eines Algorithmus oder eines mitgelieferten Wörterbuches Passwörter generiert bzw. ausprobiert.

Mit Hilfe des Programms *HACK.EXE* kann ein autorisierter Benutzer einen Angriff gegen den Account des Supervisors durchführen. Es kann, eine Schwachstelle im Betriebssystem ausnutzend, alle Benutzer des Novell Netware Servers in einen Supervisor-äquivalenten Zustand versetzten, den Supervisor ausloggen sowie dessen Passwort verändern, vorausgesetzt der Account des Supervisors ist zum Zeitpunkt der Aktivierung von *HACK.EXE* auf dem Novell Netware Server eingeloggt.

Weiterhin kann eine Attacke durch eine direkte Manipulation am Server durchgeführt werden, um beispielsweise einen Supervisor-äquivalenten Account zu generieren.

Durch das Einspielen und Aktivieren von NLMs (Netware Loadable Modules), die als Notfalltools entwickelt worden sind, besteht beispielsweise die Möglichkeit, einen speziellen Benutzer zu erzeugen, dessen Rechte auf dem Novell Netware Server äquivalent zu denen des Supervisors sind.

Diese Tools, wie z. B. *SETPWD.NLM,* arbeiten auch in Netware 4 Netzen. Deshalb sei an dieser Stelle noch einmal auf M 1.42 *Gesicherte Aufstellung von Novell Netware Servern* hingewiesen.

Die meisten dieser Programme sind frei über das Internet erhältlich. Sie sind, hinsichtlich ihrer Handhabung, auch von "Computer-Laien" zu bedienen, da sie keine spezifischen Novell Netware Kenntnisse erfordern.

G 5.59 Missbrauch von Administratorrechten unter Novell Netware 3.x

Der Supervisor Account bzw. ein Supervisor-äquivalenter Account besitzt, mit Ausnahme der Bindery Informationen (z. B. Passwörter), die vollständige Kontrolle über einen Novell Netware Server.

Hierdurch ist es einem Account der Sicherheitsstufe "Supervisor" möglich, auf alle gespeicherten Informationen des Servers zuzugreifen, wenn diese nicht durch zusätzliche Sicherheitsmechanismen, wie z. B. Verschlüsselung geschützt werden. Damit haben autorisierte Benutzer dieser Accounts die Möglichkeit, Daten anderer Benutzer zu lesen, zu löschen bzw. zu verändern.

G 5.60 Umgehen der Systemrichtlinien

Besteht lokaler Zugang zu einem nicht vernetzten PC unter Windows 95, ist es möglich, die Passwortdatei (*name.PWL*), die zu einer bestimmten Benutzer-Kennung gehört, zu löschen. Der Zugang mit dieser Benutzer-Kennung ist dann ohne Kenntnis des Benutzer-Passwortes möglich. Dies ist insbesondere dann kritisch, wenn ein nicht vernetzter Windows 95-Rechner durch Systemrichtlinien für bestimmte Benutzer eingeschränkt ist, aber eine Administrator-Kennung (z. B. *ADMIN*) existiert, die alle Rechte besitzt. Durch löschen der *ADMIN.PWL* durch einen auf diesem PC eingeschränkten, aber dennoch berechtigten Benutzer kann dieser sich anschließend als Administrator anmelden. Die für den Benutzer eingestellten Einschränkungen bzw. Systemrichtlinien werden somit umgangen.

G 5.61 Missbrauch von Remote-Zugängen für Managementfunktionen von Routern

Router verfügen über Remote-Zugänge für Managementfunktionen. Über diese Zugänge können alle Administrations- und Wartungstätigkeiten sowie Signalisierungsfunktionalitäten abgewickelt werden. Solche Remote-Zugänge sind besonders in größeren Netzen mit mehreren Routern bzw. bei der LAN-Kopplung über Weitverkehrsnetze nützlich und teilweise unverzichtbar.

Bei der Art des Remote-Zugangs lässt sich unterscheiden zwischen:

- "Modem"-Zugang über dedizierte Schnittstelle (z. B. V.24) und
- direkter Zugang über reservierte Bandbreiten.

Wird für das Netzmanagement das Protokollverfahren SNMP (Simple Network Management Protocol) eingesetzt, ergeben sich aufgrund fehlender bzw. noch nicht umgesetzter Sicherheitsfunktionalitäten weitere Gefährdungen, die über den direkten Missbrauch der ungeschützten Remote-Schnittstellen hinausgehen:

- Ein nicht autorisierter Benutzer fängt Datenpakete einer SNMP-Management-Station ab und verändert die darin enthaltenen Parameterwerte für seine Zwecke. Nach dieser Manipulation werden die manipulierten Datenpakete zur eigentlichen Zielstation gesendet. Das Empfängergerät hat keine Möglichkeit, diese Datenmanipulation zu erkennen und reagiert deshalb auf die im Paket enthaltenen Informationen so, als ob diese von der Management-Station direkt abgesandt worden wären.
- Erhält der Besitzer einer Netzmanagement-Station Zugang zum mittels SNMP verwalteten Netz, ist das Vorspiegeln einer Community (Verwaltungsbereich innerhalb von SNMP) möglich. Durch diese Maskerade täuscht ein nicht autorisierter Benutzer eine autorisierte Identität vor und kann alle Informationen der Agents (im Netz zu verwaltende Objekte, bspw. Router) auslesen sowie sämtliche Managementoperationen durchführen. Der Agent hat keine Möglichkeit zwischen der richtigen und der falschen Identität zu unterscheiden.

G 5.62 Missbrauch von Ressourcen über abgesetzte IT-Systeme

Abgesetzte IT-Systeme (z. B. Telearbeitsplätze) können meist auf vielfältige Ressourcen eines unternehmensweiten Netzes zugreifen. Grundsätzlich besteht deshalb immer die Gefahr des Daten- und Programmdiebstahls.

Bestehen zu einem Unternehmensnetz auch Zugriffsmöglichkeiten von abgesetzten IT-Systemen (z. B. Telearbeitsplätzen), besteht grundsätzlich die Gefahr, dass in dem Unternehmensnetz angebotenen Dienstleistungen missbraucht werden können. Die Bereitstellung von Kommunikationsservern im Netz (z. B. Fax-Gateway, Internet-Anbindung usw.) kann bei einer nicht erlaubten privaten Nutzung zu einem Gebührenbetrug führen.

G 5.63 Manipulationen über den ISDN-D-Kanal

Die Summe aller physikalischen Verbindungen der Kommunikationsteilnehmer zu einer ihnen zugeordneten digitalen Vermittlungsstelle bezeichnet man als Anschlussnetz. Innerhalb des Anschlussnetzes existieren zahlreiche Verteiler und Übergabepunkte, die teilweise frei zugänglich und nicht aufwendig gesichert sind (z. B. Kabelverzweiger). Die Kommunikation auf dem Anschlussnetz kann im einfachsten Fall durch das mechanische Beschädigen einer Anschlussleitung unterbrochen werden.

Weiterhin ist es mit Hilfe eines ISDN-Protokollanalysators möglich, Kommunikationsinhalte aufzuzeichnen und auszuwerten. Mittels Einschleifen eines Protokollanalysators ist ebenfalls das Manipulieren von Steuerungsinformationen im D-Kanal des ISDN möglich. Die Kommunikationskomponenten des angegriffenen Kommunikationsteilnehmers (also ISDN-Karten, ISDN-Router, TK-Anlagen etc.) können so zu Reaktionen veranlasst werden, die ihren ordnungsgemäßen Betrieb beeinträchtigen oder zur Kompromittierung gespeicherter Daten führen.

G 5.64 Manipulation an Daten oder Software bei Datenbanksystemen

Durch ein gezieltes Manipulieren von Daten werden diese vorsätzlich verfälscht oder unbrauchbar gemacht. Die entsprechenden Folgen sind in G 4.28 *Verlust von Daten einer Datenbank* und G 4.30 *Verlust der Datenbankintegrität/-konsistenz* beschrieben.

Werden die Dateien einer Datenbank oder der Datenbank-Standardsoftware gezielt gelöscht oder verändert, so führt dies zur vorsätzlichen Zerstörung des gesamten Datenbanksystems (siehe G 4.26 *Ausfall einer Datenbank*).

Es ist prinzipiell nicht verhinderbar, dass Benutzer mit den entsprechenden Zugangs- und Zugriffsberechtigungen gezielt Datenmanipulationen durchführen oder eine Datenbank zerstören können. Ist es außerdem möglich, die Zugangs- und Zugriffsberechtigungen zu umgehen (z. B. durch eine fehlerhafte Administration des DBMS), so können sich auch unberechtigte Benutzer Zugang zur Datenbank verschaffen und dort Manipulationen vornehmen.

G 5.65 Verhinderung der Dienste eines Datenbanksystems

Um die IT-Benutzer daran zu hindern, Funktionen und Dienste eines Datenbanksystems zu verwenden, die ihnen normalerweise zur Verfügung stehen, können gezielte Angriffsmethoden eingesetzt werden. Neben den in G 5.28 *Verhinderung von Diensten* (Denial of Service) aufgeführten Beispielen, kann diese Gefährdungslage im Bereich Datenbanken unter folgenden Bedingungen entstehen:

Zu viele Abfragen

Das Problem einer hohen Anzahl paralleler Abfragen tritt häufig bei Internet-Datenbanken auf, die über Schnittstellen (Interfaces), z. B. Common Gateway Interface (CGI) oder Active Server Pages (ASP), Ausgaben für Web-Browser produzieren.

Zu komplexe Abfragen

Wenn in großen Datenbanken nach Begriffen gesucht wird, die in keiner Tabelle enthalten sind, dauern Abfragen am längsten, da zumindest alle Einträge der Index-Tabelle durchsucht werden müssen. Werden in einer Abfrage mehrere solcher Begriffe mit ODER verknüpft, verlängert sich die Antwortzeit der Abfrage entsprechend.

Fehlerhafte Statements

Der Parser stellt im Datenbankmanagementsystem (DBMS) die Implementierung der vom DBMS zur Verfügung gestellten Abfragesprache (z. B. SQL) dar. Der Parser überprüft jede an die Datenbank gerichtete Abfrage auf Korrektheit gegenüber der gegebenen Abfragesprache und führt die Abfrage nach erfolgreicher Prüfung aus. Sollte die Abfragesprache nicht eindeutig und abgeschlossen definiert oder die Implementierung der Abfragesprache im Parser fehlerhaft sein, können manipulierte Statements zur Verhinderung von Diensten der Datenbank ausgenutzt werden, wenn die Statements durch den Parser akzeptiert werden. Der Parser überprüft diese Statements und führt sie nach erfolgreicher Prüfung aus, mit nicht vorhersagbaren Ergebnissen, bis hin zum Absturz.

Zu lange Ausgabe-Ergebnisse

Abfragen, die uneingeschränkt oder auf Kriterien eingeschränkt sind, die sehr oft zu finden sind, erzeugen unter Umständen sehr lange Ausgabe-Ergebnisse, die das DBMS überlasten können.

Buffer Overflow

Der Ausfall eines Datenbanksystems kann möglicherweise auch durch einen Speicherüberlauf (Buffer Overflow) herbeigeführt werden. Hierbei kann ein Angreifer beispielsweise versuchen, eine komplexe Abfrage zu konstruieren, die das DBMS stark belastet. Zusätzlich wird die Komplexität der Abfrage erhöht, indem überlange Parameterwerte hinzugefügt werden, um den Parser zu überlasten. Die Folgen sind nicht vorhersehbar und reichen bis zum Absturz des DBMS oder unkontrollierten Veränderungen an den Daten.

G 5.66 Unberechtigter Anschluss von IT-Systemen an ein Netz

Grundsätzlich kann der unberechtigte Anschluss eines IT-Systems in ein bestehendes Netz (durch ein Aufschalten auf die zugehörige Verkabelung oder durch die Nutzung von Schnittstellen in Verteiler- oder Büroräumen) nicht verhindert werden. Es gibt keinen Verkabelungstyp, der ein solches Ankoppeln verhindern würde, lediglich der erforderliche Aufwand zum Auftrennen der Verkabelung und zum Lesen bzw. Einspielen von Daten unterscheidet die verschiedenen Typen.

Die unberechtigte Integration eines Rechners in ein Netz ist nur sehr schwer zu entdecken und bleibt meistens unbemerkt. Ein solcher Zugriff betrifft den gesamten Netzverkehr in dem zugehörigen Segment und kann z. B.

- die Manipulation an Daten oder Software,
- das Abhören von Leitungen,
- die Manipulation an Leitungen,
- das Wiedereinspielen von Nachrichten,
- die Maskerade als anderer Kommunikationsteilnehmer,
- eine Analyse des Nachrichtenflusses,
- die Verhinderung von Diensten,
- die unberechtigte Ausführung von Netzmanagement-Funktionen oder
- den unberechtigten Zugang zu den aktiven Netzkomponenten

begünstigen.

G 5.67 Unberechtigte Ausführung von Netzmanagement-Funktionen

Durch die unberechtigte Ausführung von Netzmanagement-Funktionen können aktive Netzkomponenten teilweise oder vollständig kontrolliert werden. Die Kontrollmöglichkeiten werden u. a. durch das verwendete Netzmanagement-Protokoll, wie z. B. SNMP oder CMIP/CMOT bestimmt. Daraus kann ein Verlust der Netzintegrität, der Verfügbarkeit einzelner oder aller Netzbestandteile sowie der Vertraulichkeit bzw. Integrität von Daten resultieren.

Unter Verwendung eines Serviceprotokolls, wie z. B. SNMP, können dedizierte Ports aktiver Netzkomponenten aktiviert oder insbesondere auch deaktiviert werden. Weiterhin können z. B. die VLAN-Konfiguration, Routing-Tabellen, die Router-Konfiguration sowie die Konfiguration von Filtern manipuliert werden (siehe G 3.28 *Ungeeignete Konfiguration der aktiven Netzkomponenten*). Daneben kann die Möglichkeit einer Verteilung von Firmware-Updates über das Netz genutzt werden, um unberechtigt Software auf aktiven Netzkomponenten zu installieren, mit deren Unterstützung wiederum vielfältige Angriffe auf Komponenten innerhalb des Netzes durchgeführt oder unterstützt werden können.

G 5.68 Unberechtigter Zugang zu den aktiven Netzkomponenten

Aktive Netzkomponenten haben üblicherweise eine serielle Schnittstelle (RS-232), an die von außen ein Terminal oder ein tragbarer PC angeschlossen werden kann. Dadurch ist es möglich, aktive Netzkomponenten auch lokal zu administrieren.

Bei unzureichend gesicherten Schnittstellen ist es denkbar, dass Angreifer einen unberechtigten Zugang zur Netzkomponente erlangen. Sie können somit nach Überwindung der lokalen Sicherheitsmechanismen (z. B. des Passwortes) ggf. alle Administrationstätigkeiten ausüben.

Dabei können durch das Auslesen der Konfiguration aktiver Netzkomponenten ggf. schutzbedürftige Informationen über die Topologie, die Sicherheitsmechanismen und die Nutzung eines Netzes in Erfahrung gebracht werden. Ein Auslesen der Konfigurationsdaten ist z. B. durch den Anschluss eines Terminals oder tragbaren PCs an die serielle Schnittstelle der aktiven Netzkomponente, durch den Zugriff auf die aktive Netzkomponente über das lokale Netz oder durch das Mitlesen der Daten auf einem Bildschirm oder Display möglich, falls die aktive Netzkomponente gerade administriert bzw. konfiguriert wird.

G 5.69 Erhöhte Diebstahlgefahr am häuslichen Arbeitsplatz

Der häusliche Arbeitsplatz ist in der Regel nicht so abgesichert wie der Arbeitsplatz in einem Unternehmen oder einer Behörde. Dort ist, bedingt durch aufwendigere Vorkehrungen (Verwendung von Sicherheitstüren, Einbruchschutz, Pförtnerdienst usw.) die Gefahr, dass jemand in das Gebäude unbefugt eindringt, weit geringer als bei einem Privathaus.

Einbruch und Diebstahl im Privathaus dienen meist der Bereicherung. Dabei gestohlene dienstliche IT wird mit dem Ziel der Veräußerung gestohlen. Die mitentwendeten Daten können ggf. auch einen Wert darstellen, der zum Beispiel durch Erpressung oder Informationsweitergabe an Konkurrenzunternehmen realisiert werden kann.

G 5.70 Manipulation durch Familienangehörige und Besucher

Am häuslichen Arbeitsplatz ist mit Angehörigen und Besuchern der Familie zu rechnen, so dass die Gefahr besteht, dass bei unzureichender Sicherung die dienstliche IT durch diese manipuliert werden kann. So sollte auch betrachtet werden, dass durch Familienangehörige private Software (z. B. Computerspiele) aufgespielt werden könnte, dass durch Kinder die IT zerstört werden kann oder dass dienstliche Datenträger zweckentfremdet weitergegeben werden können. Diese teils fahrlässigen oder auch absichtlichen Manipulationen können sowohl die Vertraulichkeit und Integrität der dienstlichen Daten betreffen als auch die Verfügbarkeit von Daten und IT beeinträchtigen.

G 5.71 Vertraulichkeitsverlust schützenswerter Informationen

Für Informationen, die einen Schutzbedarf bezüglich ihrer Vertraulichkeit besitzen (wie Passwörter, personenbezogene Daten, firmen- oder amtsvertrauliche Informationen, Entwicklungsdaten), besteht die inhärente Gefahr, dass die Vertraulichkeit durch Unachtsamkeit oder auch durch vorsätzliche Handlungen beeinträchtigt wird. Dabei kann auf diese vertraulichen Informationen an unterschiedlichen Stellen zugegriffen werden, beispielsweise

- auf Speichermedien innerhalb von Rechnern (Festplatten),
- auf austauschbaren Speichermedien (Disketten, Magnetbänder),
- in gedruckter Form auf Papier (Ausdrucke, Akten) und
- auf Übertragungswegen während der Datenübertragung.

Auch die Art und Weise, wie die vertraulichen Informationen gewonnen werden, kann sehr unterschiedlich sein:

- Auslesen von Dateien,
- Kopieren von Dateien,
- Wiedereinspielen von Datensicherungsbeständen,
- Diebstahl des Datenträgers und anschließendes Auswerten,
- Abhören von Übertragungsleitungen und
- Mitlesen am Bildschirm.

Je höher der Vertraulichkeitsbedarf der Informationen ist, umso größer ist auch der Anreiz für Dritte, diese Informationen zu erlangen und zu missbrauchen.

G 5.72 Mißbräuchliche E-Mail-Nutzung

Der Missbrauch von E-Mailsystemen kann an verschiedenen Punkten aufsetzen, beim Benutzer, im internen Netz, bei einem der übertragenden Mailserver oder beim Empfänger.

Wenn der Zugang zum E-Mail-Programm eines Benutzers oder zum E-Mail-System einer Organisation nicht gut genug geschützt ist, kann ein Unbefugter sich unberechtigt Zugang für manipulative Zwecke verschaffen. Dabei können neben den Übertragungskosten auch Schäden dadurch entstehen, dass ein Unbefugter sich als Berechtigter ausgibt.

Ebenso muss verhindert werden, dass E-Mails von Unbefugten gelesen werden können. Vertrauliche Informationen können so bekannt werden, ihren Wert verlieren oder zum Schaden des Empfängers genutzt werden.

Beispiele:

- Ein Abteilungsleiter verließ für kurze Zeit sein Büro mit ungesichertem IT-System, auf dem das Mailprogramm bereits gestartet war und für das er sich bereits authentisiert hatte. Ein zufällig vorbeigekommener Kollege hielt es für einen gelungenen Scherz, unter dessen E-Mail-Kennung anderen Kollegen "Kündigungen" oder Arbeitsaufträge zu schicken.
- Ein Mitarbeiter verbreitet unter seiner dienstlichen E-Mail-Adresse private Ansichten, die dem Ansehen seines Arbeitgebers schaden können.

G 5.73 Vortäuschen eines falschen Absenders

Es ist relativ einfach, beim Versand von E-Mail einen falschen Absender anzugeben, da bei der Weiterleitung von SMTP-basierender E-Mail meist nicht überprüft wird, wo die Nachricht herkommt, nur wo sie hingehen soll. Darüber hinaus erlauben es viele E-Mail-Clients, beliebige Absenderangaben einzutragen. Dadurch können Schäden entstehen, wenn der Empfänger die darin enthaltenen Informationen als authentisch und verbindlich ansieht.

Beispiele:

- Die meisten der zahllosen Spam-E-Mails, die täglich die Postfächer der Benutzer vertopfen, tragen einen gefälschten Absender.
- Einige der verschiedenen E-Mail-Würmer, die seit mehreren Jahren im Internet ihr Unwesen treiben, benutzen als Absenderadresse eine Adresse aus dem E-Mail-Adressbuch des Benutzers, dessen E-Mail-Programm sie gerade befallen haben. So erhalten die nächsten Opfer die E-Mail, die den Wurm enthält, mit einer bekannten Absenderadresse und sind so eher gefährdet, die E-Mail oder gar das infizierte Attachment zu öffnen.
- Mit vielen verbreiteten E-Mail-Programmen ist es ohne Probleme möglich, eine E-Mail mit gefälschten Absenderangaben ohne Passwortüberprüfung auf den E-Mail-Server weiterzuleiten. Die so versandte E-Mail wird zwar eventuell bei nicht erfolgter Benutzer-Authentisierung im Feld "X-Sender" mit "Unverified" gekennzeichnet. Dies wird aber erfahrungsgemäß von kaum einem Empfänger bemerkt, ohnehin werden diesese Felder von den meisten E-Mail-Programmen in der Standardkonfiguration nicht angezeigt.

G 5.74 Manipulation von Alias-Dateien oder Verteilerlisten

Um häufig wiederkehrende E-Mailadressen nicht ständig neu eingeben zu müssen, kann über die Vergabe von Alias-Namen eine "sprechende" Schreibweise für E-Mailadressen gewählt werden oder es kann über die Erstellung von Verteilerlisten ein größerer Empfängerkreis komfortabel angewählt werden. Werden solche Alias-Namen oder Verteilerlisten unbefugt geändert, kann auf diese Weise die Weiterleitung einer E-Mail an einen gewünschten Empfänger unterbunden oder die Weiterleitung zu einem unerwünschten Empfänger erfolgen. Besonders gefährdet sind hier Alias-Dateien oder Adressbücher, die zentral geführt werden.

G 5.75 Überlastung durch eingehende E-Mails

Eine E-Mail-Adresse kann absichtlich blockiert werden, indem andauernd umfangreiche E-Mails (ggf. mit sinnlosem Inhalt) zugesandt werden. Dies kann beispielsweise passieren, weil der Benutzer die Netiquette nicht beachtet hat und sich dadurch in Newsgruppen unbeliebt gemacht hat. Als Netiquette (die Netz-Etiquette) werden die Höflichkeitsregeln bezeichnet, die sich mit der Zeit bei der Nutzung des Internet, insbesondere in den Newsgruppen, eingebürgert haben und deren Einhaltung gewährleisten soll, dass jeder das Internet effizient und zu aller Zufriedenheit benutzen kann.

Durch vorsätzlich erzeugtes hohes Verkehrsaufkommen kann das lokale Mailsystems überlastet werden, so dass es funktionsuntüchtig wird. Dies kann sogar solche Ausmaße annehmen, dass der Provider den Benutzer bzw. dessen ganze Organisation vom Netz nimmt.

Ein Mailsystem kann auch überlastet werden, wenn die Mitarbeiter an E-Mail-Kettenbrief-Aktionen teilnehmen. So hat schon Mitte der achtziger Jahre eine Kettenmail-Aktion zu Weihnachten weltweit viele IT-Systeme lahm gelegt. Hierbei erhielten Benutzer eine E-Mail mit Weihnachtsgrüßen und einer ansprechenden Graphik und wurden aufgefordert, diese E-Mail zu kopieren und zehn andere Benutzer weiterleiten.

G 5.76 Mailbomben

Unter dem Begriff Mailbomben werden E-Mails verstanden, die absichtlich eingebaute Schadfunktionen enthalten. Diese sind üblicherweise in den Anlagen der E-Mail enthalten. Eine solche Anlage erzeugt z. B. beim Aktivieren zum Lesen oder nach dem Auspacken Unmengen von Unterverzeichnissen oder beansprucht sehr viel Festplattenplatz. Vielfach wird auch die gezielte Überlastung von E-Mailadressen durch eingehende E-Mails mit meist sinnlosem Inhalt (siehe G 5.75 *Überlastung durch eingehende E-Mails*) als Mailbombing bezeichnet.

G 5.77 Mitlesen von E-Mails

Übertragung im Klartext

E-Mail wird im Normalfall im Klartext übertragen. Auf allen IT-Systemen, über die die Daten übertragen werden, können diese mitgelesen oder sogar unbemerkt verändert werden, wenn sie nicht kryptographisch gesichert sind. Bei der Übertragung von E-Mails über das Internet können sehr viele IT-Systeme beteiligt sein, ohne dass der genaue Übertragungsweg vorher bekannt ist. Der Übertragungsweg hängt von der Auslastung und Verfügbarkeit der Gateways und Teilen des Netzes ab. Eine E-Mail von einem Stadtteil in den anderen kann sogar über das Ausland weitergeleitet werden.

Speicherung auf dem Mailserver

Der Zugriff auf eingehende E-Mails kann auch über die beim Mailserver des Empfängers geführte Mailbox erfolgen. Sie enthält alle empfangenen E-Mails, je nach Konfiguration nicht nur die ungelesenen, sondern ein Archiv aller in den letzten Monaten eingegangenen Nachrichten. Hierauf hat mindestens der Systemadministrator des Mailservers Zugriff. In manchen Fällen werden auch Kopien ausgehender E-Mails auf dem Mailserver gespeichert. Häufig jedoch legt das Benutzer-Mailprogramm diese auf dem Rechner des Absenders ab.

Beispiele:

- Mehrere Microsoft-interne E-Mails wurden im Antitrust-Verfahren von der Gegenseite benutzt, um deren Position zu untermauern. Diese E-Mails enthielten teilweise diffamierende Aussagen über Microsofts Konkurrenten.
- Ein Anbieter stellt Dienstleistungen über das Internet zur Verfügung. Für die Nutzung ist eine Anmeldung am Server des Dienstleisters erforderlich. Die dafür notwendigen Authentisierungsinformationen werden per E-Mail an die Kunden versandt. Durch Mitlesen dieser E-Mails ist ein Angreifer in der Lage, sich unberechtigt am Server des Dienstleisters anzumelden und auf Kosten der registrierten Kunden Dienste in Anspruch zu nehmen.

G 5.78 DNS-Spoofing

Um im Internet mit einem anderen Rechner kommunizieren zu können, benötigt man dessen IP-Adresse. Diese Adresse setzt sich aus vier Zahlen zwischen 0 und 255 zusammen, also zum Beispiel 194.95.176.226. Da solche Nummern nicht sehr einprägsam sind, wird einer solchen IP-Adresse fast immer ein Name zugeordnet. Das Verfahren hierzu nennt sich DNS (Domain Name System). So kann der WWW-Server des BSI sowohl unter *http://www.bsi.bund.de* als auch unter *http://194.95.176.226* angesprochen werden, da der Name bei der Abfrage in die IP-Adresse umgewandelt wird.

Die Datenbanken, in denen den Rechnernamen die zugehörigen IP-Adressen zugeordnet sind und den IP-Adressen entsprechende Rechnernamen, befinden sich auf so genannten Nameservern. Für die Zuordnung zwischen Namen und IP-Adressen gibt es zwei Datenbanken: In der einen wird einem Namen seine IP-Adresse zugewiesen und in der anderen einer IP-Adresse der zugehörige Name. Diese Datenbanken müssen miteinander nicht konsistent sein! Von DNS-Spoofing ist die Rede, wenn es einem Angreifer gelingt, die Zuordnung zwischen einem Rechnernamen und der zugehörigen IP-Adresse zu fälschen, d. h. dass ein Name in eine falsche IP-Adresse bzw. umgekehrt umgewandelt wird.

Dadurch sind unter anderem die folgenden Angriffe möglich:

- r-Dienste (rsh, rlogin, rsh)

  Diese Dienste erlauben eine Authentisierung anhand des Namens des Clients. Der Server weiß die IP-Adresse des Clients und fragt über DNS nach dessen Namen.

- Web-Spoofing

  Ein Angreifer könnte die Adresse *www.bsi.bund.de* einem falschen Rechner zuweisen, und bei Eingabe von *http://www.bsi.bund.de* würde dieser falsche Rechner angesprochen werden.

Wie leicht es ist, DNS-Spoofing durchzuführen, hängt davon ab, wie das Netz des Angegriffenen konfiguriert ist. Da kein Rechner alle DNS-Informationen der Welt besitzen kann, ist er immer auf Informationen anderer Rechner angewiesen. Um die Häufigkeit von DNS-Abfragen zu verringern, speichern die meisten Nameserver Informationen, die sie von anderen Nameservern erhalten haben, für eine gewisse Zeit zwischen.

Ist ein Angreifer in einen Nameserver eingebrochen, kann er auch die zur Verfügung gestellten Informationen abändern. Der Fall eines direkten Einbruchs auf einen Nameserver soll hier nicht weiter betrachtet werden. Vielmehr geht es darum, prinzipielle Schwächen im DNS aufzuzeigen.

Beispiele:

- Ein Benutzer auf dem Rechner *pc.kunde.de* will zuerst auf *www.firma-x.de* und dann auf den Konkurrenten *www.firma-y.de* zugreifen. Um auf *www.firma-x.de* zugreifen zu können, muss er erst die zugehörige IP-Adresse bei seinem Nameserver *ns.kunde.de* nachfragen. Dieser kennt die

Adresse auch nicht und fragt beim Nameserver von *ns.firma-x.de* nach. Dieser antwortet mit der IP-Adresse, die von *ns.kunde.de* an den Benutzer weitergeleitet und gespeichert wird. Befindet sich in dem Antwortpaket von *ns.firma-x.de* neben der IP-Adresse von *www.firma-x.de* auch noch eine beliebige IP-Adresse für den Rechnernamen *www.firma-y.de*, so wird auch diese gespeichert. Versucht der Benutzer nun, auf *www.firma-y.de* zuzugreifen, fragt der eigene Nameserver *ns.kunde.de* nicht mehr bei dem Nameserver *ns.firma-y.de* nach, vielmehr gibt er die Informationen weiter, die ihm von *ns.firma-x.de* untergeschoben wurden.

- Firma X weiß, dass ein Benutzer mit dem Rechner *pc.kunde.de* auf den Konkurrenzrechner *www.firma-y.de* zugreifen will. Firma X verhindert dies, indem sie den Nameserver *ns.kunde.de* nach der Adresse *www.firma-x.de* fragt. Dieser muss beim Nameserver *ns.firma-x.de* nachfragen und bekommt wie in Beispiel 1 auch die falschen Angaben über *www.firma-y.de* zurück.

Diese beiden Beispiele beruhen darauf, dass ein Nameserver auch zusätzliche Daten, die er gar nicht angefordert hat, akzeptiert. In neuen Versionen bestimmter Software (z. B. *bind*) ist dieser Fehler beseitigt, so dass diese Art von Angriffen verhindert wird. Es ist allerdings unter Verwendung von IP-Spoofing noch immer möglich, falsche DNS-Einträge zu erzeugen. Dieser Angriff ist jedoch technisch viel anspruchsvoller.

G 5.79 Unberechtigtes Erlangen von Administratorrechten unter Windows NT/2000/XP/Server 2003 Systemen

Admin-Konto kann nicht gesperrt werden

Bei jeder Standardinstallation von Windows NT/2000/XP/Server 2003 wird ein lokales Administratorkonto angelegt. Dies betrifft sowohl die Client- als auch die Server-Versionen. Im Gegensatz zu selbst angelegten Konten kann dieses lokale vordefinierte Administratorkonto unter Windows NT/2000 weder gelöscht noch gesperrt werden, um zu verhindern, dass der Administrator vorsätzlich oder versehentlich ausgesperrt wird und somit die Verwaltung unmöglich wird. Problematisch in diesem Zusammenhang ist, dass das vordefinierte Administratorkonto selbst dann nicht gesperrt wird, wenn die in der Kontorichtlinie für eine Sperre eingetragene Anzahl ungültiger Kennworteingaben überschritten wird. Ohne entsprechende Gegenmaßnahmen ermöglicht dies das planmäßige Ausprobieren von Passwörtern mit Hilfe von speziellen Programmen. Erst mit Windows XP/Server 2003 ist es möglich, das lokale vordefinierte Administratorkonto zu deaktivieren. Das Konto kann aber wie auch bereits unter Windows NT/2000 nicht gelöscht werden.

Admin-Passwort im Klartext bei der Übertragung

Es gibt aber noch weitere Möglichkeiten, um in den Besitz eines zu einem Administratorkonto gehörenden Passwortes zu kommen, um damit Administratorrechte zu erlangen. Wird ein Rechner unter dem Betriebssystem Windows NT/2000/XP/Server 2003 fernadministriert, so besteht die Gefahr, dass beim Authentisierungsvorgang das Anmeldepasswort, je nach verwendetem Authentisierungsverfahren, im Klartext übertragen und damit von einem Angreifer aufgezeichnet werden kann. Selbst wenn durch Eingriffe in das System sichergestellt ist, dass die Anmeldepasswörter nur verschlüsselt übertragen werden, ist es möglich, dass ein Angreifer das verschlüsselte Passwort aufzeichnet und mit Hilfe entsprechender Software entschlüsselt. Dies gilt insbesondere für Windows NT, wenn hier das ältere NTLM-Verfahren eingesetzt wird. Unter Windows 2000/XP/Server 2003 wird standardmäßig das Kerberos-Verfahren eingesetzt, das robuster gegen solche Angriffe ist.

Admin-Passwort auf Notfalldiskette

Weiterhin wird jedes Passwort in der Registrierung und in einer Datei, die sich im Verzeichnis *%SystemRoot%\System32\Repair* bzw. auf den Notfalldisketten und gegebenenfalls auf Bandsicherungen befindet, verschlüsselt gespeichert. Gelangt ein Angreifer in den Besitz der entsprechenden Datei, so kann er mit Hilfe entsprechender Software versuchen, das benötigte Passwort zu entschlüsseln.

Schadsoftware

Schließlich ist es mit einer speziellen Schadsoftware möglich, dass ein Angreifer auf dem Windows NT Rechner, an dem er lokal angemeldet ist, ein beliebiges Benutzerkonto der Gruppe *Administratoren* hinzufügt und dem Kontoinhaber damit Administratorrechte verschafft.

Andere Beispiele für Attacken zum unberechtigten Erlangen von administrativen Berechtigungen wären unter anderem:

- Die Erweiterung der Berechtigungen (Privilege Escalation) ist auch durch die Ausnutzung von Schwachstellen in Programmen oder Diensten möglich, die mit administrativen oder Systemberechtigungen ausgeführt werden.
- Technische Attacken können zusammen mit Social Engineering Methoden eingesetzt werden. So kann beispielsweise das lokale System mit normalen Benutzerrechten manipuliert und der Administrator zum Anmelden bewegt werden.
- Kennwörter könnten unter Verwendung eines anderen Boot-Mediums (z. B. Diskette/CD-ROM/USB-Speicher) überschrieben werden.

G 5.80 Hoax

Falschmeldung

Ein Hoax (englisch für Streich, Trick, falscher Alarm) ist eine Nachricht, die eine Warnung vor neuen spektakulären Computer-Viren oder anderen IT-Problemen enthält und Panik verbreitet, aber nicht auf realen technischen Fakten basiert. Meist werden solche Nachrichten über E-Mails verbreitet. Beispielsweise wird dabei vor Computer-Viren gewarnt, die Hardware-Schäden verursachen können oder durch das bloße Öffnen einer E-Mail (nicht eines Attachments) zu Infektionen und Schäden führen können und die durch keine Antiviren-Software erkannt werden. Neben dieser Warnung wird darum gebeten, die Warnmeldung an Freunde und Bekannte weiterzuleiten. Noch wirksamer wird ein solcher Hoax, wenn als Absender eine gefälschte Adresse angegeben wird, wie zum Beispiel die eines namhaften Herstellers.

Ein Hoax ist kein Virus!

Ein solcher Hoax ist nicht zu verwechseln mit einem Computer-Virus, der tatsächlich Manipulationen am IT-System vornehmen kann. Vielmehr handelt es sich um eine irreführende Nachricht, die ohne Schaden gelöscht werden kann und sollte. Die einzigen Schäden, die ein Hoax herbeiführt, sind die Verunsicherung und Irritation der Empfänger und ggf. die Kosten an Zeit und Geld für den Weiterversand des Hoax.

Im Bereich des Mobilfunks gab es eine ganze Reihe solcher Hoax-Nachrichten, bei denen davor gewarnt wurde, dass an Mobiltelefonen die Eingabe bestimmter Tastenkombinationen oder die Wahl bestimmter Rufnummern dazu führen könnten, Gespräche abzuhören oder auf Kosten anderer zu telefonieren. Durch die Nennung bestimmter Mobiltelefon-Marken und einiger technischer Ausdrücke wird der Anschein von Seriosität erweckt. Solche Gerüchte halten sich hartnäckig und verunsichern die Benutzer.

Beispiel:

- Im Frühjahr 2000 kursierte folgende Falschmeldung per E-Mail (und teilweise sogar per Brief):

  "Wenn sie eine Nachricht auf Ihr Handy erhalten, dass sie unter der Nummer 0141-455xxx zurückrufen sollen, antworten sie auf keinen Fall darauf. Ihre Rechnung steigt sonst ins Unermessliche.

  Diese Information wurde von der "Zentralstelle zur Unterdrückung von betrügerischen Machenschaften" (Office Central de Repression du Banditisme) herausgegeben. ..."

G 5.81 Unautorisierte Benutzung eines Kryptomoduls

Gelingt es einem Dritten, ein Kryptomodul unautorisiert zu benutzen, so können Schäden verschiedenster Art die Folge sein. Beispiele für solche Schäden sind:

- Bei der unautorisierten Nutzung gelingt es dem Angreifer, geheime Schlüssel auszulesen, die Schlüssel zu verändern oder auch kritische Sicherheitsparameter zu manipulieren. Die Folge wäre, dass die kryptographischen Verfahren keine ausreichende Sicherheit mehr bieten.
- Bei der unautorisierten Nutzung manipuliert der Angreifer das Kryptomodul so, dass es zwar auf den ersten Blick korrekt arbeitet, sich jedoch tatsächlich in einem unsicheren Zustand befindet.
- Der Angreifer nutzt das Kryptomodul in Form einer Maskerade. Signiert er oder verschlüsselt er Daten bei der unautorisierten Benutzung des Kryptomoduls, so wird dies vom Empfänger der Daten so interpretiert, als hätte der autorisierte Benutzer dies vorgenommen.

Beispiel:

- Eine unautorisierte Benutzung eines Kryptomoduls wird dann möglich, wenn der reguläre Benutzer kurzfristig seinen Arbeitsplatz verlässt und das funktionsfähige Kryptomodul einsetzbar ist, ohne dass es vor unbefugtem Zugriff geschützt ist, also beispielsweise wenn eine Signatur- oder Verschlüsselungschipkarte im Rechner stecken bleibt. Damit kann jeder, der zufällig vorbeikommt, E-Mail im Namen des regulären Benutzers signieren oder auf dem IT-System gespeicherte Dateien so verschlüsseln, dass der Benutzer sie nicht mehr verwenden kann.

G 5.82 Manipulation eines Kryptomoduls

Ein Angreifer kann versuchen, ein Kryptomodul zu manipulieren, um geheime Schlüssel auszulesen oder die Schlüssel zu verändern oder auch um kritische Sicherheitsparameter zu verändern. Ein Kryptomodul kann auf verschiedene Art und Weise manipuliert sein, es kann z. B.

- ein Super-Passwort, mit dem alle anderen Passwörter umgangen werden können,
- nicht dokumentierte Testmodi, über die jederzeit Zugriff auf sensitive Bereiche genommen werden kann,
- Trojanische Pferde, d. h. Software, die neben ihrer eigentlichen Aufgabe andere, nicht direkt erkennbare Aktionen wie das Aufzeichnen von Passwörtern, durchführt,
- manipulierte Zugriffsrechte auf bestimmte Kommandos

enthalten. Andere Beispiele für solche Angriffe sind

- die Modifikation von kryptographischen Schlüsseln,
- die Beeinträchtigung der internen Schlüsselgenerierung, z. B. durch Manipulation des Zufallszahlengenerators,
- die Modifizierung der Abläufe innerhalb des Kryptomoduls,
- Modifikationen am Sourcecode oder am ausführbaren Code des Kryptomoduls,
- Über- oder Unterschreitung des zulässigen Arbeitsbereichs bzgl. Spannungsversorgung, Temperatur, EMV-Grenzwerte etc. des Kryptomoduls.

Bei Manipulationen am Kryptomodul wird der Angreifer meist versuchen, diesen Angriff zu vertuschen, so dass das Kryptomodul für Benutzer zwar auf den ersten Blick vermeintlich korrekt arbeitet, sich jedoch in einem unsicheren Zustand befindet. Es gibt allerdings auch zerstörerische Angriffe, bei denen auch die Zerstörung des Kryptomoduls bewusst in Kauf genommen wird, beispielweise wenn ein Angreifer Informationen über die Funktionsweise des Kryptomoduls erhalten will oder wenn die kryptographischen Schlüssel ausgelesen werden sollen.

Ein Angreifer kann versuchen, seine Angriffe am Aufstellungsort des Kryptomoduls durchzuführen oder es entwenden. Bei einem schlecht geschützten Aufstellungsort lassen sich die Manipulationen unter Umständen sehr schnell durchführen und bleiben dadurch evtl. lange unbemerkt. Durch den Diebstahl von Kryptomodulen kann ein Angreifer wichtige Informationen darüber bekommen, wie eine Komponente am einfachsten manipulierbar ist. Er kann die entwendeten Komponenten benutzen, um daraus sensitive Informationen wie Schlüssel, Software oder Kenntnis über Hardwaresicherheitsmechanismen zu gewinnen. Er kann aber auch die entwendete Komponente dazu benutzen, um ein authentisches Kryptomodul vorzutäuschen.

G 5.83 Kompromittierung kryptographischer Schlüssel

Beim Einsatz kryptographischer Verfahren hängt der Sicherheitszugewinn entscheidend davon ab, wie vertraulich die verwendeten geheimen kryptographischen Schlüssel bleiben. Mit Kenntnis sowohl des verwendeten Schlüssels als auch des eingesetzten Kryptoverfahrens ist es meist einfach, die Verschlüsselung umzukehren und den Klartext zu gewinnen. Daher wird ein potentieller Angreifer versuchen, die verwendeten Schlüssel zu ermitteln. Angriffspunkte dazu sind:

- Bei der Schlüsselerzeugung werden ungeeignete Verfahren eingesetzt, beispielsweise zur Bestimmung von Zufallszahlen oder zur Ableitung der Schlüssel.
- Bei der Schlüsselerzeugung werden Schlüssel ausgelesen, bevor sie auf sicheren Speichermedien gespeichert werden.
- Im laufenden Betrieb werden Schlüssel aus Kryptomodulen durch technische Angriffe ausgelesen.
- Als Backup hinterlegte Schlüssel werden entwendet.
- Bei der Eingabe von kryptographischen Schlüsseln werden die Schlüssel ausgespäht.
- Die eingesetzten Kryptoverfahren werden gebrochen. So ist es heute beispielsweise bei symmetrischen Verschlüsselungsverfahren wie dem DES möglich, den verwendeten Schlüssel mittels massiv paralleler Rechner durch Ausprobieren zu ermitteln (Brute-Force-Attacke).
- Verwendete kryptographische Schlüssel werden durch Innentäter verraten.

G 5.84 Gefälschte Zertifikate

Zertifikate dienen dazu, einen öffentlichen kryptographischen Schlüssel an eine Person zu binden. Diese Bindung des Schlüssels an den Namen der Person wird wiederum kryptographisch mittels einer digitalen Signatur einer vertrauenswürdigen dritten Stelle abgesichert. Diese Zertifikate werden von Dritten dann verwendet, um digitale Signaturen der im Zertifikat ausgewiesenen Person zu prüfen bzw. um dieser Person Daten mit dem im Zertifikat aufgezeichneten Schlüssel verschlüsselt zuzusenden.

Ist ein solches Zertifikat gefälscht, werden digitale Signaturen fälschlicherweise als korrekt geprüft und der Person im Zertifikat zugeordnet oder es werden Daten mit einem ggf. unsicheren Schlüssel verschlüsselt und versandt. Beide Angriffsmöglichkeiten können einen Täter bewegen, gefälschte Zertifikate in Umlauf zu bringen.

Gefälschte Zertifikate können auf verschiedene Weise erzeugt werden:

- Ein Innentäter der vertrauenswürdigen Stelle erstellt mit dem eigenen Signaturschlüssel ein Zertifikat mit gefälschten Angaben. Dieses Zertifikat ist authentisch und wird bei einer Prüfung als korrekt verifiziert.
- Ein Täter gibt sich als eine andere Person aus und beantragt ein Zertifikat, welches auf diese andere Person ausgestellt wird, obwohl der Täter im Besitz des geheimen Schlüssels ist, der mit dem öffentlichen Schlüssel im Zertifikat korrespondiert.
- Ein Täter erzeugt ein Zertifikat und signiert es mit einem eigenen Schlüssel. Die Fälschung fällt nur auf, wenn das Zertifikat geprüft wird und dabei festgestellt werden kann, dass das Zertifikat von einer nichtvertrauenswürdigen Stelle ausgestellt wurde.

Wenn ein Täter erst einmal ein Zertifikat mit falschen Angaben auf irgendeinem Weg erhalten hat, kann er sich gegenüber Kommunikationspartnern jederzeit als eine andere Person ausgegeben, und zwar sowohl beim Versand als auch beim Empfang von Nachrichten.

G 5.85 Integritätsverlust schützenswerter Informationen

Wenn Daten nicht mehr integer sind, kann es zu einer Vielzahl von Problemen kommen:

- Daten können im einfachsten Fall nicht mehr gelesen, also weiterverarbeitet werden.
- Daten können versehentlich oder vorsätzlich so verfälscht werden, dass dadurch falsche Informationen weitergegeben werden. Hierdurch können beispielsweise Überweisungen in falscher Höhe oder an den falschen Empfänger ausgelöst werden, die Absenderangaben von E-Mails könnten manipuliert werden oder vieles mehr.
- Wenn verschlüsselte oder komprimierte Datensätze ihre Integrität verlieren - und hier reicht die Änderung eines Bits - können sie u. U. nicht mehr entschlüsselt bzw. entpackt werden.
- Dasselbe gilt auch für kryptographische Schlüssel, auch hier reicht die Änderung eines Bits, damit die Schlüssel unbrauchbar werden. Dies führt dann ebenfalls dazu, dass Daten nicht mehr entschlüsselt oder auf ihre Authentizität überprüft werden können.
- Dokumente, die in elektronischen Archiven gespeichert sind, verlieren an Beweiskraft, wenn ihre Integrität nicht nachgewiesen werden kann.

Zu Integritätsverlusten kann es auf verschiedene Weise kommen:

- Durch die Alterung von Datenträgern kann es zu Informationsverlusten kommen.
- Bei der Datenübertragung kann es zu Übertragungsfehlern kommen. **Übertragungsfehler**
- Durch Computer-Viren können ganze Datenbestände verändert oder zerstört werden. **Computer-Viren**
- Durch Fehleingaben kann es zu so nicht gewünschten Transaktionen kommen, die sogar häufig lange Zeit nicht bemerkt werden. **Fehleingaben**
- Angreifer können versuchen, Daten für ihre Zwecke zu manipulieren, z. B. um Zugriff auf weitere IT-Systeme oder Datenbestände zu erlangen.
- Durch Manipulation der Index-Datenbank können elektronische Archive veranlasst werden, gefälschte Dokumente zu archivieren oder wiederzugeben.

G 5.86 Manipulation von Managementparametern

Auch Managementsysteme können durch bewusst herbeigeführte Fehlkonfigurationen zu einem Angriff auf ein lokales Rechnersystem benutzt werden. Die Fehlkonfigurationen können dabei auf verschiedene Arten herbeigeführt werden. Dabei sind Manipulationen sowohl an der Managementplattform als auch an den verwalteten Geräten möglich. Insbesondere Netzmanagementsysteme, die SNMP benutzen, sind für Angriffe anfällig, bei denen bewusst Managementparameter fehlkonfiguriert werden (z. B. durch einen eigenen SNMP-Client). Je nach einstellbaren Parametern reichen die Attacken von einfachen "Denial-of-service-Attacken" (z. B. durch Verstellen von IP-Adressen) bis hin zur Datenveränderung (z. B. nach Verstellen von Zugriffsrechten).

Werden Netzkomponenten durch ein Managementsystem verwaltet, so sollten alle durch das Managementsystem verwalteten Konfigurationsparameter auch nur durch das Managementsystem verändert werden. Je nach Managementsystem ist es jedoch immer noch möglich, die Konfigurationsparameter der Komponente auch lokal zu verändern. Wird ein PC z. B. über SNMP durch ein Netzmanagementsystem verwaltet, so kann ein lokaler Benutzer mit einem lokalen SNMP-Client-Programm (mit Kenntnis des SNMP-Passwortes) oder aber über ein lokales Bedienelement (z. B. bei einem Drucker) die Einstellungen verändern. Dies führt u. U. zumindest zu Inkonsistenzen im Netzmanagementsystem, kann jedoch auch bewusst zur Herbeiführung von Sicherheitslöchern benutzt werden. Beispielsweise könnte das Abfragen freigegebener Verzeichnisse über SNMP über Netz für einen Windows NT Rechner nachträglich ermöglicht werden.

G 5.87 Web-Spoofing

Bei Web-Spoofing "fälscht" ein Angreifer WWW-Server, d. h. er spiegelt durch die Gestaltung seines WWW-Servers vor, dass dieser ein bestimmter, vertrauenswürdiger WWW-Server ist. Dazu wählt er eine WWW-Adresse so, dass viele Benutzer alleine durch die Adresswahl davon ausgehen, mit einer bestimmten Institution verbunden zu sein. Selbst bei Verwendung eines richtigen Rechnernamens ist Web-Spoofing möglich, wenn ein Angreifer DNS-Spoofing verwendet (siehe G 5.78 *DNS-Spoofing*).

Beispiel:

- Unter der Adresse *www.whitehouse.com* findet sich nicht die offizielle Homepage des weißen Hauses, sondern die eines Scherzboldes.
- Die XY Bank hat die WWW-Adresse *www.xy-bank.de*. Ein Angreifer kann unter *www.xybank.de* oder *www.xy-bank.com* WWW-Seiten einrichten, die auf den ersten Blick denjenigen der XY Bank ähneln. Dazu trägt er diese Adressen auf diversen Suchmaschinen ein, wobei er Stichworte wählt, nach denen XY-Kunden voraussichtlich suchen könnten.

  Benutzer, die diese Seiten aufrufen, werden annehmen, dass sie mit dem WWW-Server ihrer Bank kommunizieren. Daher sind sie bereit, ihre Kontonummer und PIN oder andere Zugangscodes einzugeben. Vielleicht lesen sie dort auch für sie interessante, aber gefälschte Angebote wie günstige Geldanlagen oder Immobilien und wollen diese wahrnehmen. Kann die Bank diese nicht zu diesen Konditionen oder überhaupt nicht anbieten, sind die Kunden im besten Fall nur unzufrieden, im schlechtesten Fall kann es sogar zu Rechtsstreitigkeiten kommen.

Statt zu versuchen, einen vorhandenen WWW-Server zu manipulieren oder nachzuahmen, kann ein Angreifer auch ein eigenes WWW-Angebot ins Internet einbringen und dieses so gestalten, dass jeder Besucher den Eindruck hat, mit einer etablierten, seriösen Institution verbunden zu sein.

Beispiele:

- Es könnte ein Warenangebot angepriesen werden, das nur zu dem Zweck gestaltet wurde, um Kreditkartennummern von potentiellen Käufern zu erhalten.
- Es hat Fälle gegeben, in denen gutgläubige Kunden bei vermeintlichen Banken zu lukrativen Konditionen Geld anlegen wollten. Diese Banken waren ihnen nur übers Internet bekannt und erst, als die erwarteten Zinsen nicht eintrafen, fiel ihnen auf, dass es sich nur um eine, inzwischen gelöschte, private WWW-Seite handelte.

G 5.88 Missbrauch aktiver Inhalte

Während des Surfens im Internet können WWW-Seiten mit aktiven Inhalten auf den Anwenderrechner geladen werden (z. B. ActiveX oder Java-Applets). Diese Software kann gezielt zu dem Zweck erstellt worden sein, dass sie vertrauliche Daten des Benutzers ausspioniert und anschließend so ausgespähte Informationen an den Angreifer über das Internet zurückgibt.

Ein Java-fähiger Browser erlaubt es dem Benutzer, Java-Applets vom Netz zu laden und auszuführen, ohne dass der Benutzer das Applet erkannt hat. Dies stellt Java-Benutzer vor bedeutende Sicherheitsrisiken:

- Ein Java-Applet kann Standardnetzprotokolle (wie zum Beispiel SMTP) benutzen, um Daten vom Rechner des Benutzers aus zu verschicken.
- Ein Java-Applet kann das Java-System angreifen, indem es dessen Speicher korrumpiert, oder es kann das darunterliegende Betriebssystem angreifen, indem es Dateien fälscht oder wichtige Prozesse beendet.
- Ein Java-Applet kann den gesamten Speicher des Systems belegen oder hochprioritäre Nachrichten erzeugen. Der Verfügbarkeitsangriff ist auch bei der korrekten Interpretation des Java-Sicherheitsmodells möglich.

Bei ActiveX ist anders als bei Java die Funktionsvielfalt kaum eingeschränkt: Bis hin zur Formatierung der Festplatte kann ein ActiveX-Programm alle Befehle enthalten. Diese kleinen ausführbaren Codes nennt man Controls. Die meist zur Illustration oder Unterhaltung verteilten Controls können auch böswillige Elemente besitzen, die dann Zugriff auf den Datenspeicher des Anwenderrechners haben oder andere Programme - für den Benutzer unbemerkt - fernsteuern. ActiveX-Controls können die Festplatte löschen, einen Virus oder ein Trojanisches Pferd enthalten oder die Festplatte nach bestimmten Informationen durchsuchen. All dies kann passieren, ohne dass der Nutzer bzw. Betrachter des Controls dies bemerkt. Während der Betrachter ein durch Controls übertragenes Spiel ausführt, kann im Hintergrund dieses Control die E-Mail nach bestimmten Informationen durchsuchen.

Bei entsprechender Voreinstellung seines WWW-Browsers kann ein Benutzer zwar dafür sorgen, dass nur digital signierte ActiveX-Controls ausgeführt werden. Eine solche digitale Signatur beweist allerdings nur, dass der Hersteller des ActiveX-Controls bei einer Zertifizierungsstelle bekannt ist und dass das von diesem Hersteller bereitgestellte Control unverändert geladen wurde. Hierdurch wird nichts über die Funktionsweise oder Schadensfreiheit eines solchen Controls ausgesagt und auch keine Gewähr dafür übernommen.

G 5.89 Hijacking von Netz-Verbindungen

Weitaus kritischer als das Abhören einer Verbindung ist das Übernehmen einer Verbindung. Hierbei werden Pakete in das Netz eingeschleust, die entweder zum Abbruch oder Blockieren des Clients führen. Der Serverprozess kann daraufhin nicht erkennen, dass ein anderes Programm an die Stelle des Original-Clients getreten ist. Bei dieser Übernahme einer bestehenden Verbindung kann der Angreifer nach erfolgreicher Authentisierung einer berechtigten Person beliebige Aktionen in deren Namen ausüben.

Beispiel:

- Es gibt bereits eine Reihe von Programmen, die es ermöglichen, eine bestehende Telnet-Verbindung zu übernehmen.

G 5.90 Manipulation von Adressbüchern und Verteillisten

Manipulation von Adressbüchern

Auf Faxservern besteht in der Regel die Möglichkeit, Adressbücher und Verteillisten zu führen. In Adressbüchern werden u. a. die Empfänger-Faxnummern gespeichert. Auch ist es möglich, mehrere Faxempfänger in einer Gruppe z. B. für den Versand von Serien-Faxsendungen zusammenzufassen. Der Gebrauch von solchen Adressbüchern ist für den Benutzer sehr komfortabel, da eine einmal gespeicherte Empfängernummer nicht noch einmal manuell eingegeben werden muss. Vielfach wird von den Benutzern eines Faxservers vor dem Faxversand nicht mehr die Richtigkeit einer im Adressbuch eingetragenen Empfängernummer überprüft. Gleiches gilt auch für die Zuordnung einzelner Empfänger zu Gruppen. Häufig wird vor dem Versand von Serien-Faxsendungen nicht mehr überprüft, ob sich der gewünschte Kreis von Empfängern mit den Mitgliedern einer Gruppe deckt.

Mittels Verteillisten können eingehende Faxsendungen (mehreren) Empfängern zugeordnet werden.

Manipulation von Verteillisten

Sofern ein Unbefugter Adressbücher und Verteillisten verändern kann, besteht die Gefahr, dass Faxsendungen an unerwünschte Empfänger übermittelt werden. Es ist damit auch möglich, dass der Versand eines Faxes an den gewünschten Empfänger unterbunden wird. Besonders gefährdet sind hier naturgemäß die zentral geführten Adressbücher und Verteillisten.

G 5.91 Abschalten von Sicherheitsmechanismen für den RAS-Zugang

Die Sicherheit eines RAS-Zugangs hängt wesentlich von der korrekten Nutzung der angebotenen Sicherheitsmechanismen ab. In der Regel ist es jedoch möglich, das RAS-System so zu konfigurieren (Client und/oder Server), dass schwache oder keine Sicherheitsmechanismen zum Einsatz kommen. Werden z. B. die zur Datenverschlüsselung eingesetzten Mechanismen beim Verbindungsaufbau dynamisch zwischen Client und Server verhandelt (dies kann beispielsweise bei der Nutzung von IPSec oder SSL geschehen), so erfolgt diese Verhandlung meist dadurch, dass der Client dem Server eine Liste von unterstützten Verfahren (so genannte Cipher-Suites) zur Auswahl anbietet, aus denen sich der Server eines auswählt. Die Liste der verwendbaren Verfahren kann durch entsprechende Konfiguration verändert werden. Meist ist auch die Option "keine Verschlüsselung" möglich.

Ist die unverschlüsselte Verbindungsaufnahme eine erlaubte Option zwischen Client und Server, so besteht grundsätzlich die Gefahr, dass die Absicherung der übertragenen Daten deaktiviert wird. Dies betrifft insbesondere RAS-Clients, wenn den Benutzern die Möglichkeit gegeben wird, die Konfiguration des RAS-Systems bei Problemen an die lokalen Gegebenheiten anzupassen.

Beispiele:

- Die Absicherung der RAS-Kommunikation soll mittels IPSec unter Windows 2000 erfolgen. Auf dem RAS-Server ist eingestellt, dass die IPSec-Verschlüsselung angefordert, jedoch nicht erzwungen wird, so dass RAS-Clients potentiell auch ungesicherte Verbindungen aufbauen können. Da einem RAS-Benutzer die mit der Verschlüsselung einhergehenden Leistungseinbußen auf seinem älteren Laptop nicht akzeptabel erscheinen, schaltet er die IPSec-Verschlüsselung ab. Die RAS-Verbindung wird nun unverschlüsselt aufgebaut.
- Unter älteren Windows NT-Versionen kann die Verschlüsselung der RAS-Verbindung mittels MPPE (Microsoft Point to Point Encryption) nur dann durchgeführt werden, wenn als Authentisierungsverfahren MS-CHAP eingesetzt wird. Nur bei Verwendung von MS-CHAP werden die zur Verschlüsselung notwendigen Parameter zwischen Client und Server ausgetauscht. Um ein standardisiertes Authentisierungsverfahren zu benutzen, stellt ein Benutzer das CHAP-Verfahren ein. Eine Verschlüsselung der RAS-Verbindung mittels MPPE kann nun nicht mehr erfolgen, obwohl die entsprechende Option aktiviert ist.

G 5.92 Nutzung des RAS-Clients als RAS-Server

Die auf RAS-Clients eingerichtete RAS-Software erlaubt es u. U., dass auch der Client als RAS-Server fungieren kann und eingehende Verbindungen entgegennimmt (z. B. Windows-RAS). Ist diese Option aktiviert, so kann sich jeder, der die Nummer des Telefonanschlusses kennt, an den der Client angeschlossen ist, mit diesem Rechner verbinden. Gelingt es einem Angreifer, den RAS-Authentisierungsmechanismus zu überwinden (beispielsweise durch Ausprobieren oder Raten von Passwörtern, Nutzung nicht passwortgeschützter Benutzerkonten, Nutzung von Gast-Kennungen mit Standardpasswörtern), so kann auf die Daten des RAS-Clients zugegriffen werden. Ist der Client über ISDN angebunden, so kann sogar eine weitere ausgehende Verbindung (z. B. in das Firmennetz) aufgebaut werden. Ist die Verbindungsaufnahme automatisiert (Speicherung des RAS-Passwortes), so kann der Angreifer auch unberechtigt auf Daten im LAN zugreifen. Die Nutzung eines RAS-Clients als RAS-Server muss daher auf jeden Fall verhindert werden.

G 5.93 Erlauben von Fremdnutzung von RAS-Komponenten

Werden RAS-Komponenten Unbefugten absichtlich zugänglich gemacht, so kann die Sicherheit des RAS-Systems nicht mehr gewährleistet werden (siehe auch G 3.30 *Unerlaubte private Nutzung des dienstlichen Telearbeitsrechners*). Mögliche Gefährdungen sind:

Unautorisierte Verwendung von RAS-Zugängen

- RAS-Zugänge können unautorisiert verwendet werden, wenn die Sicherheitsrichtlinien nicht eingehalten werden. Beispielsweise geschieht es immer wieder, dass Administratoren aus falsch verstandener Freundlichkeit die RAS-Einwahl für nicht berechtigte Personen erlauben (beispielsweise zur Internet-Nutzung).

Weitergabe von Passwörtern oder Token

- RAS-Benutzer geben Authentisierungsdaten oder -Token an unberechtigte Dritte weiter, um diesen den entfernten Zugang zum LAN (unter ihrer Kennung) zu gewähren. Mögliche Motive dafür sind z. B., dass der Kollege gemäß RAS-Sicherheitskonzept nicht zur Nutzung von Remote Access berechtigt ist oder vergessen hat, die RAS-Nutzung rechtzeitig vor Antritt einer Dienstreise zu beantragen. Da nun ein RAS-Benutzerkonto von mehreren Benutzern verwendet wird, ist im Schadensfall keine eindeutige Identifizierung des Verursachers mehr möglich.

Unautorisierte Nutzung im privaten Umfeld

- Für den Bereich der Telearbeit ergibt sich häufig die Problematik, dass der RAS-Client durch Familienmitglieder oder Freunde von Familienmitgliedern benutzt wird. Arbeiten organisationsfremde Personen mit dem RAS-Client, so werden von diesen die für den RAS-Client geltenden Sicherheitsvorschriften in der Regel nicht beachtet. Hierdurch kann die Sicherheit des LANs beeinträchtigt werden.

Die Fremdnutzung von IT-Systemen an entfernten Standorten kann nie ganz ausgeschlossen werden, da die Sicherheitsmechanismen eines IT-Systems bei physikalischem Zugriff unterlaufen werden können.

G 5.94 Kartenmissbrauch

Jeden Tag werden Mobiltelefone verloren oder gestohlen. Neben dem unmittelbaren Verlust kann dabei weiterer finanzieller Schaden entstehen. Gelangt ein Unbefugter in den Besitz einer SIM-Karte (z. B. durch Fund oder Diebstahl), kann er auf Kosten des rechtmäßigen Karteninhabers telefonieren, sofern ihm die PIN bekannt ist oder er sie leicht erraten kann.

Daten wie Telefonbuch oder Kurznachrichten, die im Mobiltelefon oder auf der SIM-Karte gespeichert sind, können durchaus einen vertraulichen Charakter haben. Ein Verlust des Mobiltelefons oder der Karte bedeutet dann unter Umständen die Offenlegung dieser gespeicherten Informationen.

Die kryptographischen Sicherheitsmechanismen der SIM-Karten einiger Netzbetreiber waren in der Vergangenheit zu schwach ausgelegt. Dadurch war es möglich, SIM-Karten dieser Netzbetreiber zu kopieren. Dazu muss allerdings die Original-Karte dem Angreifer zur Verfügung stehen. Außerdem muss die PIN bekannt sein oder die PIN-Abfrage abgeschaltet sein, damit die IMSI ausgelesen werden kann.

Ein solcher Angriff kann von Privatbenutzern leicht verhindert und erkannt werden. Bei Mobiltelefonen, auf die unterschiedlichste Personen Zugriff haben, könnte ein solcher Angriff durchgeführt werden und würde vermutlich erst spät bemerkt werden. Dies betrifft z. B. Mobiltelefone aus einem Pool oder professionelle Mobiltelefon-Verleiher.

G 5.95 Abhören von Raumgesprächen über Mobiltelefone

unauffällig aktivieren

Mobiltelefone können dazu benutzt werden, unbemerkt Gespräche aufzuzeichnen oder abzuhören. Im einfachsten Fall kann hierzu ein Mobiltelefon benutzt werden, mit dem eine Verbindung zu einem interessierten Mithörer aufgebaut wurde und das unauffällig in einem Raum platziert wurde, z. B. bei einer Besprechung. Da aber die Akkukapazität begrenzt ist und auch das Mikrofon nicht auf Raumüberwachung ausgelegt ist, hat ein solcher Abhörversuch nur eine begrenzte Wirkung.

Ausnutzen von Leistungsmerkmalen

Durch geschickte Wahl von Leistungsmerkmalen und der Kombination mit zusätzlichen Sprechgarnituren kann evtl. auch erreicht werden, dass ein Mobiltelefon durch einen Anruf von außen in den Gesprächszustand versetzt wird, ohne dass es dies durch einen Rufton oder anderweitig signalisiert. So gibt es z. B. einen Gerätetyp, bei dem durch Betätigen bestimmter Tastenkombinationen das Display des Mobiltelefons abgeschaltet werden kann, obwohl zu dem Gerät eine Gesprächsverbindung existiert.

manipulierte Mobiltelefone

Für diesen Zweck können aber auch speziell manipulierte Mobiltelefone benutzt werden, denen nicht einmal angesehen werden kann, dass sie eingeschaltet sind. Das Mobiltelefon dient dabei als Abhöranlage, die über das Telefonnetz von jedem Ort der Welt aktiviert werden kann, ohne dass dies am Mobiltelefon erkennbar wäre. Es sind Geräte bekannt, bei denen diese Sonderfunktion mittels zusätzlicher Schaltungseinbauten realisiert ist. Diese Manipulation ist durch eine Sichtprüfung nach Zerlegen des Gerätes oder durch spezielle Untersuchungsmethoden relativ leicht nachzuweisen. Der Betrieb solcher Geräte ist in Deutschland illegal.

G 5.96 Manipulation von Mobiltelefonen

Der in G 5.95 *Abhören von Raumgesprächen über Mobiltelefone* erwähnte Einbau zusätzlicher elektronischer Schaltungen ist eine typische Hardware-Manipulation. Damit diese Manipulation durchgeführt werden kann, muss sich das zu manipulierende Gerät für eine gewisse Zeit im Besitz des Angreifers befinden.

Manipulation der Firmware

Eine andere Möglichkeit, Mobiltelefone für Abhörzwecke nutzbar zu machen, besteht in der Manipulation der geräteinternen Steuersoftware (Firmware). Derartige Manipulationen sind weitaus schwerer zu entdecken als Hardware-Manipulationen.

Eine versteckte, nicht dokumentierte Abhörfunktion könnte schon bei der Entwicklung des Gerätes (bewusst oder unbewusst) in die Steuersoftware einprogrammiert sein.

Denkbar ist jedoch auch eine nachträgliche Veränderung der Steuersoftware durch einen Dritten, z. B. wenn das Gerät bei einer Reparatur oder aus sonstigen Gründen (Verlust, Entwendung) für den Benutzer (kurzzeitig) nicht kontrollierbar ist. Die Manipulation ist nur mit eingehender Spezialkenntnis, die neben den Firmware-Entwicklern nur wenigen Angreifern zugänglich ist, machbar. Für Außenstehende ist diese Manipulation praktisch nicht nachweisbar.

Durch die Erweiterung der Menüfunktionen der Mobiltelefone mittels "SIM-Toolkit" und einer neuen Generation von SIM-Karten, die diese Funktionalität unterstützen, werden Mobiltelefone noch flexibler. Ein so ausgestattetes Mobiltelefon lässt sich per Mobilfunk vom Service-Provider mit neuen Funktionen programmieren. So kann der Kartenanbieter zum Beispiel die Menüstruktur individuell an die Bedürfnisse eines Kunden anpassen.

Dies birgt nun erst recht die Gefahr der Firmware-Manipulation, da Funktionen bereits serienmäßig in der Firmware enthalten sein können, die auch für den Umbau als Lauschsender notwendig sind. Die Wahrscheinlichkeit steigt, dass Funktionen von "außen" aufgerufen werden können, die das Mobiltelefon zu einem Lauschsender umfunktionieren. Denkbar ist auch, dass diese Funktionen ein- und ausschaltbar sind.

G 5.97 Unberechtigte Datenweitergabe über Mobiltelefone

Mobiltelefone ermöglichen den Datentransport von einem IT-System, z. B. einem PC oder Notebook, zum anderen, ohne dass eine drahtgebundene Verbindung hergestellt werden muss.

Informationen können dort, wo ein offener Zugang zu IT-Systemen möglich ist, unauffällig abgefragt und übermittelt werden. Mit Hilfe eines Mobiltelefons mit angeschlossenem oder eingebautem Modem können gespeicherte Informationen drahtlos an nahezu jeden beliebigen Ort der Welt übertragen werden.

Diese Art der unbefugten Datenweitergabe kann sowohl mit einem eigens dafür mitgebrachten oder sogar mit einem internen Mobiltelefon durchgeführt werden. Auf diese Weise lassen sich große Datenbestände unbemerkt nach außen schaffen. Durch neue Technologien wird die Übertragung von großen Datenmengen über Mobiltelefone zunehmend attraktiver. Bei GSM beträgt die maximale Datenübertragungsrate derzeit 14,4 Kbit/s. Neuere Protokolle erreichen wesentlich höhere Bandbreiten. So ist mit GPRS eine Übertragung von 53,6 Kbit/s und mit UMTS eine Übertragung von 384 Kbit/s möglich. Kbit/s,

Auch eine nachträgliche Überprüfung ist nicht immer möglich, da die Verbindungsdaten beim Netzbetreiber schon gelöscht sein können.

Beispiel:

- Ein Mitarbeiter eines Unternehmens wird aus einer Besprechung mit einem Externen gerufen, um ein wichtiges Telefonat entgegenzunehmen. Der Externe nutzt die kurze Zeitspanne ohne Beaufsichtigung, um den im Besprechungsraum aufgestellten PC mit seinem GSM-Modem zu verbinden. Anschließend initiiert er eine Datenübertragung zu einem Anschluss seiner Wahl.
- Bei der Nutzung von Remote Access über Mobiltelefon-Netze wird häufig der CLIP-Mechanismus (Rufnummernübertragung) als Authentisierungsmerkmal eingesetzt. Wird das Mobiltelefon gestohlen oder geht es verloren, kann der Authentisierungsvorgang seine Funktion nicht mehr ordnungsgemäß erfüllen. Zwar muss nach dem Einschalten von Mobiltelefonen meist eine PIN eingegeben werden, in der Regel sind die Telefone jedoch eingeschaltet. Wird das Telefon in eingeschaltetem Zustand gestohlen, so kann es prinzipiell sofort von Dritten benutzt werden. Durch rechtzeitiges Aufladen der Akkus kann die Zwangsabschaltung wegen Strommangel beliebig hinausgezögert werden und damit auch die Eingabe der PIN nach dem erneuten Einschalten.

G 5.98 Abhören von Mobiltelefonaten

Die einfachste Art, ein über ein Mobiltelefon geführtes Gespräch mitzuhören, ist einfaches Zuhören in unmittelbarer Nähe. Sehr häufig kann man erleben, wie durch lautes Telefonieren in der Öffentlichkeit sehr viele Interna preisgegeben werden (siehe auch G 3.45 *Unzureichende Identifikationsprüfung von Kommunikationspartnern*).

Generell sind mit sehr hohem Aufwand aber auch technische Abhör-Methoden denkbar.

Wenn sich z. B. ein Angreifer Zugang zu den technischen Einrichtungen des Netzbetreibers (Leitungen, Vermittlungseinrichtungen, Basisstationen) verschaffen kann, ist er in der Lage, alle Telefongespräche abzuhören, die über diese Einrichtungen geführt werden. Dies gilt sowohl für Verbindungen im Mobilfunknetz als auch im Festnetz. Ein gezieltes Abhören von Gesprächen, die einer bestimmten Rufnummer zugeordnet sind, ist aber angesichts der riesigen Datenflut extrem aufwendig.

Werden die Verbindungen über leitungsgebundene Wege von der Basisstation zu der Mobilfunkvermittlung geführt, ist ein physikalischer Angriff auf den Leitungswegen erforderlich. Wird eine Basisstation über eine unverschlüsselte Richtfunkverbindung an die Mobilfunkvermittlung angebunden, was bei einigen Netzbetreibern der Fall sein kann, besteht die Möglichkeit, diese Funksignale mit Antennen und Spezialempfängern unbemerkt aufzufangen und abzuhören. Die Gefährdung kann sich ggf. dadurch erhöhen, dass auf diesen Richtfunkstrecken alle Telefonate der angebundenen Basisstation übertragen werden.

Auch im Festnetz werden Telefongespräche gebündelt über Richtfunkstrecken übertragen. Da diese Übertragung in der Regel unverschlüsselt erfolgt, sind die übertragenen Gespräche mit einigem technischen Aufwand auch dort abhörbar.

Die Funkübertragung zwischen dem Mobiltelefon und der Basisstation wird in Deutschland in allen GSM-Mobilfunknetzen verschlüsselt. Es gibt spezielle Angriffsgeräte, die die Schwäche der einseitigen Authentisierung im GSM-Netz (nur Mobiltelefon gegenüber Basisstation) ausnutzen, indem sie den Mobiltelefonen eine Basisstation vortäuschen, die Verschlüsselung abschalten und Klarbetrieb vorgeben. Abhängig von gesetzlichen Regelungen kann auch in einigen Ländern die Übertragungsverschlüsselung ganz abgeschaltet sein. Auch andere Sicherheitsparameter wie die Häufigkeit des Schlüsselwechsels können schwächer sein.

Andere denkbare Möglichkeiten zur Abschaltung dieser Verschlüsselung sind technische Manipulationen am Mobiltelefon oder an technischen Einrichtungen des Netzbetreibers.

G 5.99 Auswertung von Verbindungsdaten bei der Nutzung von Mobiltelefonen

Bei der Mobil-Kommunikation können die übertragenen Signale auf der Funkstrecke nicht physikalisch gegen unbefugtes Mithören und Aufzeichnen abgeschirmt werden. Deshalb könnte ein Angreifer seinen Angriff ohne das bei leitungsgebundener Kommunikation bekannte Zugriffsproblem durchführen. Ein zweites, generell bei den meisten Funkdiensten auftretendes Problem resultiert daraus, dass die mobilen Kommunikationspartner aus technischen Gründen geortet werden müssen, um erreichbar zu sein. Sofern sie selbst eine Verbindung aufbauen, geben sie ebenfalls - im Zuge des Verbindungsaufbaus - Informationen über ihren Standort ab. Diese Standort-Informationen könnten durch den Netzbetreiber oder Dienstbetreiber - aber auch von Dritten - zur Bildung von Bewegungsprofilen verwendet werden.

Wenn einem Angreifer bestimmte Filtermerkmale über ein Mobiltelefon bekannt sind, könnte er (mit einem hohen technischen Aufwand) über solche Merkmale einzelne Telefonate identifizieren. Für diese oder andere Angriffe werden Kundennummer (IMSI), Mobilfunkgerätenummer (IMEI) bzw. Teilnehmerrufnummer (MSISDN) benötigt.

Die Ermittlung der Rufnummer MSISDN könnte durch einen Innentäter erfolgen, der z. B. in einer Firma Zugriff auf die dienstlichen oder privaten Telefonlisten hat.

G 5.100 Missbrauch aktiver Inhalte beim Zugriff auf Lotus Notes

Funktionen von Lotus Notes Datenbanken werden vielfach dadurch implementiert, dass aktive Komponenten beim Eintreten gewisser Ereignisse (z. B. Eingabe von Daten in ein Feld) ausgeführt werden. Die aktiven Komponenten bestehen dabei z. B. aus LotusScript- oder auch Java-Programmen und werden auch Agenten genannt. Durch die Ausführung eines Agenten können wiederum andere Agenten gestartet werden (z. B. wenn ein Agent Daten in eine andere Datenbank kopiert und diese Aktion das Ausführen von Agenten der Zieldatenbank auslöst). Generell kann zwischen serverseitiger und clientseitiger Ausführung von Agenten unterschieden werden, es sind jedoch immer beide Varianten möglich. Beim Web-Zugriff wird zusätzlich die Benutzerschnittstelle der Datenbank durch aktive Inhalte, die im Browser ausgeführt werden (JavaScript, Java-Applets) realisiert.

fehlkonfigurierte ECL

Welche aktiven Inhalte in einem Notes-Client ausgeführt werden können und welche Berechtigungen ihnen zugestanden werden, wird über die Execution Control List (ECL) gesteuert. Ist die ECL fehlkonfiguriert, so können die aktiven Inhalte auch zum Angriff auf den Client genutzt werden. Dies gilt in ähnlicher Weise für die Web-Schnittstelle, bei der keine ECL existiert, sondern nur die Sicherheitsmechanismen des Browsers genutzt werden können.

Bei falsch konfigurierter ECL könnten über aktive Inhalte beispielsweise:

- Zugriff auf lokale Datenbestände des Client-Rechners (Datenbanken, Dateien, usw.) genommen und Daten "geraubt" werden,
- auf den Clients lokale Daten verändert oder gelöscht werden und
- schädliche Programme, beispielsweise Computer-Viren oder trojanische Pferde installiert werden.

G 5.101 "Hacking Lotus Notes"

Die in den Datenbanken eines Notes-Servers gespeicherten Daten können auch für den öffentlichen Zugriff aus dem Internet bereitgestellt werden. Dies stellt besondere Anforderungen an die Sicherheit des dazu benutzten Notes-Servers. Sicherheitslücken können in diesem Fall dazu führen, dass ein Angreifer nicht nur unerlaubt auf den Notes-Server selbst zugreifen kann, sondern u. U. auch in der Lage ist, in das dahinterliegende interne Netz einzudringen.

Nachfolgend sind einige Problemfelder und potentielle Sicherheitslücken aufgeführt, die insbesondere beim öffentlichen Zugriff auf einen Notes-Server aus dem Internet beachtet werden müssen.

- Das Kommunikations-Protokoll von Lotus Notes ist zur Zeit nicht offengelegt, so dass keine gesicherten Aussagen über die Sicherheitsmechanismen gemacht werden können. Auch bei entsprechender Konfiguration muss mit einem Restrisiko gerechnet werden.

Mechanismen nicht offengelegt

- Ein Notes-Server ist ein komplexes System. Ein Serververbund erhöht die Komplexität weiter. Durch die Komplexität (auch der sicherheitsrelevanten Einstellungen) kann es zu Fehlkonfigurationen und somit auch zu Sicherheitslücken kommen.

hohe Komplexität

- Durch den großen Funktionsumfang eines Notes-Servers und die mögliche Einbindung in entsprechende Hintergrundsysteme können Sicherheitslücken unter Umständen von einem Notes-Server auf die Hintergrundsysteme durchschlagen. Dabei genügt es in der Regel, eine einzelne Schwachstelle in einem einzelnen Funktionspaket auszunutzen.

Auswirkung auf andere Systeme

- An der Web-Schnittstelle existiert keine Beschränkung für Fehlversuche bei der Authentisierung. Mit Hilfe von Browser-Clients können Angreifer deshalb beliebig oft versuchen, sich mit wechselnden Benutzernamen und Passwörtern an einem Notes-Server anzumelden und auf diese Weise unberechtigt Zugriff zu erlangen.

Brute-Force-Angriff

- Ist der Web-Zugriff auf einen Notes-Server aktiviert, betrifft dies immer *alle* Datenbanken auf dem jeweiligen Server. Dies kann leicht für vorsätzliche Angriffe ausgenutzt werden, wenn nicht für jede Datenbank sichere Zugriffsrechte vergeben sind.

direkter Datenbankzugriff

G 5.102 Sabotage

Sabotage bezeichnet die mutwillige Manipulation oder Beschädigung von Sachen mit dem Ziel, dem Opfer Schaden zuzufügen. Besonders attraktive Ziele können Rechenzentren oder Kommunikationsanbindungen von Behörden bzw. Unternehmen sein, da hier mit relativ geringen Mitteln eine große Wirkung erzielt werden kann.

punktuelle Manipulation

Die komplexe Infrastruktur eines Rechenzentrums kann durch gezielte Beeinflussung wichtiger Komponenten, gegebenenfalls durch Täter von außen, vor allem aber durch Innentäter punktuell manipuliert werden, um Betriebsstörungen hervorzurufen. Besonders bedroht sind hierbei nicht ausreichend geschützte gebäudetechnische oder kommunikationstechnische Infrastruktur sowie zentrale Versorgungspunkte, die organisatorisch oder technisch gegebenenfalls auch nicht überwacht werden und für Externe leicht und unbeobachtet zugänglich sind.

Beispiele:

Stromversorgung

- In einem großen Rechenzentrum führte die Manipulation an der USV zu einem vorübergehenden Totalausfall. Der Täter, er wurde ermittelt, hatte wiederholt die USV von Hand auf Bypass geschaltet und dann die Hauptstromversorgung des Gebäudes manipuliert. Der Totalausfall - insgesamt fanden in drei Jahren vier Ausfälle statt - führte partiell sogar zweimal zu Hardware-Schäden. Die Betriebsunterbrechungen dauerten zwischen 40 und 130 Minuten.

Wassereinbruch

- Innerhalb eines Rechenzentrums sind auch sanitäre Einrichtungen untergebracht. Durch Verstopfen der Abflüsse und gleichzeitiges Öffnen der Wasserzufuhr entstehen durch Wassereinbruch in zentralen Technikkomponenten Schäden, die zu Betriebsunterbrechungen des Produktivsystems führen.

elektronische Archive

- Für elektronische Archive stellt Sabotage ein besonderes Risiko dar, da hier meist auf kleinem Raum viele schützenswerte Dokumente verwahrt werden. Dadurch kann unter Umständen durch gezielte, wenig aufwendige Manipulationen ein großer Schaden verursacht werden.

G 5.103 Missbrauch von Webmail

Vorspiegelung einer falschen Identität

Wenn Benutzerangaben nicht ausreichend geprüft werden, kann sich ein Angreifer eine E-Mail-Adresse auf den Namen einer anderen Person besorgen und damit z. B. durch Spammails oder Beschimpfungen unter diesem Namen deren Ruf unterminieren. Wenn die E-Mail-Adressen bei einem Anbieter frei gewählt werden können, kann sich ein Angreifer eine Adresse aussuchen, mit der andere Benutzer bestimmte Assoziationen verbinden und diese damit zu unvorsichtigem Verhalten animieren.

Passwort austesten

Bei vielen Webmail-Anbietern ist der Benutzername für den Zugriff auf die Postfächer identisch mit der E-Mail-Adresse bzw. lässt sich daraus einfach ableiten. Wenn dann das Passwort nicht gut genug gewählt worden ist oder beliebig viele Fehleingaben möglich sind, kann ein Angreifer durch simples Ausprobieren das Passwort herausbekommen und hat dann freien Zugriff auf das Benutzerkonto.

Passwort "vergessen"

Durch falsch verstandene Benutzerfreundlichkeit wird es potentiellen Angreifern auch teilweise sehr einfach gemacht, sich ein Passwort und damit vollen Zugriff für ein fremdes Postfach geben zu lassen. Ein typisches Beispiel ist ein Mailprovider, der auf der Einstiegsseite schon einen Link "Passwort vergessen?" anbietet, durch den man dann zu einer Seite weitergeleitet wird, auf der nach einem vorher vereinbarten, nicht schwer zu erratenen Angabe des Postfach-Inhabers gefragt wird. Beliebt ist hier das Geburtsdatum, bei dessen Erraten auch noch durch Angaben wie "Der Monat ist nicht korrekt" weitergeholfen wird.

Beispiele:

- In dem Beispiel in G 5.40 *Abhören von Räumen mittels Rechner mit Mikrofon* wird geschildert, wie eine deutsche Politikerin in einer gefälschten Virenwarnung per E-Mail aufgefordert wurde, ein als Anlage mitgeschicktes Schutzprogramm zu öffnen, welches aber ein Trojanisches Pferd enthielt. Diese E-Mail hatte den Absender *support@xyz.de* und kam aus der Domain ihres E-Mail-Providers XYZ. Eine E-Mail von einem Absender, den sie als unbekannt eingestuft hätte, hätte sie wahrscheinlich nicht geöffnet.
- Im Webmail-Angebot Hotmail sind bereits mehrmals Sicherheitslücken bekannt geworden. Zu Problemen führt insbesondere in E-Mails eingebettetes Javascript, das dann beim Lesen der E-Mail im Browser des Empfängers ausgeführt wird. Dadurch kann der Benutzer beispielsweise durch einen Angreifer dazu aufgefordert werden, sein Passwort erneut einzugeben und dieses anschließend an den Angreifer übermittelt wird. Da Javascript auf mehrere unterschiedliche Arten in HTML-formatierte E-Mails eingebettet werden kann, gab es in der Vergangenheit Lücken beim Herausfiltern dieser aktiven Inhalte.

unsicheres Zeitfenster beim Virenschutz

Bei aktuellen Virenwarnungen kann es einige Stunden dauern, bis die Hersteller der Virenschutzprogramme die ersten wirksamen Updates bereit stellen können und diese erfolgreich auch auf allen IT-Systemen installiert sind. E-Mails, die in dieser Zeit auf dem E-Mail-Server eintreffen, können dort solange in Quarantäne genommen werden. Wenn nicht gleichzeitig auch

verhindert wird, dass E-Mails über Webmail-Accounts abgerufen werden, können hierüber PCs und Server im LAN infiziert werden.

Beispiel:

- Ende September 2001 verursachte der Virus *Nimda* etliches an Ärger und Aufregung. Nimda ist ein Wurm mit mehreren Schadfunktionen. Er verbreitet sich mittels Anhang von E-Mails, über eine bekannte Schwachstelle des Internet Information Server (IIS) von Microsoft sowie über freigegebene Laufwerke. Es dauerte teilweise bis zu 24 Stunden, ehe nach Bekanntwerden des ersten Auftretens wirksame Signaturen für Virenschutzprogramme zur Verfügung standen. In einigen großen Unternehmen infizierten Benutzer ihre PCs über Webmail mit Nimda. Über diese wurden dann IIS-Webserver innerhalb des Firmennetzes infiziert, was wiederum zu erheblichen Beeinträchtigungen im LAN führte.

G 5.104 Ausspähen von Informationen

Neben einer Vielzahl technisch komplexer Angriffe gibt es oft auch viel einfachere Methoden, um an wertvolle Informationen zu kommen. Da sensitive Daten oft nicht ausreichend geschützt werden, können diese oft auf optischem, akustischem oder elektronischen Weg ausgespäht werden.

Beispiele:

- Die meisten IT-Systeme sind durch Identifikations- und Authentisierungsmechanismen gegen eine unberechtigte Nutzung geschützt, z. B. in Form von Benutzer-ID- und Passwort-Prüfung. Wenn das Passwort allerdings unverschlüsselt über die Leitung geschickt wird, ist es einem Angreifer möglich, dieses auszulesen.

  unverschlüsseltes Passwort

- Um mit einer ec- oder Kreditkarte Geld an einem Geldausgabeautomaten abheben zu können, muss die korrekte PIN eingegeben werden. Leider ist der Sichtschutz an diesen Geräten häufig unzureichend, so dass ein Angreifer einem Kunden bei der Eingabe der PIN ohne Mühe über die Schulter schauen kann. Wenn er ihm hinterher die Karte stiehlt, kann er damit das Konto plündern. Der Kunde hat anschließend außerdem das Problem, dass er nachweisen muss, nicht fahrlässig mit seiner PIN umgegangen zu sein, sie also beispielsweise nicht auf der Karte notiert hat.

  unzureichender Sichtschutz

- Um Zugriffsrechte auf einem Benutzer-PC zu erhalten oder diesen anderweitig zu manipulieren, kann ein Angreifer dem Benutzer ein Trojanisches Pferd schicken, das er als vorgeblich nützliches Programm einer E-Mail beigefügt hat. Erfahrungsgemäß öffnen Benutzer trotz aller Aufklärung sogar dann E-Mail-Anhänge, wenn diese nicht erwartet wurden oder merkwürdige Namen tragen. Neben unmittelbaren Schäden können über Trojanische Pferde Informationen nicht nur über den einzelnen Rechner, sondern auch über das lokale Netz ausspäht werden. Insbesondere verfolgen viele Trojanische Pferde das Ziel, Passwörter oder andere Zugangsdaten auszuspähen.

  Trojanisches Pferd

- In vielen Büros sind die Arbeitsplätze akustisch nicht gut gegeneinander abgeschirmt. Dadurch können Kollegen, aber auch Besucher unter Umständen Gespräche mitgehören und dabei Kenntnis von Informationen erlangen, die nicht für sie bestimmt oder sogar vertraulich sind.

  Mithören von Gesprächen

G 5.105 Verhinderung der Dienste von Archivsystemen

Die Dienste eines elektronischen Archivs bestehen aus den folgenden Grundfunktionen:

- Erfassen und Indizieren der zu archivierenden Dokumente,
- Verwalten und Speichern der Dokumente,
- Suchen und Finden archivierter Dokumente,
- Visualisieren und Reproduzieren der Dokumente sowie
- Pflegen und Administrieren des Archivsystems.

Wenn die Dienste eines Archivsystems gestört werden, können Schäden entstehen, wie die folgenden Beispiele erläutern sollen:

- **Indizierung** Wird die Indizierung von archivierten Daten verhindert oder gestört, z. B. durch die Angabe falscher Kontextdaten, so hat das unter Umständen zur Folge, dass Daten später gar nicht oder nur unter erheblichem Aufwand wiedergefunden werden können.
- **Archivierung** Wird die Archivierung neuer Daten verhindert oder blockiert, indem z. B. durch einen Denial-of-Service-Angriff die Netzverbindung des Archivsystems blockiert wird, so kann das zur Folge haben, dass je nach Datenaufkommen ein erheblicher Rückstau entsteht, der nicht durch Backup gesichert ist. Bei einem Systemausfall wäre dann mit dem Verlust derjenigen Dokumente zu rechnen, die noch zur Archivierung anstehen. Wenn ein Archivsystem ausgewählt wird, das keine für den Benutzer sichtbare Archivbestätigung erzeugt, so besteht das Risiko, dass eventuelle Dokumentverluste zunächst unerkannt bleiben. Wenn andererseits ein System mit Archivbestätigung eingesetzt wird, so kann ein Ausbleiben der Bestätigung nachfolgende Geschäfts- oder Verwaltungsvorgänge ebenfalls verzögern.
- **Reproduktion** Wird die Reproduktion archivierter Daten unterbunden, gestört oder verzögert, so kann das zur Folge haben, dass erforderliche Dokumente nicht termingerecht beigebracht werden können, wodurch sich wirtschaftliche Schäden oder rechtliche Nachteile ergeben können.
- **Administration** Wenn die Administration des Archivsystems behindert oder verzögert wird, z. B. durch Überlastung des Personals mit Anfragen, so kann es vorkommen, dass Personen, denen der Zugriff gesperrt werden soll, weiterhin Zugriff auf das Archiv haben und dort unberechtigt Dokumente einstellen oder abrufen.
- Durch Behinderung der Administration können auch dann Schäden hervorgerufen werden, wenn dadurch die Wartung des Archivsystems beeinträchtigt oder verzögert wird. Möglicherweise können dadurch sicherheitsrelevante Software-Updates nicht zeitgerecht eingespielt oder nicht ausreichend getestet werden.

G 5.106 Unberechtigtes Überschreiben oder Löschen von Archivmedien

Auf Archivmedien sollen wichtige Daten langfristig und unverändert gespeichert werden. Daher dürfen diese nicht unberechtigt überschrieben, gelöscht oder anderweitig verändert werden. Unberechtigtes Löschen ist dann möglich, wenn Benutzerrechte falsch vergeben worden sind, d. h. wenn

- Benutzer das Recht zum "Löschen" haben, sie aber aufgrund der ihnen zu Verfügung stehenden Informationen keine sinnvolle Entscheidung treffen können, ob Datensätze gelöscht werden dürfen oder nicht, oder
- durch fehlerhafte Administration Benutzer fälschlicherweise die Berechtigung zum "Löschen" haben.

Hierbei sind wiederbeschreibbare Medien und WORM-Medien zu unterscheiden:

- Bei wiederbeschreibbaren Medien ist ein physikalisches Löschen oder Überschreiben von Datensätzen grundsätzlich möglich.
- Bei WORM-Medien ist ein physikalisches Löschen oder Überschreiben grundsätzlich nicht möglich. Allerdings bieten Archivierungssysteme in der Regel die Möglichkeit, Datensätze logisch als gelöscht zu markieren. Diese Datensätze werden beim Umkopieren auf einen neuen Datenträger dann nicht mehr mitkopiert. Sie werden also erst im Moment des Kopierens auf den neuen Datenträger aus den Datenbeständen entfernt.

In beiden Fällen kann es also bei falschem Umgang mit den Medien zu einem Integritätsverlust der gespeicherten Informationen und Daten kommen (siehe hierzu auch G 5.85 *Integritätsverlust schützenswerter Informationen*).

G 5.107 Weitergabe von Daten an Dritte durch den Outsourcing-Dienstleister

Weitergabe von Daten an Konkurrenten

Outsourcing-Dienstleister haben in der Regel mehrere Kunden. Es ist daher immer möglich, dass sich darunter auch Wettbewerber befinden. Dies ergibt sich vor allem bei großen Outsourcing-Dienstleistern und solchen, die spezielle Anforderungsbereiche wie IT-Sicherheitsdienstleistungen abdecken. Wenn ein Outsourcing-Partner parallel die Aufträge zweier Konkurrenzorganisationen bearbeitet, kann es zu Interessenskonflikten kommen, sofern keine strikte Trennung der Auftragsbearbeitung vorgenommen wird (Mandantenfähigkeit des Outsourcing-Dienstleisters).

In derartigen Situationen könnten möglicherweise Arbeitsergebnisse und Erkenntnisse aus der Projektbearbeitung durch Mitarbeiter oder Unterauftragnehmer des Dienstleisters absichtlich dem Mitbewerber direkt verfügbar gemacht werden. Ein so entstandener Schaden ist in aller Regel nicht mehr zu beheben, auch wenn einzelne Personen oder der Outsourcing-Dienstleister als ganzes später juristisch zur Verantwortung gezogen werden kann.

Datenschutz

Werden im Rahmen des Outsourcing-Vorhabens personenbezogene Daten beim Dienstleister verarbeitet oder gespeichert, so müssen auch zusätzliche Datenschutzgesichtspunkte beachtet werden. Werden etwa Kundeninformationen eines Auftraggebers kompromittiert und veröffentlicht, so besteht die Gefahr, dass das Vertrauensverhältnis zwischen dem Auftraggeber und seinen Kunden nachhaltig gestört wird.

G 5.108 Ausnutzen von systemspezifischen Schwachstellen des IIS

Wie bei fast jeder Software zeigen sich viele kleinere Programmier- und Entwicklungsfehler erst im praktischen Einsatz. Auch bei Windows und beim IIS werden immer wieder systemspezifische Schwachstellen entdeckt, die auf Programmier- und Entwicklungsfehler zurückzuführen sind. Unter bestimmten Voraussetzungen wird z. B. ein Buffer-Overflow verursacht. Insbesondere beim Zusammenwirken mit anderen Sofware-Komponenten besteht die Gefahr, dass Parameter ungenügend geprüft werden und die Funktionsweise des System beeinflussen können.

Sicherheitsrisiken entstehen nicht nur durch Programmier- und Entwicklungsfehler, auch vorhandene Beispielanwendungen und Scriptdateien können für einen Angriff auf das System ausgenutzt werden.

Bei der Standardinstallation eines IIS wird eine Reihe von Beispielanwendungen und Scriptdateien mit installiert. Diese Beispiele zeigen dem Administrator bzw. Entwickler Anwendungsmöglichkeiten des Web-Servers auf oder dienen als Vorlage für erweiterte Funktionen, z. B. Suchfunktionen. Viele Administratoren und Entwickler haben keine Kenntnisse über den vollständigen Funktionsumfang und ggf. die Existenz solcher Beispielanwendungen. Da diese Anwendungen und Scriptdateien u. U. von einem Angreifer ausgenutzt werden können, geht von ihnen eine erhebliche Gefahr für das Informationssystem aus.

Beispiele:

- Mit Hilfe so genannter Escape-Sequenzen in URLs kann eine DoS-Attacke (Denial-of-Service) auf den IIS durchgeführt werden. Escape-Sequenzen bieten die Möglichkeit, nicht druckbare Zeichen oder Sonderzeichen einzufügen. Diese Sequenzen bestehen aus einem Escape-Character, z. B. "%", und zwei hexadezimalen Ziffern. Auf dem Zielsystem werden diese Zeichen in den entsprechenden ASCII-Code umgesetzt. Beispielsweise wird der Zeichenfolge *%20* ein Leerzeichen (Blank, Space) zugeordnet.

  Werden sehr viele Escape-Sequenzen in einer URL verwendet, kann dies bei der Umsetzung zu einer vollständigen Auslastung des Prozessors führen, wodurch der IIS z. B. keine regulären Anfragen mehr beantworten kann. Ein Beispiel hierfür zeigt der Microsoft Security Bulletin MS00-023 (*http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/fq00-023.asp*).

- Im Umfang der Standardinstallation eines IIS 4.0 ist eine Anwendung enthalten, die es einem Web-Benutzer erlaubt, das Passwort eines Benutzerkontos auf dem Web-Server zu ändern. Jeder Benutzer, der Zugriff auf diese Seite hat (über HTTP), kann darüber gültige Benutzerkonten auf dem Server herausfinden. Da die Rückmeldungen des Web-Servers Auskunft über getestete Benutzerkonten geben, kann diese Schnittstelle für eine Brute-Force-Attacke auf die Konten ausgenutzt werden.

- Durch eine Schwachstelle in der Web-Seite *showcode.asp* sind Internet-Benutzer in der Lage, sich Dateien vom Web-Server anzeigen zu lassen. Wenn nicht sichergestellt ist, dass ein Ausbrechen aus dem Webroot-Verzeichnis mit Hilfe der Zeichenfolge */../* ausgeschlossen ist, können mit diesem Script auch Dateien aus anderen Verzeichnissen, z. B. *WINNT*, ausgelesen werden.

G 5.109 Ausnutzen systemspezifischer Schwachstellen beim Apache-Webserver

Wie jede Software ist auch der Apache-Webserver nicht frei von Schwachstellen und Programmierfehlern. Insgesamt ist der Apache-Webserver zwar von so spektakulären Vorfällen wie dem *Nimda*-Wurm bisher weitgehend verschont geblieben, jedoch trat beispielsweise im Herbst 2002 der Wurm *Slapper* auf, der sich eine Sicherheitslücke in der OpenSSL-Bibliothek zu Nutze machte und sich über Apache-Webserver verbreitete, die SSL benutzten. Systemspezifische Schwachstellen beim Apache-Webserver finden sich entweder im eigentlichen Webserver oder in Modulen wie *mod_ssl*, *mod_dav*, *mod_rewrite, mod_php* oder ähnlichen Erweiterungen.

Durch Ausnutzen von Schwachstellen (beispielsweise Buffer-Overflows) im Apache-Webserver oder in Erweiterungsmodulen können Angreifer im Extremfall den Serverrechner kompromittieren. Da der Apache-Webserver meist unter einem nicht privilegierten Account läuft, ist zwar das direkte Erlangen von root- oder Administratorrechten meist nicht möglich, hat ein Angreifer aber bereits einen Zugang zum Serverrechner selbst erlangt, so kann er durch Ausnutzen lokaler Schwachstellen des Betriebssystems oder anderer installierter Programme oft recht leicht erweiterte Berechtigungen erlangen.

Selbst wenn für eine Schwachstelle kein Exploit bekannt ist, der dadurch, dass ein Angreifer eigenen Code auf dem Serverrechner ausführen kann, zu einer Kompromittierung des Rechners führt, können Buffer-Overflows und ähnliche Schwachstellen dazu ausgenutzt werden, den Apache-Webserver zum Absturz zu bringen und so einen Denial-of-Service herbei zu führen.

Schwachstellen im Apache-Webserver oder in Erweiterungsmodulen können auch dazu führen, dass Zugriffsbeschränkungen umgangen werden können und so eventuell vertrauliche Dateien an unberechtigte Besucher ausgeliefert werden. Außerdem ist es möglich, dass durch eine Sicherheitslücke Konfigurationsinformationen (wie Installationspfade oder Systempfade zu WWW-Dateien) nach außen gelangen. Solche Informationen können Angriffe erleichtern, da die Angreifer in einem solchen Fall keine Pfade durchprobieren müssen.

G 5.110 Web-Bugs

Als Web-Bugs werden in E-Mail oder WWW-Seiten eingebettete Bilder bezeichnet, die beim Öffnen von einem fremden Server nachgeladen werden. Diese Bilder können sehr klein sein, beispielsweise ein mal ein Pixel große Minigrafiken. Die Bilder sind so eingebettet, dass sie im allgemeinen nicht sichtbar sind, aber beim Laden vom Ursprungsserver die Ausführung eines Skripts oder Programms veranlassen.

E-Mail

Werden Web-Bugs in HTML-formatierte E-Mails eingebettet, kann dadurch der Absender z. B. erkennen, welche E-Mail wann gelesen wurde. Beispielsweise im Zusammenhang mit unverlangt versendeten Massen-E-Mails kann dies unerwünscht sein.

WWW

Bei der Nutzung des World Wide Web müssen Benutzer grundsätzlich damit rechnen, dass außer zu dem Server, dessen WWW-Angebot sie gerade nutzen, auch zu anderen Servern Verbindungen aufgebaut werden. Dies ist zum Beispiel der Fall, wenn von einer WWW-Seite aus Bilder referenziert werden, die auf einem anderen Server liegen. Obwohl dies im Prinzip ein normaler Vorgang ist, können unter Umständen über diesen Mechanismus ungewollt Informationen an Dritte übertragen werden, wie das unten beschriebene Beispiel zeigt. Insbesondere können hierdurch vertrauliche Daten des Benutzers oder des Server-Betreibers kompromittiert werden.

Beispiel:

- Eine Universität verwendet ein frei im Internet erhältliches Software-Paket, um dynamische Inhalte auf dem WWW-Server anzubieten (CGI-Skripten). Abhängig von den Eingaben des Benutzers generiert die Software auf dem WWW-Server passende Antwort-Seiten und schickt sie an den Benutzer. Neben den eigentlichen Inhalten enthalten die generierten HTML-Seiten aber auch Verweise auf Bilder, die sich nicht auf dem Server der Universität, sondern des Programmierers der CGI-Skripten befinden. Als Folge werden diese Bilder jedesmal vom Server des Programmierers abgerufen, wenn ein Benutzer auf das Internet-Angebot der Universität zugreift. Auf diese Weise erhält der Programmierer ausführliche Informationen über die Nutzung des von ihm entwickelten Software-Pakets, aber leider auch über die Nutzung des Internet-Angebots der Universität.

G 5.111 Missbrauch aktiver Inhalte in E-Mails

Bunt, aber gefährlich!

Immer mehr E-Mails sind heutzutage auch HTML-formatiert. Einerseits ist dies oft lästig, weil nicht alle E-Mail-Clients dieses Format anzeigen können. Andererseits kann dies auch dazu führen, dass bereits bei der Anzeige solcher E-Mails auf dem Client ungewollte Aktionen ausgelöst werden, da HTML-Mail z. B. eingebetteten JavaScript- oder VisualBasic-Skript-Code enthalten kann.

Durch Kombination verschiedener Sicherheitslücken in E-Mail-Clients und Browsern ist es in der Vergangenheit immer wieder zu Sicherheitsproblemen mit HTML-formatierten E-Mails gekommen (siehe auch G 5.110 *Web-Bugs*). Ein Beispiel hierfür findet sich unter anderem im CERT-Advisory CA-2001-06 (unter *http://www.cert.org/advisories/CA-2001-06.html*).

G 5.112 Manipulation von ARP-Tabellen

ARP-Spoofing

Im Gegensatz zu einem Hub kann bei einem Switch grundsätzlich die Kommunikation zwischen zwei Stationen von keiner der anderen Stationen abgehört werden. Zu diesem Zweck pflegt der Switch eine Tabelle, die die MAC-Adressen der beteiligten Stationen den verschiedenen Ports zuordnet. Datenpakete beziehungsweise Ethernet-Frames, die an eine bestimmte MAC-Adresse adressiert sind, werden nur an den Port weitergeleitet, an dem der betreffende Rechner angeschlossen ist.

Doch nicht nur der Switch pflegt eine Tabelle mit MAC-Adressen, sondern auch die beteiligten Rechner. Mit ARP-Anfragen können diese ARP-Tabellen am beteiligten Rechner gefüllt werden. Ziel des ARP-Spoofings ist es, die ARP-Tabellen zu manipulieren (ARP-Cache-Poisoning). Dazu schickt ein Angreifer eine ARP-Antwort an das Opfer, in der er seine eigene MAC-Adresse als die des Routers ausgibt, der für das betreffende Subnetz als Standard-Gateway fungiert. Sendet das Opfer anschließend ein Paket zum eingetragenen Standard-Gateway, landet dieses Paket in Wirklichkeit beim Angreifer. Auf die selbe Weise wird der ARP-Cache des Routers so manipuliert, dass Ethernet-Frames, die eigentlich an das Opfer adressiert wurden, in Wirklichkeit beim Angreifer landen. Auf einschlägigen Internet-Seiten sind eine Reihe von Tools verfügbar, die diese Angriffsmethode ermöglichen.

MAC-Flooding

MAC-Flooding ist eine Angriffsmethode, die die Funktionsweise eines Switches beeinflusst. Switches erlernen angeschlossene MAC-Adressen dynamisch. Die MAC-Adressen werden in der Switching-Tabelle gespeichert. Der Switch weiß dadurch, an welchen Ports die entsprechenden MAC-Adressen angeschlossen sind.

Wenn nun eine angeschlossene Station mit Hilfe eines geeigneten Tools eine Vielzahl von Paketen mit unterschiedlichen Quell-MAC-Adressen sendet, speichert der Switch diese MAC-Adressen in seiner Switching-Tabelle. Sobald der Speicherplatz für die Switching-Tabelle gefüllt ist, sendet ein Switch sämtliche Pakete an alle Switch-Ports. Durch dieses "Fluten" der Switching-Tabelle mit sinnlosen MAC-Adressen kann ein Switch nicht mehr feststellen, an welche Ports tatsächliche Ziel-MAC-Adressen angeschlossen sind. Diese Angriffsmethode wird verwendet, um das Mitlesen von Paketen in geswitchten Netzen zu ermöglichen. Es sind frei verfügbare Tools auf einschlägigen Seiten im Internet verfügbar, die auf einem Switch über 155.000 MAC-Adress-Einträge innerhalb einer Minute erzeugen können.

G 5.113 MAC-Spoofing

Die MAC-Adresse ("media access control") eines Geräts ist eine vom Hersteller vorgegebene Adresse, mit der Geräte auf der OSI-Schicht 2 adressiert werden.

Verschiedene Sicherungsmechanismen auf der Netzebene (beispielsweise Port-Security bei Switches) beruhen darauf, dass eine Verbindung nur von einem Gerät mit einer bestimmten MAC-Adresse aufgebaut werden darf.

Mit Hilfe entsprechender Programme kann ein Angreifer die MAC-Adresse seines Gerätes ändern und Ethernet-Frames mit einer fremden Kennung in das Netzsegment schicken. Auf diese Weise können Sicherungsmechanismen umgangen werden, die allein auf der Verwendung einer MAC-Adresse beruhen. Der Angreifer muss sich dabei allerdings im selben Netzsegment befinden oder sogar Zugang zu demselben Switchport haben wie das Gerät, als das er sich mittels MAC-Spoofing ausgibt.

Eine Gefährdung durch MAC-Spoofing besteht auch bei drahtlosen Netzen (WLAN), bei denen am Access-Point eine entsprechende Zugangskontrolle konfiguriert wurde.

G 5.114 Missbrauch von Spanning Tree

Das Spanning Tree Protokoll ist in IEEE 802.1d spezifiziert. Spanning Tree wird verwendet, um Schleifenbildungen innerhalb eines Netzes mit mehreren Switches zu vermeiden. Bei diesem Verfahren werden redundante Netzstrukturen ermittelt und in eine zyklenfreie Struktur abgebildet. Diese Maßnahme reduziert die aktiven Verbindungswege einer beliebig vermaschten Netzstruktur auf eine Baumstruktur.

In der folgenden Abbildung ist zu erkennen, dass ein Port des unteren Switches mit Hilfe von Spanning Tree geblockt wurde. Durch Aussenden von Bridge Protocol Data Units (BPDUs), wird eine Root-Bridge, basierend auf der eingestellten Priorität und MAC-Adresse des Switches, ermittelt. In der Abbildung stellt der Switch rechts oben die Root Bridge dar.

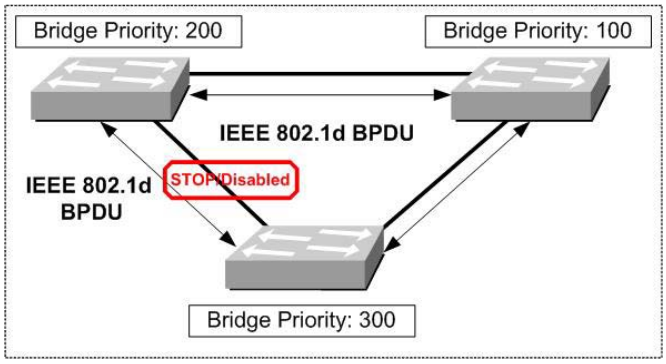


Abbildung 1: Spanning Tree

Spanning Tree bietet keine Authentisierung beim Austausch von BPDUs. Dies kann in geswitchten Netzen durch Angreifer ausgenutzt werden. Wenn ein Angreifer von einer am Switch angeschlossenen Station in der Lage ist, BPDUs auszusenden, wird mit Hilfe des Spanning Tree-Algorithmus die Topologie neu berechnet. Die Konvergenz zur Berechnung der Topologie-Änderung kann beim Spanning-Tree 30 Sekunden betragen. Dadurch kann bei der Aussendung von BPDUs die Verfügbarkeit des Netzes empfindlich gestört werden.

G 5.115 Überwindung der Grenzen zwischen VLANs

Virtual LANs (VLANs) werden zur logischen Strukturierung von Netzen verwendet. Dabei wird innerhalb eines physikalischen Netzes eine logische Netzstruktur abgebildet, indem funktionell zusammengehörende Arbeitsstationen und Server zu einem virtuellen Netz verbunden werden. Ein VLAN bildet gleichzeitig eine separate Broadcast-Domäne. Das bedeutet, dass Broadcasts nur innerhalb des VLANs verteilt werden. Ein VLAN kann sich hierbei über ein ganzes geswitchtes Netz hinziehen und braucht nicht nur auf einen einzelnen Switch beschränkt zu bleiben.

VLANs über mehrere Switches auszudehnen, wird durch unterschiedliche sogenannte Trunking-Protokolle realisiert. Hierbei wird pro Switch ein physischer Port für die Inter-Switch-Kommunikation reserviert, die logische Verbindung zwischen den Switches wird als Trunk bezeichnet. Ein Ethernet-Rahmen wird beim Informationsaustausch zwischen den Switches in das Trunking-Protokoll gekapselt. Dadurch ist der Ziel-Switch in der Lage, die Information dem entsprechenden VLAN zuzuordnen. Als Standards werden IEEE 802.1q und die proprietären Protokolle ISL (Inter Switch Link) und VTP (VLAN Trunking Protocol) des Herstellers Cisco verwendet.

Wenn sich ein Angreifer, der an einem Switch angeschlossen ist beispielsweise durch die Verwendung der Trunking-Protokolle ISL (Inter Switch Link) oder IEEE 802.1q als Switch ausgibt, ist es möglich, dadurch auf alle konfigurierten VLANs Zugriff zu erhalten und so Daten mitzulesen, die zu einem VLAN gehören, auf das der Angreifer normalerweise keinen Zugriff hat.

Mit Hilfe des proprietären Protokolls VTP werden Informationen über konfigurierte VLANs zwischen Cisco-Switches ausgetauscht. Dabei ist es möglich, die VLAN-Konfiguration eines zentralen VTP-Servers innerhalb einer VTP-Domäne auf alle beteiligten Switches zu verteilen. Dies vereinfacht zwar die Verwaltung von VLANs mit mehreren Switches, stellt gleichzeitig aber ein zusätzliches Sicherheitsrisiko dar: VTP unterstützt zwar die Authentisierung innerhalb einer VTP-Domäne, falls jedoch kein Passwort für die Authentisierung von Switches innerhalb einer Domäne gesetzt ist, kann ein Angreifer (beispielsweise auf einem eigenen Switch, der als VTP-Server konfiguriert ist) die gesamte VLAN-Architektur auf Switches der VTP-Domäne überschreiben.

G 5.116 Manipulation der z/OS-Systemsteuerung

z/OS-Systeme lassen sich über vielfältige Schnittstellen beeinflussen, zum Beispiel über die *Hardware Management Console*, die *MVS-Master-Konsole*, den *Enhanced MVS Console Service*, Automationsverfahren, entfernte MVS-Konsole und Fernwartungszugänge. Einige Sicherheitsprobleme, die mit der Verwendung dieser Schnittstellen verbunden sein können, werden nachfolgend aufgezeigt.

HMC (Hardware Management Console)

Der unbefugte Zugriff auf die HMC kann zu erheblichen Sicherheitsproblemen führen. Denn von der HMC aus kann das Systemverhalten während des Betriebs beeinflusst werden. Es können einzelne LPARs (*Logical Partitions*) bis hin zu einem ganzen Rechner-Verbund neu initialisiert werden. Darüber hinaus lassen sich über die HMC auch neue *Input/Output Control Datasets* einspielen, die beim nächsten *Initial Program Load* (IPL) aktiv werden. Dadurch besteht zum Beispiel die Gefahr, dass einer LPAR eigentlich nicht zugehörige Platten zugewiesen werden.

MVS-Master-Konsole

z/OS-Betriebssysteme werden unter anderem über MVS-Konsolen gesteuert. Die Standard-Konsolen sind mit dem System fest verbunden und benötigen weder Kennung noch Passwort. Das bedeutet, dass Personen, die physischen Zugriff auf eine hoch autorisierte MVS-Konsole haben (z. B. auf die Master-Konsole), jedes beliebige MVS-Kommando eingeben können. In der Folge können unbefugt *Batch-Jobs* oder *Started Tasks* gestoppt oder gestartet werden. Ferner lassen sich Platten an jedem System *Online* setzen, falls sie dort generiert sind. Unter Umständen lassen sich auch über MVS-Kommandos Kanalpfade nachgenerieren, und danach Platten anhängen, die gar nicht zu dieser LPAR gehören.

Enhanced MVS Console Service

Über die normalen MVS-Konsolen hinaus stellt das z/OS-Betriebssystem den EMCS (*Enhanced MVS Console Service*) zur Verfügung. Dieser wird von verschiedenen Anwendungen, wie zum Beispiel TSO, CICS oder NetView, auch als Funktion angeboten. Über EMCS können dynamisch Konsolen im Rahmen eines Script-Ablaufs angelegt werden, die nahezu alle Kommandos unterstützen, die auch bei den normalen Konsolen benutzt werden können. Wird EMCS nicht oder unzureichend über RACF-Profile geschützt, kann u. U. von jedem Terminal aus das z/OS-Betriebssystem manipuliert werden.

Gefahren bei Automation

Automationsverfahren können so programmiert sein, dass sie durch Nachrichten ausgelöst werden. Wenn die Automationsverfahren nicht speziell geschützt werden, besteht die Gefahr, dass durch das Erzeugen einer gefälschten Nachricht Automationsfunktionen unbefugt gestartet werden.

Entfernte MVS-Konsole

z/OS-Systeme können an unterschiedlichen Standorten von einer zentralen Konsole aus gesteuert werden. Hierfür wird häufig ein Software-Tool eingesetzt, das es z. B. erlaubt, die LPARs der z/OS-Systeme auch über große

Entfernungen zu steuern. Das Software-Tool emuliert eine MVS-Konsole auf einem gewöhnlichen PC. Wenn der physische oder der logische Zugang zu solchen Steuerkonsolen unzureichend geschützt ist, besteht die Gefahr, dass von dort aus unbefugt Manipulationen an entfernten z/OS-Systemen vorgenommen werden.

Fernwartungszugänge

Eine weitere Gefährdung des z/OS-Systems kann durch unsachgemäße Konfiguration der RSF-Konsole (*Remote Support Facility*) bestehen. Ein externer Angreifer kann unter Umständen Fehler in der Konfiguration ausnutzen und sich in diese Konsole einwählen (siehe auch G 5.10 *Missbrauch von Fernwartungszugängen*).

Beispiel:

Erschleichen des Special-Privilegs

- RACF wurde in einem Rechenzentrum so eingerichtet, dass RACF-Kommandos auch von einer *MVS-Master-Konsole* aus eingegeben werden konnten. Ein nicht autorisierter Mitarbeiter hatte Zutritt zu dem Raum, in dem diese Konsolen standen. Als Folge konnte er das *Special*-Privileg seiner eigenen User-ID zuweisen. Dies blieb über einen längeren Zeitraum unbemerkt.

G 5.117 Verschleiern von Manipulationen unter z/OS

Durch Änderungen an Protokolldateien oder Abschalten von Protokollierungs-Funktionen ist es möglich, Manipulationen am z/OS-System zu verschleiern.

Die meisten Komponenten des z/OS-Systems erzeugen Protokollierungsinformationen über Systemaktivitäten und -ereignisse. Diese werden regelmäßig entladen und in entsprechenden Protokolldateien (z. B. *System-Log*, *SMF-Datensätze*) gespeichert, die später ausgewertet werden können.

Protokolldateien sind veränderbar oder manipulierbar, wenn ein entsprechendes Zugriffsrecht auf die Datei besteht. Dieses kann beispielsweise durch Nachlässigkeiten bei der Systemadministration unabsichtlicht vergeben worden sein, oder ein Angreifer hat sich - etwa durch entsprechende Manipulationen - dieses Zugriffsrecht verschafft.

Eine weitere Angriffsmöglichkeit auf die Systemprotokollierung besteht darin, die Erzeugung von Protokolldaten durch entsprechende Manipulation der generierenden Komponente zu verhindern. Welche *SMF-Datensätze* geschrieben werden, ist bei z/OS beispielsweise in einem *Konfigurations-Member* eingetragen. Durch Änderungen an diesem *Member* oder durch das Setzen von *Exits* lässt sich erreichen, dass bestimmte *SMF-Sätze* nicht mehr geschrieben werden. Die üblichen Sicherheitsmonitore sind nicht in der Lage, unterdrückte Verstöße zu erkennen und zu melden, wenn keine *SMF-Sätze* oder keine Systemnachrichten geschrieben werden.

Beispiel:

Abschalten von SMF-Sätzen

- In einem Rechenzentrum gelang es einem Anwender, das Schreiben von SMF-Datensätzen abzustellen. Daraufhin nahm er bestimmte Manipulationen vor und schaltete die SMF-Funktion anschließend wieder ein. Die in diesem Zeitraum am z/OS-System vorgenommenen Änderungen ließen sich später nicht mehr nachvollziehen, denn es fehlten die Protokolldaten. Es konnte lediglich im System-Log nachgewiesen werden, dass die Kommandos von einer MVS-Konsole aus eingegeben wurden, die mehreren Personen zur Verfügung stand.

G 5.118 Unbefugtes Erlangen höherer Rechte im RACF

Gelingt es einem Anwender, seine Berechtigungen im z/OS-Sicherheitssystem RACF zu erhöhen, kann er unter Umständen unbefugt auf Dateien zuzugreifen und das System manipulieren.

Trace im Netz

Mit einem sogenannten *Trace* (Abhören des Netzverkehrs) der TCP/IP- oder TPX-Protokolle kann ein Angreifer je nach Absicherung des Netzes die Kennung und das Passwort eines Anwenders mit *Special*-Rechten ausspähen. Unter Ausnutzung dieser Kenntnisse können die eigenen Berechtigungen erhöht werden, bis zur Vergabe der *Special*-Rechte an die eigene Kennung.

APF, SVC

Zwei weitere Möglichkeiten, sich als Benutzer im z/OS-System höhere Berechtigungen zu verschaffen, sind das APF (*Authorized Programming Facility*) und die SVCs (*SuperVisor Calls*).

Gelingt es dem Anwender, Programme in APF-autorisierte Dateien einzustellen, oder gelingt es ihm, SVCs zu installieren, so kann er sich über diese mit *Special*- oder *Operations*-Rechten ausstatten (Manipulation des eigenen ACEE-Kontrollblocks). Diese stehen zwar nur temporär für die jeweilige Sitzung zur Verfügung, das Programm kann aber jedesmal neu aufgerufen werden.

Akkumulierte Rechte

Eine weitere Gefahr besteht durch sogenannte *akkumulierte Rechte* aufgrund eines unzureichenden Berechtigungsmanagements. Typisch ist dabei das folgende Szenario:

Ein Anwender wechselt in ein neues Tätigkeitsfeld. Der Anwender erhält die Rechte, die seine neue Aufgabe fordern, ohne dass die alten Rechte gelöscht werden. Auf diese Weise akkumuliert der Anwender über einen langen Zeitraum Rechte, die erheblich über die eigentlich benötigten Berechtigungen hinaus gehen.

Beispiel:

- Fachwissen ist im z/OS-Umfeld wenig verbreitet. Als Folge hielten sich fachkundige z/OS-Berater über lange Zeit in einer Firma auf und akkumulierten Rechte. Ein Administrator hat dies nur zufällig bemerkt, als das Berechtigungskonzept der Firma vollständig überarbeitet wurde.

G 5.119 Benutzung fremder Kennungen unter z/OS-Systemen

Die *Surrogat*-Berechtigung des z/OS-Sicherheitssystems RACF ermöglicht es einem Benutzer A, einen Batch-Job unter der Kennung eines anderen Benutzers B laufen zu lassen, ohne dass Benutzer A das Passwort von Benutzer B kennt. Alle Sicherheitsprüfungen erfolgen für die Kennung von Anwender B und die Protokoll- und SMF-Daten notieren Anwender B als Ausführenden der Befehle.

Es besteht die Gefahr, dass die Berechtigung *Surrogat* missbräuchlich verwendet wird, wenn nicht die notwendigen Sicherheitsvorkehrungen bei der Vergabe und bei der Überwachung eingehalten werden:

- Benutzer können u. U. unbefugt Aktionen ausführen, zu denen sie mit ihrer eigenen Kennung nicht berechtigt sind.
- Benutzer können u. U. vortäuschen, dass ein anderer Benutzer für eigene (unerlaubte) Aktionen verantwortlich sei.

G 5.120 Manipulation der Linux/zSeries Systemsteuerung

Es sind drei unterschiedliche Betriebsarten von Linux unter zSeries möglich:

- Linux Native auf zSeries Hardware
- Linux in einer zSeries LPAR
- Linux unter dem Träger-System z/VM

Weitere Informationen zu den Betriebsarten von Linux unter zSeries finden sich in der Maßnahme M 3.41 *Einführung in Linux und z/VM für zSeries-Systeme*.

In allen drei Betriebsarten von Linux unter zSeries bestehen die in Baustein B 3.102 *Unix-Server* beschriebenen Gefährdungen.

Mainframe-spezifische Gefährdungen beim Einsatz von Linux

Über die in Baustein B 3.102 *Server unter Unix* beschriebenen Gefährdungen hinaus können beim Einsatz von Linux auf zSeries-Mainframes unter anderem die folgenden Sicherheitsprobleme bestehen:

Linux in einer zSeries LPAR

Mainframe-spezifische Gefährdungen ergeben sich aus den möglichen Einwirkungen auf die zSeries Hardware:

- Durch den Zugang zu *HCD*-Funktionen (*Hardware Configuration Definition*) können Mitarbeiter Hardware-Ressourcen, wie z. B. Festplatten, unbefugt zur Linux-Partition zuordnen. Damit hat das Linux-Betriebssystem Zugriff auf die Hardware-Ressourcen.
- Der Zugang zur *HMC* (*Hardware Management Console*) erlaubt Manipulationen wie Starten, Stoppen und Zuordnung von Ressourcen zu einer LPAR. Analog ist dies in G 5.116 *Manipulation der z/OS-Systemsteuerung* für das z/OS-Betriebssystem beschrieben. Ähnlich sicherheitskritisch ist der Zugriff auf *SE*s (*Service Elements*). Das Service Element ist eine Komponente der zSeries-Hardware, die die gleichen Funktionalitäten wie eine HMC bietet.

Linux unter dem Träger-System z/VM

In diesem Szenario wird Linux auf einer emulierten Hardware einer virtuellen Maschine betrieben. Die emulierte Hardware der virtuellen Maschine wird von z/VM auf der realen zSeries-Hardware realisiert. Der physische Zugriff auf die realen Ressourcen erfolgt nur über z/VM.

Die Mainframe-spezifischen Gefährdungen ergeben sich einerseits aus den möglichen Einwirkungen auf die emulierte Hardware, andererseits aus den möglichen Einwirkungen auf z/VM.

- Der Zugang zu *HCD*-Funktionen und zur *HMC* kann - wie in der Betriebsart *Linux in einer zSeries LPAR* - missbraucht werden.
- Mitarbeiter, die kritische z/VM-Kommandos absetzen dürfen, können u. U. die Betriebsstabilität des z/VM und damit die darauf laufenden Linux-Betriebssysteme erheblich gefährden.

- Mitarbeiter, die unbefugt Zugriff auf das *DIRMAINT* Utility erhalten, können darüber z. B. neue virtuelle Systeme generieren oder Minidisks eines Linux einem anderen zuordnen. Wird z/VM RACF nicht benutzt, können über *DIRMAINT* auch Benutzerkennungen administriert werden.
- Ist im z/VM-Betriebssystem die Sicherheitskomponente z/VM RACF (Resource Access Control Facility) eingesetzt, so bestehen unter z/VM vergleichbare Gefährdungen, wie in G 3.72 *Fehlerhafte Konfiguration des z/OS-Sicherheitssystems RACF* für das z/OS-Betriebssystem beschrieben. Mitarbeiter, die hohe RACF/VM-Autorisierungen besitzen (z. B. *SPECIAL*), können über RACF/VM andere z/VM-Kennungen und -Berechtigungen manipulieren.
- Falls die Authentisierung unter Linux über eine LDAP-Anbindung mit PAM-Modul (*Pluggable Authentication Module*) durch ein z/OS-RACF erfolgt, können Linux-Kennungen und -Berechtigungen auch von Mitarbeitern mit hoher z/OS-RACF-Autorisierung beeinflusst werden.

Beispiel:

Unberechtigte Nutzung der z/VM-Administration

- Ein Mitarbeiter hatte aus historischen Gründen noch die Berechtigung, unter z/VM die Funktion DIRMAINT zu verwenden. Dies nutzte er aus, um für sich ein privates Linux zu generieren und zu benutzen. Dies führte zum Verbrauch von Ressourcen, die dadurch den ordnungsgemäßen Prozessen auf der zSeries-Maschine nicht mehr zur Verfügung standen.

G 5.121 Angriffe über TCP/IP auf z/OS-Systeme

Um ein z/OS-System über die Netzanbindung anzugreifen, sind häufig keine Spezialkenntnisse der SNA-Netzarchitektur oder von MVS erforderlich. Durch die TCP/IP-Anbindung an öffentliche Netze und die *Unix System Services* sind viele z/OS-Systeme über Standardprotokolle und Dienste, wie z. B. HTTP oder FTP, für externe Angreifer erreichbar.

Externe Angreifer können unter Umständen über die TCP/IP-Anbindung an öffentliche Netze Denial-of-Service-Angriffe gegen die angebotenen Dienste durchführen oder übertragene Daten unbefugt lesen oder manipulieren.

Interne Angreifer können über die TCP/IP-Anbindung an interne Netze versuchen, ihre Berechtigungen zu erhöhen, indem sie etwa Kennung und Passwort eines Anwenders mit *Special*-Rechten ausspähen.

G 5.122 Missbrauch von RACF-Attributen unter z/OS

Im z/OS-Sicherheitssystem RACF sind die Attribute *SPECIAL*, *OPERATIONS* und *AUDITOR* mit besonders hohen Berechtigungen ausgestattet.

Attribut *SPECIAL*

Die Kennung mit dem Attribut *SPECIAL* ist für die Administration des Sicherheitssystems RACF erforderlich. Der Besitzer dieses Attributs verfügt über die Möglichkeit, im RACF Einstellungen zu ändern. Er gibt beispielsweise den Benutzern den Zugriff auf Systemressourcen und Dateien frei. Der Inhaber der Berechtigung kann sich selbst auf sämtliche Ressourcen und Dateien des Systems Rechte vergeben. Er kann auch die im Weiteren aufgeführten Attribute an alle Benutzerkennungen vergeben.

Eine mögliche Schwachstelle besteht beim Einsatz von Systemmonitoren, die über hoch autorisierte Programmteile ihre eigene Kennung mit dem Attribut *SPECIAL* versehen können. Anwender mit Zugang zu den Systemmonitoren können dies - bei entsprechenden RACF-Rechten - ausnutzen, um ihre eigene Kennung mit höheren Zugriffsrechten zu versehen.

Attribut *OPERATIONS*

Die Kennung mit dem Attribut *OPERATIONS* wird hauptsächlich für das *Space-Management* im z/OS-System angefordert. Es beinhaltet die Rechte zum Kopieren, Lesen, Löschen oder Neuanlagen von Dateien, ohne dass ein explizites Recht für die Datei und die Benutzerkennung vergeben wurde. Dies ermöglicht es prinzipiell einem Anwender, das Attribut *OPERATIONS* für unbefugte Datenzugriffe zu missbrauchen.

Attribut *AUDITOR*

Auditoren sollen sicherheitsrelevante Ereignisse erkennen, nachvollziehen und überprüfen können. Änderungen an RACF-Definitionen sind mit dieser Berechtigung nur für audit-relevante Definitionen möglich (im Gegensatz zu *SPECIAL*), d. h. höhere Autorisierungen lassen sich damit nicht erreichen. Allerdings birgt das Attribut *AUDITOR* die Gefahr, dass umfassende Informationen, z. B. sämtliche RACF-Einstellungen, über das System ausgespäht werden können.

Beispiele:

- Ein Systemprogrammierer verfügte nicht über das Attribut *SPECIAL*. Er schrieb ein spezielles Programm und stellte es in eine APF-autorisierte Datei. Den Zugriff auf die APF-Dateien benötigte er für seine reguläre Arbeit. Über das selbst geschriebene Programm gelang es dem Systemprogrammierer, sich das Attribut *SPECIAL* zuzuweisen und unbefugt Änderungen an RACF-Einstellungen durchzuführen.

  Erschleichen des Special-Attributes

- Als in einem Unternehmen bekannt wurde, dass ein Konkurrent Kunden abwarb, wurden umgehend Nachforschungen angestellt. Wie sich herausstellte, verfügte die Benutzerkennung eines Anwenders über das Attribut *OPERATIONS*. Mit Hilfe dieses Attributs gelang es ihm, die Kundenadressen regelmäßig unerlaubt zu kopieren und weiterzugeben.

  Ausnutzen des Operation-Attributes

G 5.123 Abhören von Raumgesprächen über mobile Endgeräte

Viele mobile Endgeräte wie Laptops, PDAs oder Mobiltelefone werden mittlerweile mit integriertem Mikrofon oder Kamera ausgeliefert. Mit diesen können nicht nur Ideen oder Schnappschüsse unterwegs aufgenommen werden, sie können auch dazu benutzt werden, unbemerkt Gespräche aufzuzeichnen oder abzuhören (siehe auch G 5.95 *Abhören von Raumgesprächen über Mobiltelefone*).

Unauffällig aktivierbar

Hierzu kann beispielsweise ein PDA benutzt werden, der unauffällig in einem Raum platziert wurde, z. B. bei einer Besprechung.

Besprechungsteilnehmer rechnen normalerweise nicht damit, dass die komplette Besprechung mitgeschnitten wird.

Beispiel:

- In einer Besprechung haben fast alle Beteiligten ihre Laptops dabei und benutzen diese auch fortwährend. Einer der Teilnehmer hat unauffällig sein Rechnermikrofon aktiviert. Wie bei den meisten mobilen Endgeräten ist auch hier für die anderen Teilnehmer nicht erkennbar, dass das Mikrofon eingeschaltet ist. Er fertigt darüber einen kompletten Mitschnitt der Besprechung an und schneidet daraus kleinere Beiträge heraus. Da diese aus dem Sinnzusammenhang herausgerissen wurden, kann er damit erfolgreich ein anderes Besprechungsergebnis vorspiegeln.

G 5.124 Missbrauch der Informationen von mobilen Endgeräten

Mobile Endgeräte gehen leicht verloren und sind einfach zu stehlen (siehe auch G 5.22 *Diebstahl bei mobiler Nutzung des IT-Systems*). Je kleiner und begehrter solche Geräte sind, desto stärker ist dieses Risiko. Neben dem unmittelbaren Verlust kann dabei durch den Verlust bzw. die Offenlegung wichtiger Daten weiterer Schaden entstehen. Dieser mittelbare Schaden ist in vielen Fällen deutlich schwerwiegender als der rein materielle Verlust des Gerätes.

Beispiele:

Vertrauliche Daten auf dem PDA

- Daten wie Notizen von Besprechungen oder Adressen, die im PDA gespeichert sind, können durchaus einen vertraulichen Charakter haben. Ein Verlust des Geräts bedeutet dann unter Umständen die Offenlegung dieser gespeicherten Informationen.
- Viele mobile Endgeräte haben Sicherheitsmechanismen, die diese vor einem unbefugten Zugriff schützen sollen. Diese Sicherheitsmechanismen sind aber meistens zu schwach ausgelegt, wodurch es Angreifern ein leichtes ist, diese zu überwinden. Selbst wo sie vorhanden sind, werden sie aber häufig aus Bequemlichkeit nicht benutzt, so dass die vertraulichen Daten im Verlustfall überhaupt nicht geschützt sind.
- Häufig sind auf mobilen Endgeräten Zugangsdaten für andere IT-Systeme oder das LAN der Behörde bzw. des Unternehmens gespeichert. Wenn ein Unbefugter in den Besitz eines Laptops oder PDA mit (statischen) Zugangskennungen gelangt, ist damit ein missbräuchlicher Zugriff auf interne Daten möglich.
- Bei PDAs mit eingebautem Mobiltelefon (Smartphones) kann ein unehrlicher Finder oder Dieb auf Kosten des rechtmäßigen Besitzers telefonieren, sofern ihm die PIN bekannt ist, er sie leicht erraten kann oder wenn die Sicherheitsmechanismen des Gerätes leicht überwunden werden können.
- Viele PDAs und Laptops haben Schnittstellen für den Einsatz austauschbarer Datenspeicher wie z. B. Speicherkarten oder USB-Tokens. Bei einem unbeaufsichtigten PDA oder Laptop mit der entsprechenden Hard- und Software besteht die Gefahr, dass über diese Speichermedien große Datenmengen schnell herunterkopiert werden können. Dabei werden nicht einmal Spuren hinterlassen.

G 5.125 Unberechtigte Datenweitergabe über mobile Endgeräte

Mobile Endgeräte wie Notebooks oder PDAs sind im allgemeinen darauf ausgelegt, einen einfachen Datenaustausch mit anderen IT-Systemen zu ermöglichen. Dies kann über ein Verbindungskabel oder auch drahtlos, z. B. über Infrarot, Bluetooth oder GSM, erfolgen.

Wo ein offener Zugang zu IT-Systemen möglich ist, können Informationen unauffällig abgefragt und übermittelt werden. Die gesammelten Daten können dann mit dem mobilen Endgerät unbemerkt mitgenommen oder modifiziert werden. Eine nachträgliche Überprüfung oder gar ein Nachweis ist nicht immer möglich, da häufig die Zugriffe nicht entsprechend protokolliert wurden.

Falls das Gerät über eine drahtlose Kommunikationsschnittstelle verfügt (beispielsweise eine integrierte WLAN-Karte oder eine Bluetooth-Schnittstelle zu einem Mobiltelefon), so können die gespeicherten Informationen auch unmittelbar an jeden Ort der Welt übermittelt werden (siehe auch G 5.97 *Unberechtigte Datenweitergabe über Mobiltelefone*).

Wird in einer Organisation ein eigenes drahtloses Netz (WLAN) betrieben, so kann ein Besucher mit seinem mitgebrachten PDA den WLAN-Verkehr belauschen. Falls das drahtlose Netz nicht ausreichend abgesichert ist kann der Angreifer problemlos alle übermittelten Daten "mitschneiden" oder gar auf diesem Weg direkten Zugriff auf das Netz erlangen.

Beispiel:

- Ein Mitarbeiter eines Unternehmens wird aus einer Besprechung mit einem Externen gerufen, um ein wichtiges Telefonat entgegenzunehmen. Der Externe nutzt die kurze Zeitspanne ohne Beaufsichtigung, um den im Besprechungsraum aufgestellten PC mit seinem mobilen Endgerät zu verbinden. Anschließend transferiert er alle zugreifbaren Daten auf sein mobiles Endgerät.

G 5.126 Unberechtigte Foto- und Filmaufnahmen mit mobilen Endgeräten

Vorsicht Kamera!

Immer mehr mobile Endgeräte sind inzwischen mit eingebauten oder aufsteckbaren Kameras ausgerüstet, beispielsweise bei Laptops, PDAs oder Mobiltelefonen. Teilweise ist mit solchen Kameras sogar die Aufzeichnung von Filmen möglich. Solche mobilen Endgeräte können leicht dazu benutzt werden, in sensiblen Bereichen (beispielsweise in einer Entwicklungsabteilung) unauffällig Foto- oder gar Filmaufnahmen anzufertigen. Die Bildqualität reicht zwar meist nicht an die Qualität "richtiger" Kameras heran, trotzdem ist es wichtig, sich dieser Gefahr bewusst zu sein.

Wie beim "allgemeinen Datenklau" (siehe G 5.125 *Unberechtigte Datenweitergabe über mobile Endgeräte*) können die gemachten Bilder unmittelbar nach draußen übermittelt und anschließend wieder vom Gerät gelöscht werden. In diesem Fall ist selbst dann, wenn jemand Verdacht schöpft, ein Nachweis praktisch nicht mehr möglich.

Beispiele:

- In viele Schwimmbäder und Sportstudios dürfen mittlerweile keine Foto-Handys mehr mitgenommen werden, da es verschiedene Beschwerden über heimlich aufgenommene Fotos aus Umkleidekabinen gab. Unter anderem wurde dies öffentlich, da einige Hobby-Paparazzi ihre Fotos stolz auf Webseiten präsentiert haben.
- Viele Laptop-Modelle haben neben einem integrierten Mikrofon auch eine kleine integrierte Kamera, die je nach Auslegung für Standbilder, Videoaufnahmen oder als Webcam benutzt werden kann. Mit solchen Kameras ist es problemlos möglich, sogar aus den hintersten Reihen in einem Hörsaal nicht nur die Folien lesbar und den Redner hörbar aufzeichnen zu können, sogar Zwischenfragen können damit erstaunlich gut mitgeschnitten werden. Da die Geräte nicht als Kamera wahrgenommen werden, ist es hier schon zu unangenehmen Überraschungen gekommen, als nachträglich ungenehmigte Mitschnitte veröffentlicht wurden.

G 5.127 Spyware

Als Spyware werden Programme bezeichnet, die heimlich, also ohne darauf hinzuweisen, Informationen über einen Benutzer bzw. die Nutzung eines Rechners sammeln und an den Urheber der Spyware weiterleiten. Spyware gilt häufig als lästig, aber nicht als so gefährlich wie Computer-Viren, Würmer oder Trojaner. Durch Spyware können aber durchaus Sicherheitsprobleme entstehen, was sich beispielsweise in der unbemerkten Weitergabe von persönlichen Daten, aber auch durch die damit verbundenen unerlaubten Eingriffe in das IT-System zeigt. Dadurch können unter anderem Änderungen an der Systemkonfiguration, wie der Windows Registry, oder das Einspielen von ausführbarem Code wie DLLs, ActiveX- oder Java-Objekte gehören. Spyware kann vor allem durch unberechtigtes Herunterladen von Software, Updates oder sonstigen Dateien (Musik oder Dokumente aus zweifelhaften Quellen) aus dem Internet auf das IT-System gelangen. Spyware kann sich aber auch ohne Wissen und Zustimmung des Anwenders selbst auf einem IT-System installieren.

Adware ist keine Spyware

Oftmals wird fälschlicher Weise **Adware** auch als Spyware bezeichnet. Bei Adware handelt es sich um Software, die zusätzlich zur eigentlichen Funktionalität Werbung einblendet. Dies dient hauptsächlich zur Finanzierung von frei erhältlicher Software und es werden in der Regel keine vertraulichen Daten an Dritte übermittelt.

Beispiele:

Ausspähen von vertraulichen Daten

- Ein häufiger Spyware-Typ überwacht die Browser-Aktivitäten, was auch als "Browser Hijacking" bezeichnet wird. Dabei werden beispielsweise die Sucheinstellungen des Browsers verändert. Dadurch können vertrauliche Daten, wie Kreditkarteninformationen oder Anmeldedaten für das Online-Banking, aber auch einfach E-Mail- und Internet-Adressen ausgespäht werden. Mit diesen Informationen werden Surfprofile erstellt und Unternehmen, z. B. für den Versand von Spam, zum Kauf angeboten. Die Spyware "CoolWebSearch" sammelt z. B. auf diesem Weg Unmengen an persönlichen Daten, unter Anderem Benutzernamen und Passwörter für die Anmeldung bei eBay, Online-Banking, Betriebssystemen
- In Spyware kann auch Programme zum Mitschneiden von Tastatureingaben, sogenannte Keylogger, integriert sein. Hierbei werden alle Tastatureingaben aufgezeichnet und möglichst unbemerkt an den Angreifer übermittelt. Dieser filtert dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern.
- Spyware-Programme können aufgrund schlechter Programmierung ein IT-System zum Absturz bringen oder erhebliche Störungen verursachen. Letztere entstehen hauptsächlichen durch den Anspruch von zusätzlichen System-Ressourcen durch die Spyware-Programme.

G 5.128 Unberechtigter Zugriff auf Daten durch Einbringen von Code in ein SAP System

Kann ein Angreifer ABAP-Code in ein SAP System einbringen, so sind unberechtigte Zugriffe auf Daten möglich, da die Sicherheit eines SAP Systems durch den ABAP-Code implementiert werden muss.

Beispiele:

- Ein Entwickler bringt im Rahmen eins Software-Updates eigenen, zusätzlichen Code in ein SAP ein, welcher ihm entfernten Zugriff auf alle Programme des SAP Systems gewährt.
- Einem externen Angreifer gelingt es, durch eine Schwäche in einer unternehmenseigenen Applikation eigene Transportdateien im SAP Transportverzeichnis abzulegen. Diese werden ohne Prüfung eingespielt und installiert und können so ihre Schadwirkung entfalten.

G 5.129 Manipulation von Daten über das Speichersystem

Über eine mangelhaft konfigurierte SAN-Installation kann eine ungewollte Verbindung zwischen Netzen entstehen. Eine gravierende Gefährdung für interne Daten einer Institution kann z. B. entstehen, wenn ein Server mit SAN-Anschluss aus dem Internet erreichbar ist und so von außen kompromittiert wird.

Die Anbindung eines an das Speichersystem angeschlossenen Servers, der nicht genügend vom Internet abgeschottet ist, kann bei einer Kompromittierung des Servers auch zur Kompromittierung des Speichersystems führen. So können gegebenenfalls Daten im SAN, die anderen Maschinen zugeordnet sind, gelesen oder verändert werden.

Da so alle Sicherheits- und Überwachungsmaßnahmen wie Firewalls oder IDS (Intrusion Detection Systeme) in den IT-Netzen der Institution übergangen werden, ist das Schadenspotential sehr gross.

G 5.130 Manipulation der Konfiguration des Speichersystems

Speichersysteme stellen die letzte Verteidigungslinie der IT der Institution dar, da hier an einer Stelle eine Vielzahl von wichtigen Daten einer Organisation konzentriert wird. Daher ergeben sich für diese Systeme besondere Sicherheitsanforderungen.

Die sicherheitsrelevanten Einstellungen eines Speichersystem lassen sich über herstellerspezifische Programme, die auf einem normalen PC ausgeführt werden oder über Standard-Schnittstellen wie einem Webbrowser, einsehen und manipulieren.

Wenn es einem Angreifer gelingt, an Passwörter zu gelangen, die den Zugriff auf Konfigurationsprogramme des Speichersystems erlauben um dort Einstellungen zu verändern, kann er eine Vielzahl von Sicherheits- und Kontrollmaßnahmen umgehen.

Wenn für die Administration kein eigenes Administrationsnetz eingerichtet wurde, und wenn zur Verwaltung des Speichersystems irgendwelche Protokolle verwendet werden, in denen Passwörter im Klartext versendet werden, so kann ein Angreifer diese sehr leicht ausspähen.

Damit könnte ein Angreifer, der von außen in einen beliebigen Rechner der Institution eingebrochen ist oder der (als Innentäter) regulär auf das Intranet zugreifen darf, seine Privilegien erhöhen.

Auch wenn keine unverschlüsselten Informationen zur Verwaltung von Speichersystemen im normalen Intranet verschickt werden, besteht die Gefahr, dass ein Rechner, der Informationen zur Konfiguration des Speichersystems enthält oder der zur Konfiguration geeignet ist, kompromittiert wird. Damit werden alle Sicherheitsmaßnahmen des gesamten Speichersystem hinfällig.

G 5.131 SQL-Injection

Mit SQL-Injection wird das Einschleusen (Injizieren) schädlicher oder unerwünschter Datenbankbefehle in die Datenbankabfragen einer Applikation bezeichnet. Ermöglicht wird diese Technik durch eine unzureichende Prüfung bzw. Maskierung der Eingaben innerhalb der Applikation. Die in Eingabefelder oder Parameter der Applikation eingetragenen Daten werden benutzt, um dynamisch Anfragen an die dahinterliegende Datenbank zu generieren. Ein Angreifer verwendet bestimmte Sonderzeichen in seinen Eingaben, um die dynamisch erzeugte Datenbankanfrage zu manipulieren und so seine eigenen Befehle an die Datenbank zu schicken.

Dieses Vorgehen eröffnet einem Angreifer vielfältige Möglichkeiten:

- unberechtigter Zugriff auf Daten,
- Manipulation von Daten,
- Gewinnung von Informationen durch Auslösen von Fehlermeldungen,
- Ausführen von Betriebsystembefehlen,
- Kontrolle über die Datenbank,
- Kontrolle über den Server.

Die Gefährdung richtet sich grundsätzlich sowohl gegen Web-Applikationen als auch gegen eigenständige Applikationen. Web-Applikationen sind hier jedoch besonders betroffen, da sie häufig nicht von einer geschlossenen Benutzergruppe verwendet werden. Dadurch erhöht sich die Anzahl der potentiellen Angreifer. Außerdem bleibt der Angreifer anonym, da er in keiner lokalen Benutzerverwaltung registriert ist.

G 5.132 Kompromittierung einer RPD-Benutzersitzung unter Windows Server 2003

Unberechtigter Zugriff über Remotedesktop-Freigabe

Die Remotedesktop-Freigabe auf Basis des *Remote Desktop Protocol* (RDP) ist ein effektives und verbreitetes Mittel zur Fernwartung eines Windows-Servers und zur Nutzung von Programmen auf entfernten Computern (Remotedesktop). Der Verbindungsaufbau von einem Clientcomputer zum RDP-Server findet ohne vorherige Authentisierung des Benutzers statt. Der komplette Anmeldebildschirm des Remotedesktops wird unmittelbar auf den Bildschirm des lokalen Clients gespiegelt. Es besteht die Gefahr, dass auch ein Angreifer durch die Windows-RDP-Anmeldung einen Remote-Zugriff auf das System erlangt.

Kompromittierende Information über Anmeldeschirm

Informationen zur Betriebssystemversion und zur Domänenmitgliedschaft liegen für jeden Remotedesktop-Benutzer ohne Eingabe von Benutzernamen und Kennwort offen. Weitere Informationen könnten über Hintergrundbilder preisgegeben werden. Häufig blenden Administratoren Verwaltungsinformationen als Hintergrundbild ein oder der Serverhersteller hat bei seinen vorinstallierten Betriebsystemen ein herstellerspezifisches Hintergrundbild vorgegeben. Darüber können verwertbare Informationen erlangt werden, um das System zu analysieren und entsprechende Sicherheitslücken auszunutzen.

Abfangen von RDP-Verbindungen

Im Falle einer Unterbrechung der Netzverbindung während einer RDP-Sitzung stellt Windows Server 2003 die Sitzung automatisch ohne erneute Anmeldung wieder her, sobald der Client die Netzverbindung zum Server wieder aufgenommen hat. Zeiträume bis in den Minutenbereich können überbrückt werden. Die erhöhte Fehlertoleranz wird mit der Gefährdung der Integrität einer RDP-Sitzung erkauft. Ein Angreifer kann durch Social Engineerung oder durch Abfangen der Verbindung einen Remote-Zugriff auf das System bekommen. Eine Verbindung mit RDP Version 5.2 von Windows Server 2003 kann durch Dritte leicht abgefangen und unbemerkt umgeleitet werden. Seit Windows Server 2003 mit Service Pack 1 gibt es zwar die Absicherung mittels SSL, aber viele Clients können dann keine Verbindung mehr herstellen, z. B. Remotedesktop-Clients früherer Windows-Versionen und RDesktop für Unix/Linux. Daher kann die Absicherung mit SSL meist nicht flächendeckend eingesetzt werden und die Gefahr des Abfangens der Verbindung und des Erlangens von unerlaubtem Zugriff auf das System besteht weiterhin.

Aufgrund der beschriebenen Gefahren ist von einer erhöhten Gefährdung des Servers auszugehen, sobald RDP verwendet wird.

Beispiele:

- Ein amerikanischer Hersteller liefert Server mit vorinstallierten OEM-Versionen von Windows Server 2003 an seine Kunden aus. Beim Anmelden am Betriebssystem via Konsole oder Remotedesktop erscheint ein Hintergrundbild mit Logo des Herstellers und einem Foto der Server-Hardware. Dadurch können Schwachstellen über das System ermittelt werden und für Angriffe genutzt werden.
- Während einer Netzunterbrechung verlässt der Administrator kurz den Verwaltungs-PC, auf dem eine RDP-Sitzung läuft. Ist er nicht rechtzeitig

wieder vor Ort und ist kein Bildschirmschoner mit Kennwortschutz aktiv, könnte ein Dritter die RDP-Sitzung weiterverwenden, sobald die Netzunterbrechung beseitigt worden ist. Er hätte die vollen Berechtigungen des Administrators und könnte versehentlich oder vorsätzlich großen Schaden verursachen.

G 5.133 Unautorisierte Benutzung web-basierter Administrationswerkzeuge

Die Administration mit Webbrowser-basierten Werkzeugen hat stark an Bedeutung gewonnen. Einer der entscheidenden Vorteile für das technisch verantwortliche Personal ist die Unabhängigkeit von

- der Betriebssystem-Plattform des zu betreuenden IT-Systems
- dem Standort des zu betreuenden IT-Systems.

Unsichere Authentisierungs-methoden

Allen Werkzeugen gemein ist, dass sie kritische Anmeldedaten verwenden. Sie sind auf gängige für das Internet standardisierte Authentisierungsmethoden angewiesen, um technischem Personal autorisierten Zugriff auf die kritischen lokalen Systeme zu gewähren. Viele Administrationswerkzeuge besitzen zusätzlich eigene Authentisierungsmechanismen oder bedienen sich lokaler, teils nicht standardisierter Authentisierungs- und Sicherheitsmechanismen. Es besteht die Gefahr der Kompromittierung durch nicht autorisierte Benutzer.

Unterlaufen der IT-Sicherheitsrichtlinie

Eine hohe Gefährdung entsteht, wenn die IT-Sicherheitsrichtlinie für die Authentisierung im Netz bzw. deren Umsetzung im betrachteten IT-Verbund durch ungeeignete Authentisierungsverfahren für Web-basierte Administrationswerkzeuge unterlaufen wird. Die häufigsten Ursachen dafür sind:

- die Wahl einer falschen oder veralteten Authentisierungsmethode, weil das jeweilige Werkzeug keine stärkere Authentisierung unterstützt oder weil andere beteiligte IT-Systeme (z. B. Sicherheitsgateways) das favorisierte Protokoll nicht unterstützen
- die ungeeignete Umsetzung bzw. Übernahme der Web-basierten Authentisierung in das lokale Authentisierungssystem

Eine Gefährdung kann z. B. entstehen, wenn zum Zwecke der Nutzung Web-basierter Administrationshilfen die Windowskomponente Internetinformationsdienst aktiviert wird, ohne diese entsprechend den Empfehlungen zu konfigurieren. Eine Gefahr könnte dann darin bestehen, dass in der Standardkonfiguration nur schwächere Authentisierungsverfahren aktiviert sind. Es ist darauf hinzuweisen, dass eine mangelhafte Konfiguration ein großes Risiko für alle auf dem Markt befindlichen Lösungen zur Web-basierten Administration darstellt.

G 5.134 Fehlende Identifizierung zwischen Gesprächsteilnehmern

Sowohl bei der leitungsvermittelnde Telefonie als auch bei VoIP kann der Anrufer oft über seine Telefonnummer identifiziert werden. Der Angerufene kann dabei in seinem Telefondisplay den Anrufer erkennen, ohne dass er das Telefongespräch annehmen muss. Integrated Services Digital Network (ISDN) bietet die Möglichkeit, über CLIP (Calling Line Identification Presentation) und COLP (Connected Line Identification Presentation) der Gegenstelle die Telefonnummer zu signalisieren. Bei VoIP können diese Informationen über die Caller ID ermittelt werden. Verallgemeinert wird dies als Rufnummernanzeige bezeichnet.

Sehr oft wird die Telefonnummerübermittlung auch zur Authentisierung verwendet. Ein häufig realisiertes Beispiel für diesen Mechanismus ist, dass die Benutzer ihren Anrufbeantworter abhören können, ohne ihre PIN oder sein Passwort eingeben zu müssen.

Ein Angreifer könnte durch Änderungen an der vermittelnden Telefonanlage einem Telefon jede beliebige Telefonnummer zuweisen, die dann an den Empfänger übertragen wird. Dadurch kann er versuchen, seinem Gesprächspartner eine falsche Identität vorzuspiegeln (siehe G 5.42 *Social Engineering*).

Viele Telefone beinhalten eine Inkognito-Funktion. Der Anrufer kann diese Funktion aktivieren, wenn er verhindern möchte, dass die eigene Telefonnummer auf dem Display des Angerufenen angezeigt wird. Die Telefonnummer des Anrufers muss dennoch für den Verbindungsaufbau übertragen werden. Die Telefonübermittlungsstelle, an die das Telefon des Angerufenen angeschlossen ist, entscheidet nach dieser Angabe, ob die Telefonnummer an den Angerufenen übertragen wird. Durch eine entsprechende Programmierung der Telefonübermittlungsstelle kann die Inkognito-Funktion ignoriert werden, ohne dass die Benutzer dies wissen.

In homogenen VoIP-Netzen, in denen nur über das Datennetz telefoniert wird, treten diese Probleme in dieser Form nicht auf, da keine Inkognito-Funktionalität vorgesehen ist. In der Praxis sind homogene VoIP-Netze jedoch nur sehr selten zu finden. In der Regel sind die lokalen Netze mit einem entsprechenden Gateway verbunden, der die Kommunikation mit Anwendern anderer Telefonsysteme ermöglicht. Zwischen dem Gateway und dem Empfänger des Telefongesprächs können daher die oben genannten Probleme auch auftreten.

Innerhalb des Netzes, in dem über VoIP telefoniert wird, werden die Teilnehmer anhand ihrer IP-Adressen (bzw. MAC-Adressen) zugeordnet. Eine portbasierte Zuordnung, wie an einer leitungsvermittelnden Telefonanlage, ist bei VoIP nicht vorgesehen.

Ähnlich wie bei einer E-Mail wird dem Empfänger eines VoIP-Anrufs über die Signalisierungsinformationen unabhängig von der Absender-IP-Adresse die Caller-ID des Senders übermittelt. Die Caller-ID lässt sich ähnlich leicht wie die Absenderadresse einer E-Mail fälschen. Eine solche Fälschung kann wiederum dazu führen, dass der Empfänger falsche Rückschlüsse auf die Identität des Senders zieht. Ein Angreifer könnte sich so für einen anderen Benutzer ausgeben und ein Gespräch zu einem weiteren Benutzer aufbauen.

Der Empfänger könnte auf Grundlage der gefälschten IP-Adresse falsche Rückschlüsse auf die Identität des Senders ziehen.

Beispiel:

- Durch eine Manipulation an der Telefonanlage wird von dem Telefon eines Angreifers die Telefonnummer des Geschäftsführers eines größeren Unternehmens signalisiert. Der Angreifer nutzt diese Manipulation, um einen Mitarbeiter, der den Geschäftsführer nicht persönlich kennt, nach bestimmten internen Informationen fragen. Da er den Anrufer wegen der übertragenen Telefonnummer für den Geschäftsführer hält, gibt er alle Informationen heraus.

G 5.135 SPIT und Vishing

Der Einsatz von VoIP bietet viele Möglichkeiten, unter Vorspiegelung falscher Tatsachen an Informationen zu gelangen oder unaufgeklärte Benutzer auszunutzen. Über VoIP können Anbieter beispielsweise kostengünstig unerwünschte Werbung für ihre Produkte oder Dienstleistungen platzieren. SPIT (*Spam over IP-Telephone*), ebenso wie SPAM, der in ähnlicher Form schon bei E-Mail sehr verbreitet ist, kosten die Empfänger Zeit und Geld. Je nach Häufigkeit sind SPIT-Anrufe nicht nur eine Belästigung, sondern sie stören unter Umständen die Arbeitsabläufe in einer Institution erheblich.

Der Versand von SPIT ist für einen Anbieter vergleichsweise günstig. Kann eine paketorientierte Verbindung zu einem Benutzer über das Internet hergestellt werden, so fallen für den Anbieter keine weiteren Telefonkosten an. Durch eine entsprechend dimensionierte Internetanbindung kann er zahlreiche Werbeangebote zur gleichen Zeit versenden.

SPIT kann beispielsweise eine Sprachwerbeansage sein. Dabei wird nach Annahme des Anrufs eine Aufnahme abgespielt. Auf diese Art und Weise können Produkte oder Dienstleitungen angepriesen werden. Es kann aber auch SPIT mit betrügerischer Absicht versendet werden. Ein Beispiel hierfür ist Vishing.

Vishing

Bei Vishing (Voice Phishing) handelt es sich um eine Angriffsmöglichkeit, um an persönliche Informationen eines oder mehrerer Opfer zu gelangen. Hierbei ruft ein VoIP-basierter Dialer eine große Anzahl von gesammelten VoIP-Adressen an. Bei Rufannahme wird eine Sprachmitteilung abgespielt, die dem Opfer vortäuschen soll, dass der Anruf von einer vertrauenswürdigen Institution, wie dem Kreditinstitut, bei dem er Kunde ist, stammt. Während des Telefonats werden die Opfer aufgefordert, Informationen wie Kontonummern, PINs und TANs preiszugeben.

G 5.136 Missbrauch frei zugänglicher Telefonanschlüsse

Oft werden Telefone betrieben, die keinem Benutzer persönlich zugeordnet sind. Einige dieser Telefone, wie zum Beispiele solche in Druckerräumen, sind nur einem beschränkten Personenkreis zugänglich. Aber häufig sind auch Telefone in Parkhäusern, vor Zugangskontrollsystemen oder in für Besucher zugänglichen Bereichen zu finden.

Besitzen diese Telefone ein elektronisches Telefonbuch, in dem interne Telefonnummern gespeichert sind, so besteht die Gefahr, dass solche internen Telefonnummern ungewollt nach außen gelangen.

Beim Einsatz von VoIP-Telefonen in frei zugänglichen Bereichen müssen weitere Aspekte beachtet werden. VoIP-Telefone haben einen hohen Software-Anteil und werden häufig in Datennetzen betrieben, die auch für andere IT-Anwendungen genutzt werden. Ein Angreifer könnte deshalb versuchen, durch den direkten Zugriff auf das Gerät Schwachstellen in der VoIP-Software auszunutzen oder selbst schädliche Software zu installieren. Besonders bei Softphones besteht auch die Gefahr, dass ein Angreifer versucht, beispielsweise mit Hilfe einer bootbaren CD-ROM Administratoren-Rechte auf dem Endgerät oder auf anderen IT-Systemen im gleichen Netz zu erlangen.

VoIP-Telefone müssen an ein Datennetz angeschlossen sein. Ein Angreifer könnte an diesen Netzanschluss einen tragbaren Computer anschließen und so unter Umständen auf das von außen durch eine Firewall geschützte Netz zugreifen. Diesen Zugang kann er möglicherweise für Angriffe auf die Vertraulichkeit, Integrität und Verfügbarkeit ausnutzen. Auch ein Innentäter könnte versuchen, diese Anschlüsse zu missbrauchen, ohne dass die Angriffe von seinem Arbeitsplatzrechner ausgehen und dies protokolliert wird.

G 5.137 Auswertung von Verbindungsdaten bei der drahtlosen Kommunikation

Bei der drahtlosen Kommunikation können die übertragenen Signale auf der Funkstrecke nicht physikalisch gegen unbefugtes Mithören und Aufzeichnen abgeschirmt werden. Deshalb könnte ein Angreifer seinen Angriff ohne das bei leitungsgebundener Kommunikation bekannte Zugriffsproblem durchführen. In Funknetzen mit mehreren Basisstationen zur Versorgung großflächiger Areale, wie z. B. zellulare Mobilfunknetze, ist es zudem üblich, dass der ungefähre Aufenthaltsort der mobilen Endgeräte ermittelt wird, um deren schnelle Ereichbarkeit zu gewährleisten. Sofern sie selbst eine Verbindung aufbauen, geben sie ebenfalls - im Zuge des Verbindungsaufbaus - Informationen über ihren Standort ab. Diese Standort-Informationen könnten durch den Netzbetreiber oder Dienstbetreiber - aber auch von Dritten - zur Bildung von Bewegungsprofilen verwendet werden.

Beispiele:

- Bei WLANs auf Basis von IEEE 802.11 wird die Hardware-Adresse einer WLAN-Karte, die sogenannte MAC-Adresse, bei jeder Datenübertragung mit versendet. Dadurch ist ein eindeutiger Bezug zwischen MAC-Adresse des Funk-Clients, Ort und Uhrzeit der Datenübertragung herstellbar.

  Auf diese Weise könnten Bewegungsprofile über mobile Nutzer erstellt werden, z. B. wenn diese sich in öffentliche Hotspots einbuchen. Da dies MAC-Adresse unverschlüsselt übertragen wird, ist das Erstellen von Bewegungsprofilen keinesfalls nur den Betreibern der Hotspots möglich. Prinzipiell kann jeder, der an geeigneten öffentlichen Plätzen eine Funk-LAN-Komponente installiert, die MAC-Adressen anderer Nutzer mitlesen.

- Der Funkverkehr von Bluetooth-Verbindungen kann mit Hilfe von Bluetooth-Protokollanalysatoren passiv mitempfangen und aufgezeichnet werden. Die Synchronisation auf die Frequency-Hopping-Sequenz gelingt bei Kenntnis der Geräteadressen auch dann, wenn sich die Geräte im "Non-discoverable"-Modus befinden. Alle Schichten des Bluetooth-Protokoll-Stacks können offline betrachtet bzw. analysiert werden. Das Extrahieren und Mitlesen der übertragenen Nutzdaten (Payload) ist bei fehlender Verschlüsselung möglich. Durch den Einsatz einer Antenne mit starker Richtcharakteristik und geeigneter Elektronik zur Verstärkung eines empfangenen Bluetooth-Signals kann ein solcher "Lauschangriff" auch noch in einer größeren Entfernung als der üblichen Funktionalitätsreichweite durchgeführt werden. Eine Sendeleistungsregelung ist optional und wird nicht von jedem Bluetooth-Gerät unterstützt.

  Die Verwendung des Frequenzsprungverfahren alleine stellt leider auch kein ernsthaftes Hindernis für einen ausreichend informierten Angreifer dar, auch wenn häufig zu lesen ist, dies würde eine unberechtigte Teilnahme bzw. den Empfang und das Abhören von Bluetooth-Verbindungen wesentlich erschweren. Der Grund für die Verwendung eines Frequenzsprungverfahrens liegt darin, Übertragungsfehler aufgrund von Störungen durch den Betrieb anderer Geräte (z. B. WLANs), die dasselbe Frequenzband nutzen, klein zu halten und somit eine gute Verfügbarkeit sicherstellen zu können.

- Die eindeutigen Bluetooth-Geräteadressen können zum Verfolgen einzelner Geräte missbraucht werden. Auf diese Weise ist es möglich, Bewegungsprofile der Benutzer zu erstellen. Die Geräteadresse wird nicht nur zum Verbindungsaufbau verwendet, die Geräteadresse des Masters ist zum Teil (24 der 48 Bit) in jedem Datenpaket enthalten.

G 5.138 Angriffe auf WLAN-Komponenten

Sicherheitsmängel bei der drahtlosen Kommunikation, bei einzelnen WLAN-Clients, Access Points oder dem Distribution System können dazu führen, dass Angriffe erfolgreich sind. Dabei können interne Daten mitgelesen oder verändert werden. Es können aber auch WLAN-Komponenten so manipuliert werden, dass sie wiederum als Einstiegspunkt für Angriffe auf andere Netze und Netzkomponenten genutzt werden können.

Beabsichtigte Störung des Funknetzes

Durch das Betreiben von Störquellen, so genannten Jammern, kann ein WLAN absichtlich gestört werden. Dies kann zum kompletten Ausfall eines WLAN führen und stellt damit einen Denial-of-Service-Angriff auf physikalischer Ebene dar. Die Störquelle kann sich bei ausreichender Sendeleistung auch außerhalb des Geländes, auf dem das WLAN genutzt wird, befinden.

Vortäuschen einer gültigen Authentisierung

Ein Angreifer könnte bestimmte Steuer- und Managementsignale aufzeichnen, analysieren und diese dann erneut senden. Dadurch kann dem WLAN eine gültige Authentisierung einer WLAN-Komponenten vorgetäuscht und ein unberechtigter Zugriff auf das WLAN erschlichen werden.

Vortäuschung eines gültigen Access Points

Durch das Einschleusen fremder Access Points in ein WLAN können Man-in-the-Middle-Attacken durchgeführt werden ("Cloning" oder "Evil Twin"). Hierzu kann ein weiterer Access Point in der Nähe eines Clients installiert werden. Wenn dieser dem WLAN-Client eine stärkere Sendeleistung anbietet als der echte Access Point, wird der Client diesen als Basisstation nutzen, falls keine beidseitige Authentisierung erzwungen wird. Zusätzlich könnte auch der offizielle Access Point durch einen Denial-of-Service-Angriff ausgeschaltet werden. Die Benutzer nehmen dann an einem Netz teil, das nur vorgibt, das Zielnetz zu sein. Dadurch ist es einem Angreifer möglich, die Kommunikation abzuhören.

Auch durch Poisoning- oder Spoofing-Methoden kann ein Angreifer eine falsche Identität vortäuschen bzw. den Netzverkehr zu Systemen des Angreifers umlenken. So kann er die Kommunikation belauschen und kontrollieren.

Kompromittierung des Distribution System

Neben dem Anschluss eines fremden Access Points ist eine Kompromittierung des Distribution System ebenfalls möglich, indem ein fremder Hub oder Switch zwischen Access Point und Distribution System zwischengeschaltet wird, sofern dieser Bereich zugänglich ist.

Mit einem angeschlossenen Protokoll-Analysator kann dann der gesamte Verkehr zwischen Access Point und Distribution System aufgezeichnet werden. Zusätzlich kann über entsprechende andere Werkzeuge ein aktiver Angriff auf die Infrastruktur oder einen am Access Point assoziierten Client durchgeführt werden. Das "Brechen" der WLAN-Verschlüsselung ist dabei noch nicht einmal erforderlich, da im LAN-Bereich des Distribution Systems die Datenübertragung vollständig unverschlüsselt erfolgt, sofern nicht Verschlüsselungsmechanismen auf Protokollebene, beispielsweise mittels

VPN-Techniken, oder auf Applikationsebene eingesetzt werden.

Angriffe auf WLAN-Clients

Durch die Teilnahme eines Clients an einem WLAN entstehen auf den Clients zusätzliche Bedrohungen für die lokalen Daten. Angriffe könnten einerseits auf WLAN-Mechanismen, aber auch auf Schwachstellen des verwendeten Betriebssystems erfolgen. Ein hierdurch manipulierter Client kann zu einer Kompromittierung des gesamten WLANs und schlimmstenfalls der gesamten IT-Infrastruktur der Institution führen.

Erfolgt die Datenübertragung im WLAN unverschlüsselt, kann ein Angreifer im Falle von leicht verwertbaren Daten, beispielsweise VoIP-Gesprächsdaten, auch auf einfachste Weise die Kommunikation belauschen.

Der fehlerhaft geplante Einsatz eines WLAN-Clients beispielsweise in einem nicht vertrauenswürdigen Funknetz (Hotspot oder Ad-hoc-Netz) bringt weitere Gefahren mit sich. Einige sind im Folgenden beispielhaft aufgelistet:

- Mit Hilfe von Spoofing könnte ein Angreifer kompromittierende Werkzeuge auf dem Client eines WLAN-Benutzers installieren.
- Ein Angreifer könnte die Netzdienste und -funktionalitäten des Clients auf Schwachstellen prüfen und diese unter Umständen ausnutzen. Dadurch könnte beispielsweise ein Zugriff auf den Rechner möglich sein, weil Kennwörter ungeeignet gewählt waren oder die Personal Firewall unzureichend konfiguriert.

Angriffe auf Access Points

Angriffe können aber auch über die Clients auf andere WLAN-Komponenten und damit gekoppelte Netze erfolgen. Wenn Sicherheitsmechanismen bei mobilen Komponenten und Übertragungsstandards fehlen oder schlecht konfiguriert sind, kann dies von Angreifern ausgenutzt werden, um unbefugten Zugriff auf interne Netze von Behörden oder Unternehmen zu nehmen. Jede zusätzliche Komponente, die in ein Netz eingebunden wird, schafft zusätzliche, teilweis schwer kontrollierbare Netzzugänge. Jeder Netzanschluss kann potentiell zum Abhören des Netzes missbraucht werden.

G 5.139 Abhören der WLAN-Kommunikation

Da es sich bei Funk um ein Shared Medium handelt, können die über ein WLAN übertragenen Daten problemlos aufgezeichnet werden. Aus den aufgezeichneten Daten können unter anderem nachfolgende Informationen gewonnen werden:

- WLAN-Parameter wie SSID, genutzter Funkkanal und eingesetztes Verschlüsselungsverfahren
- MAC-Adressen der Kommunikationspartner im WLAN

Weiterhin können die Broad- und Multicasts aller Stationen in der Broadcast-Domäne, also mitunter auch von Stationen im kabelbasierten LAN, auf dem WLAN beobachtet werden, sofern diese Pakete nicht am Access Point gefiltert werden. Ein Angreifer kann damit trotz funktionierender Verschlüsselung zumindest die MAC-Adressen, und damit die Hersteller, aller Stationen in der Broadcast-Domäne, sowie verwendete Multicast-Adressen ermitteln und damit Informationen über den Einsatz von Layer-2-Protokollen erhalten. Bei mangelhafter Verschlüsselung sind beispielsweise NETBIOS Browser-Nachrichten und damit Informationen über Server-Dienste im LAN direkt zugreifbar.

Bei nicht genutzter oder zu schwacher Verschlüsselung kann weiterhin auf folgende Informationen zugegriffen werden:

- IP-Adressen und genutzte Ports der Kommunikationspartner des WLANs
- Eventuell übertragene Nutzdaten, sofern diese nicht über VPN, SSL oder sonstige Verschlüsselungsmechanismen auf Applikationsebene geschützt sind.

M 1 Maßnahmenkatalog Infrastruktur

M 1.1 Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften

Verantwortlich für Initiierung: Leiter Beschaffung, Planer

Verantwortlich für Umsetzung: Bauleiter, Errichterfirma

Für nahezu alle Bereiche der Technik gibt es Normen bzw. Vorschriften, z. B. DIN, VDE, VDMA, Richtlinien des VdS. Diese Regelwerke tragen dazu bei, dass technische Einrichtungen ein ausreichendes Maß an Schutz für den Benutzer und Sicherheit für den Betrieb gewährleisten.

Bei der Planung und Errichtung von Gebäuden, bei deren Umbau, beim Einbau technischer Gebäudeausrüstungen (z. B. interne Versorgungsnetze wie Telefon- oder Datennetze) und bei Beschaffung und Betrieb von Geräten sind entsprechende Normen und Vorschriften unbedingt zu beachten.

Ergänzende Kontrollfragen:

- Werden VDE-Vorschriften bei Ausschreibungen, Bestellungen oder Beschaffungen berücksichtigt?

M 1.2 Regelungen für Zutritt zu Verteilern

Verantwortlich für Initiierung: Leiter Haustechnik

Verantwortlich für Umsetzung: Haustechnik

Die Verteiler (z. B. für Energieversorgung, Datennetze, Telefonie) sind nach Möglichkeit in Räumen für technische Infrastruktur (siehe Baustein B 2.6 *Raum für technische Infrastruktur*) unterzubringen. Die dort geforderten Maßnahmen sind zu berücksichtigen.

Der Zutritt zu den Verteilern aller Versorgungseinrichtungen (Strom, Wasser, Gas, Telefon, Gefahrenmeldung, Rohrpost etc.) im Gebäude muss **möglich** und **geordnet** sein.

Mit **möglich** ist gemeint,

- dass Verteiler nicht bei Malerarbeiten mit Farbe oder Tapeten so verklebt werden, dass sie nur noch mit Werkzeug zu öffnen oder unauffindbar sind,
- dass Verteiler nicht mit Möbeln, Geräten, Paletten etc. zugestellt werden,
- dass für verschlossene Verteiler die Schlüssel verfügbar sind und die Schlösser funktionieren.

Mit **geordnet** ist gemeint, dass festgelegt ist, wer welchen Verteiler öffnen darf. Verteiler sollten verschlossen sein und dürfen nur von den für die jeweilige Versorgungseinrichtung zuständigen Personen geöffnet werden. Die Zugriffsmöglichkeiten können durch unterschiedliche Schließungen und eine entsprechende Schlüsselverwaltung geregelt werden (siehe dazu M 2.14 *Schlüsselverwaltung*).

Sind in Verteilern des Stromversorgungsnetzes Schmelzsicherungen eingebaut, sollten entsprechende Ersatzsicherungen (im Verteiler) bereit liegen. Eine Dokumentation der Verteiler ist entsprechend M 2.19 *Neutrale Dokumentation in den Verteilern* auszuführen.

Alle im Verteiler eingebauten Einrichtungen sind exakt und verständlich zu beschriften.

Ergänzende Kontrollfragen:

- Gibt es Regelungen für den Zutritt zu Verteilern?

M 1.3 Angepasste Aufteilung der Stromkreise

Verantwortlich für Initiierung: Leiter Haustechnik

Verantwortlich für Umsetzung: Haustechnik

Die Raumbelegung und die Anschlusswerte, für die eine Elektroinstallation ausgelegt wurde, stimmen erfahrungsgemäß nach einiger Zeit nicht mehr mit den tatsächlichen Gegebenheiten überein. Es ist also unerlässlich, bei Änderungen der Raumnutzung und bei Änderungen und Ergänzungen der technischen Ausrüstung (IT, Klimatruhe, Beleuchtung etc.) die Elektroinstallation zu prüfen und ggf. anzupassen. Das kann durch Umrangierung von Leitungen geschehen. Andernfalls kann die Neuinstallation von Einspeisung, Leitungen, Verteilern etc. erforderlich werden.

Ergänzende Kontrollfragen:

- Wird überprüft, ob die Absicherung und Auslegung der Stromkreise den tatsächlichen Bedürfnissen entspricht?
- Wann erfolgte die letzte Überprüfung?

M 1.4 Blitzschutzeinrichtungen

Verantwortlich für Initiierung: Leiter Haustechnik

Verantwortlich für Umsetzung: Haustechnik

Die direkten Auswirkungen eines Blitzeinschlages auf ein Gebäude (Beschädigung der Bausubstanz, Dachstuhlbrand u.ä.) lassen sich durch die Installation einer Blitzschutzanlage gemäß DIN/VDE 0185 verhindern. Über diesen "Äußeren Blitzschutz" hinaus ist fast zwingend der "Innere Blitzschutz", der Überspannungsschutz, erforderlich. Denn der äußere Blitzschutz schützt die elektrischen Betriebsmittel im Gebäude **nicht**. Dies ist nur durch einen Überspannungsschutz möglich (siehe dazu M 1.25 *Überspannungsschutz*), dessen hohe Kosten dem Schutzgut gegenüber gerechtfertigt sein müssen.

Für einen umfassenden Blitzschutz ist es notwendig, dass sich alle Schutzeinrichtungen auf das gleiche Potential beziehen. Der äußere Blitzschutz ist entsprechend den Forderungen der DIN VDE 0185 "Blitzschutzanlagen" mit der Potentialausgleichschiene (PAS) verbunden. Diese ist ihrerseits mit dem PEN- bzw. N- und PE-Leiter der elektrischen Installation im Gebäude verbunden. Bei einem Blitzeinschlag fällt eine dem eingeprägten Strom proportionale Spannung am Erdungswiderstand der Blitzschutzanlage ab. Das Potential der PAS und somit von N- und PE-Leitern im Gebäude steigt an und kann Werte von mehreren zehntausend Volt erreichen. Es werden Spannungen zwischen N-/PE-Leitern und den Leitern L1/L2/L3 erreicht, die das betriebsübliche Maß von 230/400 V deutlich überschreiten. Es kommt zu Schäden an Geräten und Leitungen. Ausgleichsströme zwischen Daten- und Energieversorgungsnetz, beispielsweise aufgrund defekter Schirmungen, können zur Zerstörung von IT führen (siehe dazu M 1.39 *Verhinderung von Ausgleichsströmen auf Schirmungen*). Die Betrachtung aller Netze (Gebäudeleittechnik, Weitverkehrsnetze) ist wegen möglicher Parallelverlegungen im Hinblick auf Überkopplungen genauso notwendig wie die Einbeziehung in das Gebäude führender Außenleitungen (siehe dazu M 1.5 *Galvanische Trennung von Außenleitungen*).

Beispiel:

Durch Blitzschlag entstand in der süddeutschen Niederlassung eines Dienstleistungsunternehmens ein Schaden an IT-Geräten (PCs, Server, Laserdrucker) in Höhe von ca. 10.000 Euro. Aufgrund dieses Ereignisses wurde das Gebäude mit einem äußeren Blitzschutz **ohne** inneren Blitzschutz (Überspannungsschutz) ausgestattet. Ein erneuter Blitzschlag führte nun trotz äußeren Blitzschutzes zu Schäden in annähernd gleicher Höhe.

Ergänzende Kontrollfragen:

- Ist die Notwendigkeit des äußeren Blitzschutzes tatsächlich gegeben?
- Gibt es Auflagen von Behörden oder Versicherungen?
- Wird die Blitzschutzanlage regelmäßig geprüft und gewartet?
- Existiert ggf. ein ausreichender Überspannungsschutz im Gebäude?

M 1.5 Galvanische Trennung von Außenleitungen

Verantwortlich für Initiierung: Leiter Haustechnik

Verantwortlich für Umsetzung: Haustechnik

Viele hausinterne Netze stehen in direkter galvanischer Verbindung mit Außenleitungen. Telefon-, Strom- und Datennetze mit DFÜ-Anschlüssen sind davon betroffen, aber auch Gas- und Wasserleitungen.

Über diese Netzanschlüsse können Fremd- und Überspannungen in das Gebäude verschleppt werden. Es gibt eine Reihe von elektrischen, elektronischen oder softwaregestützten Maßnahmen, Netze gegen Einflüsse von außen zu schützen. Ein absolut sicherer Schutz lässt sich aber nicht in allen Fällen garantieren. Hier bleibt nur noch die konsequente galvanische Trennung der Netzübergänge ins Gebäude. Dies kann z. B. durch den Einbau eines Schalters geschehen, der die Leitung nur bei Bedarf durchschaltet (Fernwartung).

Zum Schutz nicht trennbarer Leitungen (Telefon, Daten, Strom, Gas, Wasser) gegen Überspannungen ist die Einrichtung eines Überspannungsschutzes (M 1.25 *Überspannungsschutz*) in Erwägung zu ziehen.

M 1.6 Einhaltung von Brandschutzvorschriften

Verantwortlich für Initiierung: Leiter Haustechnik, Brandschutzbeauftragter

Verantwortlich für Umsetzung: Brandschutzbeauftragter, Haustechnik

Feuerwehr hinzuziehen

Die bestehenden Brandschutzvorschriften (z. B. nach der Norm DIN 4102 Brandverhalten von Baustoffen und Bauteilen) und die Auflagen der Bauaufsicht für Gebäude sind unbedingt einzuhalten. Die örtliche Feuerwehr sollte bei der Brandschutzplanung hinzugezogen werden.

Für Räume, in denen wichtige IT-Geräte und Datenträger (Server, Datensicherungen, etc.) untergebracht sind, sollten zudem die Regelungen der Norm EN 1047 Teil 2 beachtet werden.

Bei Besprechungs-, Schulungs- und Veranstaltungsräumen sind unter Umständen die entsprechenden Regelungen für den Brandschutz in Versammlungsstätten zu beachten. Da es hier je nach Nutzungsart unterschiedliche Zusatzforderungen wie beispielsweise hinsichtlich der Öffnungsart und -breite von Türen im Verlauf von Flucht- und Rettungswegen und Beschilderungen gibt, sollte auch hier bei der Planung die örtliche Feuerwehr befragt werden.

Es sollte eine Person benannt werden, die für die Einhaltung von Brandschutzvorschriften verantwortlich ist. Dies kann ein Brandschutzbeauftragter oder eine mit dem Aufgabengebiet betraute Person sein, die auch entsprechend geschult ist.

Es ist empfehlenswert, weitere Hinweise zum Brandschutz zu beachten, wie sie zum Beispiel in den Publikationen der VdS Schadenverhütung GmbH zu finden sind.

Fluchtwege

Besonders wichtig ist es, die Fluchtwege gut auszuschildern. Dafür sind die vorgeschriebenen Kennzeichen zu verwenden und die Vorschriften zu deren Anbringung einzuhalten. Die Fluchtwege müssen immer offen gehalten werden, das heißt insbesondere, dass sie nicht versperrt werden dürfen, z. B. durch im Flur abgestelltes Inventar oder indem die Fluchttüren abgeschlossen werden.

Damit die Feuerwehr im Brandfall schnell mit der Brandbekämpfung beginnen kann, ist es wichtig, dass die Brandmeldezentrale, das Brandmeldetableau und die Einspeisepunkte für Löschwasser durch Beschilderung schnell gefunden werden können.

Zur Verwirklichung eines effizienten Brandschutzes ist die Zusammenarbeit aller zuständigen Verfahrensbeteiligten notwendig. Hierunter fallen die Funktionen

- des Brandschutz-Beauftragten (Arbeitgeber ist für die Einhaltung der Brandschutzvorschriften verantwortlich),
- der Fachkraft für Arbeitssicherheit (in Deutschland erforderlich nach §§ 5, 6 Arbeitssicherheitsgesetz, diese ist zuständig für die Ausgestaltung des betrieblichen Brandschutzes) und
- des Sicherheitsbeauftragten (in Deutschland erforderlich nach § 22 SGB VII, dieser hat ausführende Tätigkeiten, z. B. zur Verhütung von

Arbeitsunfällen und Berufskrankheiten, und arbeitet der Fachkraft für Arbeitssicherheit zu).

Ergänzende Kontrollfragen:

- Besteht ein Gedankenaustausch mit der örtlichen Feuerwehr?
- Gibt es einen Brandschutzbeauftragten oder eine mit dem Aufgabengebiet betraute Person, die auch entsprechend geschult ist?

M 1.7 Handfeuerlöscher

Verantwortlich für Initiierung: Leiter Haustechnik, Brandschutzbeauftragter

Verantwortlich für Umsetzung: Brandschutzbeauftragter, Haustechnik

Brände möglichst im Keim ersticken

Die meisten Brände entstehen aus kleinen, anfangs noch gut beherrschbaren Brandherden. Besonders in Büros findet das Feuer reichlich Nahrung und kann sich sehr schnell ausbreiten. Der Sofortbekämpfung von Bränden kommt also ein sehr hoher Stellenwert zu.

Diese Sofortbekämpfung ist nur möglich, wenn Handfeuerlöscher in der jeweils geeigneten Brandklasse (DIN EN 3) in ausreichender Zahl und Größe (Beratung durch die örtliche Feuerwehr) im Gebäude zur Verfügung stehen. Dabei ist die räumliche Nähe zu schützenswerten Bereichen und Räumen wie Serverraum, Raum mit technischer Infrastruktur oder Belegarchiv anzustreben.

Wasserlöscher mit Eignung für Brandklasse A bis 1000 V sind durchaus für elektrisch betriebene Geräte geeignet.

Für elektronisch gesteuerte Geräte, z. B. Rechner, sollten vorzugsweise Kohlendioxyd-Löscher (Brandklasse B) zur Verfügung stehen. Die Löschwirkung wird durch Verdrängung des Sauerstoffs erreicht, deshalb ist bei Anwendung in engen, schlecht belüfteten Räumen Vorsicht geboten.

Keine Pulverlöscher im IT-Bereich

Pulverlöscher, die die Brandklassen A (feste Stoffe), B (brennbare Flüssigkeiten) und C (Gase) abdecken, sollten in Bereichen mit elektrischen und elektronischen Geräten nicht eingesetzt werden, weil die Löschschäden in der Regel unverhältnismäßig hoch sind. Es wird daher dringend empfohlen, im direkten Umfeld von Serverräumen, Datenträgerarchiven, Räumen für technische Infrastruktur und Rechenzentren keine Pulverlöscher, sondern ausschließlich geeignete Gaslöscher bereit zu halten. Nur so kann verhindert werden, dass in der Ausregung eines Brandes fälschlicher Weise ein Pulverlöscher verwendet wird.

Mitarbeiter müssen mit Feuerlöschern umgehen können

Die Feuerlöscher müssen regelmäßig geprüft und gewartet werden. Die Feuerlöscher müssen so angebracht werden, dass sie im Brandfall leicht erreichbar sind. Die Beschäftigten sollten sich die Standorte des nächsten Feuerlöschers einprägen. Die Standorte von Löschern und Hydranten sind durch vorgeschriebene Schilder kenntlich zu machen. Tragbare Feuerlöscher sind zugelassen bis zu einem Gesamtgewicht von 20 kg. Mit den überwiegend eingesetzten Geräten von 6 und 12 kg lassen sich größere Brandherde löschen als von Laien üblicherweise angenommen wird, dies ist allerdings nur bei konsequenter Vorgehensweise gegeben. Bis zur vollständigen Entladung des Löschmittels vergehen nur wenige Sekunden. Daher sind bei entsprechenden Brandschutzübungen die Mitarbeiter in die Benutzung der Handfeuerlöscher einzuweisen.

Ergänzende Kontrollfragen:

- Sind die Mitarbeiter über den Aufbewahrungsort der Handfeuerlöscher informiert?
- Wird die Nutzung der Handfeuerlöscher geübt?
- Sind die Handfeuerlöscher im Brandfall überhaupt erreichbar?

- Werden die Handfeuerlöscher regelmäßig inspiziert und gewartet?

M 1.8 Raumbelegung unter Berücksichtigung von Brandlasten

Verantwortlich für Initiierung: Leiter Haustechnik, Brandschutzbeauftragter

Verantwortlich für Umsetzung: Haustechnik, Brandschutzbeauftragter

Eine Brandlast entsteht durch alle brennbaren Stoffe, die ins Gebäude eingebracht werden. Sie ist von der Menge und vom Heizwert der Stoffe abhängig. IT-Geräte und Leitungen stellen ebenso eine Brandlast dar wie Möbel, Fußbodenbeläge und Gardinen. Maximale Brandlasten, standardisierte Heizwerte, weitere Informationen und Bestimmungen sind in der DIN 4102 zusammengestellt.

Bei der Unterbringung von IT-Geräten, Datenträgern etc. sollte eine vorherige Beachtung der vorhandenen Brandlasten im gleichen Raum und in den benachbarten Räumen erfolgen. Z. B. sollte das Datenträgerarchiv nicht in der Nähe von oder über einem Papierlager untergebracht sein.

M 1.9 Brandabschottung von Trassen

Verantwortlich für Initiierung: Leiter Haustechnik, Brandschutzbeauftragter

Verantwortlich für Umsetzung: Haustechnik, Brandschutzbeauftragter

Durchbrüche abschotten

Bei Gebäuden mit mehreren Brandabschnitten lässt es sich kaum vermeiden, dass Trassen durch Brandwände und Decken führen. Die Durchbrüche sind nach Verlegung der Leitungen entsprechend dem Brandwiderstandswert der Wand bzw. Decke zu schotten. Um die Nachinstallation zu erleichtern, können geeignete Materialien (z. B. Brandschutzkissen) verwendet werden. Entsprechende VdS-Richtlinien sind zu beachten.

Trassennutzung koordinieren

Häufig werden in einer Trasse unterschiedliche Kabel, z. B. Telefon, LAN und Haustechnik geführt. Falls Änderungen der Verkabelung anstehen, sollte bereits in der Planungsphase geklärt werden, ob in absehbarer Zeit auch andere Kabelsysteme ausgewechselt werden sollen. Entsprechende Zusammenlegung von Projekten minimiert Ausfallzeiten und erspart zusätzliche Kosten für eine mehrmalige Brandschottung.

Negativbeispiel:

In einem mehrgeschossigen Bürogebäude in Bonn wurden verschiedene Netze über eine gemeinsame Steigetrasse aus dem Keller bis in das oberste Geschoss geführt. Alle Deckendurchbrüche waren mit reichlich Reserve hergestellt, nach Verlegung der Leitungen allerdings nicht wieder verschlossen worden. Im Keller wurden im Bereich des Trassenbeginns große Papier- und Stoffmengen gelagert. Die direkt darüber beginnende Steigetrasse hätte im Brandfall wie ein Kamin gewirkt. Rauch und Feuer hätten sich in kürzester Zeit über alle Etagen ausgebreitet.

Ergänzende Kontrollfragen:

- Wurde bei der Trassenplanung der für den Brandschutz Zuständige hinzugezogen?
- Wurden mögliche Alternativen der Trassenführung geprüft?
- Werden im Anschluss an Installationsarbeiten und regelmäßige Kontrollen der Brandabschottungen durchgeführt?

M 1.10 Verwendung von Sicherheitstüren und -fenstern

Verantwortlich für Initiierung: Leiter Haustechnik

Verantwortlich für Umsetzung: Haustechnik

Sicherheitstüren und -fenster bieten gegenüber normalen Bürotüren und Fenstern Vorteile:

- In der Norm DIN EN 1627 "Fenster, Türen, Abschlüsse - Einbruchhemmung - Anforderungen, Klassifizierung" sind die Bauelemente in Widerstandsklassen (WK) eingeordnet worden. Türen gemäß der Klassifizierungen WK1 bis WK4 bieten aufgrund ihrer Stabilität einen höheren Schutz gegen Einbruch (z. B. bei Keller- und Lieferanteneingängen). **Schutz vor Einbruch**
- Als selbstschließende feuerhemmende und gegebenenfalls rauchdichte Tür (z. B. FH-Tür T30, nach DIN 18082 "Feuerschutzabschlüsse") verzögern sie die Ausbreitung eines Brandes. **Schutz bei Bränden**
- Sie schützen in der Ausführung als selbstschließende Rauchschutztür (DIN 18095-1 "Türen; Rauchschutztüren; Begriffe und Anforderungen") die Ausbreitung von Brandrauch. Brandrauch ist so feinkörnig, dass er problemlos durch Druckausgleichs- und Lüftungsöffnungen von Festplatten hindurchkommt. Für die geringen Flughöhen von Festplattenleseköpfen ist er aber immer noch viel zu groß und verursacht dort enorme Schäden. **Rauchschutz**

Es ist zu gewährleisten, dass die Sicherungsmaßnahmen aller raumumschließenden Bauelemente gleichwertig sind:

- Bei Verwendung einbruchhemmender Türen ist im Fassadenbereich die Verwendung einbruchhemmender Fenster oder Fassadenelemente (DIN V ENV 1627 - 1630) zu erwägen.
- Weiterhin ist es z. B. nicht zweckmäßig, eine einbruchhemmende Tür der höchsten Widerstandsklasse in eine Gipskartonwand einzubauen.
- Beim Einbau einer feuerhemmenden oder rauchdichten Tür ist natürlich darauf zu achten, dass auch die umgebende Wand gleichwertig feuerhemmend und rauchdicht ist und nicht durch offenen Oberlichter oder Kabeldurchführungen ein Bypass besteht.

Anforderungen zur Ausführung von Sicherheitstüren finden sich in den Maßnahmen M 1.47 *Eigener Brandabschnitt* und M 1.19 *Einbruchsschutz*.

Der Einsatz von Sicherheitstüren ist hinsichtlich der Brandschutzes über den von der Bauaufsicht und der Feuerwehr vorgeschriebenen Bereich hinaus (siehe M 1.6 *Einhaltung von Brandschutzvorschriften*) besonders bei schutzbedürftigen Räumen wie Serverraum, Beleg- oder Datenträgerarchiv sinnvoll. Bei hochschutzbedürftigen Räumen ist ein ausgewogenes Schutzkonzept zu erstellen, welches Gefahrenmeldung und Alarmierung und den Einbau von Sicherheitstüren berücksichtigt. Denn hat ein potentieller Angreifer ein ganzes Wochenende Zeit für einen Einbruchsversuch, wird ihn auch eine hochwertige einbruchhemmende Tür nicht von seinem Ziel abhalten, Daten oder Einrichtung zu entwenden oder zu zerstören.

Hinweis: Ziel eines Einbruches könnte es auch sein, Daten oder IT-Systeme zu manipulieren. Daher sollten zentrale IT-Systeme nach Einbrüchen auf ihre Integrität überprüft werden (siehe dazu auch M 6.60 *Verhaltensregeln und Meldewege bei Sicherheitsvorfällen*).

Es ist dafür zu sorgen, dass Brand- und Rauchschutztüren auch tatsächlich geschlossen und nicht (unzulässigerweise) z. B. durch Keile offen gehalten werden. Alternativ können Türen mit einem automatischen Schließmechanismus, der im Alarmfall aktiviert wird, eingesetzt werden.

Ergänzende Kontrollfragen:

- Wurde untersucht, wo Sicherheitstüren und -fenster sinnvollerweise eingebaut werden sollten?
- Wird regelmäßig überprüft, dass die Sicherheitstüren und -fenster funktionstüchtig sind?

M 1.11 Lagepläne der Versorgungsleitungen

Verantwortlich für Initiierung: Leiter Haustechnik

Verantwortlich für Umsetzung: Haustechnik

Es sind genaue Lagepläne aller Versorgungsleitungen (Strom, Wasser, Gas, Telefon, Gefahrenmeldung, Rohrpost etc.) im Gebäude und auf dem dazugehörenden Grundstück zu führen und a l l e die Leitungen betreffenden Sachverhalte aufzunehmen:

- genaue Führung der Leitungen (Einzeichnung in bemaßte Grundriss- und Lagepläne),
- genaue technische Daten (Typ und Abmessung),
- evtl. vorhandene Kennzeichnung,
- Nutzung der Leitungen, Nennung der daran angeschlossenen Netzteilnehmer,
- Gefahrenpunkte und
- vorhandene und zu prüfende Schutzmaßnahmen.

Es muss möglich sein, sich anhand der Pläne einfach und schnell ein genaues Bild der Situation zu machen. Nur so kann das Risiko, dass Leitungen bei Arbeiten versehentlich beschädigt werden, auf ein Mindestmaß reduziert werden. Eine Schadstelle ist schneller zu lokalisieren, die Störung schneller zu beheben.

Es ist sicherzustellen, dass alle Arbeiten an Leitungen rechtzeitig und vollständig dokumentiert werden. Die Pläne sind gesichert aufzubewahren und der Zugriff ist zu regeln, da sie schützenswerte Informationen beinhalten.

Ergänzende Kontrollfragen:

- Wer ist für die Pläne zuständig?
- Werden die Pläne aktualisiert?
- Werden die Pläne sicher aufbewahrt und sind sie nur von Befugten einsehbar?
- Welche Pläne existieren bereits?

M 1.12 Vermeidung von Lagehinweisen auf schützenswerte Gebäudeteile

Verantwortlich für Initiierung: Leiter Haustechnik

Verantwortlich für Umsetzung: Haustechnik

Schützenswerte Gebäudeteile sind z. B. Serverraum, Rechenzentrum, Datenträgerarchiv, Klimazentrale, Verteilungen der Stromversorgung, Schalt- und Rangierräume, Ersatzteillager.

Solche Bereiche sollten keinen Hinweis auf ihre Nutzung tragen. Türschilder wie z. B. RECHENZENTRUM oder EDV-ARCHIV geben einem potentiellen Angreifer, der zum Gebäude Zutritt hat, Hinweise, um seine Aktivitäten gezielter und damit Erfolg versprechender vorbereiten zu können.

Ist es unvermeidbar, IT in Räumen oder Gebäudebereichen unterzubringen, die für Fremde leicht von außen einsehbar sind (siehe auch M 1.13 *Anordnung schützenswerter Gebäudeteile*), so sind geeignete Maßnahmen zu treffen, um den Einblick zu verhindern oder so zu gestalten, dass die Nutzung nicht offenbar wird. Dabei ist darauf zu achten, dass z. B. nicht nur ein Fenster einer ganzen Etage mit einem Sichtschutz versehen wird.

Ergänzende Kontrollfragen:

- Welche Lagehinweise können von außerhalb erkannt werden?
- Welche Lagehinweise gibt es innerhalb eines Gebäudes?

M 1.13 Anordnung schützenswerter Gebäudeteile

Verantwortlich für Initiierung: Planer, Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Bauleiter, Leiter Haustechnik

Schützenswerte Räume oder Gebäudeteile sollten nicht in exponierten oder besonders gefährdeten Bereichen untergebracht sein:

- Kellerräume sind durch Wasser gefährdet.
- Räume im Erdgeschoss - zu öffentlichen Verkehrsflächen hin - sind durch Anschlag, Vandalismus und höhere Gewalt (Verkehrsunfälle in Gebäudenähe) gefährdet.
- Räume im Erdgeschoss mit schlecht einsehbaren Höfen sind durch Einbruch und Sabotage gefährdet.
- Räume unterhalb von Flachdächern sind durch eindringendes Regenwasser gefährdet.

Als Faustregel kann man sagen, dass schutzbedürftige Räume oder Bereiche im Zentrum eines Gebäudes besser untergebracht sind als in dessen Außenbereichen.

Optimal ist es, diese Aspekte schon in die Bauplanung für ein neues Gebäude oder in die Raumbelegungsplanung bei Einzug in ein bestehendes einzubeziehen. Bei bereits genutzten Gebäuden wird eine entsprechende Nutzungsanordnung oft mit internen Umzügen verbunden sein. Ersatzweise sollten die sich aus ohnehin erforderlichen Änderungen der Raumbelegung ergebenden Gelegenheiten konsequent genutzt werden.

Ergänzende Kontrollfragen:

- Welche schützenswerten Räume befinden sich in exponierter Lage?

M 1.14 Selbsttätige Entwässerung

Verantwortlich für Initiierung: Planer, Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Bauleiter, Leiter Haustechnik

Alle Bereiche, in denen sich Wasser sammeln und stauen kann oder in denen fließendes oder stehendes Wasser nicht oder erst spät entdeckt wird und in denen das Wasser Schäden verursachen kann, sollten mit einer selbsttätigen Entwässerung und ggf. mit Wassermeldern ausgestattet sein. Zu diesen Bereichen gehören u. a.:

- Keller,
- Lufträume unter Doppelböden,
- Lichtschächte,
- Heizungsanlage.

Erfolgt die Entwässerung passiv, also durch Bodengullys direkt in das Abwassersystem des Gebäudes, sind Rückstauklappen unerlässlich. Ohne solche Klappen wird diese Entwässerung zur Wassereintrittsöffnung, wenn das Abwassersystem überlastet wird. Nach extremen Niederschlägen dringt in der Mehrzahl aller Fälle Wasser über diesen Weg in Keller ein. Die Rückstauklappen müssen regelmäßig auf ihre Funktionstüchtigkeit hin untersucht werden.

Ist eine passive Entwässerung nicht möglich, weil das Niveau des Abwassersystems zu hoch ist, können Pumpen eingesetzt werden, die über Schwimmerschalter oder Wassersensoren automatisch eingeschaltet werden. Beim Einsatz dieser Technik sind insbesondere folgende Punkte zu beachten:

- Die Pumpenleistung muss ausreichend bemessen sein.
- Die Druckleitung der Pumpe ist mit einem Rückstauventil auszustatten.
- Es sind Vorkehrungen zu treffen, damit die Pumpe nicht durch mitgeschwämmte Gegenstände blockiert werden kann (Ansaugfilter etc.).
- Das Anlaufen der Pumpe sollte automatisch (z. B. beim Hausmeister oder der Haustechnik) angezeigt werden.
- Die Funktion von Pumpe und Schalter ist regelmäßig zu testen.
- Die Druckleitung der Pumpe darf nicht an eine in unmittelbarer Nähe vorbeigeführte Abwasserleitung angeschlossen werden. Bei einem Leck dieser Leitung würde die Pumpe das Wasser nur "im Kreis pumpen".

Ergänzende Kontrollfragen:

- Sind die wasserbedrohten Räume mit einer selbsttätigen Entwässerung ausgestattet?

M 1.15 Geschlossene Fenster und Türen

Verantwortlich für Initiierung: Leiter Haustechnik

Verantwortlich für Umsetzung: Haustechnik, Mitarbeiter

Fenster und nach außen gehende Türen (Balkone, Terrassen) sind in Zeiten, in denen ein Raum nicht besetzt sind, zu schließen. Im Keller- und Erdgeschoss und, je nach Fassadengestaltung, auch in den höheren Etagen bieten sie einem Einbrecher auch während der Betriebszeiten eine ideale Einstiegsmöglichkeit.

Während normaler Arbeitszeiten und sichergestellter kurzer Abwesenheit des Mitarbeiters kann von einer zwingenden Regelung für Büroräume sowie für Besprechungs-, Veranstaltungs- und Schulungsräumen abgesehen werden.

Wohin mit Laptops und Dokumenten?

In Besprechungs-, Veranstaltungs- und Schulungsräumen gibt es meistens keine Möglichkeit, Unterlagen, IT-Systeme und ähnliches gesondert einzuschließen. Daher sollte es möglich sein, solche Räume zumindest dann, wenn alle Teilnehmer einer Veranstaltung den Raum verlassen, abzuschließen oder ihn durch einen internen Mitarbeiter beaufsichtigen zu lassen.

Ergänzende Kontrollfragen:

- Gibt es eine Anweisung, die das Verschließen der Fenster und Außentüren fordert?
- Wird regelmäßig überprüft, ob die Fenster und Türen nach Verlassen der Räume verschlossen sind?

M 1.16 Geeignete Standortauswahl

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Planer

Bei der Planung des Standortes, an dem ein Gebäude angemietet werden oder entstehen soll, empfiehlt es sich, neben den üblichen Aspekten wie Raumbedarf und Kosten, auch Umfeldgegebenheiten die Einfluss auf die IT-Sicherheit haben zu berücksichtigen:

- In Zusammenhang mit Schwächen in der Bausubstanz kann es durch Erschütterungen naher Verkehrswege (Straße, Eisenbahn, U-Bahn) zu Beeinträchtigungen der IT kommen.
- Gebäude, die direkt an Hauptverkehrstrassen (Bundesbahn, Autobahn, Bundesstraße) liegen, können durch Unfälle beschädigt werden.
- Die Nähe zu optimalen Verkehrs- und somit Fluchtwegen kann die Durchführung eines Anschlages erleichtern.
- In der Nähe von Sendeeinrichtungen kann es zu Störungen der IT kommen.
- In der Nähe von Gewässern und in Niederungen ist mit Hochwasser zu rechnen.
- In der Nähe von Kraftwerken oder Fabriken kann durch Unfälle oder Betriebsstörungen (Explosion, Austritt schädlicher Stoffe) die Verfügbarkeit des Gebäudes (z. B. durch Evakuierung oder großräumige Absperrung) beeinträchtigt werden.

Ergänzende Kontrollfragen:

- Gibt es standortbedingte Gefährdungen?
- Wie wird diesen Gefährdungen begegnet?

M 1.17 Pförtnerdienst

Verantwortlich für Initiierung: Leiter Innerer Dienst

Verantwortlich für Umsetzung: Innerer Dienst

Die Einrichtung eines Pförtnerdienstes hat weitreichende positive Auswirkungen gegen eine ganze Reihe von Gefährdungen. Voraussetzung ist allerdings, dass bei der Durchführung des Pförtnerdienstes einige Grundprinzipien beachtet werden.

- Der Pförtner beobachtet bzw. kontrolliert alle Personenbewegungen an der Pforte.
- Unbekannte Personen ("selbst der neue Chef") haben sich beim Pförtner zu legitimieren.
- Der Pförtner hält vor Einlassgewährung eines Besuchers bei dem Besuchten Rückfrage.
- Der Besucher wird zu dem Besuchten begleitet oder an der Pforte abgeholt.
- Dem Pförtner müssen die Mitarbeiter bekannt sein. Scheidet ein Mitarbeiter aus, ist auch der Pförtner zu unterrichten, ab wann diesem Mitarbeiter der Einlass zu verwehren ist.
- In einem Besucherbuch kann der Zutritt von Fremdpersonen zum Gebäude dokumentiert werden. Die Ausgabe von Besucherausweisen oder Besucherbegleitscheinen ist zu erwägen.

Die Arbeitsbedingungen des Pförtners sind für die Aufgabenwahrnehmung geeignet auszugestalten. Die Aufgabenbeschreibung muss verbindlich festschreiben, welche Aufgaben dem Pförtner im Zusammenspiel mit weiteren Schutzmaßnahmen zukommt (z. B. Gebäudesicherung nach Dienst- oder Geschäftsschluss, Scharfschaltung der Alarmanlage, Kontrolle der Außentüren und Fenster).

M 1.18 Gefahrenmeldeanlage

Verantwortlich für Initiierung: Leiter Haustechnik, Brandschutzbeauftragter, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Haustechnik

Eine Gefahrenmeldeanlage (GMA) besteht aus einer Vielzahl lokaler Melder, die mit einer Zentrale kommunizieren, über die auch der Alarm ausgelöst wird. Ist eine Gefahrenmeldeanlage für Einbruch, Brand, Wasser oder auch Gas vorhanden und lässt sich diese mit vertretbarem Aufwand entsprechend erweitern, sollten zumindest die Kernbereiche der IT (Serverräume, Datenträgerarchive, Räume für technische Infrastruktur u. ä.) in die Überwachung durch diese Anlage mit eingebunden werden. So lassen sich Gefährdungen wie Feuer, Einbruch, Diebstahl frühzeitig erkennen und Gegenmaßnahmen einleiten. Um dies zu gewährleisten, ist die Weiterleitung der Meldungen an eine ständig besetzte Stelle (Pförtner, Wach- und Sicherheitsdienst, Feuerwehr, etc.) unumgänglich. Dabei muss sichergestellt sein, dass diese Stelle auch in der Lage ist, technisch und personell auf den Alarm zu reagieren. Hierbei sind die Aufschaltrichtlinien der jeweiligen Institutionen zu beachten.

Planung und Installation

Eine Gefahrenmeldeanlage ist ein komplexes Gesamtsystem, das dem Gebäude und dem Risiko entsprechend geplant und installiert werden muss. Planung, Installation und Wartung einer Gefahrenmeldeanlage sollte daher durch Experten durchgeführt werden. Falls diese nicht im eigenen Haus vorhanden sind, sollte auf externe Unterstützung zurückgegriffen werden. So gibt es beispielsweise eine Vielzahl unterschiedlicher Meldesysteme, die entsprechend der Sicherheitsanforderungen und der Umgebung ausgewählt werden müssen. Zur Einbruchserkennung können z. B. Bewegungsmelder, Glasbruchsensoren, Öffnungskontakte, Videokameras u. a. eingesetzt werden.

Vernetzung der Melder

Die Melder können untereinander auf verschiedene Arten vernetzt werden. In Abhängigkeit von Art und Größe der zu schützenden Bereiche und der geltenden Richtlinien müssen passende Systeme ausgewählt und installiert werden. Bei der Planung oder Erweiterung einer GMA sollte darauf geachtet werden, dass die Trassen für die Vernetzung ausreichend dimensioniert sein müssen und möglichst wenig Änderungen an der Trassenbelegung vorgenommen werden sollten.

Wartung und Funktionsprüfung

Um die Schutzwirkung der GMA aufrechtzuerhalten, ist eine regelmäßige Wartung und Funktionsprüfung (DIN VDE 0833 Teil 1-3) vorzusehen.

Ist keine GMA vorhanden oder lässt sich die vorhandene nicht nutzen, kommen als Minimallösung lokale Gefahrenmelder in Betracht. Diese arbeiten völlig selbständig, ohne Anschluss an eine Zentrale. Die Alarmierung erfolgt vor Ort oder mittels einer einfachen Zweidrahtleitung (evtl. Telefonleitung) an anderer Stelle.

Früherkennung

Für den Betrieb eines Rechenzentrums muss eine GMA zur Brand- und Einbruchdetektion installiert sein. Weitere Detektionsbereiche können nach Lage des Standorts und dessen Infrastruktur sinnvoll sein.

Es gibt Räume wie Serverraum, Datenträgerarchiv, die einen erhöhten Schutzbedarf haben. Wenn keine zentrale GMA vorhanden ist, sind dort lokale Gefahrenmelder zu installieren. Bei der Verwendung lokaler Gefahrenmelder für die Früherkennung muss dafür gesorgt werden, dass ein Alarm auch außerhalb der betroffenen Räume wahrgenommen wird. Die Meldung kann über verschiedene Wege erfolgen und sollte an eine Stelle weitergeleitet werden, die rund um die Uhr besetzt ist. Beispielsweise gibt es Lösungen, die über die TK-Anlage oder Funk Mitarbeiter über ein Mobiltelefon alarmieren können.

Vor der Planung einer GMA muss ein konsistentes Schutzkonzept für das betrachtete Gebäude erarbeitet werden. Detaillierte Informationen hierzu finden sich in der BSI-Publikation "IT-Sicherheit durch infrastrukturelle Maßnahmen" (siehe Anhang). Bei der Planung von Gefahrenmeldeanlagen für private bzw. gewerbliche Objekte sollte mit dem Sachversicherer geklärt werden, ob eine Minderung der Versicherungsprämie, insbesondere für die Einbruch-Diebstahlversicherung in Frage kommt.

Ergänzende Kontrollfragen:

- Gibt es ein Konzept für die Gefahrenerkennung, Weiterleitung und Alarmierung und wird dieses an Veränderungen bei der Nutzung angepasst?
- Wird die Gefahrenmeldeanlage regelmäßig gewartet bzw. geprüft?
- Wurden alle Mitarbeiter über die im Alarmfall einzuleitenden Schritte unterrichtet?

M 1.19 Einbruchsschutz

Verantwortlich für Initiierung: Leiter Haustechnik, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Haustechnik

Erfolgsaussichten minimieren

Erfahrungsgemäß wählen Einbrecher ihre Ziele danach aus, wie hoch das Risiko und der Aufwand im Verhältnis zum erwarteten Gewinn sind. Daher sollten alle Maßnahmen zum Einbruchsschutz darauf zielen, die Erfolgsaussichten von Tätern zu minimieren. Die gängigen Maßnahmen zum Einbruchsschutz sollten den örtlichen Gegebenheiten entsprechend angepasst werden. Dazu gehören:

- Rollladensicherungen bei einstiegsgefährdeten Türen oder Fenster,
- besondere Schließzylinder, Zusatzschlösser und Riegel,
- Sicherung von Kellerlichtschächten,
- Verschluss von nichtbenutzten Nebeneingängen,
- einbruchgesicherte Notausgänge (soweit seitens der örtlichen Bauaufsicht zugelassen),
- einbruchhemmende Türen, beispielsweise in der Qualität ET1 oder höherwertig, wenn die Gefährdungslage es erforderlich macht,
- Verschluss von Personen- und Lastenaufzügen außerhalb der Dienstzeit.

Empfehlungen hierzu geben die örtlichen Beratungsstellen der Kriminalpolizei.

Brand- und Einbruchschutz abstimmen

Bei der Planung materieller Sicherungsmaßnahmen ist darauf zu achten, dass Bestimmungen des Brand- und Personenschutzes, z. B. die Nutzbarkeit von Fluchtwegen, nicht verletzt werden. Dies gilt insbesondere für Änderungen an Brandschutzelementen, die einer Typenfreigabe unterliegen.

Den Mitarbeitern ist durch Regelungen bekanntzugeben, welche Maßnahmen zum Einbruchsschutz beachtet werden müssen.

Auch innerhalb eines Gebäudes kann der Einbau von einbruchhemmenden Elementen sinnvoll sein, wie z. B. besonderen zutrittskontrollierten Bereichen wie Serverräumen oder den Kerneinheiten eines Rechenzentrums.

Ergänzende Kontrollfragen:

- Wird geprüft, ob die Maßnahmen zum Einbruchschutz befolgt werden?
- Sind die Regelungen zum Einbruchsschutz den Mitarbeitern bekannt?

M 1.20 Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht

Verantwortlich für Initiierung: Planer, Leiter Haustechnik, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Haustechnik

Bei der Auswahl von Kabeln ist neben der Berücksichtigung von übertragungstechnischen Notwendigkeiten das Umfeld, in dem die Kabel verlegt werden sollen, zu beachten. Für die meisten Verlegebedingungen gibt es Kabel mit entsprechenden Qualitäten. Die wichtigsten sind hier zusammengestellt:

- Innen- bzw. Außenkabel,
- längswassergeschütztes Kabel für Feucht- oder Nassbereiche,
- zugentlastete Kabel für Freileitungen und extreme Steigungen,
- funktionserhaltende Kabel in feuergefährdeten Bereichen,
- geschirmte Kabel für Bereiche mit starken elektrischen und induktiven Störfeldern,
- gepanzerte Kabel für Fälle, in denen ein ausreichender mechanischer Schutz auf andere Weise nicht realisierbar ist, z. B. bei der provisorischen Verlegung auf Boden und Wänden.

Ergänzende Kontrollfragen:

- Wurde bei der Kabelauswahl der für die Betriebstechnik Zuständige über bekannte oder zu erwartende widrige Umfeldbedingungen befragt?
- Wurden möglich Alternativen der Kabelführung geprüft?

M 1.21 Ausreichende Trassendimensionierung

Verantwortlich für Initiierung: Planer, Leiter IT, Leiter Haustechnik

Verantwortlich für Umsetzung: Haustechnik

Kabeltrassen (z. B. Fußbodenkanäle, Fensterbank-Kanäle, Pritschen, Rohrtrassen im Außenbereich) sind ausreichend zu dimensionieren, d. h., dass einerseits genügend Platz vorhanden ist, um evtl. notwendige Erweiterungen des Netzes vornehmen zu können. Andererseits sind zur Verhinderung des Übersprechens (gegenseitige Beeinflussung von Kabeln) ggf. Mindestabstände zwischen Kabeln einzuhalten.

Ist es aus unterschiedlichen Gründen nicht möglich, Trassen sofort mit ausreichenden Reserven zu errichten, sollte zumindest darauf geachtet werden, dass im Bereich der Trassenführung Platz ist, um Erweiterungen unterzubringen. Bei der Auslegung von Wand- und Deckendurchbrüchen erspart dies spätere lärm-, schmutz- und kostenintensive Arbeiten.

Diese Maßnahme kann ersetzt werden durch die Auswahl anderer Kabeltypen (M 2.20 *Kontrolle bestehender Verbindungen* und M 5.3 *Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht*). Durch Verwendung weniger hochadriger Kabel kann gegenüber vielen kleinen Kabeln Platz eingespart werden. Durch den Einsatz von geschirmten Kabeln oder Lichtwellenleitern kann Übersprechen verhindert werden.

Ergänzende Kontrollfragen:

- Wurde die Möglichkeit geprüft, durch die Auswahl anderer Kabel Platz zu sparen und Übersprechen zu verhindern?

M 1.22 Materielle Sicherung von Leitungen und Verteilern

Verantwortlich für Initiierung: Planer, Leiter Haustechnik, Leiter IT

Verantwortlich für Umsetzung: Haustechnik

In Räumen mit Publikumsverkehr oder in unübersichtlichen Bereichen eines Gebäudes kann es sinnvoll sein, Leitungen und Verteiler zu sichern. Dies kann auf verschiedene Weise erreicht werden:

- Verlegung der Leitungen unter Putz,
- Verlegung der Leitungen in Stahlpanzerrohr,
- Verlegung der Leitungen in mechanisch festen und abschließbaren Kanälen,
- Verschluss von Verteilern und
- bei Bedarf zusätzlich elektrische Überwachung von Verteilern und Kanälen.

Bei Verschluss sind Regelungen zu treffen, die die Zutrittsrechte, die Verteilung der Schlüssel und die Zugriffsmodalitäten (was muss der Berechtigte ggf. vor dem Zugriff auf Leitungen tun?) festlegen.

Ergänzende Kontrollfragen:

- Wurde die Zahl der Stellen, an denen das Kabel zugänglich ist, auf ein Mindestmaß reduziert?
- Wurde die Länge zu schützender Verbindungen möglichst klein gehalten?
- Werden Zutrittsrechte restriktiv vergeben? Werden Personalwechsel und Vertretungsfälle dabei berücksichtigt?
- Werden Zutrittsrechte regelmäßig auf ihre Berechtigung/Notwendigkeit hin überprüft?

M 1.23 Abgeschlossene Türen

Verantwortlich für Initiierung: Leiter Haustechnik, Leiter IT

Verantwortlich für Umsetzung: Haustechnik, Mitarbeiter

Die Türen nicht besetzter Räume sollten abgeschlossen werden. Dadurch wird verhindert, dass Unbefugte Zugriff auf darin befindliche Unterlagen und IT-Einrichtungen erlangen. Das Abschließen einzelner Büros ist insbesondere dann wichtig, wenn sich diese in Bereichen mit Publikumsverkehr befinden oder der Zutritt nicht durch andere Maßnahmen kontrolliert wird.

Auf das Verschließen der Türen kann verzichtet werden, wenn diese flurseitig über einen Blindknauf verfügen. Voraussetzung hierfür ist allerdings, dass die befugten Mitarbeiter ihren Schlüssel stets mit sich führen.

Aufräumen statt Abschließen

In manchen Fällen, z. B. in Großraumbüros, können Büros nicht abgeschlossen werden. Dann sollte alternativ jeder Mitarbeiter vor seiner Abwesenheit seine Unterlagen ("Clear-Desk-Politik") und den persönlichen Arbeitsbereich verschließen: Schreibtisch, Schrank und PC (Schloss für Diskettenlaufwerk, Tastaturschloss), Telefon.

Auf das Verschließen der Türen kann verzichtet werden, wenn keine schutzbedürftigen Gegenstände wie Unterlagen oder Datenträger offen ausliegen und keine unbefugten Zugriffe auf die IT-Systeme im Raum (und die damit vernetzten IT-Systeme) möglich sind.

Bei laufendem Rechner kann auf das Abschließen der Türen verzichtet werden, wenn eine Sicherungsmaßnahme installiert ist, mit der die Nutzung des Rechners nur unter Eingabe eines Passwortes weitergeführt werden kann (passwortunterstützte Bildschirmschoner), der Bildschirm gelöscht wird und wenn das Booten des Rechners die Eingabe eines Passwortes verlangt.

Bei ausgeschaltetem Rechner kann auf das Verschließen des Büros verzichtet werden, wenn das Booten des Rechners die Eingabe eines Passwortes verlangt. Die gleiche Funktion erfüllen Zugangsmechanismen, die auf Token oder Chipkarten basieren.

Ergänzende Kontrollfragen:

- Wird sporadisch überprüft, ob Büros beim Verlassen verschlossen werden?
- Werden Mitarbeiter angewiesen, bei Abwesenheit ihr Büro zu verschließen?

M 1.24 Vermeidung von wasserführenden Leitungen

Verantwortlich für Initiierung: Leiter Haustechnik, Leiter IT

Verantwortlich für Umsetzung: Haustechnik, Administrator

Absperrventile vorsehen

In Räumen oder Bereichen, in denen sich IT-Geräte mit zentralen Funktionen (z. B. Server) befinden, sollten wasserführende Leitungen aller Art vermieden werden. Die einzigen wasserführenden Leitungen sollten, wenn unbedingt erforderlich, Kühlwasserleitungen, Löschwasserleitungen und Heizungsrohre sein. Zuleitungen zu Heizkörpern sollten mit Absperrventilen, möglichst außerhalb des Raumes oder Bereiches, versehen werden. Außerhalb der Heizperiode sind diese Ventile zu schließen.

Sind wasserführende Leitungen unvermeidbar, müssen Vorkehrungen getroffen werden, einen Wasseraustritt möglichst frühzeitig zu erkennen bzw. die negativen Auswirkungen zu minimieren. Als Minimalschutz kann eine Wasserauffangwanne oder -rinne unter der Leitung angebracht werden, deren Ablauf außerhalb des Raumes führt. Günstig ist es, dazu den Flur zu nutzen, da so ein eventueller Leitungsschaden früher entdeckt wird. Zur frühzeitigen Erkennung von Wassereinbrüchen oder undichten Leitungen hat es sich bewährt, Decken hell zu streichen.

Wassermelder

Optional können Wassermelder mit automatisch arbeitenden Magnetventilen eingebaut werden. Diese Magnetventile sind außerhalb des Raumes bzw. Bereiches einzubauen. Damit die Ventile auch bei Stromausfall ihre Schutzfunktion erfüllen, müssen sie im stromlosen Zustand geschlossen sein.

Als zusätzliche oder alternative Maßnahme empfiehlt sich ggf. eine selbsttätige Entwässerung (siehe M 1.14 *Selbsttätige Entwässerung*).

Alle Mitarbeiter im Bereich der IT und der Haustechnik sollten darüber informiert sein, dass in Gebäudeteilen mit IT-Systemen mit hohen Verfügbarkeitsanforderungen wasserführende Leitungen problematisch sind und was zu beachten ist.

Ergänzende Kontrollfragen:

- Werden evtl. vorhandene Wasserleitungen regelmäßig auf ihre Dichtigkeit hin überprüft (Sichtprüfung)?

M 1.25 Überspannungsschutz

Verantwortlich für Initiierung: Leiter IT, Leiter Haustechnik, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Haustechnik, Administrator

Je nach Qualität und Ausbau des Versorgungsnetzes des Energieversorgungsunternehmens und des eigenen Stromleitungsnetzes, abhängig vom Umfeld (andere Stromverbraucher) und von der geographischen Lage, können durch Induktion oder Blitzschlag Überspannungsspitzen im Stromversorgungsnetz entstehen. Überspannungsschutzmaßnahmen dienen zur Reduzierung möglicher Schäden an IT-Geräten in Netzen durch direkten Blitzeinschlag, Einkopplung und Schalthandlungen.

Auch über andere elektrisch leitende Außenanbindungen wie Telefon-, Wasser- oder Gasleitungen können Überspannungen in ein Gebäude und die dort betriebene IT gelangen. Darüber hinaus können Überspannungen auch auf interne Leitungen eingekoppelt werden.

Alle Verbindungen beachten

Ein komplettes Überspannungsschutzkonzept berücksichtigt alle externen und internen elektrisch leitenden Verbindungen und baut sich in drei Stufen auf, die sich im Wesentlichen an den Bemessungsstoßspannungen für die Überspannungskategorien gemäß DIN VDE 0110/IEC Publikation 664 orientieren:

Grobschutz

- Der Grobschutz in der Gebäudeeinspeisung ist in der Lage Überspannungen abzufangen, wie sie durch direkten Blitzeinschlag entstehen und sie auf Werte kleiner als 6000 V zu begrenzen. Bei vorhandenem äußeren Blitzschutz muss der Grobschutz blitzstromfähig sein, da mit Strömen im 100 kA-Bereich zu rechnen ist.

Mittelschutz

- Der Mittelschutz in den Etagenverteilern begrenzt die verbleibenden Überspannungen auf ca. 1500 V und ist darauf angewiesen, dass die von ihm abzufangenden Überspannungen 6000 V nicht überschreiten.

Feinschutz

- Der Feinschutz an den jeweiligen Steckdosen und den Steckverbindungen aller anderen Leitungen reduziert die verbleibenden Überspannungen auf das von den angeschlossenen Geräten verkraftbare Maß. Die Hersteller elektrischer und elektronischer Geräte sind in den meisten Ländern verpflichtet, ihre Geräte mit einem für den sicheren Betrieb erforderlichen Feinschutz auszustatten (CE-Zeichen deutet darauf hin). In Deutschland ist dies durch das Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) geregelt.

Die Schutzwirkung jeder Stufe baut auf der vorherigen auf. Der Verzicht auf eine Stufe macht den gesamten Überspannungsschutz nahezu unwirksam.

Aufbau von Schutzzonen

Ist der gebäudeweite Aufbau eines Überspannungsschutzes nicht möglich, so kann man zumindest wichtige Teile der IT (Server etc.) mit einer entsprechenden Schutzzone umgeben. Netze mit einer Vielzahl angeschlossener Geräte können, um einen möglichen Schaden klein zu halten, durch Optokoppler oder Überspannungsableiter in kleine, gegeneinander geschützte Bereiche aufgeteilt werden. Dabei müssen geschützte und nicht geschützte Bereiche bis zurück zu der Schutzeinrichtung, bei der die Teilung erfolgt, konsequent getrennt werden. Die Zuleitungen müssen mit ausreichendem Abstand geführt werden,

eine gemeinsame Verlegung in einem Kabelkanal würde die Schutzwirkung aufheben. Überspannungsschutzeinrichtungen sollten periodisch und nach bekannten Ereignissen geprüft und ggf. ersetzt werden. Insbesondere bei Neugestaltung eines Schutzkonzeptes für Überspannung sind Auslegung und Funktionsweise bestehender USV (unterbrechungsfreier Stromversorgung) und NEA (Netzersatzanlage) zu berücksichtigen.

Antistatische Bodenbeläge

Neben dem Überspannungsschutz im Versorgungsnetz müssen in Serverräumen und den Kerneinheiten eines Rechenzentrums Maßnahmen gegen elektrostatische Aufladung getroffen werden. Der Durchgangswiderstand der Bodenbeläge in solchen Räumen muss zwischen 10 und 100 Megaohm liegen. Die Einstufung nach DIN-Vorschrift 4102-1 muss mindestens "B1 schwer entflammbar" erreichen. Dies gilt auch für einen Doppelboden oder Installationsboden.

Zwei Grundvoraussetzungen sind unabhängig von Umfang und Ausbau des Überspannungsschutzes zu beachten:

- Die Leitungslänge zwischen dem Feinschutz und zu schützenden Geräten sollte 20 m nicht überschreiten. Falls doch, ist ein erneuter Feinschutz zwischenzuschalten. Verfügt ein Gerät über einen Feinschutz im Eingang, entfällt die 20 m Begrenzung.

Potentialausgleich

- Für einen funktionierenden Überspannungsschutz ist ein umfassender Potentialausgleich aller in den Überspannungsschutz einbezogenen elektrischen Betriebsmittel erforderlich! Die Mehrzahl der Schäden an IT-Geräten durch Überspannungen ist auf nicht konsequent umgesetzten Potentialausgleich zurückzuführen.

Ergänzende Kontrollfragen:

- Werden Blitz- und Überspannungsschutzeinrichtungen periodisch und nach bekannten Ereignissen geprüft und gegebenenfalls ersetzt?
- Ist ein durchgängiger Potentialausgleich realisiert?
- Wird bei Nachinstallationen darauf geachtet, dass der Potentialausgleich mitgeführt wird?

M 1.26 Not-Aus-Schalter

Verantwortlich für Initiierung: Leiter Haustechnik, Leiter IT

Verantwortlich für Umsetzung: Haustechnik

Bei Räumen, in denen elektrische Geräte in der Weise betrieben werden, dass z. B. durch deren Abwärme, durch hohe Gerätedichte oder durch Vorhandensein zusätzlicher Brandlasten ein erhöhtes Brandrisiko besteht, ist die Installation eines Not-Aus-Schalters sinnvoll. Dies sind z. B. Server- oder Technikräume. Da zur Betätigung des Not-Aus-Schalters Personal erforderlich ist, kommt er jedoch nur in solchen Bereichen in Frage, in denen ständig oder meistens Personen anwesend sind. In nicht oder nur sporadisch besetzten Bereichen ist eine Notabschaltung durch eine Brandfrühesterkennung wesentlich effektiver.

Mit Betätigung des Not-Aus-Schalters wird dem Brand eine wesentliche Energiequelle genommen, was bei kleinen Bränden zu deren Verlöschen führen kann. Zumindest ist aber die Gefahr durch elektrische Spannungen beim Löschen des Feuers beseitigt.

USV darf bei Not-Aus nicht anspringen!

Zu beachten ist, dass lokale unterbrechungsfreie Stromversorgungen (USV) nach Ausschalten der externen Stromversorgung die Stromversorgung selbsttätig übernehmen und die angeschlossenen Geräte unter Spannung bleiben. Daher ist bei der Installation eines Not-Aus-Schalters zu beachten, dass auch die USV abgeschaltet und nicht nur von der externen Stromversorgung getrennt wird.

Der Not-Aus-Schalter sollte innerhalb des Raumes neben der Eingangstür (evtl. mit Lagehinweis außen an der Tür) oder außerhalb des Raumes neben der Tür angebracht werden. Dabei ist allerdings zu bedenken, dass dieser Not-Aus-Schalter auch ohne Gefahr versehentlich oder absichtlich betätigt werden kann. Daher ist der Not-Aus-Schalter mit einer Abdeckung gegen versehentliche Betätigung zu schützen.

Negativbeispiel:

Ein Serverraum einer mittleren Behörde wurde mit ca. 10 Servern, 5 Laserdruckern und weiteren Geräten bestückt. Der Raum war nach den Gesichtspunkten des Einbruchschutzes mit entsprechenden Wänden, Fenstern und Türen ausgestattet. Ein Not-Aus-Schalter war nicht vorhanden. Es gab nur zwei Punkte, um diesen Raum gezielt stromlos schalten zu können: die Gebäudehauptverteilung im Keller oder die Verteilung des Raumes. Diese befand sich jedoch an der Wand, die der Eingangstür gegenüberlag, im Brandfalle nahezu unerreichbar.

Ergänzende Kontrollfragen:

- Ist für alle Technikräume überprüft worden, ob die Installation eines Not-Aus-Schalters sinnvoll ist?
- Sind alle Not-Aus-Schalter gegen unbeabsichtigte Betätigung geschützt?

M 1.27 Klimatisierung

Verantwortlich für Initiierung: Leiter Haustechnik, Leiter IT

Verantwortlich für Umsetzung: Haustechnik

Um den zulässigen Betriebstemperaturbereich von IT-Geräten zu gewährleisten, reicht der normale Luft- und Wärmeaustausch eines Raumes manchmal nicht aus, so dass der Einbau einer Klimatisierung erforderlich wird. Deren Aufgabe ist es, die Raumtemperatur innerhalb der von der IT vorgegebenen Toleranzgrenzen zu halten.

Werden darüber hinaus Forderungen an die Luftfeuchtigkeit gestellt, um beispielsweise elektrostatische Aufladungen zu vermeiden, kann ein Klimagerät durch Be- und Entfeuchtung auch diese erfüllen. Dazu muss das Klimagerät allerdings an eine Wasserleitung angeschlossen werden. M 1.24 *Vermeidung von wasserführenden Leitungen* ist zu beachten.

Wartung und Überwachung

Um die Schutzwirkung aufrechtzuerhalten, ist eine regelmäßige Wartung der Klimatisierungseinrichtung vorzusehen. Eine zusätzliche Überwachungseinrichtung für die Klimatisierung ist zu empfehlen, insbesondere bei Vollklimatisierung.

Da bei einem Ausfall der Klimatisierung unter Umständen viele (insbesondere wichtige) IT-Systeme abgeschaltet werden müssen, sollte diese auf eine hohe Verfügbarkeit ausgelegt sein. Sie sollte mit einer großzügigen Leistungsreserve dimensioniert sein, außerdem sollte sie einfach erweiterbar sein. Die Klimatisierung sollte bei der Notfallplanung (siehe Baustein B 1.3 *Notfallvorsorge-Konzept*) nicht vergessen werden.

Wärmelastberechnung

Für einen Serverraum oder ein Rechenzentrum ist zur Bestimmung der nötigen Kühlleistung eine exakte Wärmelastberechnung durchzuführen. Eine Frischluft-Beimischung ist dann erforderlich, wenn der oder die klimatisierten Räume ständig mit Personal besetzt sind.

Ebenso ist durch mehrere Messungen zu verschiedenen Tageszeiten zu bestimmen, ob eine Luftbefeuchtung oder -entfeuchtung in solchen Räumen erforderlich ist. Hier sind auch Herstellervorgaben für die betriebenen IT-Komponenten zu beachten.

Wärmetauscher und Rückkühlwerke sollten möglichst nicht direkt in einem Serverraum oder Rechenzentrum aufgestellt sein, um zu verhindern, dass Schäden an der Klimaanlage weitere Beeinträchtigungen verursachen, z. B. durch austretende Kühlflüssigkeit oder Kurzschlüsse.

Die Rückkühlwerke der Klimaanlage sind bei Aufstellung im Freien gegen direkten Blitzeinschlag zu schützen. Insbesondere in Hochsicherheitsbereichen sollten die Rückkühlwerke nicht für jedermann zugänglich sein und gegebenenfalls gegen Sabotage materiell geschützt werden.

Ergänzende Kontrollfragen:

- In welchen für IT genutzten Räumen können erhöhte Temperaturen auftreten?
- Werden eingesetzte Klimageräte regelmäßig gewartet?
- Welches sind die für die IT zulässigen Höchst- und Tiefstwerte für Temperatur und Luftfeuchte?

M 1.28 Lokale unterbrechungsfreie Stromversorgung

Verantwortlich für Initiierung: Leiter Haustechnik, Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Haustechnik

Mit einer unterbrechungsfreien Stromversorgung (USV) kann ein kurzzeitiger Stromausfall überbrückt werden oder die Stromversorgung solange aufrechterhalten werden, dass ein geordnetes Herunterfahren angeschlossener Rechner möglich ist. Dies ist insbesondere dann sinnvoll,

- wenn im Rechner umfangreiche Daten zwischengespeichert werden (z. B. Cache-Speicher im Netz-Server), bevor sie auf nichtflüchtige Speicher ausgelagert werden,
- beim Stromausfall ein großes Datenvolumen verloren gehen würde und nachträglich nochmals erfasst werden müsste,
- wenn die Stabilität der Stromversorgung nicht ausreichend gewährleistet ist.

offline / online

Zwei Arten der USV sind zu unterscheiden:

- offline-USV: Hierbei werden die angeschlossenen Verbraucher im Normalfall direkt aus dem Stromversorgungsnetz gespeist. Erst wenn dieses ausfällt, schaltet sich die USV selbsttätig zu und übernimmt die Versorgung.
- online-USV: Hier ist die USV ständig zwischen Netz und Verbraucher geschaltet. Die gesamte Stromversorgung läuft immer über die USV.

Beide USV-Arten können neben der Überbrückung von Totalausfällen der Stromversorgung und Unterspannungen auch dazu dienen, Überspannungen zu glätten. Auch hier gilt hinsichtlich des Überspannungsschutzes die in M 1.25 *Überspannungsschutz* erläuterte Begrenzung auf 20 m.

Werden IT-Geräte in einem Gebäude mit TN-S-Netz (siehe dazu M 1.39 *Verhinderung von Ausgleichsströmen auf Schirmungen*) mit einer lokalen USV versorgt, ist Folgendes zu beachten: Um die Schutzwirkung des TN-S-Netzes gegen Ausgleichsströme auf Schirmen von Datenleitungen aufrecht zu erhalten, ist darauf zu achten, dass USV-ausgangsseitig keine Verbindung zwischen N- und PE-Leiter (Nullung) besteht. Ggf. sind solche oft serienmäßig eingebauten Verbindungen vor Einbau in das TN-S-Netz zu entfernen.

Dimensionierung

Bei der Dimensionierung einer USV kann man in der Regel von einer üblichen Überbrückungszeit von ca. 10 bis 15 Minuten ausgehen. Die Mehrzahl aller Stromausfälle ist innerhalb von 5 bis 10 Minuten behoben, so dass nach Abwarten dieser Zeitspanne noch 5 Minuten übrig bleiben, um die angeschlossene IT geordnet herunterfahren zu können, sollte der Stromausfall länger andauern. Die meisten modernen USV-Geräte bieten Rechnerschnittstellen an, die nach einer vorher festgelegten Zeit, entsprechend dem Zeitbedarf der IT und der Kapazität der USV, ein rechtzeitiges automatisches Herunterfahren (Shut-down) einleiten können.

Für spezielle Anwendungsfälle (z. B. TK-Anlagen) kann die erforderliche Überbrückungszeit auch mehrere Stunden betragen.

Um die Schutzwirkung aufrechtzuerhalten, ist eine regelmäßige Wartung der USV vorzusehen.

Falls die Möglichkeit besteht, die Stromversorgung unterbrechungsfrei aus einer anderen Quelle zu beziehen (z. B. durch Anschluss an eine zentrale USV), so stellt dies eine Alternative zur lokalen USV dar.

Ergänzende Kontrollfragen:

- Werden die Wartungsintervalle der USV eingehalten?
- Ist ein automatisches Shut-down vorgesehen?
- Wird die Wirksamkeit der USV regelmäßig getestet?
- Haben sich Veränderungen ergeben, so dass die vorgehaltene Kapazität der USV nicht mehr ausreichend ist?

M 1.29 Geeignete Aufstellung eines IT-Systems

Verantwortlich für Initiierung: Leiter Haustechnik, Leiter IT

Verantwortlich für Umsetzung: Haustechnik, Benutzer

Bei der Aufstellung eines IT-Systems sollten verschiedene Voraussetzungen beachtet werden, die die Sicherheit, aber auch Lebensdauer und Zuverlässigkeit der Technik verbessern und die Ergonomie berücksichtigen (siehe auch M 3.9 *Ergonomischer Arbeitsplatz*). Einige seien hier genannt:

- Ein IT-System sollte möglichst so aufgestellt sein, dass nur die befugten Benutzer die Bildschirminhalte einsehen können. Bei einem Standort in der Nähe eines Fensters oder einer Tür können die Bildschirmaktivitäten eventuell von außerhalb beobachtet werden.
- **Schutz vor Manipulationen**
  Um zu verhindern, dass IT-Systeme manipuliert werden können, sollten sie so aufgestellt werden, dass nur Berechtigte Zutritt haben. IT-Systeme in Bereichen, in denen sich häufig Externe aufhalten, müssen mit zusätzlichen Maßnahmen gegen Diebstahl und Manipulationen geschützt werden.
- Ein IT-System sollte nicht in unmittelbarer Nähe der Heizung aufgestellt werden, um eine Überhitzung zu vermeiden.
- Ein IT-System sollte nicht der direkten Sonneneinstrahlung ausgesetzt sein.
- **Vorsicht vor Schmutz**
  Staub und Verschmutzungen sollten vermieden werden, da die mechanischen Bauteile (Laufwerke für Wechselmedien, mechanische Maus, Festplatten) beeinträchtigt werden können.
- Der Aufstellungsort sollte so gewählt sein, dass Schäden durch Außeneinwirkungen wie Überschwemmungen, Rohrbrüche, erhöhte Luftfeuchtigkeit, elektrische Interferenzen, elektromagnetische Einstrahlungen möglichst vermieden werden.

Alle Mitarbeiter sollten darüber informiert sein, welche Einwirkungen schädlich für IT-Systeme sind, damit sie mithelfen können, diese zu vermeiden. Dazu gehören z. B. Verschmutzungen durch Essen oder Getränke, Zigarettenrauch oder -asche, aber auch der falsche Einsatz von Reinigungsmitteln.

Je nach Umgebung kann es auch sinnvoll sein, zusätzliche Hilfsmittel zum Schutz der IT einzusetzen, wie z. B. Abdeckungen für Tastaturen oder Bildschirmfolien, die den seitlichen Einblick verhindern.

Ergänzende Kontrollfragen:

- Sind IT-Systeme so aufgestellt, dass sie vor unbefugtem Zugriff geschützt sind?
- Sind durch den Aufstellungsort bedingte Ausfälle in der Vergangenheit zu beobachten gewesen?

M 1.30 Absicherung der Datenträger mit TK-Gebührendaten

Verantwortlich für Initiierung: TK-Anlagen-Verantwortlicher, Datenschutzbeauftragter

Verantwortlich für Umsetzung: Administrator

Auf den TK-Anlagen fallen während des Betriebes Gebührendaten an. Diese enthalten Informationen über:

- Zeit und Datum eines Gespräches,
- Quell- und Zielrufnummer sowie die
- Gesprächsdauer.

Gebührendaten sind personenbezogene Daten im Sinne der einschlägigen Bundes- und Landesdatenschutzgesetze. Hieraus folgt, dass auch nach den im folgenden vorgeschlagenen Maßnahmen des IT-Grundschutzes in jedem Fall eine gesonderte Betrachtung im Hinblick auf die Anforderungen der Datenschutzgesetze (z. B. aus der Anlage zum § 9 Bundesdatenschutzgesetz) durchzuführen ist.

Diese Daten können sowohl auf der Festplatte der TK-Anlage selbst als auch auf einem externen Gebührenrechner gespeichert werden. In vielen Fällen wird es eine Kombination beider Varianten geben. Die Rechner sind - wenn möglich - so zu schützen, dass nur Berechtigte auf die Gebührendaten zugreifen können. Dazu ist es erforderlich, den Gebührenrechner in einem besonders geschützten Raum (siehe Baustein B 2.4 *Serverraum*) aufzustellen. Für Einrichtungen, auf denen Gebührendaten gespeichert sind, müssen ferner die Maßnahmen M 1.23 *Abgeschlossene Türen*, M 2.5 *Aufgabenverteilung und Funktionstrennung*, M 2.6 *Vergabe von Zutrittsberechtigungen*, M 2.7 *Vergabe von Zugangsberechtigungen*, M 2.8 *Vergabe von Zugriffsrechten*, M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* und M 2.17 *Zutrittsregelung und -kontrolle* realisiert werden.

Es ist zu dokumentieren, welche Personen in welchen Rollen Zugriff auf die Gebührendaten haben.

Ergänzende Kontrollfragen:

- Wer hat Zugriff auf die Gebührendaten?
- Wie wird der Zugriffsschutz realisiert?
- Haben nur die Benutzer mit berechtigtem Interesse Zugriffsrecht?
- Wo befinden sich die Sicherungskopien und wer hat dort Zugang?
- Wie werden die Datenträger entsorgt?
- Wie lange werden die Daten gespeichert?

M 1.31 Fernanzeige von Störungen

Verantwortlich für Initiierung: Leiter IT, TK-Anlagen-Verantwortlicher, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

IT-Geräte und Supportgeräte, die keine oder nur seltene Bedienung durch eine Person erfordern, werden oft in ge- und verschlossenen Räumen untergebracht (z. B. Serverraum). Das führt dazu, dass Störungen, die sich in ihrem Frühstadium auf die IT noch nicht auswirken und einfach zu beheben sind, erst zu spät, meist durch ihre Auswirkungen auf die IT, entdeckt werden. Feuer, Funktionsstörungen einer USV oder der Ausfall eines Klimagerätes seien als Beispiele für solche "schleichenden" Gefährdungen angeführt.

Durch eine Fernanzeige ist es möglich, solche Störungen früher zu erkennen. Viele Geräte, auf die man sich verlassen muss, ohne sie ständig prüfen oder beobachten zu können, haben heute einen Anschluss für Störungsfernanzeigen. Die technischen Möglichkeiten reichen dabei von einfachen Kontakten, über die eine Warnlampe eingeschaltet werden kann, bis zu Rechnerschnittstellen mit dazugehörigem Softwarepaket für die gängigen Betriebssysteme. Über die Schnittstellen ist es oft sogar möglich, jederzeit den aktuellen Betriebszustand der angeschlossenen Geräte festzustellen und so Ausfällen rechtzeitig begegnen zu können.

Ergänzende Kontrollfragen:

- Wissen die durch die Fernanzeige Alarmierten, welche Handlungen auszuführen sind?

M 1.32 Geeignete Aufstellung von Druckern und Kopierern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um zu verhindern, dass Drucker manipuliert werden oder die Druckausgaben von Unbefugten kopiert oder mitgelesen werden können, sollten Drucker so aufgestellt werden, dass nur Berechtigte Zutritt haben. Zumindest sollten Drucker nicht in Bereichen aufgestellt werden, in denen sich häufig Externe aufhalten, insbesondere also nicht in der Nähe von Besprechungs-, Veranstaltungs- oder Schulungsräumen. Hiervon ausgenommen sind lediglich solche Drucker, die speziell für diese Bereiche vorgesehen sind, beispielsweise in Schulungsräumen.

Häufig stehen in Druckerräumen auch Kopierer. Aus Sicherheitssicht ist zu hinterfragen, ob hierdurch die Gefahr steigt, dass auf die Schnelle Kopien von herumliegenden Ausdrucken angefertigt werden. Andererseits zeigt die Erfahrung, dass selbst wenn Ausdrucke einfach mitgenommen werden, schimpfen erfahrungsgemäß die meisten Benutzer auf die Technik und denken nicht daran, dass der Ausdruck auch in böser Absicht von jemand anderem entfernt worden sein kann.

Um solche Probleme zu vermeiden, ist es sinnvoll, Drucker und Kopierer so aufzustellen, dass sie vom eigenen Personal gut eingesehen werden können. Also beispielsweise sollten Drucker und Kopierer nicht in eine düstere Ecke gestellt werden, sondern durch eine Glastür vom Sekretariat einsehbar sein.

Besser ist es, Drucker und Kopierer in einem geschlossenen Raum aufzustellen, zu dem nur Berechtigte Zutritt haben. Dies ist bei höherem Schutzbedarf zu empfehlen.

Noch besser ist es bei großen Druckern, wenn die Ausdrucke in nur für den jeweiligen Empfänger zugängliche Fächer durch eine vertrauenswürdige Person verteilt werden. Druckerausgaben müssen daher mit dem Namen des Empfängers gekennzeichnet sein. Dieses kann automatisch durch die Druckprogramme erfolgen. Bei sehr hohem Schutzbedarf sollte geprüft werden, ob diese Lösung geeignet ist.

Benutzer stellen häufig erst am Drucker fest, dass sie das falsche Dokument ausgedruckt haben oder dass noch eine Kleinigkeit geändert werden muss. Solche Ausdrucke werden dann häufig direkt beim Drucker in einen offenen Papierkorb geworfen. Da damit auch vertrauliche Dokumente in falsche Hände geraten können, empfiehlt es sich, einen Vernichter direkt neben Netz-Druckern aufzustellen. Ersatzweise müssen die Benutzer darauf hingewiesen werden, dass solche Dokumente nicht liegengelassen werden dürfen und anderweitig zu vernichten sind.

Ergänzende Kontrollfragen:

- Sind Drucker und Druckerausgaben vor unbefugtem Zugriff geschützt?

M 1.33 Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Da die Umfeldbedingungen bei mobilem Einsatz meist außerhalb der direkten Einflussnahme der Benutzer liegen, müssen diese versuchen, mobile IT-Systeme wie Laptops oder PDAs auch außer Haus sicher aufzubewahren. Hierfür können nur einige Hinweise gegeben werden, die bei der mobilen Nutzung zu beachten sind:

- Schutz vor Diebstahl
  - Nach Möglichkeit sollten die Zeiten, in denen das Gerät unbeaufsichtigt bleibt, minimiert werden.

    Nicht unbeobachtet zurücklassen
  - Wird ein tragbarer PC oder PDA in einem Kraftfahrzeug aufbewahrt, so sollte das Gerät von außen nicht sichtbar sein. Das Abdecken des Gerätes oder das Einschließen in den Kofferraum bieten Abhilfe. Ein mobiles IT-System kann einen hohen Wert darstellen, der potentielle Diebe anlockt, zumal tragbare IT-Systeme leicht veräußert werden können.
  - Wird das mobile IT-System in fremden Büroräumen vor Ort benutzt, so ist entweder dieser Raum nach Möglichkeit auch bei kurzzeitigem Verlassen zu verschließen oder das Gerät mitzunehmen. Wird der Raum für längere Zeit verlassen, sollte zusätzlich das mobile IT-System ausgeschaltet werden oder ein Zugriffsschutz aktiviert, um eine unerlaubte Nutzung zu verhindern.
  - In Hotelräumen sollte das mobile IT-System nicht offen herumliegen. Das Verschließen des Gerätes in einem Schrank behindert Gelegenheitsdiebe.

    Gelegenheit macht Diebe
  - Einige neuere Geräte bieten zusätzlich die Möglichkeit zum Anketten des Gerätes. Der Diebstahl setzt dann den Einsatz von Werkzeug voraus.
- Ein mobiles IT-System sollte nie extremen Temperaturen ausgesetzt werden. Insbesondere der Akku, aber auch das Display können anderenfalls beschädigt werden. Insbesondere sollten weder IT-Geräte noch Akkus in geparkten Autos zurückgelassen werden.

  Vorsicht vor extremen Temperaturen
- Ebenso sollten mobile Endgeräte vor Umwelteinflüssen geschützt werden, die diese schädigen können, also beispielsweise vor Feuchtigkeit durch Regen oder Spritzwasser.

  Auch Feuchtigkeit schadet
- Mobile Endgeräte sind auch nicht unzerstörbar, daher sollten sie auch bei kürzeren Transportwegen möglichst stoßgeschützt befördert werden. Bei Laptops sollte beispielsweise das Gerät zusammengeklappt werden, da sowohl die Scharniere als auch der Bildschirm bei einem Sturz leicht beschädigt werden können. Grundsätzlich ist es immer empfehlenswert, für den Transport ein schützendes Behältnis zu verwenden.

Es ist empfehlenswert, für die Benutzer mobiler IT-Systeme ein Merkblatt zu erstellen, das die wichtigsten Hinweise und Vorsichtsmaßnahmen zur geeigneten Aufbewahrung und zum sicheren Transport der Geräte enthält.

Ergänzende Kontrollfragen:

- Werden die Benutzer von tragbaren IT-Systemen auf die geeignete Aufbewahrung hingewiesen?

M 1.34 Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Tragbare IT-Systeme wie Laptops, PDAs oder Mobiltelefone sind durch ihre Bauform immer beliebte Ziele für Diebstähle. Daher müssen sie auch dann sicher aufzubewahrt werden, wenn sie sich im vermeintlichen sicheren Büro befinden. Aus diesem Grund sind natürlich die in Baustein B 2.3 *Büroraum* beschriebenen Maßnahmen zu beachten. Da ein tragbares IT-Systeme jedoch besonders leicht zu transportieren und zu verbergen ist, sollte das Gerät außerhalb der Nutzungszeiten weggeschlossen werden, also beispielsweise in einem Schrank oder Schreibtisch verschlossen werden oder angekettet werden.

Ergänzende Kontrollfragen:

- Wie werden tragbare IT-Systeme in den Büros aufbewahrt?

M 1.35 Sammelaufbewahrung tragbarer IT-Systeme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Sind in einer Behörde bzw. einem Unternehmen eine Vielzahl von tragbaren IT-Systemen im (mobilen) Einsatz und wechseln die Benutzer häufig, kann es angebracht sein, die zeitweise nicht genutzten Laptops in einer Sammelaufbewahrung (Pool) zu halten. Der dafür genutzte Raum sollte den Anforderungen, die in Baustein B 2.6 *Raum für technische Infrastruktur* beschriebenen werden, entsprechen.

Darüber hinaus ist die Stromversorgung der Laptops sicherzustellen, damit die Batterien dieser Geräte den sofortigen Einsatz erlauben. Zusätzlich müssen die Rücknahme und die Ausgabe von tragbaren IT-Systemen dokumentiert werden.

Ergänzende Kontrollfragen:

- Wer hat Zutritt zur Sammelaufbewahrung der IT-Systeme?
- Wird die Ausgabe und Rücknahme der Laptops dokumentiert?

M 1.36 Sichere Aufbewahrung der Datenträger vor und nach Versand

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer, Poststelle

Vor dem Versand eines Datenträgers ist zu gewährleisten, dass für den Zeitraum zwischen dem Speichern der Daten auf dem Datenträger und dem Transport ein ausreichender Zugriffsschutz besteht. Sind die zu übermittelnden Daten auf den Datenträger geschrieben, so sollte dieser bis zum Transport in entsprechenden Behältnissen (Schrank, Tresor) verschlossen aufbewahrt werden. Die für den Transport oder für die Zustellung Verantwortlichen (z. B. Poststelle) sind auf sachgerechte und sichere Aufbewahrung und Handhabung des Datenträgers hinzuweisen.

Ergänzende Kontrollfragen:

- Sind die Mitarbeiter darauf hingewiesen worden, für den Transport vorgesehene Datenträger nicht frei zugänglich aufzubewahren?

M 1.37 Geeignete Aufstellung eines Faxgerätes

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter Haustechnik

Verantwortlich für Umsetzung: Benutzer, Fax-Verantwortlicher, Haustechnik

Ein Faxgerät sollte in einem Bereich installiert werden, der nicht öffentlich zugänglich ist. Eine Kontrolle des Zutritts zu diesem Bereich oder der Nutzung des Faxgerätes ist sinnvoll.

Sinnvollerweise kann dies durch die Aufstellung in einem ständig besetzten Raum (z. B. Geschäftszimmer, Sekretariat, Poststelle) erreicht werden. Außerhalb der Dienstzeiten oder bei Abwesenheit der berechtigten Benutzer sollte das Gerät eingeschlossen werden (Raum oder Schrank). Wichtig ist in diesem Zusammenhang, dass verhindert werden muss, dass eingegangene Faxsendungen von Unberechtigten eingesehen oder entnommen werden können (siehe M 2.48 *Festlegung berechtigter Faxbediener*).

Ergänzende Kontrollfragen:

- Wer kann das Faxgerät unkontrolliert nutzen?
- Zu welchen Zeiten ist dies einfach möglich (Mittagspause, Schichtwechsel, ...)?
- Wie wird der Zugang zum Faxgerät kontrolliert?
- Wie wird das Gerät außerhalb der Dienstzeiten geschützt?

M 1.38 Geeignete Aufstellung eines Modems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer, Administrator

Um den Missbrauch von Modems zu verhindern, muss sichergestellt werden, dass nur Berechtigte physikalischen Zugriff darauf haben. Missbrauch bedeutet hier zum einem die Durchführung unbefugter Datenübertragungen, durch die Kosten verursacht, Viren eingeschleppt oder Interna nach außen transferiert werden können, und zum anderen das unbefugte Ändern oder Auslesen der Modem-Konfiguration, wodurch Sicherheitslücken entstehen können.

Um den physikalischen Zugriff auf ein externes Modem oder ein PCMCIA-Modem abzusichern, ist z. B. bei einem ständig benutzten Modem das Abschließen des Raumes oder bei einem nur zeitweise benutzten Modem das sichere Aufbewahren des inaktiven Modems in einem Schrank zu gewährleisten. Die Maßnahmen des Bausteins B 2.3 *Büroraum*, sind zu beachten.

Ein internes Modem besitzt aufgrund des Einbaus in ein IT-System einen höheren inhärenten physikalischen Zugriffsschutz. Hier würde es reichen, die Maßnahmen der Bausteine B 2.3 *Büroraum* oder B 2.4 *Serverraum* zu beachten.

Wenn über ein Modem oder einen Modem-Pool Zugänge zum internen Netz geschaffen werden, ist das Baustein B 3.301 *Sicherheitsgateway (Firewall)* zu beachten. Über Modems darf kein Zugang zum internen Netz unter Umgehung einer bestehenden Firewall geschaffen werden.

Wenn mit einem Modem-Pool weitere externe Zugänge zu einem durch eine Firewall geschützten Netz geschaffen werden sollen, muss dieser auf der unsicheren Seite der Firewall aufgestellt werden (siehe auch M 2.77 *Integration von Servern in das Sicherheitsgateway*). Der Modem-Pool sollte zusammen mit dem zugehörigen Server in einem gesicherten Serverraum aufgestellt sein. Die Maßnahmen des Bausteins B 2.4 *Serverraum* sind zu beachten.

M 1.39 Verhinderung von Ausgleichsströmen auf Schirmungen

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Haustechnik

Um Ausgleichsströme auf den Schirmungen von Datenleitungen in Gebäuden zu verhindern, gibt es verschiedene Möglichkeiten:

geschirmte Datenleitungen

Ausgleichsströme können im TN-C-Netz vermieden werden, indem nur solche IT-Geräte miteinander über geschirmte Datenleitungen miteinander verbunden werden, die an einer gemeinsamen Elektro-Verteilung angeschlossen sind. Bei jeder Erweiterung des Datennetzes ist diese Bedingung zu prüfen und sicherzustellen.

Einseitiges Auflegen der Schirmung

Als Maßnahme gegen Ausgleichsströme im TN-C- bzw. TN-CS-Netz wird häufig das ausschließlich einseitige Auflegen der Schirmung von Datenleitungen vorgeschlagen. Hinsichtlich der Ausgleichsströme ist dieses Vorgehen auch tatsächlich wirksam. Aus anderen Gründen sollte dieses Mittel aber als absolute Ausnahme äußerst restriktiv angewandt werden:

- Geschirmte Leitungen, deren Schirmung nur einseitig aufgelegt ist, werden deutlich stärker durch Störstrahlungen von außen beeinflusst. Gleichzeitig strahlen sie selbst stärker ab, als ungeschirmte symmetrische Leitungen. Es muss also bei einseitiger Schirmauflegung mit mehr Störungen der Datenübertragung (z. B. der Verfügbarkeit bzw. Integrität) gerechnet werden, als bei allen anderen Kabeln. Die stärkere Aussendung auswertbarer Abstrahlung derartiger Leitungen kommt als Risiko bei der Betrachtung der Vertraulichkeit von Informationen hinzu.
- Selbst wenn man alle technischen Nachteile der einseitigen Schirmauflegung hinzunehmen bereit ist, bleibt das Problem der Durchgängigkeit. Es bedarf konsequenter Kontrolle bei allen Arbeiten im Datennetz, um sicher zu stellen, dass einseitig aufgelegte Schirmungen nicht doch irgendwann beidseitig aufgelegt werden. Solche Fehlauflegungen sind nachträglich nur mit sehr großen Suchaufwand festzustellen.

Potentialausgleich

Die optimale, weil sicherste Möglichkeit besteht darin, das Stromverteilnetz im gesamten Gebäude komplett als TN-S-Netz auszulegen. Dabei wird der PE- und der N-Leiter ab der Potentialausgleichsschiene (PAS) getrennt geführt. Einzelmaßnahmen an IT-Geräten sind dann in der Regel nicht mehr erforderlich. Zu beachten ist jedoch der Hinweis in M 1.28 *Lokale unterbrechungsfreie Stromversorgung* hinsichtlich der Bildung eines neuen TN-S-Netzes für die angeschlossenen Geräte.

Die nachfolgenden Zeichnungen erläutern die Entstehung von Ausgleichsströmen auf Schirmungen und die möglichen Gegenmaßnahmen:

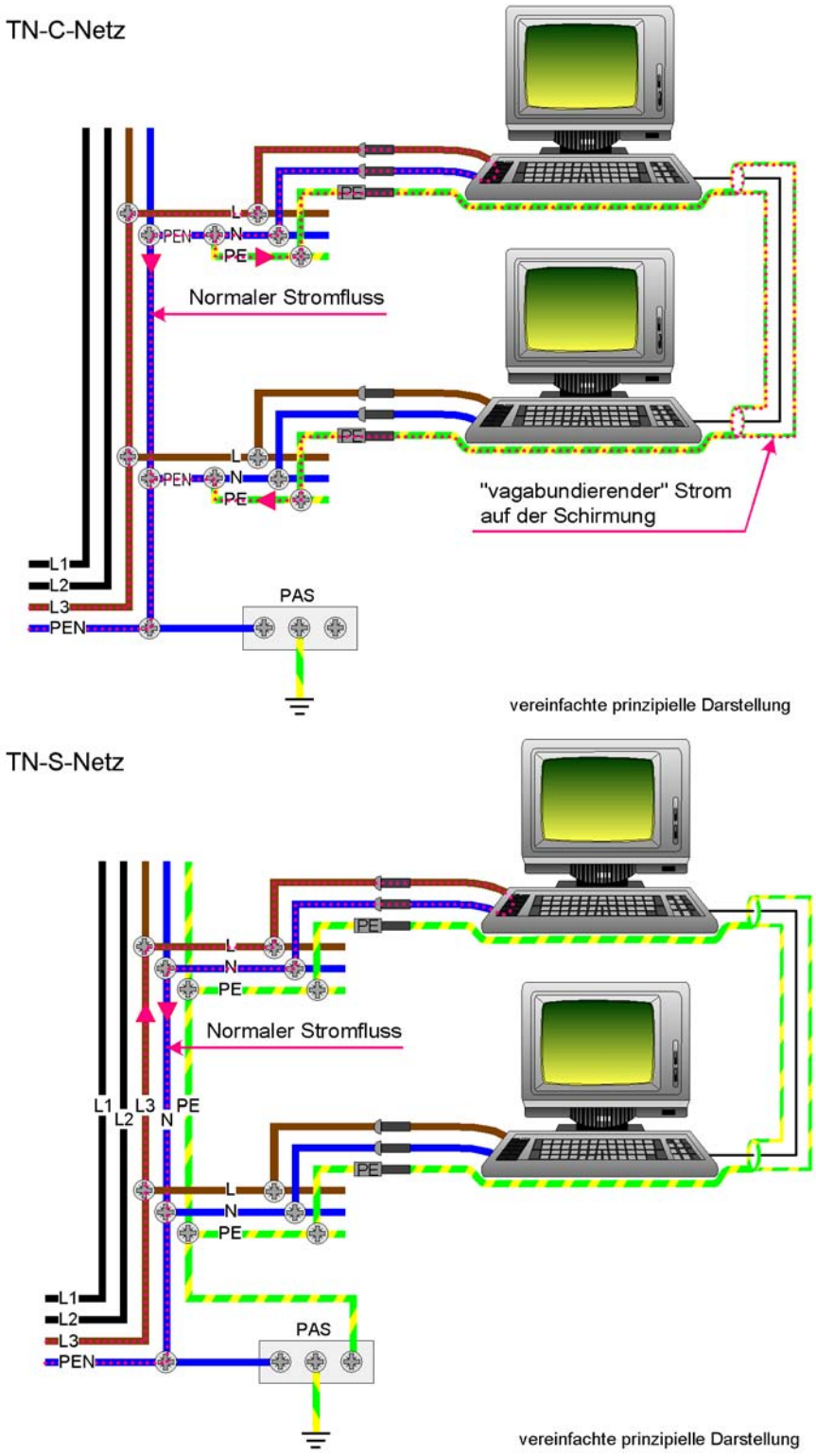


Abb. 1: Entstehung von Ausgleichsströmen auf Schirmungen und die möglichen Gegenmaßnahmen

Ergänzende Kontrollfragen:

- Welche Netzart ist in der Liegenschaft vorhanden?
- Wie und durch wen werden die Schutzbedingungen (eine gemeinsame Verteilung oder nur einseitig aufgelegter Schirm) geprüft?
- Werden Änderungen im Datennetz mit der Haustechnik abgestimmt?

M 1.40 Geeignete Aufstellung von Schutzschränken

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Innerer Dienst

Aufgrund des in der Regel hohen Gewichts von Schutzschränken muss vor der Aufstellung die Tragfähigkeit des Fußbodens am Aufstellungsort geprüft werden.

Schutzschränke, die aufgrund ihrer geringen Größe relativ einfach weggetragen werden könnten, sollten in der Wand oder im Boden verankert werden.

Eventuell vorhandene Herstellerhinweise zur geeigneten Aufstellung (z. B. freie Lüftungsöffnungen, Kabelführungen) sind zu berücksichtigen.

Ergänzende Kontrollfragen:

- Wie wird der Diebstahl eines Schutzschrankes verhindert?

M 1.41 Schutz gegen elektromagnetische Einstrahlung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Beschaffer, Haustechnik

Werden in einem Schutzschrank informationstechnische Geräte untergebracht, so kann durch benachbarte Einrichtungen elektromagnetische Strahlung erzeugt werden, die die Funktion der Geräte beeinträchtigt (insbesondere in industriellen Produktionsbereichen). Durch Nachrüstung von Filtern und Türdichtungen kann die Einstrahlung innerhalb des Schutzschrankes reduziert werden. Gleichzeitig verhindern diese Maßnahmen auch eine Verbreitung von kompromittierender Abstrahlung der im Schrank befindlichen Geräte.

Ergänzende Kontrollfragen:

- Ist eine Gefährdung durch elektromagnetische Einstrahlung gegeben?

M 1.42 Gesicherte Aufstellung von Novell Netware Servern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um den manipulationssicheren Betrieb von Novell Netware Servern sicherzustellen, ist es zwingend erforderlich, die Novell Netware Server in einer gesicherten Umgebung aufzustellen. Dies kann entweder ein Serverraum sein (siehe Baustein B 2.4 *Serverraum*) oder ein Serverschrank, wenn kein separater Serverraum zur Verfügung steht (siehe Baustein B 2.4 *Serverraum*). Unbefugte dürfen zum Aufstellungsort von Novell Netware Servern keinen unbeaufsichtigten Zugang erhalten. Das Diskettenlaufwerk von Novell Netware Servern ist darüber hinaus standardmäßig mit einem Diskettenschloss zu verschließen.

M 1.43 Gesicherte Aufstellung aktiver Netzkomponenten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Planer

Verantwortlich für Umsetzung: Leiter Haustechnik, Administrator

Um den manipulationssicheren Betrieb eines Netzes sicherzustellen, ist es erforderlich, aktive Netzkomponenten (wie Router, Switches, ISDN-Router) in einer gesicherten Umgebung zu betreiben. Dies kann entweder ein Serverraum sein (siehe Baustein B 2.4 *Serverraum*) oder, wenn kein separater Serverraum zur Verfügung steht, ein Serverschrank (siehe Baustein 4.4 *Schutzschränke*). Unbefugte Personen dürfen zum Aufstellungsort der Geräte keinen unbeaufsichtigten Zugang erhalten.

Dabei sollte beachtet werden, dass Hersteller von Schutzschränken oft Standardschlösser einsetzen, so dass mit einem beliebigen Schlüssel des Schrankherstellers alle Schränke geöffnet werden können. Daher muss gegebenenfalls das serienmäßige Schloss eines Schutzschranks gegen ein individuelles Schloss ausgetauscht werden.

Außerdem sollten die Geräte so aufgestellt werden, dass sie vor elektromagnetischen oder magnetischen Feldern geschützt sind. Zusätzlich sollten sie mit Kontrollmechanismen ausgestattet sein, die eine Überschreitung der zulässigen Toleranzen bei Feuchtigkeit und Temperatur signalisieren.

Der Schutz von Routern und Switches vor unbefugtem Zugriff ist auch deswegen sehr wichtig, weil für viele Geräte Passwort-Recovery-Prozeduren für das Rücksetzen von Passwörtern bekannt sind, die zumeist den physikalischen Zugang zu den Geräten (Konsolenanschluss) voraussetzen. Oft verfügen die Geräte auch über PCMCIA-Slots: Entsprechende PCMCIA-Karten können für die allgemeine Speicherung von Daten verwendet werden und bieten eine komfortable Möglichkeit, Konfigurationsdaten auszutauschen, Updates vorzunehmen oder Image-Dateien einzuspielen.

Das serielle Konsolen-Interface (RS-232-Port) ermöglicht den Anschluss eines PC oder Terminals, um Administrations- oder Konfigurationsarbeiten durchzuführen. Das Passwort für den Zugriff auf die Konsole muss schriftlich an einem sicheren Ort hinterlegt sein (siehe auch M 2.22 *Hinterlegen des Passwortes*).

Zusätzlich muss den Gefahren durch Diebstahl, Vandalismus und unbefugtem Ausschalten des Geräts vorgebeugt werden.

Ergänzende Kontrollfragen:

- Sind die aktiven Netzkomponenten in verschlossenen Schränken untergebracht?
- Wurden die Standardschlösser ausgewechselt?
- Wurde die Konsole mit einem sicheren Passwort gesichert?
- Sind die Passwörter hinterlegt?

M 1.44 Geeignete Einrichtung eines häuslichen Arbeitsplatzes

Verantwortlich für Initiierung: Leiter Haustechnik, Personalrat/Betriebsrat, Vorgesetzte

Verantwortlich für Umsetzung: Haustechnik, Mitarbeiter

Für den häuslichen Arbeitsplatz ist die Nutzung eines Arbeitszimmers wünschenswert. Zumindest sollte der häusliche Arbeitsplatz von der übrigen Wohnung durch eine Tür abgetrennt sein.

Die Einrichtung sollte unter Berücksichtigung von Ergonomie, Sicherheit und Gesundheitsschutz ausgewählt werden.

Dies bedeutet u. a.:

- ausreichend Platz für Möbel und Bildschirmarbeitsplatz,
- regelbare Raumtemperatur und ausreichende Lüftungsmöglichkeiten,
- Abschirmung gegenüber Lärmquellen,
- Tageslicht sowie ausreichend künstliche Beleuchtung,
- Sichtschutz des Monitors, falls er durch ein Fenster beobachtet werden könnte,
- Vermeidung von störenden Blendungen, Reflexen oder Spiegelungen am Arbeitsplatz und
- Anschlüsse für Telefon und Strom.

Dienstlich genutzte IT sollte vom Arbeitgeber bereitgestellt werden, um z. B. per Dienstanweisung ausschließen zu können, dass die IT für private Zwecke benutzt wird.

Ergänzende Kontrollfragen:

- Werden betroffene Mitarbeiter mit einem häuslichen Arbeitsplatz regelmäßig oder sporadisch befragt, ob der Arbeitsplatz ihren gesundheitlichen oder betrieblichen Ansprüchen entsprechen?

M 1.45 Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger

Verantwortlich für Initiierung: Leiter Haustechnik, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Mitarbeiter

Dienstliche Unterlagen und Datenträger dürfen auch außerhalb der offiziellen Bürogebäude, also z. B. am häuslichen oder einem mobilen Arbeitsplatz, nur den autorisierten Mitarbeitern zugänglich sein. Außerhalb der Nutzungszeit müssen sie so aufbewahrt werden, dass kein Unbefugter darauf zugreifen kann.

Aufbewahrung zuhause

Am häuslichen Arbeitsplatz muss aus diesem Grund ein verschließbares Behältnis (Schreibtisch, Rollcontainer, Schrank o. Ä.) verfügbar sein. Der Verschluss muss mindestens Angriffen mit einfach herzustellenden oder einfach zu erwerbenden Nachschließmitteln (Büroklammer, Dietrich etc.) standhalten. Es sollten Möbelschlösser mit mindestens 4 Zuhaltungen und mindestens 1000 Schließvarianten eingesetzt werden. Zudem ist darauf zu achten, dass der Verschluss nicht durch einfaches Entfernen z. B. einer Rückwand leicht umgangen werden kann. Insgesamt sollte die Schutzwirkung des Behältnisses den Sicherheitsanforderungen der darin zu verwahrenden Unterlagen und Datenträger entsprechen.

Aufbewahrung unterwegs

Bei Arbeitsplätzen unterwegs sollten weder dienstliche Unterlagen noch mobile IT-Systeme unbeaufsichtigt bleiben. Sie sollten zumindest gegen einfache Wegnahme gesichert werden, also beispielsweise mit Diebstahlsicherungen versehen werden, in Schränke geschlossen werden oder andere, einfache Maßnahmen ergriffen werden. Außerdem ist es empfehlenswert, dienstliche Unterlagen und mobile IT-Systeme in einem verschließbaren Aktenkoffer zu transportieren.

Ergänzende Kontrollfragen:

- Steht für den häuslichen Arbeitsplatz ein verschließbares Behältnis zur Verfügung?
- Sind die Mitarbeiter darauf hingewiesen worden, dass die Unterlagen und Datenträger verschlossen aufzubewahren sind?

M 1.46 Einsatz von Diebstahl-Sicherungen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT

Diebstahl-Sicherungen sind überall dort einzusetzen, wo große Werte zu schützen sind bzw. dort, wo andere Maßnahmen - z. B. geeignete Zutrittskontrolle zu den Arbeitsplätzen - nicht umgesetzt werden können, wie etwa bei Laptops im mobilen Einsatz. Diebstahl-Sicherungen machen außerdem dort Sinn, wo Publikumsverkehr herrscht oder die Fluktuation von Benutzern sehr hoch ist. Dabei sollte immer bedacht werden, dass die zu schützenden Werte nur zu einem kleinen Teil aus den Wiederbeschaffungskosten für das Gerät bestehen, sondern bei Laptops und ähnlichen IT-Systemen der Wert der darauf gespeicherten Daten berücksichtigt werden muss.

Mit Diebstahl-Sicherungen sollten je nach zu schützendem Objekt nicht nur das IT-System selber, sondern auch Monitor, Tastatur und anderes Zubehör ausgestattet werden.

Auf dem Markt sind die unterschiedlichsten Diebstahl-Sicherungen erhältlich. Diese können zunächst in mechanische und elektronische Sicherungen unterteilt werden.

Zu den mechanischen Sicherungen gehören unter anderem Kabelsicherungen, Gehäusesicherungen (um das Gehäuse gegen Öffnung zu schützen.), Sicherheitsplatten und Sicherheitsgehäuse. Es gibt hier zum einem Hardware-Sicherungen, die dem Diebstahl von IT-Geräten vorbeugen, z. B. durch das Verbinden des IT-Systems mit einem Schreibtisch. Es gibt zum anderen auch eine Reihe von Sicherungsmechanismen, die das Öffnen des Gehäuses verhindern sollen, um dem Diebstahl von Teilen oder der Manipulation von sicherheitsrelevanten Einstellungen wie dem Entfernen von Sicherheitskarten vorzubeugen.

Bei der Beschaffung mechanischer Sicherungen ist die Wahl eines guten Schlosses wichtig, das über eine auf die jeweiligen Bedürfnisse abgestimmte Schließanlage verfügt. Je nach Produkt sind verschiedene Schließanlagen möglich:

- gleichschließend: Ein Schlüssel passt auf alle Gerätesicherungen einer Institution, Abteilung, etc. Dies hat den Vorteil, dass der Aufwand für die Schlüsselverwaltung geringer ist. Es hat aber auch den Nachteil, dass sehr viele gleichartige Schlüssel im Umlauf sein können und dass im Schadensfall häufig keine Beweissicherung möglich ist.
- verschiedenschließend: Jede Gerätesicherung hat einen individuellen Schlüssel. Dies hat den Nachteil, dass der Aufwand für die Schlüsselverwaltung höher ist. Es hat aber den Vorteil, dass es weniger Schlüsseldubletten gibt.
- Hauptschlüsselsystem: Jede Gerätesicherung hat einen individuellen Schlüssel, kann zusätzlich aber auch durch einen Hauptschlüssel geöffnet werden. Dies hat den Vorteil, dass der Aufwand für die Schlüsselverwaltung geringer ist. Es hat aber den Nachteil, dass solche Systeme teurer in der Anschaffung sind.

Die meisten Notebooks - aber auch viele andere Geräte - haben einen kleinen Schlitz, welcher mit einem Ketten- oder Schloss-Symbol gekennzeichnet ist. Diese kleine Öffnung (ca. 3 x 7 mm) befindet sich seitlich oder hinten am Gerät. Es gibt eine breite Palette von Kabelsicherungen und anderen Produkten, welche diese Öffnung für die Sicherung von Geräten nutzt.

Bei Kabelsicherungen muss dann nur eine Kabelschlinge um ein solides Objekt in der Nähe des Gerätes gelegt, das zugehörige Schloss durch die entstandene Lasche gezogen und abgeschlossen werden.

Für Geräte, die diese Öffnung nicht haben - oder diese nicht stark genug ist - gibt es Sicherungsprodukte, bei denen eine stabile Platte auf das Gerät geklebt wird. An dieser wird dann das Sicherungskabel befestigt.

Daneben gibt es elektronische Sicherungen, die beispielsweise einen akustischen Abschreckungs-Alarm am Gerät selber auslösen, der potentielle Diebe dazu bringen soll, dass Gerät liegen zu lassen.

Bei Neuanschaffung von IT-Geräten sollte darauf geachtet werden, dass diese Ösen am Gehäuse besitzen, um sie an anderen Gegenständen befestigen zu können, und dass die Gehäuse abschließbar sind.

Ergänzende Kontrollfragen:

- Sind im letzten Jahr IT-Systeme oder IT-Komponenten gestohlen worden?
- Wie werden IT-Systeme oder IT-Komponenten vor Diebstahl geschützt?

M 1.47 Eigener Brandabschnitt

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Planer

Die Festlegung von Brandabschnitten ist für den Brandschutz eines Rechenzentrums von größter Wichtigkeit. Die Wirkung zuverlässiger Brand- und Rauchabschnitte hat sich bei vielen Großbränden eindrucksvoll bestätigt.

Die an Brandwände bzw. an die Größe der Brandabschnitte von Rechenzentren gestellten Anforderungen sollten über die in einschlägigen Normen, wie z. B. den Landesbauordnungen bzw. der DIN 4102, gestellten Forderungen hinaus gehen.

Schutzziel für die Brandwand bzw. den Brandabschnitt sollte nicht nur der Personen- und Gebäudeschutz, sondern auch der Schutz des Inventars und dessen Verfügbarkeit sein. Somit ist nicht nur die Brandausbreitung durch Flammenwirkung und heiße Rauchgase, sondern auch Wärmestrahlung und Ausbreitung von kaltem Rauch zu verhindern.

Die nach DIN 4102 noch zulässige Wärmestrahlung kann für die Gebäudeeinrichtung, insbesondere im wärmeempfindlichen IT-Bereich, bereits vernichtende Wirkung haben. Aus diesen Gründen sollten mehrere Brand- und Rauchabschnitte im Bauvorhaben realisiert werden, die so groß wie nötig und so klein wie möglich sind.

Für ein Rechenzentrum ist zu prüfen, inwieweit weitere interne Brandabschnitte geschaffen werden sollten. Sollte ein eigener Brandabschnitt für die Kerneinheiten (IT-Räume, Datenträgerarchiv) erforderlich sein, so müssen Wände, Türen und auch notwendige Wand- und Deckendurchbrüche den F90-Anforderungen genügen.

EN 1047-2 für die maximale Luftfeuchte beachten

Neben der baurechtlich erforderlichen Berücksichtigung der Norm DIN 4102 sollte für Rechenzentren, Serverräume und Datenträgerarchive die Norm EN 1047-2, speziell unter dem Aspekt der maximalen relativen Luftfeuchte (Abschnitt 4.1, Tabelle 1) beachtet werden.

Wenn der Brandabschnitt des Rechenzentrums z. B. Büroeinheiten beherbergt, so sind innerhalb des Brandabschnitts F30-Wände und T30-Türen zwischen diesen Büros und dem RZ-Kernbereich hinreichend. Die Büros sind dann in die Brandmeldeanlage mit einzubeziehen.

Es ist in der Planung und auch im Betrieb sicherzustellen, dass in solchen Räumen, die im Brandabschnitt des RZ liegen, keine besonderen Brandlasten vorhanden sind.

Ergänzende Kontrollfragen:

- Sind die Räumlichkeiten in sinnvolle Brandabschnitte unterteilt?

M 1.48 Brandmeldeanlage

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Planer

Neben der Aufstellung einer speziell auf den IT-Bereich zugeschnittenen Brandschutzordnung sowie von Alarm- und Einsatzplänen, ist die Installation einer Brandmeldeanlage von größter Wichtigkeit.

Da mehr als 90 % aller Brandschäden in Rechenzentren durch Feuer im Umfeld verursacht werden, empfiehlt es sich, diese Bereiche in die Überwachung durch die Brandmeldeanlage zu integrieren. Zum Einsatz sollten Puls- bzw. Trendmelder (optisches Streulichtprinzip) kommen.

Die Identifikation des auslösenden Melders muss möglich sein. Zur Lokalisierung des Brandherdes und der Brandausbreitung ist diese Identifikation der Brandmelder ein besonders wichtiges Hilfsmittel.

Eine empfehlenswerte Mindestkonfiguration einer Brandmeldeanlage in der Infrastruktur besteht aus

- Kanalmeldern in den Klimakanälen für Zuluft und Abluft
- Meldern in der Frischluftansaugung, mit automatischer Sperrung der Frischluft, wenn Störgrößen erkannt werden.

Alle Meldungen der Brandmeldeanlage und auch Störmeldungen sollten, sofern möglich, auf einer ständig besetzte Stelle, z. B. der Pförtnerloge, auflaufen.

Nach Möglichkeit sollte direkte Aufschaltung zur Berufsfeuerwehr erfolgen.

Beispiel:

Während einer Besprechung der Leitungsebene eines Rechenzentrums bemerkte ein Teilnehmer, der sich kurz in einem Nebenzimmer aufhielt, zufällig das Entstehen eines Großbrandes in einen nahegelegenen Chemiebetrieb. Sein Hinweis auf den Brand ermöglichte dem Leiter des Rechenzentrums, die Abschaltung der Frischluftzufuhr zu veranlassen. Nur wenige Minuten später wäre der rußige Brandrauch von der Ansaugung, die über keine Detektion verfügte, in die Rechnerräume befördert worden.

regelmäßige Überprüfung

Die Funktionsfähigkeit aller Komponenten einer Brandmeldeanlage muss regelmäßig überprüft werden. Auch wenn die Instandhaltung und Betrieb der Brandmeldeanlage über eine Wartungsfirma erfolgt, sollten zwei Mitarbeiter mit elementaren Grundfunktionen (zumindest mit allen Betriebszuständen und Statusmeldungen) der Anlage vertraut sein und als Ansprechpartner für die Wartungsfirma dienen.

Es sollten sporadisch einige der Melderlinien manuell auf ihre Funktionsfähigkeit getestet werden.

Ergänzende Kontrollfragen:

- Wann wurde die Funktionsfähigkeit der Brandmeldeanlage zuletzt überprüft?

M 1.49 Technische und organisatorische Vorgaben für das Rechenzentrum

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Planer

Ein Rechenzentrum sollte als geschlossener Sicherheitsbereich konzipiert sein. Dieser sollte möglichst nur eine Zugangstür und keine Fenster haben, da alle Zutrittsmöglichkeiten überwacht werden müssen (siehe auch M 1.10 *Verwendung von Sicherheitstüren und -fenstern*). Der Zutritt sollte durch hochwertige Zutrittskontrollmechanismen geschützt werden. Bei der Planung eines Rechenzentrums bzw. der Auswahl geeigneter Räumlichkeiten sollten potentielle Gefährdungen durch Umgebungseinflüsse möglichst minimiert werden. So ist Gefahrenpotentialen wie Wassereinbrüchen bei Flachdächern oder in Kellerräumen genauso zu begegnen wie EMV-Störquellen, z. B. Mobilfunk-Sendeeinrichtungen oder Drehstromaggregaten.

Einbruchsschutz

Ein angemessener baulicher und technischer Einbruchsschutz ist für ein Rechenzentrum unabdingbar. Empfehlungen hierzu sind in Maßnahme M 1.19 Einbruchsschutz und in der BSI-Publikation "IT-Sicherheit durch infrastrukturelle Maßnahmen" (siehe Anhang) aufgeführt.

Redundanz

Für die in Rechenzentren betriebenen IT-Komponenten wird in vielen Fällen ein hohes Maß an Verfügbarkeit gefordert. Diesen Anforderungen kann durch redundante Auslegung der infrastrukturellen und technischen Einrichtungen Rechnung getragen werden (siehe Maßnahme M 1.52 *Redundanzen in der technischen Infrastruktur*).

Trennung von Grob- und Feintechnik

Um eine Mischung zwischen der Grobtechnik (Energieversorgung, Klimatechnik) und der Feintechnik (Rechner) im Rechenzentrum zu vermeiden, sollten getrennte Raumeinheiten geplant werden. Die technische Infrastruktur des Rechenzentrums ist in separaten Räumen zu installieren. In Rechenzentren hoher Verfügbarkeit dürfen bei der Schutzkonzeption die kommunikations- bzw. nachrichtentechnischen Komponenten "nach draußen" nicht außer acht gelassen werden. Ist ihr Schutz nicht im gleichen Maß, wie der der technischen Kernkomponenten sichergestellt, ist die Verfügbarkeit nicht gewährleistet. Beispielweise ist zu beachten, dass der Schutzbedarf der aktiven Netzkomponenten, die an der Außenkommunikation beteiligt sind (wie Router und Switches), dem Schutzbedarf der Kernbereiche des Rechenzentrums entspricht. Dies betrifft sowohl den materiellen Schutz, als auch Detektion, Meldung und Alarmierung.

Wünschenswert wäre es, wenn die Gewerke für

- Nachrichtentechnik,
- Klimatisierung und Lüftung
- Energieversorgung,
- Lager usw.

jeweils in einem eigenen Raum (optional auch eigenen Brandabschnitt) untergebracht werden.

Versorgungsleitungen vermeiden

Bei der Planung sollte auch darauf geachtet werden, dass die Trassen der Versorgungsleitungen des Gebäudes, z. B. für Wasser oder Gas, (siehe M 1.24 *Vermeidung von wasserführenden Leitungen*) nicht in unmittelbarer Nähe oder gar durch sensible Bereiche des Rechenzentrums verlaufen.

Zutritt nur für Administratoren

Ein Rechenzentrum ist ein sicherheitsrelevanter Bereich, daher sollten dort nur die Administratoren der dort aufgestellten IT-Systeme Zutritt haben. Durch eine darauf abgestimmte Zutrittsregelung muss für eigene Mitarbeiter und wichtiger noch für nur zeitweilig Beschäftigte, z. B. zu Wartungsarbeiten im Rechenzentrum tätige, sichergestellt werden, dass sie keinen Zugriff auf Systeme außerhalb ihres Tätigkeitsbereiches erhalten.

Es sollte verboten werden, in ein Rechenzentrum tragbare IT-Systeme, Mobiltelefone oder Kameras mitzubringen, wenn diese nicht unter der Kontrolle der jeweiligen Institution stehen. Generell sollte der Betrieb von Mobiltelefonen in Rechenzentren untersagt werden, da diese den Betrieb der IT-Systeme erheblich stören können. Ausnahmen hiervon müssen abgestimmt sein (siehe M 2.188 *Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung)*.

Bei der Planung von Umbau- oder Neubaumaßnahmen eines Rechenzentrums sollten die im folgenden beschriebenen Parameter berücksichtigt werden.

In der Praxis hat sich für einen Rechnersaal ein Seitenverhältnis von 1:1 bis maximal 2:3 als günstig erwiesen. Diese Aufteilung erleichtert die strukturierte Anordnung von IT-Komponenten und deren Verkabelung im Rechenzentrum.

Sofern die baulichen Gegebenheiten es zulassen, ist die Installation eines Doppelbodens empfehlenswert. Seine Höhe ist abhängig von der technischen Ausstattung und Nutzung. Wenn der Doppelboden zur Klimatisierung genutzt wird, sollte er ca. 50 cm Höhe haben.

Bei der Bemaßung von IT-Räumen sind mindestens folgende Rahmenmaße empfehlenswert:

Lichte Raumhöhe ab Doppelboden:	3,00 m
Stützenabstände	6,00 m
Rohbaumaß Türenbreite	1,10 m
Rohbaumaß Türenhöhe	2,10 m

Decken und Doppelböden sollten auf eine Traglast von mindestens 1000 kg/m2 ausgelegt sein.

Der Doppelboden muss eine hohe Passgenauigkeit und ab einer Höhe von 20 cm eine Brandschutzqualität von F30 in geschlossenem Zustand aufweisen. Generell sollten die Sicherheitsrichtlinien für Doppelböden vom Bundesverband Systemböden e. V., Düsseldorf beachtet werden.

Hinweis: Die Doppelböden und abgehängten Decken müssen mit dem IT-Raum abschließen. Es dürfen durch solche Konstruktionen keine ungesicherten Zugänge geschaffen werden.

Flure sollten mindestens eine Breite von 1,80 m aufweisen und mit rutschfesten, glatten Bodenbelägen, die höheren Transportlasten widerstehen, ausgelegt sein.

Aufzüge als vertikale Transportwege innerhalb des Rechenzentrums sollten eine Tragkraft von mindestens 1500 kg haben. Die lichten Kabineninnenmaße sollten mindestens 2,80 m in der Tiefe, 1,50 m in der Breite und 2,20 m in der Höhe betragen.

Ergänzende Kontrollfragen:

- Gibt es technische und organisatorische Vorgaben für das Rechenzentrum?
- Ist das Rechenzentrum als geschlossener Sicherheitsbereich konzipiert worden?
- Ist der Zutritt zum Serverraum geregelt?
- Wurde bei der Planung auf eine ausreichende Trennung der Grob- und Feintechnik geachtet?

M 1.50 Rauchschutz

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Planer

Rauch stellt bei Bränden die größte Personengefährdung dar. Mehr als 90 % der Brandtoten sind durch Raucheinwirkungen (Vergiftungen) zu beklagen. Aber auch die IT-Hardware kann durch Rauch erheblich in Mitleidenschaft gezogen werden. Daher ist auf einen umfassenden Rauchschutz Wert zu legen.

Die folgenden Empfehlungen sollten zum Rauchschutz berücksichtigt werden:

- Brandschutztüren sollten Rauchschutzqualität aufweisen.
- Rauchschutztüren in Fluren sollten durch Rauchschalter gesteuert werden. Solche Türen können immer offen stehen, da sie bei Rauchdetektion selbsttätig schließen. **Rauchschutztüren**
- Die Lüftungsanlage bzw. die Klimaanlage sollte eine Entrauchung von IT-Räumen gestatten.
- In Klimakanälen (Zu- und Abluft) sollten Kanalmelder installiert sein. **Kanalmelder**
- In der Frischluftansaugung sollten Melder installiert sein, die automatisch diese sperren, wenn Störgrößen (Rauch) erkannt werden.

Die Mitarbeiter müssen unterrichtet werden, welche Warnsignale die Rauchschutz-Komponenten haben und wie sie darauf zu reagieren haben.

Die Funktionsfähigkeit aller Rauchschutz-Komponenten muss regelmäßig überprüft werden.

Ergänzende Kontrollfragen:

- Wann wurde die Funktionsfähigkeit der Rauchschutz-Komponenten zuletzt überprüft?

M 1.51 Brandlastreduzierung

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Planer, Leiter IT, Leiter Haustechnik

Hohe Brandlasten entstehen z. B. durch die Konzentration von IT-Systemen, falsche Auswahl von Baumaterialien, leicht brennbare Büroausstattung und große Papiermengen. In vielen Fällen können solche Brandlasten auf einfache Weise vermieden werden.

Bei Rechenzentren - ebenso wie bei anderen Gebäuden - sollte bereits in der Planungsphase die Reduzierung unnötiger Brandlasten berücksichtigt werden. Nicht brennbare Materialien sind für den Ausbau zu bevorzugen (Baustoffklasse A).

Um den sicheren Betrieb unter Gesichtspunkten des Brandschutzes zu gewährleisten und Grenzwerte nicht zu überschreiten, sollte schon in der Planungsphase eine überschlägige Berechnung der späteren Brandlasten erfolgen. Dabei sind die Brandklassen der Einrichtungen bzw. der Baustoffklassen der Materialien zu berücksichtigen. Dadurch werden später Schwierigkeiten bei der brandschutztechnischen Abnahme durch Bauaufsichtsbehörden und Feuerwehr vermieden.

Andererseits ist im laufenden Rechenzentrums-Betrieb dafür Sorge zu tragen, dass beispielsweise Brandlasten im Doppelboden in Form von nicht mehr benötigten Kabeln entfernt werden.

Aus Büroräumen sollten nicht mehr benötigte Akten entfernt und in speziell dafür vorgesehenen Archiven gelagert werden.

Eine der häufigsten Beispiele für unnötige Brandlasten in Räumen, die für die IT genutzt werden, ist Verpackungsmaterial, beispielsweise Pappe oder Styropor. Aus den IT-Räumen ist Verpackungsmaterial umgehend zu entfernen und in dafür vorgesehene Lagerräume zu transportieren, wenn es noch benötigt wird.

Ergänzende Kontrollfragen:

- Wird regelmäßig überprüft, ob sich Brandlasten in den genutzten Räumlichkeiten anhäufen?

M 1.52 Redundanzen in der technischen Infrastruktur

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Planer

Bestehen besondere Anforderungen an die Verfügbarkeit eines Rechenzentrums bzw. eines Serverraums, so sind Redundanzen auch im Bereich der technischen Infrastruktur zu schaffen.

N+1 Prinzip

Es bietet sich beispielsweise an, beim Einsatz von Klimaanlagen ausreichend Redundanz vorzuhalten. Werden beispielweise von einer Komponente 6 Stück benötigt, so sollten 7 beschafft werden. Damit können Lastspitzen, z. B. in heißen Sommern abgefangen werden und auch bei Ausfall eines Gerätes oder bei Wartungsarbeiten bleibt die Verfügbarkeit der Klimatisierung insgesamt erhalten.

Auch für Kommunikationsverbindungen sollte geprüft werden, in welchen Bereichen Redundanzen vorgehalten werden müssen (siehe auch M 6.18 *Redundante Leitungsführung*). Dies gilt um so mehr, wenn sich zentrale Netzknoten oder zentrale aktive Komponenten in unkontrollierten Bereichen befinden.

In einem Rechenzentrum ist auch die Stromversorgung redundant auszulegen. Empfehlungen hierzu finden sich in Maßnahme M 1.56 *Sekundär-Energieversorgung*.

Falls sich die sekundäre Stromversorgung nicht in einem angrenzenden Brandabschnitt befindet, sollte über eine redundante Verkabelung der Stromversorgung nachgedacht werden.

Ergänzende Kontrollfragen:

- Ergibt sich aus der Schutzbedarfsfeststellung die Notwendigkeit von Redundanzen in der technischen Infrastruktur?

M 1.53 Videoüberwachung

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Planer

Die Maßnahmen zur Außenhautsicherung (siehe M 1.55 Perimeterschutz) und Zutrittskontrolle können durch den Einsatz von Videotechnik ergänzt werden. Videoüberwachungsanlagen, ob eigenständig oder ergänzend zu anderen Sicherheitstechniken, werden zur Erreichung folgender Schutzziele eingesetzt:

- Abschreckung
- Fassadenüberwachung
- Identifizierung
- Überwachung
- Alarmierung
- Erkennung und Lokalisierung von Gefahren
- Schadenverhütung
- Dokumentation und Auswertung von Regelabweichungen

Bei der Planung einer Videoüberwachung ist auf eine konsistente Einbettung in das gesamte Schutzkonzept zu achten. Dies gilt umso mehr, wenn die Überwachungsterminals weit vom zu schützenden Bereich entfernt sind. Eine Videoüberwachung ohne Auswertungs- und Alarmierungsmechanismen macht außer zur Abschreckung keinen Sinn. Die benötigten zentralen Technikkomponenten sind in geeigneter Umgebung aufzustellen und zu schützen.

Bei der Planung bzw. Installation einer Videoüberwachung sollte der Datenschutzbeauftragte und der Personal- bzw. Betriebsrat hinzugezogen werden.

Ergänzende Kontrollfragen:

- Ist die Videoüberwachung konsistent in das Schutzkonzept eingebettet?
- Wird die Funktionsfähigkeit der Videoüberwachungsanlage regelmäßig überprüft?

M 1.54 Brandfrühesterkennung / Löschtechnik

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Planer

Bei entstehenden Bränden in IT-Anlagen kann das Wegschalten der elektrischen Energie bereits ausreichend sein, um den Brand zu verzögern oder zu beenden.

Für die Überwachung von IT-Systemen kann eine objektbezogene Überwachung durch sogenannte Multidetektoren vorgenommen werden. In Ergänzung der konventionellen Brandmeldetechnik (geometrische Raumüberwachung) stellt die Objektüberwachung (also die Überwachung innerhalb einzelner IT-Komponenten) eine zusätzliche Melderebene dar. Diese Multidetektoren können sowohl für eine objektbezogene Löschung als auch für die Abschaltung der Stützenergie des betroffenen Gerätes herangezogen werden.

Wenn eine zusätzliche Löschung als notwendig anzusehen ist, bietet es sich aus Kosten- und Personenschutz-Gründen an, nur einzelne Objekte (z. B. 19 Zoll Schränke) mit Löschgasen individuell abzusichern. Die Objektschutzanlagen sollten sich an der VdS-Richtlinie 2304 bezüglich Planung, Brandmeldung, Löschung orientieren sowie an den Einbauhinweisen der Hersteller und deren Vorgaben für den Betrieb und die Instandhaltung.

Für die Raumüberwachung im IT-Bereich eignet sich die Installation von optischen Rauchmeldern. Auch der Doppelboden sollte durch ebensolche Rauchmelder überwacht werden

Bestehen besondere Anforderungen an die Verfügbarkeit eines Rechenzentrums bzw. Serverraums oder beinhalten diese besonders hochwertige oder schwer nachzubeschaffende IT-Komponenten, ist der Einsatz einer automatischen Löschanlage mit Inertgasen (Kohlendioxid, Inergen, Argon, Stickstoff, FM 200, etc.) zu erwägen.

Erstickungsgefahr bei Löschgasen

Der Erstickungseffekt für Flammen gilt ebenso für Menschen, wenn sauerstoff-verdrängende Löschgase eingesetzt werden. So besteht bei einer Kohlendioxid-Konzentration von mehr als 8 Volumenprozent akute Lebensgefahr. Daher fordern in der Bundesrepublik Deutschland die berufsgenossenschaftlichen Richtlinien (ZH 1/206 Sicherheitsregeln für Kohlendioxid-Feuerlöschanlagen vom April 1988) den Einsatz von Verzögerungseinrichtungen, "wenn die Einsatzmenge bezogen auf das Gesamtvolumen des Raumes, in dem das geschützte Objekt untergebracht ist, eine höhere Löschkonzentration als 5 Volumenprozent herbeiführt".

Die Planung einer Löschgasanlage sollte grundsätzlich nur durch einen Fachplaner erfolgen.

Ergänzende Kontrollfragen:

- Wie wird sichergestellt, dass Brände so früh wie möglich erkannt werden?

M 1.55 Perimeterschutz

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Planer

Falls das Gebäude oder Rechenzentrum innerhalb eines Grundstücks liegt, auf dem zusätzliche Sicherheitseinrichtungen installiert werden können, sollten Maßnahmen ergriffen werden, um von außen wirkende Gefährdungen vom Rechenzentrum abzuhalten.

Insbesondere kann hier die erste Stufe einer Zutritts- und vor allem Zufahrtsregelung geschaffen werden.

Je nach Schutzbedarf und topologischen Gegebenheiten kann ein Perimeterschutz aus folgenden Komponenten bestehen:

- Äußere Umschließung oder Umfriedung, z. B. Zaunanlage, Mauerwerk und Zaunüberwachung

  Äußere Umfriedung

  Dies bietet

  - Schutz gegen unbeabsichtigtes Überschreiten einer Grundstücksgrenze,
  - Schutz gegen beabsichtigtes gewaltloses Überwinden der Grundstücksgrenze sowie
  - Schutz gegen beabsichtigtes gewaltsames Überwinden der Grundstücksgrenze.

- Freiland-Sicherungsmaßnahmen, z. B. Geländegestaltung, Zufahrtssperren, Beleuchtung des Geländes und des Gebäudes, Bewachungsunternehmen, Videoüberwachung und Detektionssensorik auf dem Gelände

  Freiland-Sicherungsmaßnahmen

  Dies bietet Schutz gegen unbemerkten Zutritt eines Eindringlings für die Fläche zwischen Umfriedung und Gebäude.

- Äußere Personen- und Fahrzeugidentifikation, z. B. Videogegensprechanlage, Personen- bzw. Fahrzeugschleuse, Tür- bzw. Toröffnung und Zutrittskontrolleinheiten

  Personen- und Fahrzeugkontrollen

  Dies bietet Schutz gegen erkennbar (visuell, akustisch oder sensorisch) unberechtigte Zutrittsversuche als erste Stufe des Zutrittskontrollkonzeptes. Diese Aufgabe kann durch einen Pförtnerdienst unterstützt werden (siehe auch M 1.17 *Pförtnerdienst*).

Bevor Maßnahmen aus dem Bereich Perimeterschutz realisiert werden, muss in jedem Fall ein stimmiges Schutzkonzept erarbeitet werden, das die oben genannten Aspekte und den Gebäudeschutz umfasst. Anderenfalls besteht die Gefahr, dass vergleichsweise teure Sicherheitsmaßnahmen umgesetzt werden, beispielsweise aufwändige Zaunanlagen und ausgefeilte Gelände-Videoüberwachung, die in keinem Verhältnis zur Gebäudesicherung stehen und daher nicht angemessen sind.

Das Schutzkonzept sollte darauf ausgerichtet sein, mit den zur Verfügung stehenden Ressourcen möglichst wirksame Schutzmaßnahmen aufzubauen. Dies betrifft besonders den Bereich Perimeterschutz. Die hier ergriffenen Maßnahmen sollten die Gesamtsicherheit erhöhen und nicht nur das Image einer "Hochsicherheitskulisse" vermitteln, da sich qualifizierte Angreifer allein durch den Anblick von hohen Zäunen und Videoüberwachung kaum von ihrem Vorsatz abbringen lassen.

Beispiel:

Wenn ein Angreifer zwei Minuten benötigt, um den Weg über den Zaun bis zum Gebäude zu nehmen und anschließend nur eine halbe Minute für das Eindringen ins Gebäude, stimmt die Relation nicht. Dies gilt um so mehr, wenn das Eintreffen von Einsatzkräften der örtlichen Polizei nach Alarmierung durch ein privates Bewachungsunternehmen beispielsweise acht Minuten dauert. In dieser Zeit könnte ein Einbrecher schon wieder nach vollbrachter Tat das Gelände verlassen haben. Er wäre zwar bemerkt und auf Videomaterial aufgenommen worden, bei geeigneter Maskierung jedoch kaum zu identifizieren.

Ergänzende Kontrollfragen:

- Gibt es ein Schutzkonzept, das sowohl den Perimeterschutz als auch den Gebäudeschutz umfasst?

M 1.56 Sekundär-Energieversorgung

Verantwortlich für Initiierung: Leiter Haustechnik, Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Haustechnik

Die primäre Energieversorgung aus dem Netz eines Energieversorgungs-Unternehmens (EVU) muss bei erhöhten Anforderungen an die Verfügbarkeit um Maßnahmen zur Notfall-Versorgung des Rechenzentrums selbst ergänzt werden. Dabei sollte auch nicht weitere wichtige Infrastruktur des Gebäudes, wie z. B. die Notbeleuchtung und die Feuerwehr-Aufzüge, vergessen werden.

Die Sekundär-Energieversorgung eines Rechenzentrums besteht dann üblicherweise aus einer zentralen USV für das Rechenzentrum und einer Netzersatzanlage (NEA). Falls die örtlichen Gegebenheiten und das Anforderungsprofil an die Verfügbarkeit des Rechenzentrums es zulassen, kann statt einer NEA auch eine zweite Einspeisung aus dem Netz eines zweiten Energieversorgungs-Unternehmens diese Auffang-Funktion erfüllen.

Während eine Online-USV (siehe M 1.28 *Lokale unterbrechungsfreie Stromversorgung*) Schwankungen oder kurzfristige Unterbrechungen der Stromversorgung überbrückt, fängt eine Netzersatzanlage außerdem längerfristige Stromausfälle auf.

Der gesamten IT-Umgebung wird eine zentrale Online-USV vorgeschaltet. Die Regel-Elektronik dieser USV muss für das frequenz- und phasenrichtige Einkoppeln bei Anlauf der Netzersatzanlage und nach Wiederanlauf der Stromversorgung des EVU sorgen.

Bei der Dimensionierung der Notstromaggregate sollte darauf geachtet werden, dass die Nennleistung des Netzersatzes über der Volllast-Betriebsleistung des Rechenzentrums liegen sollte. Damit kann sichergestellt werden, dass die Netzersatzanlage, z. B. bei gleichzeitigem Anlauf mehrerer Verbraucher, die benötigte Leistung zur Verfügung stellen kann.

Bei der Übergabe der Versorgung von der USV an die NEA ist sicherzustellen, dass eine schrittweise Weiterschaltung ohne Überlastung der NEA und daraus resultierendem Wiederanlauf der USV erfolgt. Dabei müssen die individuellen Anforderungen der IT-Infrastruktur und der sonstigen von der NEA versorgten Gebäudeteile mit Hilfe eines abgestimmten Lastmanagements berücksichtigt werden.

Für die Dimensionierung der Batterien der zentralen USV ist die Überbrückungszeit bei Netzausfall entscheidend. Diese setzt sich aus folgenden Faktoren zusammen:

- Wartezeit auf Netzrückkehr. Erst nach dieser Wartezeit von 1 bis 5 Minuten läuft die NEA an.
- Umschaltzeit bis zur Lastübernahme durch die NEA. In dieser Zeit versorgt die USV alle Verbraucher der IT-Anlage mit Strom.

- Zeit mit verminderter Leistungsabnahme. Bei Absinken der Batterieladekapazität sollte eine verminderte Leistungsabnahme eingeleitet werden. Hierzu müssen unkritischere Verbraucher vom Netz genommen werden.
- Zeit mit Leistungsabnehmer für notwendige kritische Verbraucher. Bei weiterem Absinken der Batteriekapazität dürfen nur noch die wichtigsten Leistungsverbraucher mit Strom versorgt werden. Spätestens hier muss automatisch ein Not-Shutdown mit kontrollierter Zwangsabschaltung des IT-Betriebes erfolgen, auch wenn reversible Datenverluste dabei in Kauf genommen werden müssen.

Um die Schutzwirkung der Sekundär-Energieversorgung aufrechtzuerhalten, ist eine regelmäßige Wartung vorzusehen.

Ergänzende Kontrollfragen:

- Werden die Wartungsintervalle von USV und NEA eingehalten?
- Werden die USV und die NEA in regelmäßigen Testläufen unter realistischer Belastung auf Funktionsfähigkeit geprüft?
- Wird der Tankinhalt bei dieselbetriebenen NE-Anlagen regelmäßig kontrolliert?

M 1.57 Aktuelle Infrastruktur- und Baupläne

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Planer

Baupläne, Fluchtwegpläne, Feuerwehrlaufkarten etc. (siehe auch M 1.11 *Lagepläne der Versorgungsleitungen* und M 5.4 *Dokumentation und Kennzeichnung der Verkabelung*) sollten umgehend nach jeder Umbaumaßnahme, Erweiterung der Infrastruktur und Sicherheitstechnik auf den aktuellen Stand gebracht werden.

Dies ist erforderlich, um

- das definierte Sicherheitsniveau halten,
- Notfallsituationen optimal begegnen,
- Revisionen erleichtern und
- Maßnahmen vollständig und angemessen planen und durchführen zu können.

Es ist nicht ausreichend, die Pläne beispielsweise nur bei der zuständigen Bauverwaltung zu lagern. Im Schadens- oder Notfall, z. B. bei Kabelschäden oder Wasserrohrbrüchen kann wichtige Zeit für die Fehlerlokalisierung und -beseitigung verloren gehen. Derjenige, der die Pläne verwaltet, z. B. im Hausdienst, sollte auch in der Lage sein, sie zu lesen. Gegebenenfalls ist Personal entsprechend zu schulen und einzuweisen.

Ergänzende Kontrollfragen:

- Wurde der Architekt oder der Standortplaner bei Umbaumaßnahmen auch mit der Aktualisierung der Pläne beauftragt?

M 1.58 Technische und organisatorische Vorgaben für Serverräume

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Ein Serverraum sollte als geschlossener Sicherheitsbereich konzipiert sein. Dieser sollte möglichst gut zu sichernde Zugangstüren und Fenster haben, da alle Zutrittsmöglichkeiten überwacht werden müssen (siehe auch M 1.10 *Verwendung von Sicherheitstüren und -fenstern*). Der Zutritt sollte durch hochwertige Zutrittskontrollmechanismen geschützt werden. Bei der Planung eines Serverraumes bzw. der Auswahl geeigneter Räumlichkeiten sollten potentielle Gefährdungen durch Umgebungseinflüsse möglichst minimiert werden. So ist Gefahrenpotentialen wie Wassereinbrüchen bei Flachdächern oder in Kellerräumen genauso zu begegnen wie EMV-Störquellen, z. B. Mobilfunk-Sendeeinrichtungen oder Drehstromaggregaten.

Versorgungsleitungen vermeiden

Bei der Planung sollte auch darauf geachtet werden, dass die Trassen der Versorgungsleitungen des Gebäudes, z. B. für Wasser oder Gas (siehe M 1.24 *Vermeidung von wasserführenden Leitungen*), nicht in unmittelbarer Nähe oder gar durch sensible Bereiche des Serverraums verlaufen.

Für die in Serverräumen betriebenen IT-Komponenten wird in vielen Fällen ein hohes Maß an Verfügbarkeit gefordert. Diesen Anforderungen kann durch redundante Auslegung der infrastrukturellen und technischen Einrichtungen Rechnung getragen werden (siehe Maßnahme M 1.52 *Redundanzen in der technischen Infrastruktur*).

Zutritt nur für Administratoren

Ein Serverraum ist ein sicherheitsrelevanter Bereich, daher sollten dort nur die Administratoren der dort aufgestellten IT-Systeme Zutritt haben. Durch eine darauf abgestimmte Zutrittsregelung muss für eigene Mitarbeiter und wichtiger noch für nur zeitweilig Beschäftigte, z. B. zu Wartungsarbeiten tätige, sichergestellt werden, dass sie keinen Zugriff auf Systeme außerhalb ihres Tätigkeitsbereiches erhalten.

IT-Systeme, die von Externen betreut werden, sollten in separaten Räumen aufgestellt werden. Es ist außerdem zu überlegen, IT-Systeme mit unterschiedlichem Schutzbedarf oder aus verschiedenen Bereichen in getrennten Serverräumen aufzustellen, um den Kreis der Zutrittsberechtigten klein zu halten.

In einem Serverraum sollten sich auf keinen Fall Geräte oder Ausrüstung befinden, die den Zutritt für einen großen Benutzerkreis erforderlich machen, also z. B. Fax-Geräte oder Fotokopierer. Brennbare Materialen wie Druckerpapier sollten ebenfalls nicht in einem Serverraum gelagert werden.

Es sollte verboten werden, in einen Serverraum tragbare IT-Systeme, Mobiltelefone oder Kameras mitzubringen, wenn diese nicht unter der Kontrolle der jeweiligen Institution stehen. Generell sollte der Betrieb von Mobiltelefonen in Rechenzentren untersagt werden, da diese den Betrieb der IT-Systeme erheblich stören können. Ausnahmen hiervon müssen abgestimmt sein (siehe M 2.188 *Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung)*.

Ergänzende Kontrollfragen:

- Gibt es technische und organisatorische Vorgaben für Serverräume?
- Sind die Serverräume als geschlossene Sicherheitsbereiche konzipiert worden?
- Ist der Zutritt zum Serverraum geregelt?

M 1.59 Geeignete Aufstellung von Speicher- und Archivsystemen

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator

Aufstellungsort absichern

Da in Speicher- und Archivsystemen wichtige Behörden- bzw. Unternehmensdaten konzentriert aufbewahrt werden, müssen deren IT-Komponenten in gesicherten Räumen aufgestellt werden, zu denen nur Berechtigte Zutritt haben. Dies betrifft neben den eingesetzten Servern und Netzkomponenten insbesondere die Speichereinheiten (Plattenarrays, Bandlaufwerke, Disc-Jukeboxen).

Für die geeignete Aufstellung dieser IT-Komponenten sind alle relevanten Maßnahmen, die in den IT-Grundschutz-Katalogen zur Infrastruktur-Sicherheit beschrieben sind, zu realisieren. Je nach Art und Größe des Speicher- oder Archivsystems sind die Bausteine B 2.1 *Gebäude*, B 2.9 *Rechenzentrum*, B 2.4 *Serverraum* bzw. B 2.7 *Schutzschränke* heranzuziehen. Hierbei sollte besonders auf eine ausreichende Zuverlässigkeit der infrastrukturellen Komponenten (Stromzufuhr, etc.) geachtet werden. Beim Einsatz von Speichersystemen sind zudem angemessene Redundanzen in der technischen Infrastruktur zu schaffen (siehe M 1.52 *Redundanzen in der technischen Infrastruktur*), um die Verfügbarkeit dieser zentralen Ressourcen so gut wie möglich zu unterstützen.

Für die langfristige Aufbewahrung der verwendeten Archiv-Speichermedien sind die in M 1.60 *Geeignete Lagerung von Archivmedien* genannten Lagerbedingungen einzuhalten. Vor allem die zweckmäßige Klimatisierung von Speichermedien, aber auch der Archivsysteme selbst ist hier zu beachten.

Lagerbedingungen in Speicherkomponenten

Häufig werden elektronische Archive so realisiert, dass Archivmedien im dauerhaften Zugriff durch die Speichereinheit gehalten werden. Hierzu kommen vielfach dedizierte Speichereinheiten zum Einsatz, die selbsttätig Wechselmedien verwalten und einlegen können, beispielsweise Roboter für Bandlaufwerke oder Jukeboxen für Disc-Medien. Wenn ein Speicher- oder Archivsystem solche Komponenten beinhaltet, werden in der Regel die Archivmedien während ihrer gesamten Lebensdauer nicht mehr aus der Speichereinheit ausgelagert. Das bedeutet, dass die an Archivmedien zu stellenden Lagerbedingungen (bezüglich Klimatisierung, Zugriffsschutz, etc.) bereits in der Speicherkomponente erfüllt und überwacht werden müssen.

Bei Auswahl des Speicher- oder Archivsystems ist daher als Kriterium zu berücksichtigen, dass die erforderlichen Lagerbedingungen für Archivmedien in Speicherkomponenten eingehalten werden können bzw. welcher Zusatzaufwand hierfür entsteht.

Ergänzende Kontrollfragen:

- Sind die IT-Grundschutzmaßnahmen für den Aufstellungsort des Speichersystems oder des elektronischen Archivs realisiert?
- Sind die Lagerbedingungen für Archivmedien bekannt und dokumentiert?
- Werden die Lagerbedingungen für Archivmedien in den verwendeten Dauer-Speichereinheiten eingehalten?

M 1.60 Geeignete Lagerung von Archivmedien

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator

Für den Langzeiteinsatz von Archivmedien sind besonders der Zugriffsschutz sowie klimatische Lagerbedingungen zu beachten und deren Einhaltung zu überwachen.

Online-Zugriff

Sofern Archivmedien im Online-Zugriff, also im Archivsystem bzw. in Speicherlaufwerken gehalten werden, ist keine räumliche Trennung zwischen Archivsystem und Archivmedium realisierbar. Für die geeignete Lagerung von Archivmedien sind damit die in M 1.59 *Geeignete Aufstellung von Speicher- und Archivsystemen* genannten Empfehlungen umzusetzen.

Offline-Lagerung

Wenn Archivmedien außerhalb des Archivsystems "offline" gelagert werden, so sind die im Baustein B 2.5 *Datenträgerarchiv* beschriebenen Maßnahmen unter besonderer Berücksichtigung der Anforderungen an die Klimatisierung anzuwenden.

Klimatisierung

Die klimatischen Anforderungen an die Haltbarkeit von Archivmedien hängen von den eingesetzten Archivmedien ab. Hersteller geben hierzu vereinzelt unverbindliche Hinweise zu den Lagerbedingungen (z. B. hinsichtlich der Temperatur und Luftfeuchte) und zur Haltbarkeit der Medien an.

Für den langfristigen Einsatz elektronischer Archivsysteme müssen die konkreten Lagerbedingungen jedoch von den Herstellern der eingesetzten Archivmedien verbindlich erfragt werden. Da hiervon die Haltbarkeit der Archivmedien abhängt, sollten folgende Punkte vor der Auswahl der verwendeten Archivmedien geklärt werden (siehe auch M 4.169 *Verwendung geeigneter Archivmedien*):

Herstellerangaben einfordern

- Die klimatischen und physikalischen Lagerbedingungen für die betrachteten Archivmedien sollten seitens des Herstellers ausreichend detailliert beschrieben sein (inklusive der Auswirkungen auf die maximale Lebensdauer). Diese Angabe sollte verbindlich sein, möglichst mit einer Garantieerklärung des Herstellers bei Einhaltung der Lagerbedingungen.

technische Realisierbarkeit prüfen

- Die technische Realisierung einer geeigneten Lagerung kann unter Umständen sehr komplex sein. Je nach den vorhandenen technischen und infrastrukturellen Vorgaben können bestimmte Archivmedien auch gänzlich ungeeignet sein. Daher müssen im Vorfeld die Möglichkeit und der Aufwand für die technische Realisierung einer geeigneten Lagerung geprüft werden.

Die Lagerbedingungen sollten im Betriebshandbuch des Archivsystems dokumentiert werden. Zusätzlich muss sichergestellt werden, dass die Lagerbedingungen kontinuierlich eingehalten und überwacht werden (siehe auch M 1.27 *Klimatisierung*).

Physikalische Schutzmaßnahmen

Über die klimatischen Bedingungen hinaus müssen die verwendeten Archivmedien vor unautorisiertem Zugriff und mechanischer Beschädigung oder

Veränderung geschützt werden. Hierzu wird insbesondere auf die im Baustein B 2.5 *Datenträgerarchiv* genannten Maßnahmen verwiesen.

Zutrittskontrolle

Neben einer Kontrolle des Zutritts zum Datenträgerraum, Brandschutz und Schutz vor Wassereinwirkung sind je nach Art der verwendeten Archivmedien weitere Maßnahmen zu realisieren, z. B. zum Schutz vor Einwirkung von Magnetfeldern auf Magnetbänder.

Hierfür sind verbindliche Empfehlungen von Herstellern zu mechanischen Lagerbedingungen einzuholen und zu beachten.

Alarmierung und Reaktion

Bei Nichteinhaltung der Lagerbedingungen muss eine Alarmierung und Reaktion erfolgen. Hierzu sind organisationsspezifisch Eskalationsprozeduren und -wege zu definieren.

Ergänzende Kontrollfragen:

- Bestehen verbindliche Herstelleraussagen zu klimatischen und physikalischen Lagerbedingungen?
- Können die vom Hersteller empfohlenen klimatischen und physikalischen Lagerbedingungen eingehalten werden?
- Sind die Lagerbedingungen im Betriebshandbuch des Archivsystems dokumentiert?
- Bestehen Eskalationsprozeduren bei Nichteinhaltung der Lagerbedingungen?

M 1.61 Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Benutzer, Vorgesetzte

Verantwortlich für Umsetzung: Benutzer

Dank immer kleinerer und leistungsfähigerer IT-Systeme ist es heutzutage möglich, nahezu überall zu arbeiten. Dadurch kann jede beliebige Umgebung zu einem mobilen Arbeitsplatz werden, also beispielsweise ein Hotelzimmer, der Sitzplatz in Eisenbahn oder Flugzeug oder eine Räumlichkeit beim Kunden. Solche mobilen Arbeitsplätze können vom IT-Benutzer leider nur sehr beschränkt eingerichtet werden und müssen im Allgemeinen so genutzt werden, wie sie vorgefunden wurden. Daher ist immer zuerst von jedem mobilen IT-Benutzer zu entscheiden, ob die jeweilige Umgebung geeignet ist, um als mobiler Arbeitsplatz genutzt zu werden. Gründe, die dagegen sprechen könnten, sind beispielsweise die folgenden:

- Die zu bearbeitenden Informationen sind zu sensibel, um außerhalb der geschützten Büroumgebung bearbeitet zu werden (siehe auch M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen* und M 2.218 *Regelung der Mitnahme von Datenträgern und IT-Komponenten*).
- Die Umgebung erlaubt es nicht, ohne Einsichtnahme Dritter zu arbeiten, z. B. bei engen Sitzplätzen in der Bahn oder dem Flugzeug.
- Es ist keine Stromversorgung oder keine Netzanbindung vorhanden.
- Die Nutzung von mobilen IT-Geräten ist verboten, z. B. im Flugzeug oder in fremden Büros.

Einige für mobiles Arbeiten wünschenswerte Aspekte sind außerdem die folgenden:

- Es sollte ein stabiler Platz zum Abstellen der mobilen IT-Systeme vorhanden sein. Viele mobile IT-Systeme werden durch Stürze zerstört.
- Die Umgebung sollte nicht zu laut sein.
- Die Umgebung sollte ausreichend beleuchtet sein, Monitorlicht alleine reicht auf Dauer nicht. Störende Blendungen, Reflexen oder Spiegelungen sollten vermieden werden.
- Der Monitor sollte so aufgestellt werden können, dass die Eingaben nicht beobachtet werden können. Für Laptops gibt es auch spezielle Monitor-Folien, die eine Einsichtnahme von der Seite verhindern.
- Die Umgebung sollte außerdem so sein, dass die mobilen IT-Systeme nicht beeinträchtigt werden, also nicht zu feucht, zu kalt oder zu warm sein. Während der Benutzung liegt dies natürlich auch im eigenen Interesse des Benutzers, die IT-Geräte sollten aber auch entsprechend aufbewahrt werden.

- Mobile IT-Geräte sollten gegen Diebstahl geschützt werden (siehe auch M 1.46 *Einsatz von Diebstahl-Sicherungen*). Die Umgebung sollte hierfür die notwendigen Bedingungen bieten. Um beispielsweise einen Laptop mit einem Kabelschloss gegen einfache Wegnahme zu sichern, muss es die Möglichkeit geben, das Kabelschloss an einen festen Gegenstand anzuschließen. Wenn möglich, sollten Fenster und Türen des mobilen Arbeitsplatzes beim Verlassen geschlossen werden. Dies ist z. B. bei Hotelzimmern oder Besprechungsräumen möglich, im Zug unter Umständen schwierig.

In fremden Umgebungen wie z. B. Hotels ist auch immer empfehlenswert, sich über das richtige Verhalten bei Bränden oder anderen Notfällen zu informieren, z. B. über Warntöne und Fluchtwege.

Ergänzende Kontrollfragen:

- Werden betroffene Mitarbeiter darüber informiert, was sie bei Auswahl und Nutzung eines mobilen Arbeitsplatzes beachten sollten?

M 1.62 Brandschutz von Patchfeldern

Verantwortlich für Initiierung: Brandschutzbeauftragter

Verantwortlich für Umsetzung: Haustechnik, Brandschutzbeauftragter, Planer

Sowohl die internen Leitungen des Hausnetzes als auch die externen des öffentlichen Netzes laufen in irgend einer Form auf Leitungsverteilern oder Patchfeldern auf, von denen aus sie über Anschlussleitungen mit Servern, Routern, etc verbunden sind.

Um zu verhindern, dass diese Leitungsverteiler und Patchfelder durch einen Brand der aktiven IT (Server, Router, etc.) beschädigt werden, sind sie mit einem geeigneten Brandschutz gegenüber dieser aktiven IT abzuschotten.

Sind Möglichkeiten und Einrichtungen vorhanden, um einen Brand frühzeitig zu erkennen und zu löschen (Objekt- oder Raumlöschung), kann eine E-30-Schottung (nach DIN 4102 Brandverhalten von Baustoffen und Bauteilen) ausreichend sein. Sind solche Einrichtungen nicht vorhanden und sieht das Brandschutzkonzept ausschließlich die Löschung durch hilfeleistende Kräfte (eigenes Personal, Feuerwehr) vor, ist eine E-90-Schottung dringend zu empfehlen.

Sind die Leitungsverteiler und Patchfelder einerseits in einem Raum für technische Infrastruktur (siehe Baustein B 2.6 *Raum für technische Infrastruktur*) und die Server, Router etc. andererseits in einem Serverraum (siehe Baustein B 2.4 *Serverraum*) sauber voneinander getrennt untergebracht, kann die entsprechende Abschottung durch geeignete Maßnahmen im Baukörper realisiert werden.

Wenn keine getrennten Räume genutzt werden können und die Leitungsverteiler und Patchfelder im Serverraum angeordnet werden müssen, besteht die Möglichkeit, diese in geeigneten Wand- oder Standverteilern mit dem erforderlichen Funktionserhalt (E-30 oder E-90) anzuordnen. Dabei ist aber besonders darauf zu achten, dass auch alle von außen kommenden Zuleitungen aus dem Haus- und dem öffentlichen Netz innerhalb des Raums in gleicher Weise (z. B. durch geeignete Kabelkanäle) gegen Brand geschützt werden.

Bei beiden Lösungen ist darauf zu achten, dass die Durchführung der Anschlussleitungen von den Leitungsverteilern und Patchfeldern zu den IT-Geräten durch die Brandschutzkonstruktion zu jeder Zeit mit geeigneten Brandschutzmitteln verschlossen ist. Wegen der Notwendigkeit, einfach und rasch an diesen Durchführungen arbeiten zu können, ohne den Brandschutz jedes Mal aufwändig wiederherstellen zu müssen, empfehlen sich hierfür (bei häufigen Arbeiten) Brandschutzkissen oder (bei selteneren Arbeiten) Pressschotts. Verwendete Brandschutzkissen müssen außerdem gegen Herausfallen gesichert werden.

Ergänzende Kontrollfragen:

- Sind auch die Zuführungsleitungen ausreichend geschützt?
- Stimmt der gewählte und realisierte Funktionserhalt (E-30 oder E-90) mit den vorhandenen Möglichkeiten der Brandmeldung und -löschung überein?

- Werden die Durchführungen nach Arbeiten im Bereich der Rangierung wieder ordnungsgemäß verschlossen?
- Werden gegebenenfalls verwendete Brandschutzkissen gegen Herausfallen gesichert?

M 1.63 Geeignete Aufstellung von Access Points

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Innerer Dienst, Administrator

Sichere Montage von Access Points

Um Manipulationen an den Access Points vorzubeugen, sollten diese in Metallgehäusen untergebracht oder mit Metallbügeln gesichert werden, die eine Wandmontage ermöglichen. Möglich ist die Unterbringung in Doppelböden, Zwischendecken oder abgehängten Decken und die Nutzung von externen Antennen. Je nach Antennenform kann so selbst durch einen Fachmann nicht mehr erkannt werden, ob es sich um einen Brandmelder oder um die Antenne eines Access Points handelt.

Räumlichkeiten bzw. Örtlichkeiten, in denen sich nicht vertrauenswürdige Personen für eine längere Zeit unbeobachtet aufhalten können, scheiden bei Anbringung der Access Points im Sichtbereich und ohne tarnende Form prinzipiell als Montage-Ort aus (Außengelände, Treppenhäuser). In diesen Bereichen können jedoch Access Points ohne Routing-Funktionalitäten aufgestellt werden. Dadurch können Informationen zum detaillierten Aufbau des Netzes nicht von unbefugten Personen ausgelesen werden. Somit wird die Angriffsfläche auf das WLAN und ein eventuell damit verbundenes LAN verringert.

Als Mindestschutz sollte eine feste Verschraubung des Access Points an einer ohne Hilfsmittel nicht zugängliche Stelle bzw. an eine nicht einsehbare Stelle erfolgen.

Positionierung der Access Points

Durch die Aufstellung und Ausrichtung von Access Points wird die Übertragungsqualität und der Durchsatz eines WLANs essentiell beeinflusst. Generell gilt, dass die Ausbreitung der Funkwellen in Bereichen, die nicht durch das WLAN versorgt werden sollen, möglichst stark zu reduzieren ist. Auf diese Weise wird nicht nur die Angriffsfläche verringert, sondern auch der eigentlich gewünschte Abdeckungsbereich besser versorgt. Hierzu können Richtantennen verwendet werden, welche die Abstrahlung von elektromagnetischen Wellen in gewisse Raumrichtungen bündeln und so einen richtungsabhängigen Verstärkungseffekt (als Antennengewinn bezeichnet) erzielen. Dieser Verstärkungseffekt muss mit der Sendeleistung am Access Point abgestimmt werden. Manche Access Points unterstützen eine flexible Einstellung der Sendeleistung. Auf diese Weise kann der Abdeckungsbereich mit der notwendigen Leistung ausgeleuchtet werden, und der Zugriff auf das WLAN von außen wird gleichzeitig erschwert, da hier nun vergleichsweise schlechte Empfangsbedingungen herrschen. Voraussetzung ist eine geeignete Positionierung der Access Points bzw. der Antennen. Diese kann auf Basis einer entsprechenden Ausleuchtungsmessung geschehen.

Bei der Versorgung von Außenbereichen sind Außeninstallationen (Antennen und gegebenenfalls Access Points) vor Witterungseinflüssen, elektrischen Entladungen und unberechtigtem Zugriff geeignet zu schützen. Die Anbringung von Access Points außerhalb von Gebäuden ist nach Möglichkeit zu vermeiden.

Schutz für Antennen im Außenbereich

Die Anbringung von Antennen auf Gebäudedächern muss so erfolgen, dass die Antenne gegen Blitzschlag gesichert ist. Die Höhe der Antenne muss genügend unter der des Blitzableiters liegen, und der Abstand zum Blitzableiter muss genügend groß sein. Dies gilt auch für den einzuhaltenden Abstand zu Hochspannungsleitungen. Antennen im Außenbereich, die möglicherweise von der Gefahr elektrischer Entladungen betroffen sind (dies gilt stets für Antennen, die auf Dächern montiert werden), sollten über einen speziellen Überspannungsschutz angeschlossen werden, der Strom- und Spannungsstöße schnell erkennt und ableitet. Dieser Überspannungsschutz wird zwischen Antenne und Access Point (typischerweise innerhalb des Gebäudes oder an einem vergleichbar geschützten Platz) montiert und muss über eine ausreichende Erdung verfügen. Access Points sollten generell nicht in Bereichen installiert werden, die von elektrischen Entladungen betroffen sein können.

Werden im Ausnahmefall Access Points außerhalb eines geeignet klimatisierten Gebäudes installiert, ist sicher zu stellen, dass der Access Point ausreichend gegen eindringende Feuchtigkeit, Frost und Hitze geschützt ist. Außenantennen sind geeignet gegen Schnee-Ablagerung zu schützen. Sie sind entweder windgeschützt anzubringen, oder die Anbringung muss auch bei hohen Windstärken so fest sein, dass sich die Antennenausrichtung nicht verstellt.

Ergänzende Kontrollfragen:

- Wie sind Access Points vor unbefugtem Zugriff geschützt?
- Ist sichergestellt, dass Access Points nur den gewünschten Abdeckungsbereich versorgen? Versorgen sie diesen optimal?

M 1.64 Vermeidung elektrischer Zündquellen

Verantwortlich für Initiierung: Brandschutzbeauftragter, Leiter Haustechnik

Verantwortlich für Umsetzung: Haustechnik, Mitarbeiter

Der überwiegende Teil baulicher Brandschutzmaßnahmen zielt darauf ab, sich entwickelnde Brände einzugrenzen, sowie die Flucht von Personen und den Einsatz von Rettungskräften zu ermöglichen. Auf die Entstehung von Bränden haben diese Maßnahmen meist nur geringen Einfluss.

Hier muss der Mensch in seinem täglichen Arbeitsumfeld besondere Aufmerksamkeit und Vorsorge walten lassen. Neben den allseits bekannten und offensichtlichen Brandquellen wie Aschenbechern, der "Kippe im Papierkorb" oder weihnachtlichem Kerzenschmuck muss auch den weniger offensichtlichen elektrischen Zündquellen Beachtung geschenkt werden.

Elektrogeräte

Beim Kauf neuer privater Haushaltsgeräte werden die noch funktionierenden Altgeräte als "Spende" im Betrieb weiter genutzt. Dabei wird übersehen, dass gerade alte Elektrogeräte mit ihren altersbedingt viel wahrscheinlicheren Defekten eine besonders hohe Brandgefährdung darstellen.

Die Nutzung privater Elektrogeräte innerhalb eines Unternehmens oder einer Behörde ist daher klar zu regeln. Sie sollte nur als Ausnahme gestattet sein, wenn derartige Geräte vorher durch eine Elektrofachkraft geprüft und für sicher befunden wurden. Genehmigte Geräte sollten speziell gekennzeichnet werden, so dass ungenehmigte Geräte einfach erkannt und aus dem Verkehr gezogen werden können.

Besonders Kühlschränke, die im Dauerbetrieb laufen, und Kaffeemaschinen, die oft stundenlang eingeschaltet bleiben, sollten nur in Räumen betrieben werden, die ausdrücklich und baulich dafür vorgesehen sind (Teeküchen etc.).

Steckdosenleisten

Egal wie viele Steckdosen vom Architekten vorgesehen wurden, es sind immer zu wenig oder sie sind am falschen Platz. Um dann fehlende Steckdosen bereitzustellen, werden oft Steckdosenleisten verwendet. Sind diese von unzureichender Qualität oder werden sie unsachgemäß eingesetzt (siehe auch G 4.62 *Verwendung unzureichender Steckdosenleisten*) stellen solche Steckdosenleisten ein gefährliche Zündquelle dar.

Die Verwendung von Steckdosenleisten sollte so weit wie möglich vermieden werden. Fehlende Steckdosen sollten durch eine Elektrofachkraft in vorhandenen Kanalsystemen nachgerüstet oder fachgerecht auf Putz montiert werden.

Ist dies nicht möglich und somit die Verwendung von Steckdosenleisten unvermeidbar, ist zu beachten:

- Es dürfen ausschließlich hochwertige Steckdosenleiste verwendet werden, die von einer Elektrofachkraft geprüft und für sicher befunden wurden.
- Es sollten einzelne ausreichend große Steckdosenleiste benutzt werden statt mehrerer kleiner.

- Steckdosenleisten dürfen keinesfalls hintereinander gesteckt werden.
- Steckdosenleisten dürfen auf keinen Fall überlastet werden. In der Regel liegt die Grenze bei 3500 Watt. Hier ist unbedingt das Typenschild zu beachten.
- Steckdosenleisten dürfen sich weder im Fußbereich am Arbeitsplatz noch in Verkehrsflächen befinden.

Elektroverteilung

Die gesamte Elektroverteilung, hauptsächlich Schutzschalter sowie Verschraubungen und Klemmstellen, unterliegt wie alle technischen Geräte einer Alterung. Sie ist daher in regelmäßigen Abständen gemäß DIN VDE 0105-100:2005-06 "Betrieb von elektrischen Anlagen" zu überprüfen.

Im Schadensfall muss ein Gewerbetreibender den Nachweis über den einwandfreien Zustand der Elektroanlage gegenüber den Gewerbeaufsichtsämtern, den Berufsgenossenschaften und den Versicherungen führen.

In Deutschland schreibt die Berufsgenossenschaftliche Vorschrift für Sicherheit und Gesundheit bei der Arbeit (BGV, A3 - Elektrische Anlagen und Betriebsmittel) folgende regelmäßige Prüfungen vor:

- Elektrische Anlagen und ortsfeste Geräte: mindestens alle 4 Jahre
- ortsveränderliche Geräte: je nach Gerätetyp mindestens alle 6 Monate bis zu mindestens alle 2 Jahre

Zu den ortsveränderlichen Geräten gehören unter anderem Steckdosenleisten, aber auch viele IT-Geräte wie beispielsweise Arbeitsplatzrechner.

Lüfter

Durch Staub blockierte Lüfter können zur Überhitzung der zu kühlenden IT-Geräte führen, aber auch selbst zu einem Brandherd werden (siehe auch G 4.63 *Verstaubte Lüfter*).

Lüfter sind folglich in regelmäßigen Abständen auf freien Rundlauf und auf Staubablagerung hin zu untersuchen und zu reinigen. Dies sollte mindestens einmal im Jahr und bei erkennbarem Bedarf auch öfter erfolgen (siehe auch M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*).

Protokollierung

Alle Prüfungen und deren Ergebnisse sind in geeigneter Form zu dokumentieren.

Ergänzende Kontrollfragen:

- Gibt es schriftlich niedergelegte Regeln zur Nutzung privater Elektrogeräte, zur Verwendung von Steckdosenleisten, zur Prüfung der Elektroverteilung und von Lüftern?
- Gibt es eine elektrotechnische Fachkraft, welche die oben genannten Prüfungen durchführt?
- Werden Durchführung und Ergebnisse der Prüfungen protokolliert.

M 2 Maßnahmenkatalog Organisation

M 2.60	Sichere Administration eines Modems	
M 2.61	Regelung des Modem-Einsatzes	
M 2.62	Software-Abnahme- und Freigabe-Verfahren	
M 2.63	Einrichten der Zugriffsrechte	
M 2.64	Kontrolle der Protokolldateien	
M 2.65	Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System	
M 2.66	Beachtung des Beitrags der Zertifizierung für die Beschaffung	
M 2.67	Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste	
M 2.68	Sicherheitskontrollen durch die Benutzer beim Einsatz von Peer-to-Peer-Diensten	
M 2.69	Einrichtung von Standardarbeitsplätzen	
M 2.70	Entwicklung eines Konzepts für Sicherheitsgateways	
M 2.71	Festlegung einer Policy für ein Sicherheitsgateway	
M 2.72	Anforderungen an eine Firewall	**entfallen**
M 2.73	Auswahl geeigneter Grundstrukturen für Sicherheitsgateways	
M 2.74	Geeignete Auswahl eines Paketfilters	
M 2.75	Geeignete Auswahl eines Application-Level-Gateways	
M 2.76	Auswahl und Einrichtung geeigneter Filterregeln	
M 2.77	Integration von Servern in das Sicherheitsgateway	
M 2.78	Sicherer Betrieb eines Sicherheitsgateways	
M 2.79	Festlegung der Verantwortlichkeiten im Bereich Standardsoftware	
M 2.80	Erstellung eines Anforderungskatalogs für Standardsoftware	
M 2.81	Vorauswahl eines geeigneten Standardsoftwareproduktes	
M 2.82	Entwicklung eines Testplans für Standardsoftware	
M 2.83	Testen von Standardsoftware	
M 2.84	Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware	
M 2.85	Freigabe von Standardsoftware	
M 2.86	Sicherstellen der Integrität von Standardsoftware	
M 2.87	Installation und Konfiguration von Standardsoftware	

M 2.178	Erstellung einer Sicherheitsleitlinie für die Faxnutzung	
M 2.179	Regelungen für den Faxserver-Einsatz	
M 2.180	Einrichten einer Fax-Poststelle	
M 2.181	Auswahl eines geeigneten Faxservers	
M 2.182	Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen	
M 2.183	Durchführung einer RAS-Anforderungsanalyse	
M 2.184	Entwicklung eines RAS-Konzeptes	
M 2.185	Auswahl einer geeigneten RAS-Systemarchitektur	
M 2.186	Geeignete Auswahl eines RAS-Produktes	
M 2.187	Festlegen einer RAS-Sicherheitsrichtlinie	
M 2.188	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung	
M 2.189	Sperrung des Mobiltelefons bei Verlust	
M 2.190	Einrichtung eines Mobiltelefon-Pools	
M 2.191	Etablierung des IT-Sicherheitsprozesses	**entfallen**
M 2.192	Erstellung einer IT-Sicherheitsleitlinie	
M 2.193	Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit	
M 2.194	Erstellung einer Übersicht über vorhandener IT-Systeme	**entfallen**
M 2.195	Erstellung eines IT-Sicherheitskonzepts	
M 2.196	Umsetzung des IT-Sicherheitskonzepts nach einem Realisierungsplan	**entfallen**
M 2.197	Integration der Mitarbeiter in den Sicherheitsprozess	
M 2.198	Sensibilisierung der Mitarbeiter für IT-Sicherheit	
M 2.199	Aufrechterhaltung der IT-Sicherheit	
M 2.200	Managementreporte und -bewertungen der IT-Sicherheit	
M 2.201	Dokumentation des IT-Sicherheitsprozesses	
M 2.202	Erstellung eines Handbuchs zur IT-Sicherheit	**entfallen**
M 2.203	Aufbau einer Informationsbörse zur IT-Sicherheit	**entfallen**
M 2.204	Verhinderung ungesicherter Netzzugänge	
M 2.205	Übertragung und Abruf personenbezogener Daten	
M 2.206	Planung des Einsatzes von Lotus Notes	
M 2.207	Festlegen einer Sicherheitsrichtlinie für Lotus Notes	

M 2.208	Planung der Domänen und der Zertifikatshierarchie von Lotus Notes	
M 2.209	Planung des Einsatzes von Lotus Notes im Intranet	
M 2.210	Planung des Einsatzes von Lotus Notes im Intranet mit Browser-Zugriff	
M 2.211	Planung des Einsatzes von Lotus Notes in einer DMZ	
M 2.212	Organisatorische Vorgaben für die Gebäudereinigung	
M 2.213	Wartung der technischen Infrastruktur	
M 2.214	Konzeption des IT-Betriebs	
M 2.215	Fehlerbehandlung	
M 2.216	Genehmigungsverfahren für IT-Komponenten	
M 2.217	Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen	
M 2.218	Regelung der Mitnahme von Datenträgern und IT-Komponenten	
M 2.219	Kontinuierliche Dokumentation der Informationsverarbeitung	
M 2.220	Richtlinien für die Zugriffs- bzw. Zugangskontrolle	
M 2.221	Änderungsmanagement	
M 2.222	Regelmäßige Kontrollen der technischen IT-Sicherheitsmaßnahmen	**entfallen**
M 2.223	Sicherheitsvorgaben für die Nutzung von Standardsoftware	
M 2.224	Vorbeugung gegen Trojanische Pferde	
M 2.225	Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten	
M 2.226	Regelungen für den Einsatz von Fremdpersonal	
M 2.227	Planung des Windows 2000 Einsatzes	
M 2.228	Festlegen einer Windows 2000 Sicherheitsrichtlinie	
M 2.229	Planung des Active Directory	
M 2.230	Planung der Active Directory-Administration	
M 2.231	Planung der Gruppenrichtlinien unter Windows 2000	
M 2.232	Planung der Windows 2000 CA-Struktur	
M 2.233	Planung der Migration von Windows NT auf Windows 2000	
M 2.234	Konzeption von Internet-PCs	
M 2.235	Richtlinien für die Nutzung von Internet-PCs	

M 2.236 Planung des Einsatzes von Novell eDirectory

M 2.237 Planung der Partitionierung und Replikation im Novell eDirectory

M 2.238 Festlegung einer Sicherheitsrichtlinie für Novell eDirectory

M 2.239 Planung des Einsatzes von Novell eDirectory im Intranet

M 2.240 Planung des Einsatzes von Novell eDirectory im Extranet

M 2.241 Durchführung einer Anforderungsanalyse für den Telearbeitsplatz

M 2.242 Zielsetzung der elektronischen Archivierung

M 2.243 Entwicklung des Archivierungskonzepts

M 2.244 Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung

M 2.245 Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung

M 2.246 Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung

M 2.247 Planung des Einsatzes von Exchange/Outlook 2000

M 2.248 Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000

M 2.249 Planung der Migration von "Exchange 5.5-Servern" nach "Exchange 2000"

M 2.250 Festlegung einer Outsourcing-Strategie

M 2.251 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben

M 2.252 Wahl eines geeigneten Outsourcing-Dienstleisters

M 2.253 Vertragsgestaltung mit dem Outsourcing-Dienstleister

M 2.254 Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben

M 2.255 Sichere Migration bei Outsourcing-Vorhaben

M 2.256 Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb

M 2.257 Überwachung der Speicherressourcen von Archivmedien

M 2.258 Konsistente Indizierung von Dokumenten bei der Archivierung

M 2.259	Einführung eines übergeordneten Dokumentenmanagements
M 2.260	Regelmäßige Revision des Archivierungsprozesses
M 2.261	Regelmäßige Marktbeobachtung von Archivsystemen
M 2.262	Regelung der Nutzung von Archivsystemen
M 2.263	Regelmäßige Aufbereitung von archivierten Datenbeständen
M 2.264	Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung
M 2.265	Geeigneter Einsatz digitaler Signaturen bei der Archivierung,
M 2.266	Regelmäßige Erneuerung technischer Archivsystem-Komponenten,
M 2.267	Planen des IIS-Einsatzes,
M 2.268	Festlegung einer IIS-Sicherheitsrichtlinie
M 2.269	Planung des Einsatzes eines Apache Webservers
M 2.270	Planung des SSL-Einsatzes beim Apache Webserver (zusätzlich),
M 2.271	Festlegung einer Sicherheitsstrategie für den WWW-Zugang,
M 2.272	Einrichtung eines WWW-Redaktionsteams,
M 2.273	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates,
M 2.274	Vertretungsregelungen bei E-Mail-Nutzung,
M 2.275	Einrichtung funktionsbezogener E-Mailadressen,
M 2.276	Funktionsweise eines Routers
M 2.277	Funktionsweise eines Switches
M 2.278	Typische Einsatzszenarien von Routern und Switches
M 2.279	Erstellung einer Sicherheitsrichtlinie für Router und Switches
M 2.280	Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches
M 2.281	Dokumentation der Systemkonfiguration von Routern und Switches
M 2.282	Regelmäßige Kontrolle von Routern und Switches
M 2.283	Software-Pflege auf Routern und Switches
M 2.284	Sichere Außerbetriebnahme von Routern und Switches
M 2.285	Festlegung von Standards für z/OS-Systemdefinitionen

M 2.1 Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Leiter IT, Leiter Organisation

Für die Aufgabenbereiche "IT-Einsatz" und "IT-Sicherheit" müssen sowohl Verantwortlichkeiten als auch Befugnisse festgelegt sein.

Für den "IT-Einsatz" ist eine Festlegung der Fachverantwortung und der Betriebsverantwortung vorzunehmen. Der Fachverantwortliche ist zuständig für die Erarbeitung der fachlichen Vorgaben, die es in einem IT-Verfahren umzusetzen gilt. Hingegen umfasst die Betriebsverantwortung unter anderem folgende Aufgaben:

- Datenerfassung,
- Arbeitsplanung und -vorbereitung,
- Datenverarbeitung,
- Nachbereitung von Datenausgaben,
- Datenträgerverwaltung und
- Überwachung des Verfahrensbetriebes.

Übergreifende Regelungen zur "IT-Sicherheit" als ein Aspekt des IT-Einsatzes müssen verbindlich festgelegt werden. Es empfiehlt sich, Regelungen über

- Datensicherung,
- Datenarchivierung,
- Datenträgertransport,
- Datenübertragung,
- Datenträgervernichtung,
- Dokumentation von IT-Verfahren, Software, IT-Konfiguration,
- Gebrauch von Passwörtern,
- Zutrittsberechtigungen,
- Zugangsberechtigungen,
- Zugriffsberechtigungen,
- Betriebsmittelverwaltung,
- Kauf und Leasing von Hardware und Software,
- Wartungs- und Reparaturarbeiten,
- Software: Abnahme und Freigabe,
- Software: Anwendungsentwicklung,
- Datenschutz,

- Schutz gegen Computer-Viren,
- Revision,
- Notfallvorsorge und
- Vorgehensweise bei der Verletzung der Sicherheitspolitik

zu treffen. Hinweise dazu finden sich in den nachfolgenden Maßnahmenbeschreibungen.

Daneben dürfen die Regelungen für Informationssicherheit nicht vernachlässigt werden. Diese sollten mit denen für IT-Sicherheit und auch Geheimschutz in geeigneter Weise zusammengeführt werden. Hierzu gehören beispielsweise:

- geeigneter Umgang mit geschäftskritischen Informationen,
- Vertraulichkeitsvereinbarungen,
- Einbeziehung des Sicherheitsbeauftragten bei Aufträgen und Projekten, die geschäftskritische Informationen betreffen,
- Unterrichtungen über den geeigneten Umgang mit geschäftskritischen Informationen, beispielsweise im Kontakt mit Kunden oder auf Reisen,
- Klassifikation von Informationen entsprechend ihres Schutzbedarfs.

Diese Regelungen sind den betroffenen Mitarbeitern in geeigneter Weise bekannt zu geben (siehe M 3.2 *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*). Es empfiehlt sich, die Bekanntgabe zu dokumentieren. Darüber hinaus sind sämtliche Regelungen in der aktuellen Form an einer Stelle vorzuhalten und bei berechtigtem Interesse zugänglich zu machen.

Die getroffenen Regelungen sind regelmäßig zu aktualisieren, um Missverständnisse, ungeklärte Zuständigkeiten und Widersprüche zu verhindern. Alle Regelungen sollten ein Erstellungsdatum oder eine Versionsnummer enthalten, um die Aktualität schnell erkennen zu können.

Ergänzende Kontrollfragen:

- Welche Regelungen sind in Kraft?
- Werden die Regelungen regelmäßig überarbeitet?
- Wie werden die Regelungen den Mitarbeitern bekannt gegeben?

M 2.2 Betriebsmittelverwaltung

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Leiter IT, Leiter Organisation

Betriebsmittel (oder Sachmittel) für den IT-Einsatz sind alle erforderlichen Mittel wie Hardware-Komponenten (Rechner, Tastatur, Drucker usw.), Software (Systemsoftware, Individualprogramme, Standardprogramme und Ähnliches), Verbrauchsmaterial (Papier, Toner, Druckerpatronen), Datenträger (Magnetbänder, Disketten, Streamertapes, Festplatten, Wechselplatten, CD-ROMs und Ähnliches). Die Betriebsmittelverwaltung umfasst die Abwicklung der Aufgaben:

- Beschaffung der Betriebsmittel,
- Prüfung vor Einsatz,
- Kennzeichnung und
- Bestandsführung.

Regelung der Beschaffung

Die **Beschaffung** von Betriebsmitteln ist beim Einsatz von Informationstechnik von besonderer Bedeutung. Mit einem geregelten Beschaffungsverfahren lassen sich insbesondere die Ziele unterstützen, die mit dem Einsatz von Informationstechnik angestrebt werden: Leistungssteigerung, Wirtschaftlichkeit, Verbesserung der Kommunikationsmöglichkeiten.

Neben reinen Wirtschaftlichkeitsaspekten kann durch ein geregeltes Beschaffungsverfahren - das von zentraler Stelle aus vorgenommen werden kann - auch die Neu- und Weiterentwicklung im Bereich der Informationstechnik stärker berücksichtigt werden.

Hausstandards

Eine zentrale Beschaffung sichert darüber hinaus die Einführung und Einhaltung eines "Hausstandards", der die Schulung der Mitarbeiter und Wartungsaktivitäten vereinfacht.

Mit einem geregelten **Prüfverfahren vor Einsatz** der Betriebsmittel lassen sich unterschiedliche Gefährdungen abwenden. Beispiele sind:

- Die Vollständigkeit von Lieferungen (z. B. Handbücher oder Anschlusskabel) sollte überprüft werden, um die Verfügbarkeit aller Lieferteile zu gewährleisten.
- Neue PC-Software sowie neue vorformatierte Datenträger sollte mit einem Computer-Viren-Suchprogramm getestet werden.
- Es sollten Testläufe neuer Software auf speziellen Test-Systemen durchgeführt werden, damit diese reibungslos in den Betrieb übernommen werden können.
- Die Kompatibilität neuer Hardware- und Softwarekomponenten mit den vorhandenen sollte vor der Beschaffung überprüft werden, damit es nicht zu Fehlkäufen kommt.

Erst mit Hilfe einer **Bestandsführung** der eingesetzten Betriebsmittel ist es möglich, den Verbrauch zu ermitteln und rechtzeitig erforderliche Nachbestellungen zu veranlassen. Darüber hinaus ermöglicht die Bestandsführung

Vollständigkeitskontrollen, Überprüfung des Einsatzes von nicht genehmigter Software oder die Feststellung der Entwendung von Betriebsmitteln. Hierzu bedarf es einer eindeutigen **Kennzeichnung** der wesentlichen Betriebsmittel mit eindeutigen Identifizierungsmerkmalen (z. B. gruppierte fortlaufende Inventarnummern). Zusätzlich sollten die Seriennummern vorhandener Geräte wie Bildschirm, Drucker, Festplatten etc. dokumentiert werden, damit sie nach einem Diebstahl identifiziert werden können.

Bestandsverzeichnisse

Für die Bestandsführung müssen die Betriebsmittel in Bestandsverzeichnissen aufgelistet werden. Ein solches Bestandsverzeichnis muss Auskunft geben können über:

- Identifizierungsmerkmale,
- Beschaffungsquellen, Lieferzeiten,
- Verbleib der Betriebsmittel,
- Lagervorhaltung,
- Aushändigungsvorschriften und
- Wartungsverträge, Wartungsintervalle.

Löschung und Vernichtung

Um den Missbrauch von Daten zu verhindern, sollte die Löschung oder Vernichtung von Betriebsmitteln geregelt sein. Insbesondere ist der Umgang mit Altpapier zu regeln. Es sollte geeignete Entsorgungsmöglichkeit für Verbrauchsgüter mit höherem Schutzbedarf geben, z. B. so genannte Schredder oder Aktenvernichter für Papier. Aktenvernichter gibt es für verschiedene Arten von Verbrauchsgütern wie Papier, Magnetbänder, Disketten und CDs. Außerdem gibt es sie in verschiedenen Sicherheitsstufen, hier ist unter anderem entscheidend, wie die Partikelgröße ist, in die das Ausgangsmaterial zerlegt wird.

Nach der Norm DIN 32757-1 können Vernichtungsgeräte in 5 Sicherheitsstufen eingeteilt werden. Für die Informationsträgervernichtung bei mittlerem Schutzbedarf sollten Vernichtungsgeräte der Sicherheitsstufe 3 verwendet werden. Für sonstige Informationsträger, die nur unlesbar gemacht werden sollen, reichen Geräte der Sicherheitsstufen 2 oder 1 aus. Bei höherem Schutzbedarf sollten Geräte der Sicherheitsstufen 4 oder 5 eingesetzt werden.

Bei Sicherheitsstufe 3 dürfen die Partikelgrößen gemäß DIN 32757-1 nicht größer sein als 4 x 80 mm2 bzw. 320 mm2 sein.

Geeignete Vernichtungsgeräte, die der Norm DIN 32757 entsprechen, sind in der BSI-Publikation 7500 aufgeführt.

Alle Verbrauchsgüter, aus denen Informationen gewonnen werden könnten, wie z. B. Zwischenträgerfolien oder fehlerhafte Ausdrucke, sollten vor der Entsorgung vernichtet oder durch eine zuverlässige Fachfirma entsorgt werden. Das Gleiche gilt beim Austausch informationstragender Ersatzteile, wie z. B. photoelektrische Trommeln von Fotokopiergeräten.

Ergänzende Kontrollfragen:

- Ermöglicht die Bestandsführung eine Vollständigkeitskontrolle?

- Welche Prüfverfahren vor Einsatz sind eingeführt worden? Welche Ergebnisse wurden erzielt?
- Ist der Beschaffungsablauf geregelt oder gibt es die Möglichkeit, die Betriebsmittelverwaltung bei Beschaffungsvorgängen zu umgehen?
- Wie aktuell ist das Bestandsverzeichnis?
- Auf welche Weise wird nicht mehr benötigtes Verbrauchsmaterial entsorgt?

M 2.3 Datenträgerverwaltung

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Archivverwalter, IT-Verfahrensverantwortlicher

Aufgabe der Datenträgerverwaltung als Teil der Betriebsmittelverwaltung ist es, den Zugriff auf Datenträger im erforderlichen Umfang und in angemessener Zeit gewährleisten zu können. Dies erfordert eine geregelte Verwaltung der Datenträger, die eine einheitliche Kennzeichnung sowie eine Führung von Bestandsverzeichnissen erforderlich macht. Weiterhin ist im Rahmen der Datenträgerverwaltung die sachgerechte Behandlung und Aufbewahrung der Datenträger, deren ordnungsgemäßer Einsatz und Transport und schließlich auch noch die Löschung bzw. Vernichtung der Datenträger zu gewährleisten.

Bestandsverzeichnisse ermöglichen einen schnellen und zielgerichteten Zugriff auf Datenträger. Bestandsverzeichnisse geben Auskunft über: Aufbewahrungsort, Aufbewahrungsdauer, berechtigte Empfänger.

Die äußerliche **Kennzeichnung** von Datenträgern ermöglicht deren schnelle Identifizierung. Die Kennzeichnung sollte jedoch für Unbefugte keine Rückschlüsse auf den Inhalt erlauben (z. B. die Kennzeichnung eines Magnetbandes mit dem Stichwort "Telefongebühren"), um einen Missbrauch zu erschweren. Eine festgelegte Struktur von Kennzeichnungsmerkmalen (z. B. Datum, Ablagestruktur, lfd. Nummer) erleichtert die Zuordnung in Bestandsverzeichnissen.

Für eine **sachgerechte Behandlung** von Datenträgern sind die Herstellerangaben, die üblicherweise auf der Verpackung zu finden sind, heranzuziehen. Hinsichtlich der **Aufbewahrung** von Datenträgern sind einerseits Maßnahmen zur Lagerung (magnetfeld-/staubgeschützt, klimagerecht) und andererseits Maßnahmen zur Verhinderung des unbefugten Zugriffs (geeignete Behältnisse, Schränke, Räume) zu treffen.

Der **Versand oder Transport** von Datenträgern muss in der Weise erfolgen, dass eine Beschädigung der Datenträger möglichst ausgeschlossen werden kann (z. B. Magnetbandversandtasche, luftgepolsterte Umschläge). Die Verpackung des Datenträgers ist an seiner Schutzbedürftigkeit auszurichten (z. B. mittels verschließbaren Transportbehältnissen). Versand- oder Transportarten (z. B. Kuriertransport) müssen ebenso festgelegt werden wie das Nachweisverfahren über den Versand (z. B. Begleitzettel, Versandscheine) und den Eingang beim Empfänger (z. B. Empfangsbestätigung). Der Datenträger darf über die zu versendenden Daten hinaus, keine "Restdaten" enthalten. Dies kann durch physikalisches Löschen erreicht werden. Stehen hierzu keine Werkzeuge zur Verfügung, so sollte der Datenträger zumindest formatiert werden. Dabei sollte sichergestellt werden, dass mit dem zugrunde liegenden Betriebssystem eine Umkehr des Befehls nicht möglich ist. Weiterhin ist zu beachten, dass vor Abgabe wichtiger Datenträger eine Sicherungskopie erstellt wird. Weitere Ausführungen zum Versand und Transport von Datenträgern enthält das Baustein B 5.2 *Datenträgeraustausch*.

Für die interne Weitergabe von Datenträger können Regelungen getroffen werden wie Quittungsverfahren, Abhol-/Mitnahmeberechtigungen sowie das Führen von Bestandsverzeichnissen über den Verbleib der Datenträger.

Für den Fall, dass **von Dritten erhaltene Datenträger** eingesetzt werden, sind Regelungen über deren Behandlung vor dem Einsatz zu treffen. Werden zum Beispiel Daten für PCs übermittelt, sollte generell ein Computer-Viren-Check des Datenträgers erfolgen. Dies gilt entsprechend auch vor dem erstmaligen Einsatz neuer Datenträger. Es ist empfehlenswert, nicht nur beim Empfang, sondern auch vor dem Versenden von Datenträgern diese auf Computer-Viren zu überprüfen.

Eine geregelte Vorgehensweise für die **Löschung** oder **Vernichtung** von Datenträgern verhindert den Missbrauch der gespeicherten Daten. Vor der Wiederverwendung von Datenträgern muss die Löschung der gespeicherten Daten vorgenommen werden; siehe hierzu: M 2.167 *Sicheres Löschen von Datenträgern*.

Ergänzende Kontrollfragen:

- Liegt ein (tages-)aktuelles Bestandsverzeichnis vor?
- Prüft der Archivverwalter die Berechtigung einer Datenträgeranforderung?
- Werden Vollständigkeitskontrollen des Datenträgerbestands vorgenommen?

M 2.4 Regelungen für Wartungs- und Reparaturarbeiten

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator, Benutzer

Um die IT vor Störungen zu bewahren, ist die ordnungsgemäße Durchführung von Wartungsarbeiten von besonderer Bedeutung. Die **rechtzeitige Einleitung** von Wartungsarbeiten und die Überprüfung ihrer Durchführung sollte von einer zentralen Stelle aus wahrgenommen werden (z. B. Beschaffungsstelle). Dabei sollten die Wartungsarbeiten von vertrauenswürdigen Personen oder Firmen ausgeführt werden, falls sie nicht von eigenem Personal durchgeführt werden können.. Die Hinweise des IT-Herstellers müssen dabei unbedingt beachtet werden. Bei regelmäßigen Wartungsarbeiten durch Externe kann der Abschluss eines Wartungsvertrages vorteilhaft sein.

Für jedes IT-System sollte dokumentiert werden, wann es gewartet wurde und welche Fehler dabei behoben wurden(z. B. Gerätepass oder Geräte- bzw. Konfigurationsmanagementsystem). Es empfiehlt sich außerdem, ein Informationssystem für Wartungs- und Reparaturarbeiten einzurichten. Mit einem solchen System können anstehende Arbeiten geplant und durchgeführte Arbeiten dokumentiert sowie der erfolgreiche Verlauf kontrolliert werden.

Außerdem sollte darin dokumentiert sein, wer für die Wartung oder Reparatur von Geräten verantwortlich ist.

Regelmäßige Reinigung von IT-Geräten

Sicherheit = Ordnung + Sauberkeit

Alle Arten von IT-Geräten sollten regelmäßig gereinigt werden. Die hierfür empfehlenswerten Intervalle hängen von der Art des Gerätes bzw. der Einsatzumgebung ab. Mindestens einmal pro Jahr sollte aber eine Reinigung erfolgen, nicht nur weil es unangenehm ist, mit verschmutzten Geräten zu arbeiten, sondern auch weil Verschmutzungen deren Funktionsfähigkeit beeinträchtigen können.

Beispiele: Tastaturen sollten spätestens dann gesäubert werden, wenn sie klebrig werden oder einzelne Tasten klemmen. Ein Arbeitsplatz-PC sollte gelegentlich auch von innen von Staub befreit werden, sofern die Herstellerangaben nicht eine andere Vorgehensweise vorschlagen. Bei Druckern kann bei nachlässiger Reinigung die Druckqualität leiden oder Komponenten beschädigt werden. Typische Problempunkte hier sind die Druckerwalze und der Druckkopf.

Zu viel Staub in IT-Systemen kann zu einem Hitzestau führen. Durch Verunreinigungen auf Platinen (besonders wirkungsvoll sind Kombinationen aus Staub und Teer- und Nikotinablagerungen) können Kriechströme verursacht werden.

Vorgaben der Hersteller beachten

Ablagerungen sollten daher regelmäßig vorsichtig entfernt werden. Insbesondere sollte für eine wirkungsvolle Lüftung aller IT-Systeme gesorgt werden. Alle Belüfter und Lüftungskomponenten müssen von störenden Verunreinigungen frei gehalten werden. Bei der Reinigung von IT-Geräten sind unbedingt die Vorgaben des Herstellers zu beachten, sowohl bei der

Vorgehensweise und Werkzeug-Auswahl als auch bei den Mindest-Wartungsintervallen.

Wartungs- und Reparaturarbeiten im Hause

Für Wartungs- und Reparaturarbeiten im Hause, vor allem wenn sie durch Externe durchgeführt werden, sind Regelungen über deren **Beaufsichtigung** zu treffen: während der Arbeiten sollte eine fachkundige Kraft die Arbeiten soweit beaufsichtigen, dass sie beurteilen kann, ob während der Arbeit unautorisierte Handlungen vollzogen werden. Weiterhin ist zu überprüfen, ob der Wartungsauftrag im vereinbarten Umfang ausgeführt wurde.

Als **Maßnahmen vor und nach Wartungs- und Reparaturarbeiten** sind einzuplanen:

- Wartungs- und Reparaturarbeiten sind gegenüber den betroffenen Mitarbeitern rechtzeitig anzukündigen. **Arbeiten ankündigen**
- Wartungstechniker müssen sich auf Verlangen ausweisen.
- Der Zugriff auf Daten durch den Wartungstechniker ist soweit wie möglich zu vermeiden. Falls erforderlich, sind Speichermedien vorher auszubauen oder zu löschen (nach einer kompletten Datensicherung), insbesondere wenn die Arbeiten extern durchgeführt werden müssen. Falls das Löschen nicht möglich ist (z. B. aufgrund eines Defektes), sind die Arbeiten auch extern zu beobachten bzw. es sind besondere vertragliche Vereinbarungen zu treffen und vertrauenswürdige Firmen auszuwählen.
- Die dem Wartungstechniker eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen bzw. zu löschen. **Rechte für Wartungstechniker minimieren**
- Nach der Durchführung von Wartungs- oder Reparaturarbeiten sind, je nach "Eindringtiefe" des Wartungspersonals, Passwortänderungen erforderlich. Im PC-Bereich sollte ein Computer-Viren-Check durchgeführt werden. **Passwörter hinterher ändern!**
- Die durchgeführten Wartungsarbeiten sind zu dokumentieren (Umfang, Ergebnisse, Zeitpunkt, Firmenname sowie eventuell Name des Wartungstechnikers).
- Beauftragte Firmen sollten schriftlich zusichern, dass sie einschlägige Sicherheitsvorschriften und Richtlinien (z. B. Brandschutz, VdS 2008 Schweiß-, Löt- und Trennschleifarbeiten) beachten. Dies gilt für alle Tätigkeiten, bei denen eine direkte oder indirekte Gefahr für Gebäude oder Menschen entstehen können. Letztlich kommt es darauf an, dass das vor Ort eingesetzte Personal mit diesen Regeln vertraut ist. **Wartungsvertrag**
- Im Anschluss an die Wartungs- oder Reparaturarbeiten ist die ordnungsgemäße Funktion der gewarteten Anlage zu überprüfen. Insbesondere die Rücknahme der für Testzwecke vorgenommenen Eingriffe ist zu kontrollieren. **Nach Reparatur Funktionsfähigkeit prüfen**

Externe Wartungs- und Reparaturarbeiten

Werden IT-Systeme zur Wartung oder Reparatur außer Haus gegeben, sind alle sensitiven Daten, die sich auf Datenträgern befinden, vorher physikalisch

zu löschen. Ist dies nicht möglich, weil aufgrund eines Defekts nicht mehr auf die Datenträger zugegriffen werden kann, sind die mit der Reparatur beauftragten Unternehmen auf die Einhaltung der erforderlichen IT-Sicherheitsmaßnahmen zu verpflichten. Entsprechend M 3.2 *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen* sind mit diesen vertragliche Regelungen über die Geheimhaltung von Daten zu treffen. Insbesondere ist festzulegen, dass Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig gelöscht werden. Ebenso sind die Pflichten und Kompetenzen des externen Wartungspersonals sorgfältig festzulegen.

Protokollierung aller Wartungsarbeiten

Bei der Durchführung externer Wartungsarbeiten muss protokolliert werden, welche IT-Systeme oder Komponenten wann an wen zur Reparatur gegeben wurden, wer dies veranlasst hat, was der Wartungs- bzw. Reparaturauftrag umfasst, zu welchem Zeitpunkt die Reparatur abgeschlossen sein sollte und wann das Gerät wieder zurückgebracht wurde. Um dies nachhalten zu können, ist eine Kennzeichnung der IT-Systeme oder Komponenten erforderlich, aus der zum einem hervorgeht, welcher Organisation diese gehören, und zum anderen eine eindeutige Zuordnung innerhalb der Organisation möglich ist.

Beim Versand oder Transport der zu reparierenden IT-Komponenten sollte darauf geachtet werden, dass Beschädigungen und Diebstahl vorgebeugt wird. Befinden sich auf den IT-Systemen noch sensitive Informationen, müssen sie entsprechend geschützt transportiert werden, also z. B. in verschlossenen Behältnissen oder durch Kuriere. Weiterhin müssen Nachweise über den Versand (Reparaturauftrag, Begleitzettel, Versandscheine) und den Eingang beim Empfänger (Empfangsbestätigung) geführt und archiviert werden.

Passwörter

Bei IT-Systemen, die durch Passwörter geschützt sind, müssen je nach Umfang der Reparaturarbeiten und der Art der Passwortabsicherung, alle oder einige Passwörter entweder bekannt gegeben oder auf festgelegte Einstellungen wie "REPARATUR" gesetzt werden, damit die Wartungstechniker auf die Geräte zugreifen können.

Überprüfung nach Fertigstellung

Nach der Rückgabe der IT-Systeme oder Komponenten sind diese auf Vollständigkeit zu überprüfen. **Alle** Passwörter sind zu ändern. PC-Datenträger sind nach der Rückgabe mittels eines aktuellen Viren-Suchprogramms auf Computer-Viren zu überprüfen. Alle Dateien oder Programme, die sich auf dem reparierten Gerät befinden, sind auf Integrität zu überprüfen.

Fernwartung

Regelungen für die Fernwartung können der Maßnahme M 5.33 *Absicherung der per Modem durchgeführten Fernwartung* entnommen werden.

Ergänzende Kontrollfragen:

- Wissen die Mitarbeiter, dass Wartungspersonal bei Arbeiten im Haus beaufsichtigt werden muss?
- Werden Nachweise über durchgeführte Wartungsarbeiten geführt?
- Liegt ein Fristenplan für Wartungsarbeiten vor?

M 2.5 Aufgabenverteilung und Funktionstrennung

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Leiter IT, Leiter Organisation

Die von der Behörde bzw. dem Unternehmen im Zusammenhang mit dem IT-Einsatz wahrzunehmenden Funktionen sind festzulegen. Zu unterscheiden sind hier zwei Ebenen:

- Die erste Ebene besteht aus den Funktionen, die den IT-Einsatz ermöglichen oder unterstützen wie Arbeitsvorbereitung, Datennachbereitung, Operating, Programmierung, Netzadministration, Rechteverwaltung, Revision.
- Die zweite Ebene besteht aus den Funktionen, die die zur Aufgabenerfüllung bereitstehenden IT-Verfahren anwenden. Beispiele solcher Funktionen sind: Fachverantwortlicher, IT-Anwendungsbetreuer, Datenerfasser, Sachbearbeiter, Zahlungsanordnungsbefugter.

Im nächsten Schritt ist die **Funktionstrennung** festzulegen und zu begründen, d. h. welche Funktionen nicht miteinander vereinbar sind, also auch nicht von **einer** Person gleichzeitig wahrgenommen werden dürfen. Vorgaben hierfür können aus den Aufgaben selbst oder aus gesetzlichen Bestimmungen resultieren. **Beispiele** dafür sind:

- Rechteverwaltung und Revision,
- Netzadministration und Revision,
- Programmierung und Test bei eigenerstellter Software,
- Datenerfassung und Zahlungsanordnungsbefugnis,
- Revision und Zahlungsanordnungsbefugnis.

Insbesondere wird deutlich, dass meistens operative Funktionen nicht mit kontrollierenden Funktionen vereinbar sind.

Nach der Festlegung der einzuhaltenden Funktionstrennung kann die Zuordnung der Funktionen zu Personen erfolgen. Vertreterregelungen sind ebenfalls zu berücksichtigen und zu dokumentieren (siehe auch M 3.3 *Vertretungsregelungen*).

Die hier getroffenen Festlegungen sind zu dokumentieren und bei Veränderungen im IT-Einsatz zu aktualisieren. Sollte bei dieser Zuordnung eine Person miteinander unvereinbare Funktionen wahrnehmen müssen, so ist dies in einer entsprechenden Dokumentation über die Funktionsverteilung besonders hervorzuheben.

Ergänzende Kontrollfragen:

- Ist die Aufzählung der relevanten Funktionen umfassend?
- Sind die definierten Funktionstrennungen vollständig?
- Wird die Funktionstrennung personell aufrechterhalten?

M 2.6 Vergabe von Zutrittsberechtigungen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter Organisation, Leiter Haustechnik

Vor der Vergabe von Zutrittsberechtigungen für Personen sind die schutzbedürftigen Räume eines Gebäudes zu bestimmen, z. B. Büro, Datenträgerarchiv, Serverraum, Operating-Raum, Maschinensaal, Belegarchiv, Rechenzentrum. Der Schutzbedarf eines Raumes ist festzustellen anhand der im Raum befindlichen Informationstechnik sowie am Schutzbedarf der eingesetzten IT-Anwendungen und ihrer Informationen.

Anschließend ist festzulegen, welche Person zur Ausübung der wahrgenommenen Funktion welches Zutrittsrecht benötigt. Dabei ist die vorher erarbeitete Funktionstrennung (M 2.5 *Aufgabenverteilung und Funktionstrennung*) zu beachten. Unnötige Zutrittsrechte sind zu vermeiden.

Um die Zahl zutrittsberechtigter Personen zu einem Raum möglichst gering zu halten, sollte auch beim IT-Einsatz der Grundsatz der Funktionstrennung berücksichtigt werden. So verhindert z. B. eine getrennte Lagerung von IT-Ersatzteilen und Datenträgern den unerlaubten Zugriff eines Wartungstechnikers auf die Datenträger.

Die Vergabe und Rücknahme von Zutrittsberechtigungen ist zu dokumentieren. Bei der Rücknahme einer Zutrittsberechtigung muss die Rücknahme des Zutrittsmittels gewährleistet sein. Zusätzlich ist zu dokumentieren, welche Konflikte bei der Vergabe der Zutrittsberechtigungen an Personen aufgetreten sind. Gründe für Konflikte können vorliegen, weil Personen Funktionen wahrnehmen, die bezüglich der Zutrittsberechtigungen der Funktionstrennung entgegenstehen, oder aufgrund räumlicher Notwendigkeiten (siehe M 3.3 *Vertretungsregelungen*).

Berechtigungskonzept

Zur Überwachung der Zutrittsberechtigung können Personen (Pförtner, Schließdienst) oder technische Einrichtungen (Ausweisleser, biometrische Verfahren wie Irisscanner oder Fingerabdruck, Sicherheitstürschloss bzw. Schließanlage) eingesetzt werden (siehe M 2.14 *Schlüsselverwaltung*). Der Zutritt zu schutzbedürftigen Räumen von nicht autorisiertem Personal (z. B. Besuchern, Reinigungs- und Wartungspersonal) darf nur bei Anwesenheit oder in Begleitung Zutrittsberechtigter erfolgen.

Regelungen über die Vergabe und Rücknahme von Zutrittsberechtigungen für Fremdpersonal und Besucher müssen ebenfalls getroffen werden.

Ergänzende Kontrollfragen:

- Liegt eine Dokumentation vor, die den Schutzbedarf von IT-Räumen ausweist?
- Wird die Dokumentation schutzbedürftiger Räume und zutrittsberechtigter Personen aktualisiert?
- Ist die Liste mit der Vertretungsregelung auf dem aktuellen Stand?

M 2.7 Vergabe von Zugangsberechtigungen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Fachverantwortliche

Zugangsberechtigungen erlauben der betroffenen Person oder einem autorisierten Vertreter, bestimmte IT-Systeme bzw. System-Komponenten und Netze zu nutzen. Dies ist für jede nutzungsberechtigte Person aufgrund ihrer Funktion, unter Beachtung der Funktionstrennung (siehe M 2.5 *Aufgabenverteilung und Funktionstrennung*), im einzelnen festzulegen. Entsprechend der Funktion ist der Zugang zum Rechner zu definieren, z. B. Zugang zum Betriebssystem (Systemverwalter) oder Zugang zu einer IT-Anwendung (Anwender). Ergänzend hierzu muss sichergestellt sein, dass personelle und aufgabenbezogene Änderungen unverzüglich berücksichtigt werden.

Der Zugang soll - sofern technisch möglich - erst nach einer Identifikation (z. B. durch Name, User-ID oder Chipkarte) und Authentisierung (z. B. durch ein Passwort) des Nutzungsberechtigten möglich sein und protokolliert werden.

Die Ausgabe bzw. der Einzug von Zugangsmitteln wie Benutzer-Kennungen oder Chipkarten ist zu dokumentieren. Regelungen über die Handhabung von Zugangs- und Authentisierungsmitteln (z. B. Umgang mit Chipkarten, Passworthandhabung, siehe M 2.11 *Regelung des Passwortgebrauchs*) müssen ebenfalls getroffen werden.

Zugangsberechtigungen sollten bei längerwährender Abwesenheit einer berechtigten Person vorübergehend gesperrt werden, um Missbrauch zu verhindern, z. B. bei Krankheit oder Urlaub. Dies sollte zumindest bei Personen mit weitreichenden Berechtigungen wie Administratoren erfolgen.

Es ist notwendig, die vorgenannten Festlegungen auf ihre korrekte Einhaltung sporadisch zu kontrollieren.

Ergänzende Kontrollfragen:

- Wird die Vergabe sowie der Einzug von Zugangsberechtigungen und Zugangsmitteln dokumentiert?
- Wird bei der Vergabe von Zugangsberechtigungen die Funktionstrennung eingehalten?
- Werden die Benutzer zum korrekten Umgang mit Zugangsmitteln geschult?
- Falls die Nutzung von Zugangsmitteln protokolliert wird, werden diese Protokolle auch in regelmäßigen Abständen ausgewertet?

M 2.8 Vergabe von Zugriffsrechten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Fachverantwortliche

Über Zugriffsrechte wird geregelt, welche Person im Rahmen ihrer Funktion bevollmächtigt wird, IT-Anwendungen oder Daten zu nutzen. Die Zugriffsrechte (z. B. Lesen, Schreiben, Ausführen) auf IT-Anwendungen, Teilanwendungen oder Daten sind von der Funktion abhängig, die die Person wahrnimmt, z. B. Anwenderbetreuung, Arbeitsvorbereitung, Systemprogrammierung, Anwendungsentwicklung, Systemadministration, Revision, Datenerfassung, Sachbearbeitung. Dabei sollten immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist ("Need-to-know-Prinzip"). Umgesetzt werden müssen die Zugriffsrechte durch die Rechteverwaltung des IT-Systems.

Eine Vielzahl von IT-Systemen lassen es zu, dass verschiedene Rechte als Gruppenrechte bzw. als Rechteprofil definiert werden (z. B. Gruppe Datenerfassung). Diese Definition entspricht der technischen Umsetzung der Rechte, die einer Funktion zugeordnet werden. Für die Administration der Rechte eines IT-Systems ist es vorteilhaft, solche Gruppen oder Profile zu erstellen, da damit die Rechtezuteilung und deren Aktualisierung erheblich vereinfacht werden kann.

Die Festlegung und Veränderung von Zugriffsrechten ist vom jeweils Verantwortlichen zu veranlassen und zu dokumentieren. Aus der Dokumentation muss hervorgehen:

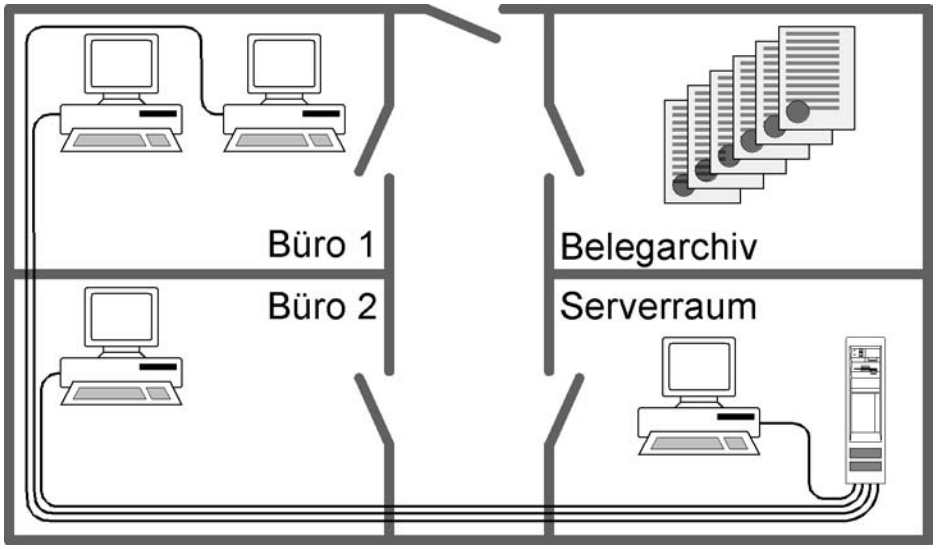
- welche Funktion unter Beachtung der Funktionstrennung (siehe M 2.5 *Aufgabenverteilung und Funktionstrennung*) mit welchen Zugriffsrechten ausgestattet wird,
- welche Gruppen bzw. Profile eingerichtet werden,
- welche Person welche Funktion wahrnimmt,
- welche Zugriffsrechte eine Person im Rahmen welcher Rolle erhält (hierbei sollten auch die Zugriffsrechte von Vertretern erfasst werden) und
- welche Konflikte bei der Vergabe von Zugriffsrechten aufgetreten sind. Diese Konflikte können z. B. daraus resultieren, dass eine Person unvereinbare Funktionen wahrnimmt oder daraus, dass abhängig vom IT-System die Trennung bestimmter Zugriffsrechte nicht vorgenommen werden kann.
- welche Personen in einem Notfall welche Zugriffsrechte erhalten, z. B. da sie zum Krisenstab gehören.

Ergänzende Kontrollfragen:

- Liegt eine aktuelle Dokumentation der vergebenen Zugriffsrechte vor?
- Werden beantragte Zugriffsrechte oder Änderungen erteilter Zugriffsrechte von den Verantwortlichen bestätigt und geprüft?
- Existiert ein geregeltes Verfahren für den Entzug von Zugriffsrechten?

Die Vorgehensweise bei der Funktionstrennung und der Rechtevergabe wird am nachfolgenden Beispiel erläutert.

Die betrachtete IT-Anwendung sei ein Reisekosten-Abrechnungssystem. Die relevanten Räume sind in nachfolgender Graphik erläutert. Das IT-System besteht aus einem LAN, an dem neben der Bedienkonsole drei PCs als Arbeitsplatzrechner angeschlossen sind.



Schritt 1: Aufgabenverteilung und Funktionstrennung

Folgende Funktionen sind für das betrachtete Reisekosten-Abrechnungssystem notwendig:

1. LAN-Administration
2. Revision
3. Datenerfassung
4. Sachbearbeitung mit Feststellung der rechnerischen Richtigkeit
5. Sachbearbeitung mit Feststellung der sachlichen Richtigkeit
6. Sachbearbeitung mit Anordnungsbefugnis

Folgende Funktionen sind aufgrund der Sachzwänge nicht miteinander vereinbar:

- Funktion 1 und Funktion 2 (die Administration darf sich nicht selbst kontrollieren)
- Funktion 2 und Funktion 6 (der Anordnungsbefugte darf sich nicht selbst kontrollieren)
- die Kombination der Funktionen 4 oder 5 mit 6 (das Vier-Augen-Prinzip wäre verletzt für Zahlungsanweisungen)

Diese Funktionen werden durch folgende Personen wahrgenommen:

		Hr. Mayer	Fr. Schmidt	Hr. Müller	Fr. Fleiß
1.	LAN-Administration	X			
2.	Revision		X		
3.	Datenerfassung			X	
4.	Sachbearbeitung rechn.			X	
5.	Sachbearbeitung sachl.			X	
6.	Anordnungsbefugnis				X

Schritt 2: Vergabe von Zutrittsrechten

Nachfolgend wird der Schutzbedarf der einzelnen Räume begründet und in der Tabelle die Vergabe der Zutrittsrechte dokumentiert:

- Serverraum:

  der unbefugte Zutritt zum Server muss verhindert werden, weil die Verfügbarkeit Integrität und Vertraulichkeit der gesamten Anwendung von dieser zentralen Komponente abhängig ist

- Belegarchiv:

  für die Rechnungslegung bedarf es der Aufbewahrung der Reisekostenabrechnungen. Es ist sicherzustellen, dass die Belege vollständig und unverändert aufbewahrt werden

- Büro 1:

  in diesem Büro erfolgt die Dateneingabe in Verbindung mit der Feststellung der rechnerischen Richtigkeit und die Feststellung der sachlichen Richtigkeit. Für die Gewährleistung der Korrektheit dieser Vorgänge muss verhindert werden, dass Unbefugte Zutritt zu den Arbeitsplatzrechnern erhalten.

- Büro 2:

  hier erfolgt die Anordnungsbefugnis für die Auszahlung der Reisekosten am APC. Dieser Vorgang darf nur von einer befugten Person vorgenommen werden. Unbefugten ist der Zutritt zu verwehren.

		Server-raum	Beleg-archiv	Büro 1	Büro 2
1.	LAN-Administration	X			
2.	Revision	X	X	X	X
3.	Datenerfassung			X	
4.	Sachbearbeitung rechn.		X	X	
5.	Sachbearbeitung sachl.		X	X	
6.	Anordnungs-befugnis		X	X	X

Schritt 3: Vergabe von Zugangsberechtigungen

Aufgrund der Funktionen ergeben sich folgende Zugangsberechtigungen:

		Betriebs-system Server	Anwen-dung Pro-tokollaus-wertung	Anwen-dung Datener-fassung	Anwen-dung Belegbe-arbeitung
1.	LAN-Administration	X			
2.	Revision	X	X		X
3.	Datenerfassung			X	
4.	Sachbearbeitung rechn.				X
5.	Sachbearbeitung sachl.				X
6.	Anordnungs-befugnis				X

Schritt 4: Vergabe von Zugriffsrechten

Im folgenden werden die Zugriffsrechte, die eine Funktion zur Ausübung benötigt, dargestellt. Es bezeichnen:

A = Recht zur Ausführung der Anwendung/Software

L = Leserecht auf Daten

S = Schreibrecht, d. h. Erzeugen von Daten

M = Recht zum Modifizieren von Daten

Ö = Recht zum Löschen von Daten

U = Recht zum Unterschreiben von Zahlungsanweisungen

		Betriebs-system Server	Protokoll-aus-wertung	Anwen-dung Datener-fassung	Anwen-dung Belegbe-arbeitung
1.	LAN-Administration	A,L,S,M,Ö			
2.	Revision	A,L	A,L,Ö		A,L
3.	Datenerfassung			A,S	
4.	Sachbearbeitung rechn.				A,L,M
5.	Sachbearbeitung sachl.				A,L,M
6.	Anordnungsbefugnis				A,L,U

Eine solche Dokumentation erleichtert die Rechteverteilung. Angenommen, dass Frau Schmidt den Arbeitgeber wechseln würde und ihre Stelle neu besetzt werden müsste, so lässt sich anhand der obigen Tabellen einfach feststellen, welche der ehemaligen Rechte Frau Schmidts zu löschen und für die neue Kraft einzurichten sind. Wenn die neue Kraft zusätzlich vertretungsweise die Funktion Sachbearbeitung mit Anordnungsbefugnis übernehmen soll, so wird anhand der durchzuführenden Rechteverteilung der Konflikt offenbar, dass die neue Kraft im Vertretungsfall Manipulationen unbemerkt durchführen könnte.

M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT

Es ist durchaus üblich, dass Mitarbeiter eigene Hard- und Software wie beispielsweise private Mobiltelefone, PDAs oder Kameras auch dienstlich oder zumindest in den Diensträumen verwenden. Da die Nutzung von zusätzlicher Hardware über Standardschnittstellen wie USB und weitgehende Plug-and-Play-Funktionalität immer einfacher wird, muss deren Einsatz geregelt werden. Die IT-Sicherheit kann dabei beispielsweise durch externe USB-Speichermedien (z. B. Festplatten, Memory-Sticks) oder private PDAs beeinträchtigt werden.

Es muss daher geregelt sein, wie Hard- und Software abgenommen, freigegeben, installiert bzw. benutzt werden darf. Maßnahmen, die zu diesem Zweck umgesetzt werden sollten, sind z. B.: M 2.216 *Genehmigungsverfahren für IT-Komponenten*, M 2.62 *Software-Abnahme- und Freigabe-Verfahren* bzw. Baustein B 1.10 *Standardsoftware* und M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*.

Das Einspielen bzw. Benutzen nicht freigegebener Hard- und Software muss verboten und außerdem durch technische Möglichkeiten soweit möglich verhindert werden. Bei den meisten Betriebssystemen kann dies durch Einschränkung der Benutzerumgebung erreicht werden. Damit soll verhindert werden, dass Programme mit unerwünschten Auswirkungen eingebracht werden. Zusätzlich soll verhindert werden, dass das System über den festgelegten Funktionsumfang hinaus unkontrolliert genutzt wird. Es kann sinnvoll sein (z. B. um Makro-Viren vorzubeugen), dieses Nutzungsverbot auch auf das Einspielen privater Daten auszudehnen.

Bei Software ist zu dokumentieren, welche Versionen ausführbarer Dateien freigegeben wurden (inklusive Erstellungsdatum und Dateigröße). Die freigegebenen Programme sind regelmäßig auf Veränderungen zu überprüfen.

Nutzungsverbote nicht freigegebener Hard- und Software sollten schriftlich fixiert werden, alle Mitarbeiter sind darüber zu unterrichten. Ausnahmeregelungen sollten einen Erlaubnisvorbehalt vorsehen.

Ergänzende Kontrollfragen:

- Gibt es ein Genehmigungs- und Registrierverfahren für Hard- und Software?
- Sind Nutzungsverbote schriftlich fixiert?
- Sind alle Mitarbeiter über Nutzungsverbote unterrichtet?
- Wird in regelmäßigen Abständen an Nutzungsverbote erinnert?
- Welche Möglichkeiten bestehen, unautorisiert Software einzuspielen oder zu nutzen?
- Welche Möglichkeiten bestehen an den einzelnen Rechnern, Software selbständig zu entwickeln?

- Gibt es Regelungen über die Programmierung und die Weitergabe von Makros aus leistungsfähigen Standardprodukten wie z. B. Textverarbeitung, Tabellenkalkulation und Datenbanken?
- Existieren Listen mit den freigegebenen Versionen ausführbarer Dateien, die insbesondere Erstellungsdatum und Dateigröße beinhalten?
- Wird regelmäßig überprüft, ob die freigegebenen Versionen ausführbarer Dateien verändert wurden?
- Besteht die Möglichkeit, das Einspielen von Software technisch zu verhindern?
- Ist die Nutzung von externen Speichermedien aller Art (z. B. USB-Memory-Sticks, Kameras, PDAs und Mobiltelefonen) geregelt?

M 2.10 Überprüfung des Hard- und Software-Bestandes

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter IT, IT-Sicherheitsmanagement, Vorgesetzte

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Um Verstöße gegen das Verbot der Nutzung nicht freigegebener Hard- und Software feststellen zu können, ist eine regelmäßige Überprüfung des Hard- und Software-Bestandes notwendig. Ist die Zahl der IT-Systeme sehr groß, kann eine stichprobenartige Überprüfung durchgeführt werden. Die Ergebnisse der Überprüfung sind zu dokumentieren, um auch Wiederholungsfälle feststellen zu können.

Wird bei der Überprüfung nicht genehmigte Hardware gefunden, muss dafür gesorgt werden, dass die IT-Komponenten nicht weiter vorschriftswidrig betrieben werden. Es muss zudem ermittelt werden, wer für den Betrieb verantwortlich ist, um geeignete Konsequenzen ergreifen zu können. Bei konkreten Verdachtsfällen ist bei der Kontrolle der Hardware auf Manipulationen und Zusatzgeräte, die z. B. zur Aufzeichnung von Tastaturanschlägen verwendet werden, zu achten.

Sollte bei der Überprüfung nicht freigegebene Software gefunden werden, so ist die Entfernung zu veranlassen. Um diese Überprüfung durchführen zu können, muss der überprüfenden Instanz die entsprechende Befugnis durch die Unternehmens- bzw. Behördenleitung verliehen werden. Zusätzlich muss der prüfenden Instanz bekannt sein, welche Software auf welchem IT-System freigegeben ist (Software-Bestandsverzeichnis).

Um bei der Vielzahl der üblicherweise eingesetzten Software effizient ein Software-Bestandsverzeichnis führen zu können, sollte hierfür ein entsprechendes Tool eingesetzt werden. Für die typische Client-Server-Umgebung sollte es netzfähig sein.

Vor der Festlegung einer Regelung zur Überprüfung des Hard- und Software-Bestandes sollte der Betriebs- bzw. Personalrat hinzugezogen werden.

Für solche IT-Systeme, die für den Wirkbetrieb des IT-Verbunds nicht erforderlich sind wie z. B. Testsysteme, kann anstelle einer regelmäßigen Überprüfung eine anlassbezogene Überprüfung durchgeführt werden. Beispielsweise kann die Prüfung auf solchen IT-Systemen immer dann vorgenommen werden, wenn Änderungen an der Konfiguration vorgenommen werden oder wenn das IT-System nach längerer Pause wieder in Betrieb gesetzt wird. Voraussetzung ist jedoch, dass für alle IT-Systeme die Maßnahme M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software* in Kraft ist.

Ergänzende Kontrollfragen:

- In welchem Turnus werden Überprüfungen des Hard- und Software-Bestandes durchgeführt?
- Sind Fälle aufgetreten, dass unautorisierte Software genutzt wurde?
- Wie wird verfahren, wenn ein Verstoß festgestellt wird?

M 2.11 Regelung des Passwortgebrauchs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Benutzer

Werden in einem IT-System Passwörter zur Authentisierung verwendet, so ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung des Systems entscheidend davon abhängig, dass das Passwort korrekt gebraucht wird. Dafür ist es empfehlenswert, eine Regelung zum Passwortgebrauch einzuführen und den IT-Benutzer diesbezüglich zu unterweisen.

praktikabler Kompromiss

Vorgaben für die Passwortgestaltung müssen immer einen praktikablen Kompromiss zwischen folgenden Sicherheitszielen darstellen:

1. Die Zeichenzusammensetzung des Passwortes muss so komplex sein, dass es nicht leicht zu erraten ist.
2. Die Anzahl der möglichen Passwörter im vorgegebenen Schema muss so groß sein, dass es nicht in kurzer Zeit durch einfaches Ausprobieren ermittelt werden kann.
3. Das Passwort darf nicht zu kompliziert sein, damit der Besitzer mit vertretbarem Aufwand in der Lage ist, es auswendig zu lernen.

Regeln für Benutzer

Folgende Regeln zum Passwortgebrauch sollten deshalb beachtet werden:

- Das Passwort darf nicht leicht zu erraten sein. Namen, Kfz-Kennzeichen, Geburtsdatum usw. dürfen deshalb nicht als Passwörter gewählt werden.
- Innerhalb des Passwortes sollte mindestens ein Zeichen verwendet werden, das kein Buchstabe ist (Sonderzeichen oder Zahl).
- Wenn für das Passwort alphanumerische Zeichen gewählt werden können, sollte es mindestens 8 Zeichen lang sein.
- **Sperrung nach Fehlversuchen**

  Wenn für das Passwort nur Ziffern zur Verfügung stehen, sollte es mindestens 6 Zeichen lang sein **und** das Authentisierungssystem sollte den Zugang nach wenigen Fehlversuchen sperren (für eine bestimmte Zeitspanne oder dauerhaft).
- Es muss getestet werden, wie viele Stellen des Passwortes vom Rechner wirklich überprüft werden.
- Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Passwörter ersetzt werden.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Das Passwort muss geheim gehalten werden und sollte nur dem Benutzer persönlich bekannt sein.
- **Hinterlegung in verschlossenem Umschlag**

  Das Passwort sollte allenfalls für die Hinterlegung schriftlich fixiert werden, wobei es in diesem Fall in einem verschlossenen Umschlag sicher aufbewahrt werden muss. Wird es darüber hinaus aufgeschrieben, ist das Passwort zumindest so sicher wie eine Scheckkarte oder ein Geldschein aufzubewahren (siehe M 2.22 *Hinterlegen des Passwortes*).
- Das Passwort muss regelmäßig gewechselt werden, z. B. alle 90 Tage.

- Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt geworden ist oder der Verdacht besteht.
- Alte Passwörter sollten nach einem Passwortwechsel nicht mehr gebraucht werden.
- Die Eingabe des Passwortes sollte unbeobachtet stattfinden.

Anforderungen an IT-Systeme

Falls IT-technisch möglich, sollten folgende Randbedingungen eingehalten werden:

- Die Wahl von Trivialpasswörtern (z. B. "BBBBBBBB", "123456") sollte verhindert werden.
- Jeder Benutzer muss sein eigenes Passwort jederzeit ändern können.

Einmalpasswörter

- Für die Erstanmeldung neuer Benutzer sollten Einmalpasswörter vergeben werden, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen. In Netzen, in denen Passwörter unverschlüsselt übertragen werden, empfiehlt sich die dauerhafte Verwendung von Einmalpasswörtern (siehe M 5.34 *Einsatz von Einmalpasswörtern*).
- Nach dreifacher fehlerhafter Passworteingabe sollte das Authentisierungssystem den Zugang sperren (für eine bestimmte Zeitspanne oder dauerhaft).
- Bei der Authentisierung in vernetzten Systemen sollten Passwörter selbst im Intranet nicht unverschlüsselt übertragen werden. Erfolgt die Authentisierung über ein ungesichertes Netz hinweg, so dürfen Passwörter keinesfalls unverschlüsselt übertragen werden.
- Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.
- Die Passwörter müssen im System zugriffssicher gespeichert werden, z. B. mittels Einweg-Verschlüsselung (Hashfunktionen).
- Der Passwortwechsel sollte vom System regelmäßig initiiert werden.
- Die Wiederholung alter Passwörter beim Passwortwechsel sollte vom IT-System verhindert werden (Passworthistorie).

Ergänzende Kontrollfragen:

- Sind die Benutzer über den korrekten Umgang mit Passwörtern unterrichtet worden?
- Wird die Passwort-Güte kontrolliert?
- Wird der Passwort-Wechsel erzwungen?
- Ist jeder Benutzer im Netz mit einem Passwort ausgestattet?

M 2.12 Betreuung und Beratung von IT-Benutzern

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter IT

Verantwortlich für Umsetzung: Leiter IT

Der Einsatz von IT-Systemen erfordert eine umfassende Schulung der IT-Benutzer. Neben der Schulung, die die IT-Benutzer in die Lage versetzt, die eingesetzte Informationstechnik sachgerecht einzusetzen, bedarf es einer Betreuung und Beratung der IT-Benutzer für die im laufenden Betrieb auftretenden Probleme. Diese Probleme können aus Hardware-Defekten oder fehlerhafter Software-Installation resultieren, aber auch aus Bedienungsfehlern. Alle Benutzer sollten die Stelle bzw. Personen kennen, an die sie sich bei IT-Problemfällen wenden können. Der IT-Support sollte auch Hinweise auf potenzielle Sicherheitsprobleme aufnehmen und an die Zuständigen, z. B. das IT-Sicherheitsmanagement-Team, weiterleiten.

zeitnahe IT-Betreuung

In größeren Institutionen kann es daher sinnvoll sein, eine zentrale Stelle mit der Betreuung der IT-Benutzer zu beauftragen und diese allen Mitarbeitern bekannt zu geben. Diese Notwendigkeit kann sich insbesondere bei einer hohen Zahl dezentraler Systeme wie PCs als praktikabel erweisen. Dabei ist sicherzustellen, dass der IT-Support während der Arbeitszeiten der Benutzer zur Verfügung steht, damit IT-Probleme zeitnah gelöst werden können. Da bei gleitender Arbeitszeit Benutzer zu unregelmäßigen Zeiten an ihrem Arbeitsplatz sein können, sollten Service-Zeiten festgelegt werden, die den Anforderungen der jeweiligen Institution gerecht werden und die sich an den Zeiten orientieren sollten, zu denen der Großteil der Mitarbeiter arbeiten.

telefonische Hotline

Für die Betreuung von IT-Benutzern sollte eine telefonische Hotline eingerichtet werden, da viele Probleme telefonisch schneller als auf schriftlichem Weg gelöst werden können. Eine Unterstützung nur per E-Mail ist nicht ausreichend, da beim Ausfall eines IT-Systems, des Netzes oder der beteiligten Server das Problem unter Umständen auf diese Weise nicht geschildert werden kann.

Ergänzende Kontrollfragen:

- An wen können sich IT-Benutzer in Problemfällen wenden?
- Ist sichergestellt, dass IT-Probleme zeitnah bearbeitet werden?

M 2.13 Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter Haustechnik, Benutzer

Betriebsmittel oder Sachmittel, die schützenswerte Daten enthalten (Druckerpapier, Disketten, Streamertapes, Magnetbänder, Festplatten, CD-ROM, USB-Sticks aber auch spezielle Tonerkassetten, Kohlepapier oder Carbonbänder) und nicht mehr gebraucht werden oder aufgrund eines Defektes ausgesondert werden sollen, sind so zu entsorgen, dass keine Rückschlüsse auf vorher gespeicherte Daten möglich sind. Bei funktionstüchtigen Datenträgern sollten die Daten physikalisch gelöscht werden. Nicht funktionierende oder nur einmal beschreibbare Datenträger wie CD-ROMs müssen mechanisch zerstört werden (siehe M 2.216 *Genehmigungsverfahren für IT-Komponenten*).

Die Art der Entsorgung schutzbedürftigen Materials sollte in einer speziellen Anordnung geregelt werden, entsprechende Entsorgungseinrichtungen sind vorzuhalten (siehe auch DIN 32757).

Wird schutzbedürftiges Material vor der Entsorgung gesammelt, so ist die Sammlung unter Verschluss zu halten und vor unberechtigtem Zugriff zu schützen.

Soweit im Unternehmen bzw. in der Behörde keine umweltgerechte und sichere Entsorgung durchgeführt werden kann, sind damit beauftragte Unternehmen auf die Einhaltung erforderlicher IT-Sicherheitsmaßnahmen zu verpflichten. Ein Mustervertrag findet sich unter den Hilfsmitteln zum IT-Grundschutz auf den BSI-Webseiten.

Ergänzende Kontrollfragen:

- Werden in der genannten Regelung alle schutzbedürftigen Materialien behandelt?
- Ist der Entsorgungsvorgang verlässlich?
- Werden die genannten Entsorgungsbestimmungen eingehalten?

M 2.14 Schlüsselverwaltung

Verantwortlich für Initiierung: Leiter Organisation, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter Haustechnik

Für alle Schlüssel des Gebäudes (von Etagen, Fluren und Räumen) ist ein Schließplan zu fertigen. Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln ist zentral zu regeln. Reserveschlüssel sind vorzuhalten und gesichert aufzubewahren. Das gleiche gilt auch für alle Identifikationsmittel wie Magnetstreifen- oder Chipkarten. Zu beachten bleibt:

- Ist eine Schließanlage vorhanden, sind für schutzbedürftige Bereiche eigene Schließgruppen zu bilden. Je nach Anforderungen sind einzelne Räume aus der Schließgruppe herauszunehmen und mit Einzelschließung zu versehen.
- Nicht ausgegebene Schlüssel und die Reserveschlüssel sind gegen unbefugten Zugriff geschützt aufzubewahren.
- Die Ausgabe der Schlüssel erfolgt nur in begründeten und nachvollziehbaren Fällen an hierfür autorisierte Personen gegen Quittung und ist zu dokumentieren. Auch im Vertretungsfall darf ein Schlüssel nicht einfach weitergegeben werden, sondern hat über die Schlüsselausgabe zu erfolgen. Nur über diesen Umweg kann eine lückenlose Dokumentation als Nachweis über den Verbleib des Schlüssels erfolgen.
- Es sind Vorkehrungen zu treffen, wie bei Verlust einzelner Schlüssel zu reagieren ist (Meldung, Ersatz, Kostenerstattung, unter Umständen Regressfrage wegen mangelnder Sorgfaltspflicht prüfen), Austausch des Schlosses, Austausch von Schließgruppen etc.).
- Bei Zuständigkeitsänderungen von Mitarbeitern sind deren Schließberechtigungen zu prüfen und nicht mehr benötigte Schlüssel einzuziehen.
- Beim Ausscheiden von Mitarbeitern sind alle Schlüssel einzuziehen (Aufnahme der Schlüsselverwaltung in den Laufzettel der noch vor dem Ausscheiden zu erledigenden Stationen).
- Schlösser und Schlüssel zu besonders schutzbedürftigen Bereichen (zu denen nur sehr wenige Schlüssel ausgegeben werden sollten) können bei Bedarf auch ohne vorherige Ankündigung im Verdachtsfall getauscht werden, um so illegal nachgefertigten Schlüsseln die Funktion zu nehmen.

Ergänzende Kontrollfragen:

- Welche Regelungen gibt es zur Schlüsselverwaltung?
- Werden die Vertretungsregelungen beachtet?
- Werden diese Regelungen von den Mitarbeitern angenommen?

M 2.15 Brandschutzbegehungen

Verantwortlich für Initiierung: Leiter Haustechnik , Leiter IT

Verantwortlich für Umsetzung: Brandschutzbeauftragter

Bei der Errichtung und der Nutzung von Gebäuden sind alle geltenden Brandschutzvorschriften zu beachten. Diese werden durch DIN- und VDE-Vorschriften festgeschrieben und durch Auflagen der Bauaufsicht ergänzt (siehe auch M 1.6 *Einhaltung von Brandschutzvorschriften*).

Die Erfahrungen zeigen, dass nach Nutzungsbeginn im täglichen Betrieb diese Regelungen immer nachlässiger gehandhabt werden - bis hin zur völligen Ignoranz. Einige **Beispiele:**

- Fluchtwege werden blockiert, z. B. durch Möbel und Papiervorräte.
- Brandabschnittstüren bzw. Rauchschutztüren werden durch Keile offen gehalten.
- Zulässige Brandlasten werden durch anwachsende Kabelmengen oder geänderte Nutzungen überschritten.
- Brandabschottungen werden bei Arbeiten geöffnet und/oder beschädigt und nicht ordnungsgemäß wiederhergerichtet.
- Rauchmelder in der Nähe von "Raucherecken" werden bewusst außer Funktion gesetzt.

Brandschutzbegehungen sollten ein- bis zweimal im Jahr angekündigt oder unangekündigt erfolgen.

Da die Handlungsweise der Mitarbeiter in der Regel nicht vom böswilligen Vorsatz, sondern von der betrieblichen Notwendigkeit oder Bequemlichkeit bestimmt wird, kann es nicht Sinn einer Brandschutzbegehung sein, Täter zu finden und zu bestrafen. Vielmehr sollten die vorgefundenen Mängel dazu Anlass geben, die Zustände sofort und ggf. auch deren Ursachen unverzüglich zu beheben.

Ergänzende Kontrollfragen:

- Werden Brandschutzbegehungen regelmäßig durchgeführt und festgestellte Mängel behoben?

M 2.16 Beaufsichtigung oder Begleitung von Fremdpersonen

Verantwortlich für Initiierung: Leiter Organisation

Verantwortlich für Umsetzung: Mitarbeiter

Kann ich Ihnen weiterhelfen?

Personen, die nicht der Institution angehören, wie Besucher, Handwerker, Wartungs- und Reinigungspersonal sollten, außer in Räumen, die ausdrücklich dafür vorgesehen sind, nicht unbeaufsichtigt sein (siehe auch M 2.6 *Vergabe von Zutrittsberechtigungen*). Alle Mitarbeiter sollten darauf hingewiesen werden, dass sie Betriebsfremde, die sie unbeaufsichtigt innerhalb der Behörde oder des Unternehmens antreffen, von diesem Moment an unter ihre Obhut nehmen müssen. Dies dient nicht nur der Sicherheit aller, sondern ist auch ein positiver Serviceaspekt für Betriebsfremde.

Wird es erforderlich, einen Externen allein im Büro zurückzulassen, sollte ein Kollegen ins Zimmer oder der Besucher zu einem Kollegen gebeten werden.

Ist es nicht möglich, Fremdpersonen (z. B. Reinigungspersonal) ständig zu begleiten oder zu beaufsichtigen, sollte zumindest der persönliche Arbeitsbereich abgeschlossen werden: Schreibtisch, Schrank und PC (Schloss für Diskettenlaufwerk, Tastaturschloss), siehe auch M 2.37 *"Der aufgeräumte Arbeitsplatz"*.

Auch zu Hause keine Arbeitsunterlagen liegen lassen

Für den häuslichen Arbeitsplatz gilt, dass Familienmitglieder und Besucher sich nur dann alleine im Arbeitsbereich aufhalten dürfen, wenn alle Arbeitsunterlagen verschlossen aufbewahrt sind und die IT über einen aktivierten Zugangsschutz gesichert ist.

Die Notwendigkeit dieser Maßnahme ist den Mitarbeitern zu erläutern und in einer Sicherheitsrichtlinie festzuhalten. Eine Dokumentation über den Aufenthalt von Fremdpersonen kann in einem Besucherbuch geführt werden.

Ergänzende Kontrollfragen:

- Werden die Mitarbeiter dazu angehalten, entsprechend zu handeln?
- Wie sieht die tatsächliche Praxis im Hause aus?

M 2.17 Zutrittsregelung und -kontrolle

Verantwortlich für Initiierung: Leiter Organisation, Leiter Haustechnik

Verantwortlich für Umsetzung: Leiter Haustechnik, Mitarbeiter, Planer

Der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen ist zu regeln und zu kontrollieren (siehe M 2.6 *Vergabe von Zutrittsberechtigungen*). Die Maßnahmen reichen dabei von einer einfachen Schlüsselvergabe bis zu aufwendigen Identifizierungssystemen mit Personenvereinzelung, wobei auch die Nutzung eines mechanischen Schlüssels nebst Schloss eine Zutrittsregelung darstellt. Für eine Zutrittsregelung und -kontrolle ist es erforderlich, dass

- der von der Regelung betroffene Bereich eindeutig bestimmt wird,
- die Zahl der zutrittsberechtigten Personen auf ein Mindestmaß reduziert wird; diese Personen sollen gegenseitig ihre Berechtigung kennen, um Unberechtigte als solche erkennen zu können,
- der Zutritt anderer Personen (Besucher) erst nach vorheriger Prüfung der Notwendigkeit erfolgt,
- erteilte Zutrittsberechtigungen dokumentiert werden.

Die Vergabe von Rechten allein reicht nicht aus, wenn deren Einhaltung bzw. Überschreitung nicht kontrolliert wird. Die Ausgestaltung von Kontrollmechanismen sollte nach dem Grundsatz erfolgen, dass einfache und praktikable Lösungen oft ebenso effizient sind wie aufwendige Technik. Beispiele hierfür sind:

- Information und Sensibilisierung der Berechtigten,
- Bekanntgabe von Berechtigungsänderungen,
- sichtbares Tragen von Hausausweisen, ggf. Vergabe von Besucherausweisen,
- Begleitung von Besuchern,
- Verhaltensregelungen bei erkannter Berechtigungsüberschreitung und
- Einschränkung des ungehinderten Zutritts für nicht Zutrittsberechtigte (z. B. Tür mit Blindknauf, Schloss für Berechtigte mit Schlüssel, Klingel für Besucher).

Bei der Zutrittskontrolle werden verschiedene bauliche, organisatorische und personelle Maßnahmen benötigt. Deren Zusammenwirken sollte in einem Zutrittskontrollkonzept geregelt sein, das die generellen Richtlinien für den Perimeter-, Gebäude- und Geräteschutz festlegt. Dazu gehören:

- Festlegung der Sicherheitszonen

  Zu schützende Bereiche können etwa Grundstücke, Gebäude, Serverräume, Räume mit Peripheriegeräten, Archive, Kommunikationseinrichtungen und die Haustechnik sein. Da diese Bereiche häufig sehr unterschiedliche Sicherheitsanforderungen aufweisen, kann es sinnvoll sein, diese in verschiedene Sicherheitszonen aufzuteilen.

- Vergabe von Zutrittsberechtigungen (siehe M 2.6 *Vergabe von Zutrittsberechtigungen*)
- Bestimmung eines Verantwortlichen für Zutrittskontrolle

  Dieser vergibt die Zutrittsberechtigungen an die einzelnen Personen entsprechend den in der Sicherheitspolitik festgelegten Grundsätzen.
- Definition von Zeitabhängigkeiten

  Es ist zu klären, ob zeitliche Beschränkungen der Zutrittsrechte erforderlich sind. Solche Zeitabhängigkeiten können etwa sein: Zutritt nur während der Arbeitszeit, Zutritt einmal täglich oder befristeter Zutritt bis zu einem fixierten Datum.
- Festlegung der Beweissicherung

  Hier ist zu bestimmen, welche Daten bei Zutritt zu und Verlassen von einem geschützten Bereich protokolliert werden. Dabei bedarf es einer sorgfältigen Abwägung zwischen den Sicherheitsinteressen des Systembetreibers und den Schutzinteressen der Privatsphäre des Einzelnen.
- Behandlung von Ausnahmesituationen

  Es ist u. a. sicherzustellen, dass im Brandfall die Mitarbeiter schnellstmöglich die gefährdeten Zonen verlassen können.

Ergänzend kann der Einbau von Ausweislesern verschiedenster Qualitäten, von Schleusen und Vereinzelungseinrichtungen sinnvoll sein. Zur Schlüsselverwaltung siehe M 2.14 *Schlüsselverwaltung.*

Im Betrieb eines Rechenzentrums ist die Absicherung der Kerneinheiten durch starke Zutrittskontrollmechanismen zwingend erforderlich. Als Identifikations- bzw. Authentikationskennzeichen kommen dabei Besitz, Wissen und biometrische Merkmale in Frage. Ein starker Zutrittskontrollmechanismus muss mindestens zwei dieser drei Kennzeichen berücksichtigen. Aus heutiger Sicht sind biometrische Verfahren als *alleinige* Zutrittskontrolle nicht zu empfehlen.

Die Terminals zur Zutrittskontrolle müssen gegen Manipulationen geschützt werden. Dafür müssen diese so angebracht werden, dass Vertraulichkeit bei der Eingabe von Daten gewährleistet ist. Außerdem sollten alle zur Dateneingabe erforderlichen Einheiten in einem Gerät kombiniert sein, also beispielweise eine Tastatur zur PIN-Eingabe.

Befinden sich nicht alle Einheiten in einem Gerät, muss die Datenübertragung zwischen diesen verschlüsselt erfolgen. Werden also z. B. berührungslose Ausweisleser eingesetzt, so muss die Datenübertragung zwischen Karte und Leser verschlüsselt erfolgen.

Ergänzende Kontrollfragen:

- Existiert ein Konzept für die Zutrittskontrolle?
- Werden die Zutrittskontroll-Maßnahmen regelmäßig auf ihre Wirksamkeit überprüft?

M 2.18 Kontrollgänge

Verantwortlich für Initiierung: Haustechnik, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Haustechnik, IT-Sicherheitsmanagement

Eine Maßnahme kann nur so gut wirken, wie sie auch tatsächlich umgesetzt wird. Kontrollgänge bieten das einfachste Mittel, die Umsetzung von Maßnahmen und die Einhaltung von Auflagen und Anweisungen zu überprüfen.

Die Kontrollgänge sollen nicht dem Finden von Tätern dienen, um diese zu bestrafen. Sinn der Kontrollen soll es in erster Linie sein, erkannte Nachlässigkeiten möglichst sofort zu beheben (Fenster zu schließen, Unterlagen in Aufbewahrung zu nehmen etc.). In zweiter Linie können Ursachen für diese Nachlässigkeiten erkannt und evtl. in der Zukunft vermieden werden.

Die Kontrollgänge sollten durchaus auch während der Dienstzeit erfolgen und zur Information der Mitarbeiter über das Wie und Warum von Regelungen genutzt werden. So werden sie von allen Beteiligten eher als Hilfe denn als Gängelung angesehen.

M 2.19 Neutrale Dokumentation in den Verteilern

Verantwortlich für Initiierung: Leiter Haustechnik

Verantwortlich für Umsetzung: Leiter Haustechnik, Planer

In jedem Verteiler sollte sich eine Dokumentation befinden, die den derzeitigen Stand von Rangierungen und Leitungsbelegungen wiedergibt. Diese Dokumentation ist möglichst neutral zu halten. Nur bestehende und genutzte Verbindungen sind darin aufzuführen. Es sollen, soweit nicht ausdrücklich vorgeschrieben (z. B. für Brandmeldeleitungen) keine Hinweise auf die Nutzungsart der Leitungen gegeben werden. Leitungs-, Verteiler-, und Raumnummern reichen in vielen Fällen aus. Alle weitergehenden Informationen sind in einer Revisions-Dokumentation aufzuführen.

Ergänzende Kontrollfragen:

- Wie wird sichergestellt, dass die Dokumentation immer aktuell ist?
- Wie wird sichergestellt, dass keine unzulässigen Informationen in dieser Dokumentation enthalten sind?

M 2.20 Kontrolle bestehender Verbindungen

Verantwortlich für Initiierung: Leiter Haustechnik, Leiter IT

Verantwortlich für Umsetzung: Leiter Haustechnik, Planer

Alle Verteiler und Zugdosen sind einer (zumindest stichprobenartigen) Sichtprüfung zu unterziehen. Dabei ist auf folgende Punkte zu achten:

- Spuren von gewaltsamen Öffnungsversuchen an verschlossenen Verteilern,
- Aktualität der im Verteiler befindlichen Dokumentation,
- Übereinstimmung der tatsächlichen Beschaltungen und Rangierungen mit der Dokumentation,
- Unversehrtheit der Kurzschlüsse und Erdungen nicht benötigter Leitungen und
- unzulässige Einbauten/Veränderungen.

Neben der reinen Sichtkontrolle kann zusätzlich eine funktionale Kontrolle durchgeführt werden. Dabei werden bestehende Verbindungen auf ihre Notwendigkeit und die Einhaltung technischer Werte hin geprüft. In zwei Fällen ist diese Prüfung anzuraten:

- bei Verbindungen, die sehr selten genutzt und bei denen Manipulationen nicht sofort erkannt werden,
- bei Verbindungen, auf denen häufig und regelmäßig schützenswerte Informationen übertragen werden.

Ergänzende Kontrollfragen:

- In welchem Turnus werden bestehende Verbindungen kontrolliert?
- Wie werden festgestellte Unregelmäßigkeiten dokumentiert und verfolgt?
- Wem sind welche festgestellten Unregelmäßigkeiten zu melden?
- Wer führt die Beseitigung von Unregelmäßigkeiten durch und wer kontrolliert diese Arbeiten?

M 2.21 Rauchverbot

Verantwortlich für Initiierung: Leiter Haustechnik

Verantwortlich für Umsetzung: Mitarbeiter

In Räumen mit IT oder Datenträgern (Serverraum, Datenträgerarchiv, aber auch Belegarchiv), in denen Brände oder Verschmutzungen zu hohen Schäden führen können, sollte ein Rauchverbot erlassen werden. Dieses Rauchverbot dient gleicherweise dem vorbeugenden Brandschutz wie der Betriebssicherheit von IT mit mechanischen Funktionseinheiten.

Ergänzende Kontrollfragen:

- Wird das Rauchverbot in schutzbedürftigen Räumen eingehalten?

M 2.22 Hinterlegen des Passwortes

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Benutzer

Ist der Zugriff auf ein IT-System durch ein Passwort geschützt, so müssen Vorkehrungen getroffen werden, die bei Abwesenheit eines Mitarbeiters, z. B. im Urlaubs- oder Krankheitsfall, seinem Vertreter den Zugriff auf das IT-System ermöglichen.

Hierfür gibt es verschiedene Möglichkeiten, die von den benutzten IT-Systemen bzw. IT-Anwendungen und von den IT-Sicherheitsrichtlinien der jeweiligen Organisation abhängen. So kann z. B. das Passwort an einer geeigneten Stelle hinterlegt werden. Bei typischen Mehrbenutzersystemen kann auch der Administrator die benötigten Benutzerrechte freigeben oder das Passwort auf einen neuen Wert setzen. Bei vielen IT-Systemen bzw. IT-Anwendungen können aber Gruppen eingerichtet werden, so dass die eingetragenen Vertreter im Abwesenheitsfall Zugriff auf das System haben.

Alle genannten Lösungen haben verschiedene Vor-, aber auch Nachteile, so dass genau abgewogen werden muss, welche Lösung die in der jeweiligen Situation am geeignetesten ist.

Die folgenden Beispiele sollen dies aufzeigen:

Die Buchhalterin Frau Müller arbeitet an einem Windows-PC, der als Client in einem LAN angeschlossen ist. Um für den Vertretungsfall alle potentiellen Problembereiche abzudecken, wurden ihre Tätigkeitsbereiche mit ihr durchgegangen und Lösungen entwickelt.

Gruppen-Berechtigungen

- Sie ist für die Bearbeitung aller Vorgänge mit den Partnerfirmen A-K zuständig. Die zu bearbeitenden Daten befinden sich in einer Datenbank auf dem Server PF1. Im Vertretungsfall können ihre Kollegen Schmidt und Eifrig unter ihren eigenen Benutzer-Kennungen diese Daten bearbeiten, da sie die entsprechenden Berechtigungen in der Datenbank haben.

Arbeitsergebnisse gehören auf den Server

- Einige von ihr erstellte Dokumente befinden sich auf ihrem PC. Es wurde eine Vereinbarung getroffen, dass sie alle für den Betrieb wichtigen Dateien in Projektverzeichnisse auf den Server einstellt. Falls im Vertretungsfall ein Zugriff notwendig wird, kann der Administrator diesen ermöglichen. Dies muss schriftlich dokumentiert werden. Frau Müller erhält darüber anschließend eine E-Mail.
- Frau Müller benutzt für die Kundenverwaltung der betreuten Firmen eine alte, aber stabile IT-Anwendung. Da diese es technisch nicht zulässt, dass Vertretungsregelungen auf dem Weg von Zugriffsberechtigungen eingeführt werden, erhält der Vertreter Herr Schmidt das Passwort für ihren Zugang. Dadurch kann er bei ihrer Abwesenheit anfallende Änderungen einpflegen.

- Einige finanzrelevante Vorgänge müssen mit einer digitalen Signatur autorisiert werden. Allen Mitarbeitern sind dafür persönliche kryptographische Schlüssel auf Chipkarten ausgehändigt worden, die nicht weitergegeben werden dürfen. Im Vertretungsfall unterzeichnet ihr Vertreter mit seiner digitalen Signatur.

Passwort-Hinterlegung muss durchdacht sein

Eine Hinterlegung von Passwörtern ist immer mit einem großen organisatorischen Aufwand verbunden: Bei der Passwort-Hinterlegung sind die benötigten aktuellen Passwörter durch jeden Mitarbeiter an einer geeigneten Stelle (z. B. im Sekretariat in einem Safe in einem geschlossenen Umschlag) zu hinterlegen. Bei jeder Änderung eines der Passwörter ist dieses zu aktualisieren. Es darf kein Passwort dabei vergessen werden. (Manchmal werden für den Zugriff auf eine Anwendung auf einem Rechner bis zu fünf verschiedene Passwörter benötigt.) Es darf nicht möglich sein, dass Unbefugte auf die hinterlegten Passwörter Zugriff nehmen. Wird es notwendig, eines der hinterlegten Passwörter zu nutzen, so sollte dies nach dem Vier-Augen-Prinzip, d. h. von zwei Personen gleichzeitig, geschehen. Jeder Zugriff darauf muss dokumentiert werden.

Passwörter sollten möglichst nur dann hinterlegt werden, wenn es keine andere (technische) Lösung gibt. Dabei ist immer zu beachten, dass die Hinterlegung von Passwörtern einen falschen Signalcharakter für den sicheren Umgang mit Passwörtern vermittelt. Passwörter dürfen nicht unter Tastaturen oder ähnlichen Orten "hinterlegt" und auch nicht unter Kollegen weitergegeben werden, nur weil es einfacher ist, als den Administrator um die Vergabe einer notwendigen Zugriffsberechtigung zu bitten.

Passwörter sollten aber immer dann sicher hinterlegt werden, wenn diese die einzige Möglichkeit sind, auf das IT-System oder die IT-Anwendung Zugriff zu nehmen. Dies ist z. B. meistens bei Administrator-Zugängen oder Einzelplatz-Systemen der Fall.

Es sollte daher eine Regelung geben, in der beschrieben ist, welche Art von Passwörtern hinterlegt werden sollten und welche Rahmenbedingungen dafür geschaffen werden müssen.

Telearbeiter

Bei einem Telearbeiter ist sicherzustellen, dass dessen Passwörter für die IT-Systeme am häuslichen Arbeitsplatz auch in der Institution hinterlegt werden, damit im Notfall sein Vertreter auf die im Telearbeitsrechner gespeicherten Daten zugreifen kann.

Administratoren

Bei allen von Administratoren betreuten Systemen, insbesondere bei vernetzten Systemen, ist durch regelmäßige Überprüfung sicherzustellen, dass das aktuelle Systemadministrator-Passwort hinterlegt ist.

Ergänzende Kontrollfragen:

- Existiert eine Regelung zur Hinterlegung von Passwörtern?
- Sind die hinterlegten Passwörter vollständig und aktuell?
- Ist die ordnungsgemäße Verwendung eines hinterlegten Passwortes geregelt?
- Wird anhand der Aktualisierungen der hinterlegten Passwörter die Wechselsystematik kontrolliert?
- Wurde überprüft, ob es Alternativen zur Passwort-Hinterlegung gibt?

M 2.23 Herausgabe einer PC-Richtlinie

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Benutzer

Um einen sicheren und ordnungsgemäßen Einsatz von Informationstechnik in größeren Unternehmen bzw. Behörden zu fördern, sollte eine Richtlinie erstellt werden, in der verbindlich vorgeschrieben wird, welche Randbedingungen eingehalten werden müssen und welche IT-Sicherheitsmaßnahmen zu ergreifen sind. Die Richtlinie ist allen Benutzern zur Kenntnis zu geben, beispielsweise in elektronischer Form auf einem Intranet-Server. Jeder neue Benutzer muss die Kenntnisnahme der Richtlinie bestätigen, bevor er die Informationstechnik nutzen darf. Nach größeren Änderungen an der Richtlinie oder nach spätenstens 2 Jahren ist eine erneute Bestätigung erforderlich.

Im Folgenden soll grob umrissen werden, welche Inhalte für eine solche Richtlinie sinnvoll sind:

Zielsetzung und Begriffsdefinitionen

Der erste Teil der Richtlinie dient dazu, die Anwender für IT-Sicherheit zu sensibilisieren und zu motivieren. Gleichzeitig werden die für das gemeinsame Verständnis notwendigen Begriffe definiert, wie z. B. PC, Server, Netz, Anwender, Benutzer, schutzbedürftige Objekte.

Geltungsbereich

In diesem Teil muss verbindlich festgelegt werden, für welche Teile des Unternehmens bzw. der Behörde die Richtlinie gilt.

Rechtsvorschriften und interne Regelungen

Hier wird im Überblick dargestellt, welche wesentlichen Rechtsvorschriften, z. B. das Bundesdatenschutzgesetz und das Urheberrechtsgesetz, einzuhalten sind. Anhand von Beispielen sollte deutlich gemacht werden, welche Auswirkungen dies auf die Nutzung der Informationstechnik im jeweiligen Umfeld hat. Darüber hinaus kann diese Stelle genutzt werden, um alle relevanten betriebsinternen Regelungen aufzuführen.

Verantwortungsverteilung

In diesem Teil wird definiert, welcher Funktionsträger im Zusammenhang mit dem IT-Einsatz welche Verantwortung tragen muss. Dabei sind insbesondere die Rollen Benutzer, Vorgesetzte, Administrator, Revisor, Datenschutzbeauftragter und IT-Sicherheitsmanagement-Team zu unterscheiden.

Ansprechpartner

Die Richtlinie sollte Ansprechpartner und Kontaktinformationen (Telefon, E-Mail etc.) für die Benutzer zu Fragen der IT-Sicherheit enthalten oder aufzeigen, wo diese Informationen gefunden werden können. Dabei sollte beachtet werden, dass es häufig zu Verwirrung führt, wenn den Benutzern zu viele unterschiedliche Ansprechpartner genannt werden. Besser ist es meist, nur wenige unterschiedliche Ansprechpartner zu benennen, die dann bei Bedarf die Benutzer an die richtige Stelle verweisen (Help-Desk-Konzept).

Umzusetzende und einzuhaltende IT-Sicherheitsmaßnahmen

Im letzten Teil der Richtlinie für die IT-Nutzung ist festzulegen, welche IT-Sicherheitsmaßnahmen vom Benutzer einzuhalten bzw. umzusetzen sind. Dies kann je nach Schutzbedarf auch über die IT-Grundschutz-Maßnahmen hinausgehen. Typische Beispiele für IT-Sicherheitsmaßnahmen am Arbeitsplatz sind das sichere An- und Abmelden am PC, der ordnungsgemäße Umgang mit Passwörtern und Verhaltensregeln bei der Nutzung des Internets.

Sind Telearbeiter im Unternehmen bzw. in der Behörde beschäftigt, sollte die Richtlinie um die Telearbeitsplatz-spezifischen Regelungen ergänzt werden.

Ergänzende Kontrollfragen:

- Existiert eine Richtlinie für die IT-Nutzung?
- Wie wird die Einhaltung der Richtlinie überprüft?
- Wird regelmäßig geprüft, ob die Inhalte der Richtlinie, insbesondere die einzuhaltenden IT-Sicherheitsmaßnahmen, noch aktuell sind?
- Steht die Richtlinie für die IT-Nutzung jedem Benutzer zur Verfügung?
- Wird die Richtlinie bei den Schulungen zu IT-Sicherheitsmaßnahmen berücksichtigt?

M 2.24 Einführung eines IT-Passes

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Leiter IT

Der erste Schritt bei der Erstellung eines IT-Sicherheitskonzeptes besteht darin, sich einen Überblick über die vorhandenen Systeme, Anwendungen und Daten zu verschaffen. Für eine kleine Institution ist es im Allgemeinen effektiv, anhand der vorhandenen IT-Systeme vorzugehen. Daher ist es für kleine Institutionen hilfreich, wenn für jedes IT-System ein IT-Pass vorhanden ist, der die wichtigsten Informationen des IT-Systems zusammenfasst.

Schneller Überblick für kleine Institutionen

Der IT-Pass soll dem IT-Verantwortlichen einen Überblick über die vorhandenen Computer in seiner Institution verschaffen und ein schnelles effektives Reagieren bei Problemen ermöglichen. Der IT-Pass ist immer dann sinnvoll einzusetzen, wenn es sich um eine sehr kleine Institution mit wenigen IT-Systemen handelt, bei der sich umfangreiche Strukturanalysen nicht lohnen. Hierzu müssen zunächst für jedes IT-System folgende Informationen erfasst werden:

- Bezeichnung des IT-Systems (Inventarisierungsnummer)
- Ansprechpartner für Problemfälle, z. B. Service- und Hotline-Nummern für den Ausfall und die Wartung des Systems
- Informationen zum Betriebssystem
- Informationen zum Virenscanner (verwendetes Produkt und die Vorgehensweise, wie Updates bzw. Patches eingespielt werden)
- Standort des System (Raum)
- Übersicht über die wichtigsten Informationen und Anwendungen, die auf dem System gespeichert sind bzw. laufen
- Schutzbedarf abhängig von Grundwerten Vertraulichkeit, Integrität und Verfügbarkeit
- Informationen zur Systeminstallation und zur Systemkonfiguration
- zur Verfügung stehendes Zubehör
- durchgeführte Wartungen und Reparaturen
- Art der durchgeführten Datensicherungen

Hinweis: Die direkt an Endgeräte angeschlossenen Drucker werden nicht als eigenständige Komponenten, sondern als Teil des jeweiligen Endgeräts erfasst. In den IT-Pässen können sie unter Peripherie oder Hardware aufgeführt werden.

Gleichartige IT-Systeme wie Anwender-PCs können auch in Gruppen zusammengefasst werden. Falls Mobiltelefone oder PDAs genutzt werden, sollte zusammenfassend für diese Geräte ebenfalls ein IT-Pass erstellt werden, wobei die Felder des Passes entsprechend anzupassen sind.

Auch für Telefonanlagen und Anschlüsse an Datennetze sollten die wichtigsten Informationen in Form eines IT-Passes dokumentiert werden.

Um den Schutzbedarf des IT-Systems zu dokumentieren, sollte der IT-Pass für jede wichtige Anwendung festhalten, ob dort z. B. personenbezogene Daten verarbeitet werden, und den Schutzbedarf abhängig von den Grundwerten Vertraulichkeit, Integrität und Verfügbarkeit festlegen.

Zusätzlich können die durchgeführten IT-Sicherheitsmaßnahmen am IT-System dokumentiert werden, so dass z. B. im Schadensfall schnell reagiert werden kann.

Die IT-Pässe sollten entweder vom IT-Sicherheitsmanagement oder vom Administrator geführt werden. Sie können auch durch Mitarbeiter ausgefüllt werden, müssen aber dann danach inhaltlich und auf Vollständigkeit geprüft werden. Die IT-Pässe sollten zentral gesammelt werden. Da sich bei gleichartigen IT-Systemen wie PCs viele Antworten wiederholen, ist es hilfreich, die IT-Pässe elektronisch zu führen.

Bei Änderungen an einem IT-System sind die Einträge im IT-Pass sofort anzupassen, so dass die Dokumentation immer auf dem aktuellen Stand ist.

IT-Pässe erleichtern die Durchführung von Kontrolltätigkeiten entschieden, da die Dokumentation aller durchgeführten relevanten Änderungen und IT-Sicherheitsmaßnahmen aus den IT-Pässen hervorgehen. Außerdem unterstützt das Führen solcher IT-Pässe die regelmäßige Pflege der IT und IT-Sicherheitsmaßnahmen, beispielsweise in Bezug auf Datensicherungen und Passwort-Änderungen. Dies dient auch der Notfallvorsorge.

Ein Muster eines solchen IT-Passes findet sich unter den Hilfsmitteln zum IT-Grundschutz auf dem BSI-Webserver im "IT-Grundschutzprofil für eine kleine Institution".

M 2.25 Dokumentation der Systemkonfiguration

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator

Planung, Steuerung, Kontrolle und Notfallvorsorge des IT-Einsatzes basieren auf einer aktuellen Dokumentation des vorhandenen IT-Systems. Nur eine aktuelle Dokumentation der Systemkonfiguration ermöglicht im Notfall einen geordneten Wiederanlauf des IT-Systems.

physikalische und logische Netzkonfiguration

Bei einem Netzbetrieb ist die physikalische Netzstruktur (siehe M 5.4 *Dokumentation und Kennzeichnung der Verkabelung*) und die logische Netzkonfiguration zu dokumentieren. Dazu gehören auch die Zugriffsrechte der einzelnen Benutzer (siehe M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*) und der Stand der Datensicherung. Weiterhin sind die eingesetzten Applikationen und deren Konfiguration sowie die Dateistrukturen auf allen IT-Systemen zu dokumentieren.

Verfügbarkeit der Dokumentation

Dabei ist auf Aktualität und Verständlichkeit der Dokumentation zu achten, damit auch ein Vertreter die Administration jederzeit weiterführen kann. Die System-Dokumentation ist so aufzubewahren, dass sie im Bedarfsfall jederzeit verfügbar ist. Wenn sie in elektronischer Form geführt wird, sollte sie entweder regelmäßig ausgedruckt oder auf einem transportablen Datenträger gespeichert werden. Der Zugriff auf die Dokumentation ist auf die zuständigen Administratoren zu beschränken.

Vorgehensweise zum Herauf- bzw. Herunterfahren

In der System-Dokumentation sollten alle Schritte dokumentiert sein, die beim Herauf- bzw. Herunterfahren von IT-Systemen zu beachten sind. Dies ist insbesondere bei vernetzten IT-Systemen wichtig. Hier muss z. B. häufig eine bestimmte Reihenfolge beim Mounten von Laufwerken oder Starten von Netzdiensten eingehalten werden.

Ergänzende Kontrollfragen:

- Ist die vorhandene Dokumentation aktuell?
- Kann aufgrund der Dokumentation die Administration weitergeführt werden?

M 2.26 Ernennung eines Administrators und eines Vertreters

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, TK-Anlagen-Verantwortlicher

Verantwortlich für Umsetzung: -

Um einen geordneten Betrieb von IT-Systemen zu ermöglichen, sind für alle IT-Systeme und Netze Administratoren zu bestimmen. Ihnen obliegt neben allgemeinen Administrationsarbeiten insbesondere die Benutzerverwaltung einschließlich der Verwaltung der Zugriffsrechte. Zusätzlich sind sie für die Sicherheitsbelange aller von ihnen betreuten IT-Systeme zuständig.

Überschneidungen und Lücken in der Aufgabenverteilung vermeiden

Bei größeren Behörden bzw. Unternehmen mit einer Vielzahl verschiedener IT-Systeme und Teilnetzen muss außerdem sichergestellt sein, dass die Aufgaben zwischen den verschiedenen Administratoren so verteilt sind, dass es zu keinen Zuständigkeitsproblemen kommt, also weder zu Überschneidungen noch zu Lücken in der Aufgabenverteilung. Darüber hinaus sollte die Kommunikation zwischen den verschiedenen Administratoren möglichst reibungslos ablaufen. Hierzu können z. B. regelmäßige Administratoren-Treffen durchgeführt werden, bei denen typische Probleme und Lösungsmöglichkeiten bei der täglichen Arbeit thematisiert werden.

Rollentrennung zwischen Administration und Revision

Beim Einsatz von Protokollierung sollte auf die Rollentrennung von Administration und Revision geachtet werden. Hier ist zu überprüfen, inwieweit die IT-Systeme dies unterstützen.

separate Administratorkennung für den Vertreter

Um bei Verhinderung eines Administrators die Funktionen weiter aufrechtzuerhalten, ist ein Vertreter zu benennen. Hierbei ist darauf zu achten, dass dieser eine eigene Administratorkennung erhält (siehe auch M 2.38 *Aufteilung der Administrationstätigkeiten*). Auf keinen Fall darf aus Bequemlichkeit im Vertretungsfall einfach das Passwort weitergegeben werden.

Für die Übernahme von Administrationsaufgaben muss gewährleistet sein, dass jedem Administrator und ebenso den Vertretern für eine sorgfältige Aufgabenerfüllung auch die hierfür erforderliche Zeit zur Verfügung steht. Hierbei muss auch berücksichtigt werden, dass Aus- und Fortbildungsmaßnahmen erforderlich sind.

z/OS-spezifische Administrationsaufgaben

Die spezifischen Administrationstätigkeiten beim Einsatz von z/OS-Systemen werden in M 2.295 *Systemverwaltung von z/OS-Systemen* erläutert.

Ergänzende Kontrollfragen:

- Wurden alle Administratoren und Vertreter ausreichend geschult?
- Wurden Zuständigkeiten für die Administration geändert und die notwendigen Schulungsmaßnahmen eingeleitet?

M 2.27 Verzicht auf Fernwartung der TK-Anlage

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, TK-Anlagen-Verantwortlicher

Verantwortlich für Umsetzung: -

Der Verzicht auf Fernwartung ist eine wirkungsvolle Maßnahme, um Externe an Manipulationen an der TK-Anlagenkonfiguration zu hindern. Für Einzelanlagen und kleine Anlagenverbunde mit geringen räumlichen Entfernungen zwischen den einzelnen Verbundmitgliedern kann dies auch aus ökonomischen Gründen sinnvoll sein.

Vorteil: Im Gegensatz zu allen anderen in Baustein B 3.401 *TK-Anlage* aufgeführten Maßnahmen kann hierdurch garantiert werden, dass auch bei direktem Zugriff auf die Leitungen der Telekom keine Zugriffsmöglichkeit auf den Wartungseingang der Anlage möglich ist. Eine ähnliche Sicherheit wäre sonst nur unter Zuhilfenahme von Kryptomitteln erreichbar.

Nachteil: Alle Wartungsarbeiten müssen direkt an der Anlage durchgeführt werden. Ohne zusätzliche Maßnahmen, z. B. Verlagerung des Wartungs-PCs in den Nachbarraum, hat das Wartungspersonal auch immer Zutritt zur TK-Anlage. Oft werden die Remote-Schnittstellen nicht nur für den Zweck der Fernwartung genutzt. Über dieselben Schnittstellen werden teilweise auch Fernsignalisierungen geführt, die für den Betrieb eines TK-Netzes notwendig sind. In solchen Fällen wäre mit dem Verzicht auf Fernwartung auch ein Verzicht auf ein zentrales Netzmanagement verbunden. Soll eine Remote-Schnittstelle nur für Fernsignalisierungszwecke via Modem benutzt werden, so sollte dieses Modem so konfiguriert werden, dass keine Rufe entgegengenommen werden.

Ergänzende Kontrollfragen:

- Welche Gründe sprechen für und welche gegen den Verzicht der Fernwartung?
- Wurde die Entscheidung über die Fernwartung herbeigeführt?

M 2.28 Bereitstellung externer TK-Beratungskapazität

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, TK-Anlagen-Verantwortlicher

Verantwortlich für Umsetzung: -

Um in schwierigen Fällen schnell auf fachkundige Hilfe zurückgreifen zu können, sollte schon beim Kauf bzw. der Miete einer TK-Anlage an die Bereitstellung entsprechender Beratungsdienstleistung gedacht werden. Wichtig hierbei ist, dass in einer Notfallsituation die Unterstützung schnell erfolgen kann, da der Ausfall einer TK-Anlage die Handlungsfähigkeit einer gesamten Institution erheblich beeinträchtigen und ggf. nur für kurze Zeit toleriert werden kann.

Ergänzende Kontrollfragen:

- Wie lange kann auf die TK-Anlage verzichtet werden?
- In welcher Zeit kann Unterstützung seitens des Herstellers in Anspruch genommen werden?
- Welche Zeit wird für einen kompletten "Restart" der Anlage auf Basis der Datensicherungsbestände benötigt?

M 2.29 Bedienungsanleitung der TK-Anlage für die Benutzer

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, TK-Anlagen-Verantwortlicher

Verantwortlich für Umsetzung: Administrator

Dem Benutzer der TK-Anlage sind die notwendigen Unterlagen zur Bedienung seiner Endgeräte (z. B. Bedienungsanleitung für das Telefon) zur Verfügung zu stellen. Neben der normalen Bedienung seines Telefons sollte der Benutzer vor allem in der Lage sein, etwaige Warnanzeigen (LEDs oder Piktogramme im Display) und -töne zu interpretieren (siehe M 3.12 *Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne*).

Ergänzende Kontrollfragen:

- Liegen an allen Endgeräten die richtigen Bedienungsanleitungen vor?
- Kann der Benutzer die ihm zur Verfügung stehenden Leistungsmerkmale richtig anwenden?
- Kennt der Benutzer die Warnanzeigen und -töne?

M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Regelungen für die Einrichtung von Benutzern / Benutzergruppen bilden die Voraussetzung für eine angemessene Vergabe von Zugriffsrechten und für die Sicherstellung eines geordneten und überwachbaren Betriebsablaufs.

Es sollte ein Formblatt existieren, um von jedem Benutzer bzw. für jede Benutzergruppe zunächst die erforderlichen Daten abzufragen:

- Name, Vorname,
- Vorschlag für die Benutzer- bzw. Gruppenkennung, wenn diese nicht durch Konventionen vorgegeben sind,
- Organisationseinheit,
- Erreichbarkeit (z. B. Telefon, Raum),
- ggf. Projekt,
- ggf. Angaben über die geplante Tätigkeit im System und die dazu erforderlichen Rechte sowie die Dauer der Tätigkeit,
- ggf. Restriktionen auf Zeiten, Endgeräte, Plattenvolumen, Zugriffsberechtigungen (für bestimmte Verzeichnisse, Remote-Zugriffe, etc.), eingeschränkte Benutzerumgebung,
- ggf. Zustimmung von Vorgesetzten.

Falls Zugriffsberechtigungen vergeben werden, die über den Standard hinausgehen, sollte dies begründet werden. Dieses kann auch in elektronischer Form erfolgen durch ein spezielles Login, dessen Name und Passwort den einzurichtenden Benutzern bekanntgegeben wird. Dort wird ein entsprechendes Programm durchlaufen, das mit einem Logout endet. Die erfassten Daten können zur Vorlage beim Vorgesetzten ausgedruckt werden. Ein Passwort, das einem neuen Benutzer für die erstmalige Systemnutzung mitgeteilt wird, muss danach gewechselt werden. Dies sollte vom System initiiert werden.

Es sollte eine begrenzte Anzahl von Rechteprofilen festgelegt werden. Ein neuer Benutzer wird dann einem solchen Profil zugeordnet und erhält damit genau die für seine Tätigkeit erforderlichen Rechte. Dabei sind die systemspezifischen Möglichkeiten bei der Einrichtung von Benutzern und Gruppen zu beachten. Es ist sinnvoll, Namenskonventionen für die Benutzer- und Gruppennamen festzulegen (z. B. Benutzer-ID = Kürzel Organisationseinheit || lfd. Nummer).

Die Zugriffsberechtigung für Dateien ist auf Benutzer bzw. Gruppen mit berechtigtem Interesse zu beschränken. Wenn mehrere Personen auf eine Datei zugreifen müssen, soll für diese eine Gruppe eingerichtet werden. In der Regel muss jedem Benutzer eine eigene Benutzer-Kennung zugeordnet sein, es dürfen nicht mehrere Benutzer unter derselben Kennung arbeiten. Für jeden Benutzer muss ein eindeutiges Heimatverzeichnis angelegt werden.

spezielle Logins für die Benutzerverwaltung

Für die Einrichtungsarbeiten im System sollte eine administrative Rolle geschaffen werden: Die Einrichtung sollte mit Hilfe eines speziellen Logins, unter dem ein entsprechendes Programm oder Shellskript gestartet wird, erfolgen. Die zuständigen Administratoren können Benutzer bzw. Benutzergruppen somit nur auf definierte Weise einrichten, und es ist nicht erforderlich, ihnen Rechte für andere Administrationsaufgaben zu geben.

Besondere Unix-Maßnahmen

Diese Maßnahme wird unter Unix ergänzt durch folgende Maßnahmen:

- M 4.13 *Sorgfältige Vergabe von IDs*
- M 4.19 *Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen*
- M 4.20 *Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen*

Besondere z/OS-Maßnahmen

Diese Maßnahme wird unter z/OS ergänzt durch folgende Maßnahmen:

- M 2.289 *Einsatz restriktiver z/OS-Kennungen*
- M 2.297 *Deinstallation von z/OS-Systemen*
- M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*

Andere Betriebssysteme

Bei anderen Betriebssystemen sind die dort beschriebenen Hinweise in ähnlicher Weise umzusetzen (siehe dazu auch die betriebssystemspezifischen Bausteine).

Ergänzende Kontrollfragen:

- Gibt es organisatorische Regelungen zur Einrichtung von Benutzern bzw. Benutzergruppen?
- Gibt es ein Programm zur Einrichtung von Benutzern bzw. Benutzergruppen?

M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Es muss eine Dokumentation der am IT-System zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile erfolgen. Dabei gibt es verschiedene Dokumentationsmöglichkeiten wie beispielsweise über

- vorgegebene Administrationsdateien des Systems,
- individuelle Dateien, die vom zuständigen Administrator verwaltet werden,
- in Papierform.

Es sollte eine geeignete Form ausgewählt werden, möglichst einheitlich für die gesamte Institution.

Umfang der Dokumentation

Dokumentiert werden sollten insbesondere folgende Angaben zur Rechtevergabe an Benutzer und Benutzergruppen:

Zugelassene Benutzer:

- zugeordnetes Rechteprofil (gegebenfalls Abweichungen vom verwendeten Standard-Rechteprofil)
- Begründung für die Wahl des Rechteprofils (und gegebenfalls der Abweichungen)
- Zuordung des Benutzers zu einer Organisationeinheit, Raum- und Telefonnummer
- Zeitpunkt und Grund der Einrichtung
- Befristung der Einrichtung

Zugelassene Gruppen:

- zugehörige Benutzer
- Zeitpunkt und Grund der Einrichtung
- Befristung der Einrichtung

Die Dokumentation der zugelassenen Benutzer und Rechteprofile sollte regelmäßig (mindestens alle 6 Monate) daraufhin überprüft werden, ob sie den tatsächlichen Stand der Rechtevergabe widerspiegelt und ob die Rechtevergabe noch den Sicherheitsanforderungen und den aktuellen Aufgaben der Benutzer entspricht.

z/OS-spezifische Empfehlungen

Für das Betriebssystem z/OS finden sich weitere Empfehlungen in den folgenden Maßnahmen:

- M 2.289 *Einsatz restriktiver z/OS-Kennungen*
- M 2.297 *Deinstallation von z/OS-Systemen*
- M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*

Die vollständige Dokumentation ist Voraussetzung für Kontrollen der vergebenen Benutzerrechte.

Die Dokumentation muss so gespeichert beziehungsweise aufbewahrt werden, dass sie vor unbefugtem Zugriff geschützt ist und so, dass auch bei einem größeren IT-Sicherheitsvorfall oder IT-Ausfall darauf zugegriffen werden kann. Falls die Dokumentation in elektronischer Form erfolgt, muss sie in das Datensicherungsverfahren einbezogen werden.

Ergänzende Kontrollfragen:

- Sind Aufzeichnungen über die zugelassenen Benutzer und Gruppen und deren Rechteprofile vorhanden?
- Sind die Aufzeichnungen aktuell?
- Wann wurden die Aufzeichnungen das letzte Mal überprüft?
- Sind die Aufzeichnungen vor unberechtigten Zugriffen ausreichend geschützt?

M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Falls Benutzer nur bestimmte Aufgaben wahrzunehmen brauchen, ist es oftmals nicht erforderlich, ihnen alle mit einem eigenen Login verbundenen Rechte (ggf. sogar Systemadministrator-Rechte) zu geben. Beispiele sind bestimmte Tätigkeiten der routinemäßigen Systemverwaltung (wie Erstellung von Backups, Einrichten eines neuen Benutzers), die mit einem Programm menügesteuert durchgeführt werden, oder Tätigkeiten, für die ein Benutzer nur ein einzelnes Anwendungsprogramm benötigt. Insbesondere bei Aushilfskräften sollte darauf geachtet werden, dass diese nur die Dienste verwenden und nur auf die Daten zugreifen dürfen, die sie tatsächlich benötigen. Wenn ihre Tätigkeit beendet ist, sollte deren Accounts deaktiviert und alle anderen Zugangsberechtigungen entfernt werden (siehe auch M 4.17 *Sperren und Löschen nicht benötigter Accounts und Terminals*).

Restricted Shell und chroot verwenden

Für diese Benutzer sollte eine eingeschränkte Benutzerumgebung geschaffen werden. Sie kann z. B. unter Unix durch eine Restricted Shell (*rsh*) und eine Beschränkung der Zugriffspfade mit dem Unix-Kommando *chroot* realisiert werden. Für einen Benutzer, der nur ein Anwendungsprogramm benötigt, kann dieses als Login-Shell eingetragen werden, so dass nach dem Einloggen dieses direkt gestartet und er bei Beendigung des Programms automatisch ausgeloggt wird.

Nutzung von Editoren und Compilern einschränken

Der verfügbare Funktionsumfang des IT-Systems kann für einzelne Benutzer oder Benutzergruppen eingeschränkt werden. Die Nutzung von Editorprogrammen oder Compilern sollte verhindert werden, wenn dies nicht für die Aufgabenerfüllung des Benutzers erforderlich ist. Dies kann bei Stand-alone-Systemen durch die Entfernung solcher Programme und bei vernetzten Systemen durch die Rechtevergabe geregelt werden.

Ergänzende Kontrollfragen:

- Welche Benutzerumgebung und welche Startprozedur ist für die jeweiligen Benutzer eingerichtet worden?
- Gibt es Regelungen für die Benutzerumgebungen von Aushilfskräften?

M 2.33 Aufteilung der Administrationstätigkeiten unter Unix

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

In den meisten Unix-Systemen gibt es nur eine Administrationsrolle (den *Super-User* namens *root* mit der Benutzer-ID (UID) 0). Personen mit Zugang zu dieser Rolle haben die volle Kontrolle über das System. Insbesondere können sie unabhängig von Zugriffsrechten jede Datei lesen, verändern und löschen.

Vier-Augen-Prinzip

Das Super-User-Passwort darf nur den Administratoren bekannt sein. Die Weitergabe des Passworts ist auf die in Regelungen festgelegte Fälle zu beschränken und zu dokumentieren. Der Super-User-Login *root* kann durch Anwendung des Vier-Augen-Prinzips zusätzlich geschützt werden, z. B. durch organisatorische Maßnahmen wie ein geteiltes Passwort. Dabei muss das Passwort eine erhöhte Mindestlänge (12 oder mehr Zeichen) haben. Hierbei muss darauf geachtet werden, dass das Passwort in voller Mindestlänge vom System überprüft wird.

Rollentrennung

Bei etlichen Unix-Systemen ist eine Aufgabenteilung durch die Ausnutzung vorhandener Administratorrollen möglich. Diese Rollen sollen dann durch verschiedene Personen wahrgenommen werden.

Eine Reihe von Administrationstätigkeiten können auch ohne Zugang zum Login *root* ausgeführt werden. Wenn es Administratoren mit solchen Spezialaufgaben gibt, sollte davon Gebrauch gemacht werden. Insbesondere, wenn in großen Systemen mehrere Personen mit Administrationsaufgaben betraut werden müssen, kann das Risiko durch eine entsprechende Aufgabenteilung vermindert werden. Es gibt dazu zwei Möglichkeiten:

- Schaffung administrativer Logins: Sie haben zwar die UID 0, jedoch wird beim Login nur ein Programm gestartet, mit dem die administrative Aufgabe ausgeführt werden kann und das mit einem Logout endet. Beispiele: Einrichten neuer Benutzer, Mounten eines Laufwerks. Zu UNIX V.4 können z. B. die administrativen Login-Namen *setup*, *sysadm*, *powerdown*, *checkfsys*, *mountfsys* und *umountfsys* mit den gleichnamigen Programmen eingerichtet werden.
- Benutzung von Logins ohne UID 0: Diese Login-Namen (*sys*, *bin*, *adm*, *uucp*, *nuucp*, *daemon* und *lp*) sind Eigentümer von Dateien und Programmen, die für die Funktionalität des Systems entscheidend sind und die daher besonderem Schutz unterliegen. Sie sind in den meisten Unix-Systemen zur Verwaltung der entsprechenden Dienste vorgegeben.

Hilfsprogramme einsetzen

Um festzustellen, welche Logins Administratorrechte haben, sollten regelmäßig Hilfsprogramme (z. B. *cops, tiger*) eingesetzt werden, die nach Logins mit der UID 0 in der Passwort-Datei suchen.

Ergänzende Kontrollfragen:

- Welchen Personen ist das Super-User-Passwort bekannt?
- Sind Administrator-Rollen getrennt worden?
- Welche Logins haben die UID 0?
- Gibt es Logins mit UID 0 und Shell-Zugriff?

M 2.34 Dokumentation der Veränderungen an einem bestehenden System

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Überblick über das System

Um einen reibungslosen Betriebsablauf zu gewährleisten, muss der Administrator einen Überblick über das System haben bzw. sich verschaffen können. Dieses muss auch für seinen Vertreter möglich sein, falls der Administrator unvorhergesehen ausfällt. Der Überblick ist auch Voraussetzung, um Prüfungen des Systems (z. B. auf problematische Einstellungen, Konsistenz bei Änderungen) durchführen zu können.

Daher sollten die Veränderungen, die Administratoren am System vornehmen, dokumentiert werden, nach Möglichkeit automatisiert. Dieses gilt insbesondere für Änderungen an Systemverzeichnissen und -dateien.

neue Betriebssysteme oder Updates

Bei Installation neuer Betriebssysteme oder bei Updates sind die vorgenommenen Änderungen besonders sorgfältig zu dokumentieren. Möglicherweise kann durch die Aktivierung neuer oder durch die Änderung bestehender Systemparameter das Verhalten des IT-Systems (insbesondere auch Sicherheitsfunktionen) maßgeblich verändert werden.

Freigabe und Dokumentation ausführbarer Dateien

Unter Unix müssen ausführbare Dateien, auf die auch andere Benutzer als der Eigentümer Zugriff haben oder deren Eigentümer *root* ist, vom Systemadministrator freigegeben und dokumentiert werden (siehe auch M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*). Insbesondere müssen Listen mit den freigegebenen Versionen dieser Dateien geführt werden, die außerdem mindestens das Erstellungsdatum, die Größe jeder Datei und Angaben über evtl. gesetzte s-Bits enthalten. Sie sind Voraussetzung für den regelmäßigen Sicherheitscheck und für Überprüfungen nach einem Verlust der Integrität.

Ergänzende Kontrollfragen:

- Werden Logbücher über Systemveränderungen geführt?
- Sind die Aufzeichnungen aktuell und vollständig?
- Kann aufgrund der Aufzeichnungen die Administration weitergeführt werden?
- Sind die Aufzeichnungen vor unberechtigtem Zugriff geschützt?

M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Gegen bekannt gewordene und durch Veröffentlichungen zugänglich gemachte Sicherheitslücken müssen die erforderlichen organisatorischen und administrativen Maßnahmen ergriffen werden. Sicherheitsrelavante Updates oder Patches für die eingesetzte Hard- und Software müssen gegebenenfalls installiert werden (siehe auch M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*). Sind keine entsprechenden Updates oder Patches verfügbar, so muss eventuell zusätzliche Sicherheitshardware bzw. Sicherheitssoftware eingesetzt werden.

Es ist daher sehr wichtig, dass sich die Systemadministratoren regelmäßig über neu bekannt gewordene Schwachstellen informieren. Informationsquellen zu diesem Thema sind beispielsweise:

- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) (siehe *http://www.bsi.bund.de/*)
- Hersteller bzw. Distributoren von Programmen und Betriebssystemen. Diese informieren oft registrierte Kunden über bekannt gewordene Sicherheitslücken ihrer Systeme und stellen korrigierte Varianten des Systems oder Patches zur Behebung der Sicherheitslücken zur Verfügung.
- Computer Emergency Response Teams (CERTs). Dies sind Computer-Notfallteams, die als zentrale Anlaufstelle für präventive und reaktive Maßnahmen in bezug auf sicherheitsrelevante Vorfälle in Computersystemen dienen. CERTs informieren in sogenannten *Advisories* über aktuelle Schwachstellen in Hard- und Softwareprodukten und geben Empfehlungen zu deren Behebung. Verschiedene Organisationen oder Verbände unterhalten eigene CERTs.

  Das ursprüngliche CERT der Carnegie Mellon Universität diente als Vorbild für viele weitere derartige Teams und ist heute eine Art "Dach-CERT":

  Computer Emergency Response Team / Coordination Center (CERT/CC), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890,

  Telefon: +1-412-268-7090 (24-Stunden-Hotline), E-Mail: *cert@cert.org*, WWW: *http://www.cert.org*

  Die CERT-Mitteilungen werden in Newsgruppen (*comp.security.announce* und *info.nsfnet.cert*) und über Mailinglisten (Aufnahme durch E-Mail an: *cert-advisory-request@cert.org*) veröffentlicht.

  In Deutschland exisiteren unter anderem folgende CERTs:

- CERT-Bund, Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn, Telefon: 01888-CERTBUND

bzw. 01888-23782863, Fax: 01888-9582-5427, E-Mail: *certbund@bsi.bund.de*, WWW: *http://www.bsi.bund.de/certbund/*

- DFN-CERT, DFN-CERT, Zentrum für sichere Netzdienste GmbH, Heidenkampsweg 41, D-20097 Hamburg, Telefon: 040-808077-555, Fax: -556, E-Mail: *info@dfn-cert.de*, WWW: *http://www.dfn-cert.de*. Das DFN-CERT bietet verschiedene Mailinglisten an, siehe *http://www.dfn-cert.de/infoserv/dml.html*.
- An verschiedenen Hochschulen existieren CERTs, die auch Informationen öffentlich zur Verfügung stellen. Ein Beispiel ist das RUS-CERT der Universität Stuttgart (siehe *http://cert.uni-stuttgart.de*).

- Hersteller- und systemspezifische sowie sicherheitsspezifische Newsgruppen oder Mailinglisten. In solchen Foren werden Hinweise auf existierende oder vermutete Sicherheitslücken oder Fehler in diversen Betriebssystemen und sonstigen Softwareprodukten diskutiert. Besonders aktuell sind meist die englischsprachigen Mailinglisten wie *Bugtraq*, von denen es an vielen Stellen öffentlich zugängliche Archive gibt, beispielsweise unter *http://www.securityfocus.com*.
- manche IT-Fachzeitschriften veröffentlichen ebenfalls regelmäßig Beiträge mit einer Übersicht über neue Sicherheitslücken in verschiedenen Produkten.

Verschiedene Informationsquellen nutzen

Idealerweise sollten sich die Administratoren und der IT-Sicherheitsbeauftrage bei mindestens zwei verschiedenen Stellen über Sicherheitslücken informieren. Dabei ist es empfehlenswert, neben den Informationen des Herstellers auch eine "unabhängige" Informationsquelle zu benutzen.

Die Administratoren sollten jedoch in jedem Fall auch produktspezifische Informationsquellen des Herstellers nutzen, um beispielsweise darüber Bescheid zu wissen, ob für ein bestimmtes Produkt beim Bekanntwerden von Sicherheitslücken überhaupt Patches oder Updates bereitgestellt werden. Bei Produkten, für die der Hersteller keine Sicherheitspatches mehr zur Verfügung stellt, muss rechtzeitig geprüft werden, ob ein Einsatz unter diesen Umständen noch zu verantworten ist und durch welche zusätzlichen Maßnahmen ein Schutz der betroffenen Systeme trotzdem gewährleistet werden kann.

Ergänzende Kontrollfragen:

- Steht der Administrator in regelmäßigem Kontakt zu den Herstellern der betreuten Systeme? Sind diese Systeme registriert? Sind Wartungsverträge abgeschlossen worden?
- Welche Informationsmöglichkeiten sind bekannt? Welche werden genutzt?
- Werden neue Informationsquellen erschlossen?
- Werden bekannt gewordene Sicherheitslücken schnellstmöglich behoben?

M 2.36 Geregelte Übergabe und Rücknahme eines tragbaren PC

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Laptops und andere tragbare IT-Systeme werden je nach Einsatzzweck nur von einem einzelnen Mitarbeiter eingesetzt, z. B. als Arbeitsplatzrechner, der auch mobil genutzt wird. Sie können aber auch abwechselnd von verschiedenen Mitarbeitern genutzt werden, z. B. für Präsentationen. Je nach Einsatzart ergeben sich verschiedene Sicherheitsanforderungen. Daher sollte Einsatzzweck und -art im Vorfeld sorgfältig geplant werden.

Bei der Nutzung als Arbeitsplatzrechner werden diese typischerweise abwechselnd mobil und stationär genutzt. Dabei kann auf verschiedene Netze zugegriffen werden. Dafür müssen die Laptops so abgesichert sein, dass auf der einen Seite durch den mobilen Einsatz weder wichtige Daten der Laptops kompromittiert, manipuliert oder verloren gehen können. Auf der anderen Seite dürfen über die Laptops keine Gefährdungen in die internen Netze eingeschleppt werden.

Wenn Laptops abwechselnd von verschiedenen Personen genutzt werden, ist eine geregelte Übergabe extrem wichtig. Damit dies gut funktioniert, sollte ein Laptop-Pool eingerichtet werden (siehe M 1.35 *Sammelaufbewahrung tragbarer IT-Systeme*).

Geregelte Übergabe und Rücknahme

Bei der Übergabe und Rücknahme eines tragbaren IT-Systems sind folgende Punkte zu beachten:

Übergabe:

- Der neue Benutzer wird aufgefordert, direkt bei der Übergabe das alte Passwort des Laptops bzw. das Standardpasswort zu ändern.
- Dem neuen Benutzer sollte ein Merkblatt für den sicheren Umgang mit dem tragbaren IT-system übergeben werden.
- Damit jederzeit nachvollziehbar ist, wo sich die Geräte befinden, sollte jeder Benutzer mit Namen, Organisationseinheit, Telefonnummer, Einsatzzweck in ein Übergabe-/Rücknahmejournal eingetragen werden.

Rücknahme bzw. Weitergabe:

- Der Benutzer gibt sein zuletzt benutztes Passwort bekannt bzw. stellt ein Standardpasswort wie "LAPTOP" ein.
- Der Laptop muss mittels eines aktuellen Viren-Suchprogramms auf einen Computer-Viren-Befall überprüft werden.
- Der Benutzer muss sicherstellen, dass vor Übergabe des Gerätes sämtliche Daten, die der Benutzer noch benötigt, auf ihm zugängliche Datenträger (z. B. seinen PC) übertragen werden. Darüber hinaus hat der Benutzer dafür Sorge zu tragen, dass sämtliche von ihm erzeugten Dateien und Daten (nach Möglichkeit physikalisch) gelöscht werden. Hierfür müssen geeignete Tools vorhanden sein.

- Die Rückgabe des Laptops und das Untersuchungsergebnis der Virensuche werden dokumentiert. Die Vollständigkeit des Gerätes, des Zubehörs und der Dokumentation ist sicherzustellen.
- Um sicherzustellen, dass die definierte sichere Grundkonfiguration vorhanden ist und sich keine sensiblen Dateien mehr auf dem Laptop befinden, sollte der Laptop mit einer Referenzinstallation neu installiert werden (siehe hierzu M 4.28 *Software-Reinstallation bei Benutzerwechsel eines Laptops*).
- Zurückgegebene Datenträger werden neu formatiert.

Die vorgesehenen Einsatzarten der Laptops sind zu dokumentieren.

Ergänzende Kontrollfragen:

- Wurde der Einsatz von Laptops vor Beschaffung und Installation geplant?
- Welche Dokumentation existiert über die Planung der Laptops?
- Wird die Weitergabe eines tragbaren IT-Systems an Kollegen dokumentiert?
- Werden die dabei zu beachtenden Sicherheitsmaßnahmen eingehalten?

M 2.37 "Der aufgeräumte Arbeitsplatz"

Verantwortlich für Initiierung: Leiter Organisation, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Mitarbeiter

Jeder Mitarbeiter sollte dazu angehalten werden, seinen Arbeitsplatz "aufgeräumt" zu hinterlassen. Ein IT-Benutzer hat nicht nur dafür Sorge zu tragen, dass bei Verlassen seines Arbeitsplatzes entsprechende Vorkehrungen getroffen sind, dass Unbefugte keinen Zugang zu IT-Anwendungen oder Zugriff auf Daten erhalten. Alle Mitarbeiter müssen mit der gleichen Sorgfalt auch ihre Arbeitsplätze überprüfen und sicherstellen, dass keine sensiblen Informationen frei zugänglich sind und kein Verlust an Verfügbarkeit, Vertraulichkeit oder Integrität entstehen kann. Es darf nicht möglich sein, dass Unbefugte auf Datenträger (wie Disketten, USB-Sticks oder Festplatten) oder Unterlagen (Ausdrucke) zugreifen können.

Für eine kurze Abwesenheit während der Arbeitszeit ist es ausreichend, den Raum zu verschließen, sofern dies möglich ist. Bei geplanter Abwesenheit eines Mitarbeiters (z. B. längere Besprechungen, Dienstreisen, Urlaub, Fortbildungsveranstaltungen) ist der Arbeitsplatz so aufzuräumen, dass keine schutzbedürftigen Datenträger oder Unterlagen unverschlossen am Arbeitsplatz zurückgelassen werden. Dafür ist es natürlich erforderlich, dass die Mitarbeiter ausreichend dimensionierte und verschließbare Staumöglichkeiten haben, z. B. stabile Schränke.

Auch Passwörter dürfen auf keinen Fall sichtbar (als Klebezettel am Monitor, an einem leicht zu erratenden Ort wie z. B. unter der Schreibtischauflage oder in der unverschlossenen Schreibtischschublade) aufbewahrt werden (siehe M 2.2 *Betriebsmittelverwaltung)*. Ebenfalls sollten eindeutige Hinweise (z. B. Namen von Familienangehörigen oder sogenannte Trivialpasswörter wie aufeinanderfolgende Buchstaben und Zahlen) für das schnelle Erraten ausgeschlossen werden (siehe M 2.11 *Regelung des Passwortgebrauchs)*.

M 2.38 Aufteilung der Administrationstätigkeiten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Viele Netzbetriebssysteme bieten die Möglichkeit, die Administratorrolle aufzuteilen und Administrationstätigkeiten an verschiedene Benutzer zu verteilen.

So können z. B. unter Novell Netware 3.11 die folgenden Administratorrollen eingerichtet werden: Workgroup Manager, User Account Manager, File Server Console Operator, Print Server Operator, Print Queue Operator.

Unter Windows NT können durch die gezielte Vergabe von Benutzerrechten an einzelne Benutzer oder besser an Gruppen definierte Administratorrollen geschaffen werden. Neben der Gruppe der Administratoren sind hier die Gruppen Hauptbenutzer (d. h. Administratoren mit eingeschränkten Rechten), Sicherungs-Operatoren, Druck-Operatoren, Server-Operatoren sowie Reproduktions-Operatoren zu nennen. Darüber hinaus können weitere Rollen durch explizite Zuweisung von Benutzerrechten definiert werden (siehe auch M 4.50 *Strukturierte Systemverwaltung unter Windows NT*).

Wenn es Administratorrollen für Spezialaufgaben gibt, sollte davon Gebrauch gemacht werden. Insbesondere, wenn in großen Systemen mehrere Personen mit Administrationsaufgaben betraut werden müssen, kann das Risiko der übergroßen Machtbefugnis der Administratorrollen durch eine entsprechende Aufgabenteilung vermindert werden, so dass Administratoren nicht unkontrolliert unautorisierte oder unbeabsichtigte Veränderungen am System vornehmen können.

Trotz des Aufteilens von Administrationstätigkeiten legt das System meist noch automatisch einen Account für einen Administrator an, der keinen Beschränkungen unterliegt, den Supervisor. Das Supervisor-Passwort sollte, wenn überhaupt, nur einem kleinen Personenkreis bekannt sein. Es darf keinem der Subadministratoren bekannt sein, damit diese nicht auf diese Weise ihre Rechte erweitern können. Das Passwort ist gesichert zu hinterlegen (siehe M 2.22 *Hinterlegen des Passwortes*). Das Supervisor-Login kann durch Anwendung des Vier-Augen-Prinzips zusätzlich geschützt werden, z. B. durch organisatorische Maßnahmen wie ein geteiltes Passwort. Dabei muss das Passwort eine erhöhte Mindestlänge (12 oder mehr Zeichen) haben. Hierbei muss darauf geachtet werden, dass das Passwort in voller Mindestlänge vom System überprüft wird.

Ergänzende Kontrollfragen:

- Welchen Personen ist das Supervisor-Passwort bekannt?
- Sind Administrator-Rollen getrennt worden?

M 2.39 Reaktion auf Verletzungen der Sicherheitsvorgaben

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Es ist festzulegen, welche Reaktion auf Verletzungen der Sicherheitsvorgaben erfolgen soll, um eine klare und sofortige Reaktion gewährleisten zu können.

Untersuchungen sollten durchgeführt werden, um festzustellen, wie und wo die Verletzung entstanden ist. Anschließend müssen die angemessenen schadensbehebenden oder -mindernden Maßnahmen durchgeführt werden. Soweit erforderlich, müssen zusätzliche schadensvorbeugende Maßnahmen ergriffen werden. Die durchzuführenden Aktionen hängen sowohl von der Art der Verletzung als auch vom Verursacher ab.

Es muss geregelt sein, wer für Kontakte mit anderen Organisationen verantwortlich ist, um Informationen über bekannte Sicherheitslücken einzuholen (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*) oder um Informationen über aufgetretene Sicherheitslücken weiterzugeben. Es muss dafür Sorge getragen werden, dass eventuell. mitbetroffene Stellen schnellstens informiert werden (siehe Baustein B 1.8 *Behandlung von Sicherheitsvorfällen*).

Ergänzende Kontrollfragen:

- Ist die Vorgehensweise bei Verdacht auf Verletzung der Sicherheitsvorgaben klar definiert?

M 2.40 Rechtzeitige Beteiligung des Personal-/Betriebsrates

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Bei allen Maßnahmen, die prinzipiell die Verhaltens- oder Leistungsüberwachung von Mitarbeiter ermöglichen, z. B. Protokollierung, bedarf es der Mitbestimmung der Personalvertretung. Maßnahmen, die geeignet sind eine Verhaltens- oder Leistungsüberwachung eines Mitarbeiters zu ermöglichen - z. B. Protokollierung -, bedürfen der Mitbestimmung der Personalvertretung. Grundlage dessen sind in Deutschland die Betriebsverfassungs- und Personalvertretungsgesetze von Bund und Ländern. In anderen Ländern ist die Einbeziehung der Personalvertretung nicht immer erforderlich. Die rechtzeitige und umfassende Information des Betriebs- oder Personalrates empfiehlt sich aber grundsätzlich, da dies Zeitverzögerungen bei der Umsetzung von Maßnahmen im Bereich des IT-Grundschutzes verhindern kann.

Bei bereits bestehendem Verdacht, dass ein Sicherheitsvorfall (siehe Baustein 3.8 *Behandlung von Sicherheitsvorfällen*) durch einen internen Mitarbeiter ausgelöst wurde und entsprechende Nachforschungen durchgeführt werden sollen, die auf Sanktionen hinauslaufen, sind die Beteiligungsrechte des Personal-/Betriebsrates unbedingt zu beachten. Unterbleibt eine ordnungsgemäße Beteiligung der Mitarbeitervertretung, kann das eventuell erforderliche weitere Verfahren (gegebenenfalls vor dem Arbeitsgericht) je nach Schwere des Vorfalls für eine Abmahnung oder Kündigung aufgrund von Formfehlern gravierend beeinflusst werden.

Große Outsourcing-Dienstleister berichten aus der Praxis, dass eine frühzeitige Einbindung der Personalvertretung des Auftraggebers, möglichst schon in der Angebotsphase, sehr zum Gelingen des Projektes beitragen kann. Wechselbereitschaft der Mitarbeiter, Motivation, Arbeitszufriedenheit und zügige Projektabwicklung können durch Kooperation aller Beteiligten positiv beeinflusst werden.

M 2.41 Verpflichtung der Mitarbeiter zur Datensicherung

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Da die Datensicherung eine wichtige IT-Sicherheitsmaßnahmen ist, sollten die betroffenen Mitarbeiter auf die Einhaltung des Datensicherungskonzeptes bzw. des Minimaldatensicherungskonzeptes verpflichtet werden. Eine regelmäßige Erinnerung und Motivation zur Datensicherung sollte erfolgen.

Ergänzende Kontrollfragen:

- Wird die Verpflichtung zur Datensicherung schriftlich dokumentiert?
- Wird die Durchführung von Kontrollen auf Einhaltung der Datensicherungsverpflichtung vorgenommen?

M 2.42 Festlegung der möglichen Kommunikationspartner

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Datenschutzbeauftragter,

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Sollen Informationen an einen Kommunikationspartner übertragen werden, so muss sichergestellt werden, dass der Empfänger die notwendigen Berechtigungen zum Weiterverarbeiten dieser Informationen besitzt. Werden Informationen zwischen mehreren kommunizierenden Stellen ausgetauscht, so soll für alle Beteiligten ersichtlich sein, wer diese Informationen ebenfalls erhalten hat bzw. erhalten wird. Um die oben genannten Kriterien zu erfüllen, bedarf es einer Festlegung, welche Kommunikationspartner welche Informationen erhalten dürfen.

Auch aus Datenschutzgründen (siehe z. B. BDSG, Übermittlungskontrolle) sollte eine Übersicht erstellt werden, welche Empfänger berechtigt sind, Informationen, insbesondere personenbezogene Daten, per Datenträgeraustausch erhalten können.

Ergänzende Kontrollfragen:

- Existiert eine Festlegung für etwaige Kommunikationsbeziehungen?
- Werden die genannten Übersichten regelmäßig aktualisiert?

M 2.43 Ausreichende Kennzeichnung der Datenträger beim Versand

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Neben den in Maßnahme M 2.3 *Datenträgerverwaltung* dargestellten Umsetzungshinweisen ist bei einer ausreichenden Kennzeichnung von auszutauschenden Datenträgern darauf zu achten, dass Absender und (alle) Empfänger unmittelbar zu identifizieren sind. Die Kennzeichnung muss den Inhalt des Datenträgers eindeutig für den Empfänger erkennbar machen. Es ist jedoch bei schützenswerten Informationen wichtig, dass diese Kennzeichnung für Unbefugte nicht interpretierbar ist.

Darüber hinaus sollten die Datenträger mit den für das Auslesen **notwendigen Parametern** gekennzeichnet werden. So sind bei der Übermittlung von Magnetbändern unter anderem das Label, die Geschwindigkeit (z. B. 800 bpi), die Satzlänge, Blocklänge und Satzformat (z. B. 132 Byte, 13200 Byte, Fixed) auf einem Etikett zu vermerken.

Datum des Versandes, eventuelle Versionsnummern oder Ordnungsmerkmale können gegebenenfalls nützlich sein.

Ergänzende Kontrollfragen:

- Ist geregelt, wie auszutauschende Datenträger gekennzeichnet werden müssen?
- Wird stichprobenartig die Einhaltung der Kennzeichnungsvorgaben geprüft?

M 2.44 Sichere Verpackung der Datenträger

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer, Poststelle

Neben den in Maßnahme M 2.3 *Datenträgerverwaltung* dargestellten Umsetzungshinweisen sollte die Verpackung dergestalt sein, dass Manipulationen am Datenträger durch Veränderungen an der Verpackung erkennbar sind.

Mögliche Maßnahmen sind die Verwendung von

- Umschlägen mit Siegel,
- verplombten Behältnissen oder
- Umschlägen, die mit Klebefilm überklebt und anschließend mit nicht-wasserlöslicher Tinte mehrmals unregelmäßig überzeichnet werden.

Verfügt der Datenträger über einen Schreibschutz (Schieber bei Disketten, Schreibring bei Bändern) so sollte dieser genutzt werden. Sollen Manipulationen an den Informationen auf dem Datenträger selbst erkannt werden, sind Verschlüsselungs- oder Checksummen-Verfahren einzusetzen (siehe M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*).

Ergänzende Kontrollfragen:

- Sind für den sicheren Transport verschiedener Datenträger entsprechende Transportbehältnisse vorgesehen und vorrätig?
- Ermöglichen die Transportbehältnisse dem Empfänger die Kontrolle, dass keine Manipulationen am Inhalt stattgefunden haben?

M 2.45 Regelung des Datenträgeraustausches

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer, Poststelle

Sollen zwischen zwei oder mehreren Kommunikationspartnern Datenträger ausgetauscht werden, so sind zum ordnungsgemäßen Austausch folgende Punkte zu beachten:

- Die Adressierung muss eindeutig erfolgen, um eine fehlerhafte Zustellung zu vermeiden. So sollte neben dem Namen des Empfängers auch Organisationseinheit und die genaue Bezeichnung der Behörde/des Unternehmens angegeben sein. Entsprechendes gilt für die Adresse des Absenders.
- Dem Datenträger sollte (optional) ein Datenträgerbegleitzettel beigelegt werden, der folgende Informationen umfasst:
  - Absender,
  - Empfänger,
  - Art des Datenträgers,
  - Seriennummer (soweit vorhanden),
  - Identifikationsmerkmal für den Inhalt des Datenträgers,
  - Datum des Versandes, ggf. Datum bis wann der Datenträger spätestens den Empfänger erreicht haben muss,
  - Hinweis, dass Datenträger auf Viren überprüft sind,
  - Parameter, die zum Lesen der Informationen benötigt werden, z. B. Bandgeschwindigkeit.

  Jedoch sollte nicht vermerkt werden,

  - welches Passwort für die eventuell geschützten Informationen vergeben wurde,
  - welche Schlüssel ggf. für eine Verschlüsselung der Informationen verwendet wurde,
  - welchen Inhalt der Datenträger hat.
- Der Versand des Datenträgers kann (optional) dokumentiert werden. Für jede stattgefundene Übermittlung ist dann in einem Protokoll festzuhalten, wer wann welche Informationen erhalten hat. Je nach Schutzbedarf beziehungsweise Wichtigkeit der übermittelten Informationen ist der Empfang zu quittieren ein Quittungsvermerk und dem erwähnten Protokoll beizufügen.
- Es sind jeweils Verantwortliche für den Versand und für den Empfang zu benennen.
- Die Versandart ist festzulegen.

Ergänzende Kontrollfragen:

- Sind Regelungen bekanntgegeben worden, wie ein Datenträgeraustausch stattzufinden hat?
- Sind die für den Datenträgeraustausch Verantwortlichen hinsichtlich möglicher Gefährdungen ausreichend sensibilisiert?

M 2.46 Geeignetes Schlüsselmanagement

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, IT-Verfahrensverantwortlicher

Die Verwendung kryptographischer Sicherheitsmechanismen (z. B. Verschlüsselung, digitale Signatur) setzt die vertrauliche, integere und authentische Erzeugung, Verteilung und Installation von geeigneten Schlüsseln voraus. Schlüssel, die Unbefugten zur Kenntnis gelangt sind, bei der Verteilung verfälscht worden sind oder gar aus unkontrollierter Quelle stammen (dies gilt auch für die Schlüsselvereinbarung zwischen Kommunikationspartnern), können den kryptographischen Sicherheitsmechanismus genauso kompromittieren wie qualitativ schlechte Schlüssel, die auf ungeeignete Weise erzeugt worden sind. Qualitativ gute Schlüssel werden in der Regel unter Verwendung geeigneter Schlüsselgeneratoren erzeugt (s. u.). Für das Schlüsselmanagement sind folgende Punkte zu beachten:

Schlüsselerzeugung

Die Schlüsselerzeugung sollte in sicherer Umgebung und unter Einsatz geeigneter Schlüsselgeneratoren erfolgen. Kryptographische Schlüssel können zum einen direkt am Einsatzort (und dann meistens durch den Benutzer initiiert) oder zum anderen zentral erzeugt werden. Bei der Erzeugung vor Ort müssen meistens Abstriche an die Sicherheit der Umgebung gemacht werden, bei einer zentralen Schlüsselgenerierung muss sichergestellt sein, dass sie ihre Besitzer authentisch und kompromittierungsfrei erreichen.

Geeignete Schlüsselgeneratoren müssen kontrollierte, statistisch gleichverteilte Zufallsfolgen unter Ausnutzung des gesamten möglichen Schlüsselraums produzieren. Dazu erzeugt z. B. eine Rauschquelle zufällige Bitfolgen, die mit Hilfe einer Logik nachbereitet werden. Anschließend wird unter Verwendung verschiedener Testverfahren die Güte der so gewonnenen Schlüssel überprüft.

Einige Kryptomodule, insbesondere solche, die keinen integrierten Zufallszahlengenerator besitzen, greifen auf Benutzereingaben zur Schlüsselerzeugung zurück. Beispielsweise werden hier Passwörter abgefragt, aus denen dann ein Schlüssel abgeleitet wird, oder der Benutzer wird gebeten, beliebigen Text einzutippen, um zufällige Startwerte für die Schlüsselgenerierung zu erhalten. Solche Passwörter sollten dabei gut gewählt sein und möglichst lang sein. Wenn möglichst "zufällige" Benutzereingaben angefordert werden, sollten diese auch zufällig, also schlecht vorhersagbar, sein.

Schlüsseltrennung

Kryptographische Schlüssel sollten möglichst nur für einen Einsatzzweck dienen. Insbesondere sollten für die Verschlüsselung immer andere Schlüssel als für die Signaturbildung benutzt werden. Dies ist sinnvoll,

- damit bei der Offenlegung eines Schlüssels nicht alle Verfahren betroffen sind,

- da es manchmal erforderlich sein kann, Verschlüsselungsschlüssel weiterzugeben (Vertretungsfall),
- da es unterschiedliche Zyklen für den Schlüsselwechsel geben kann.

Schlüsselverteilung / Schlüsselaustausch

Kryptographische Kommunikationsbeziehungen können nur dann funktionieren, wenn die Kommunikationspartner über aufeinander abgestimmte kryptographische Schlüssel verfügen. Dazu müssen alle Kommunikationspartner mit den dazu erforderlichen Schlüsseln versorgt werden. Zur Schlüsselverteilung und zum Schlüsselaustausch können unterschiedliche Verfahren verwendet werden. Die Unterschiede ergeben sich aus der Anwendung verschiedener kryptographischer Verfahren und Mechanismen bzw. aus ihrer Kombination (siehe M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*). Unter Schlüsselverteilung wird hier die initiale Versorgung der Kommunikationspartner mit Grundschlüsseln verstanden. Die Schlüssel werden dazu von einer meist zentralen Schlüsselerzeugungsstelle (z. B. einem Trust Center) an die einzelnen Kommunikationspartner übermittelt.

Die Verteilung der Schlüssel sollte auf geeigneten Datenträgern (z. B. Chipkarten) oder über Kommunikationsverbindungen (z. B. LAN, WAN) vertraulich (z. B. mit KEK - Key Encryption Key - verschlüsselt), integer (z. B. MAC-gesichert) und authentisch (z. B. digital signiert gemäß Signatur-Gesetz) erfolgen. Die unbefugte Kenntnisnahme bzw. Verfälschung der Schlüssel muss verhindert oder wenigstens erkannt werden können.

Mit Schlüsselaustausch wird die Schlüsseleinigungsprozedur zwischen zwei Kommunikationspartnern auf einen Sitzungsschlüssel (Session Key) bezeichnet. Der Session Key ist ein Schlüssel, der nur eine begrenzte Zeit, etwa für die Dauer einer Kommunikationsverbindung, verwendet wird. Diese Zeit muss festgelegt werden, da Sitzungen sehr lange dauern können. Die Festlegung erfolgt z. B. durch einen relativen Zeitablauf oder durch einen Paketzähler. Für jede neue Verbindung wird ein neuer Session Key zwischen den Kommunikationspartnern ausgehandelt.

Moderne Systeme bedienen sich heute asymmetrischer kryptographischer Verfahren zur Schlüsselverteilung und zum Schlüsselaustausch. Zum Nachweis der Authentizität der öffentlichen Schlüssel kann eine vertrauenswürdige Zertifizierungsstelle eingerichtet werden. Die Kommunikationsteilnehmer müssen sich gegenüber der Zertifizierungsstelle ausweisen und dort ihren öffentlichen Schlüssel mittels einer digitalen Signatur der Zertifizierungsstelle beglaubigen lassen. Das so erzeugte digitale Zertifikat sollte mindestens den öffentlichen Schlüssel und ein Identifikationsmerkmal des Kommunikationsteilnehmers, die Gültigkeitsdauer des Zertifikats und die digitale Signatur der Zertifizierungsstelle enthalten. Mit Kenntnis des öffentlichen Signaturschlüssels der Zertifizierungsstelle ist jeder Kommunikationsteilnehmer in der Lage, die Authentizität des öffentlichen Schlüssels des Kommunikationspartners zu verifizieren.

Schlüsselinstallation und -speicherung

Im Zuge der Schlüsselinstallation ist die authentische Herkunft sowie die Integrität der Schlüsseldaten zu überprüfen. Generell sollten Schlüssel nie in klarer Form, sondern grundsätzlich verschlüsselt im System gespeichert werden. Bei Software-Verschlüsselungsprodukten muss berücksichtigt werden, dass Schlüssel zumindest zeitweise während des Ver-/Entschlüsselungsprozesses in Klarform im PC-System vorliegen müssen. Bieten die IT-Systeme, auf denen das kryptographische Produkt eingesetzt ist, keinen ausreichenden Zugriffsschutz für die Schlüssel, sollten diese nicht auf diesem IT-System gespeichert werden. Es bietet sich dann eine bedarfsorientierte manuelle Eingabe an. Eine andere Möglichkeit wäre die Auslagerung der Schlüssel auf einen externen Datenträger, der dann aber sicher verwahrt werden muss, wie unter Schlüsselarchivierung beschrieben. Aus Sicherheitsaspekten ist deshalb der Einsatz von Hardware-Verschlüsselungskomponenten vorzuziehen, bei denen die Schlüssel vom Datenträger (z. B. Chipkarte) verschlüsselt auf direktem Weg in die Verschlüsselungskomponente geladen werden und diese nie in Klarform verlassen.

Auf jeden Fall muss sichergestellt werden, dass bei der Installation des Verschlüsselungsverfahrens voreingestellte Schlüssel geändert werden.

Schlüsselarchivierung

Für Archivierungszwecke sollte das kryptographische Schlüsselmaterial auch außerhalb des Kryptomoduls in überschlüsselter Form speicherbar und gegebenenfalls wieder einlesbar sein. Dazu können mehrere Schlüssel zu einem Satz zusammengefasst werden, der dann ebenfalls mit Hilfe eines KEK (Key-Encryption-Key: Überschlüsselungsschlüssel) kryptiert wird. Der KEK muss entsprechend sicher (z. B. auf Chipkarte im Safe) aufbewahrt werden. Teilt man einen man den KEK in zwei Teilschlüssel, so lässt sich das "Vier-Augen-Prinzip" umsetzen: zwei verschiedene Personen haben Zugriff auf je einen Datenträger (z. B. Chipkarte, Diskette), auf der sich nur jeweils einer der beiden Teilschlüssel befindet. Um den KEK zu generieren, müssen sich beide Datenträger gleichzeitig oder nacheinander in der Leseeinheit des Kryptomoduls befinden.

Zugriffs- und Vertreterregelung

In der Sicherheitsrichtlinie sollten Fragen bzgl. der Zugriffs- und Vertretungsrechte geregelt sein. Entsprechende Mechanismen müssen vom Schlüsselmanagement und von den einzusetzenden Kryptomodulen/-geräten unterstützt werden (z. B. Schlüsselhinterlegung für den Fall, dass ein Mitarbeiter das Unternehmen verlässt oder wegen Krankheit längere Zeit ausfällt, siehe auch Schlüsselarchivierung).

Schlüsselwechsel

Im Kryptokonzept muss basierend auf der Sicherheitsrichtlinie festgelegt werden, wann und wie oft Schlüssel gewechselt werden müssen. Je größer die Menge verschlüsselter Daten ist, die einem Angreifer für eine Analyse zur Verfügung steht, um so größer ist bei manchen Verfahren die Chance, dass das Analyseverfahren erfolgreich ist. Ein regelmäßiger Schlüsselwechsel mini-

miert die Angriffsmöglichkeiten auf verschlüsselte Daten. Die Wechselfrequenz ist von verschiedenen Faktoren abhängig. Dabei spielt die Art des verschlüsselten Mediums (z. B. Langzeitdatenträger, Datenübertragungsmedium) ebenso eine Rolle wie der kryptographische Algorithmus, die Detektion von Angriffen (z. B. Diebstahl oder Verlust eines Schlüssels) und die Schutzwürdigkeit der Daten. Weitere Faktoren bei der Festlegung der Wechselfrequenz sind die Häufigkeit des Schlüsseleinsatzes, das relevante Bedrohungspotential und die Sicherheit der lokalen Aufbewahrung der Schlüssel.

Je nach verwendetem Verfahren sind für jede einzelne Kommunikationsverbindung neue Schlüssel auszuhandeln, also Sitzungsschlüssel (Session Keys) zu verwenden. Dies sollte natürlich für die Benutzer unbemerkt durch die Verfahren gesteuert werden. Schlüsselwechsel bedeutet hierbei den Austausch der Masterkeys, die die Grundlage bilden, auf der die Sitzungsschlüssel gebildet werden, und sollte natürlich auch regelmäßig durchgeführt werden.

Besteht der Verdacht, dass ein verwendeter Schlüssel offen gelegt wurde, so ist dieser Schlüssel nicht mehr zu verwenden und alle Beteiligten sind zu informieren. Bereits mit diesem Schlüssel verschlüsselte Informationen sind zu entschlüsseln und mit einem anderen Schlüssel zu verschlüsseln.

Schlüsselvernichtung

Nicht mehr benötigte Schlüssel (z. B. Schlüssel, deren Gültigkeitsdauer abgelaufen sind) sind auf sichere Art zu löschen bzw. zu vernichten (z. B. durch mehrfaches Löschen/Überschreiben und/oder mechanische Zerstörung des Datenträgers). Auf Produkte mit unkontrollierbarer Schlüsselablage sollte generell verzichtet werden.

Ergänzende Kontrollfragen:

- Ist ein Verantwortlicher für das Schlüsselmanagement benannt?
- Werden die zu schützenden Daten getrennt von den bei der Verschlüsselung verwendeten Schlüsseln übertragen?
- Werden die zu verwendenden Schlüssel hinreichend häufig gewechselt?
- Kann eine lokale sichere Aufbewahrung der Schlüssel sichergestellt werden?

M 2.47 Ernennung eines Fax-Verantwortlichen

Verantwortlich für Initiierung: Leiter Innerer Dienst, Vorgesetzte

Verantwortlich für Umsetzung: Innerer Dienst

Für jedes Faxgerät ist ein Verantwortlicher zu benennen, der folgende Aufgaben übernehmen muss:

- Verteilung der eingehenden Faxsendungen an die Empfänger,
- Koordination der Versorgung des Faxgerätes mit notwendigen Verbrauchsgütern,
- geeignete Entsorgung von Fax-Verbrauchsgütern,
- Löschen von Restinformationen im Faxgerät vor Wartungs- und Reparaturarbeiten,
- Beaufsichtigung von Wartungs- und Reparaturarbeiten (siehe M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*),
- gelegentliche Kontrolle programmierter Zieladressen und Protokolle, insbesondere nach Wartungs- und Reparaturarbeiten,
- Ansprechpartner bei Problemen bei der Faxnutzung.

Ergänzende Kontrollfragen:

- Ist der Fax-Verantwortliche in seine Aufgaben eingewiesen worden?
- Wird die Zuverlässigkeit des Fax-Verantwortlichen gelegentlich geprüft?

M 2.48 Festlegung berechtigter Faxbediener

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Innerer Dienst

Die Berechtigung zur Bedienung des Faxgerätes ist auf einen ausgewählten Kreis zuverlässiger Mitarbeiter zu beschränken. Diese Mitarbeiter sind in die korrekte Handhabung des Gerätes einzuweisen und mit den erforderlichen IT-Sicherheitsmaßnahmen vertraut zu machen. Jeder berechtigte Benutzer sollte darüber unterrichtet werden, wer das Gerät bedienen darf und wer der Fax-Verantwortliche ist. Darüber hinaus sollte am Faxgerät eine verständliche Bedienungsanleitung ausliegen.

Durch die Einschränkung des Faxbedienerkreises auf die für den operativen Einsatz notwendige Mindestzahl wird erreicht, dass die Anzahl der Personen, die eingehende Faxsendungen mitlesen können, begrenzt ist.

Ergänzende Kontrollfragen:

- Ist die Anzahl der Fax-Benutzer so gewählt, dass der betriebliche Einsatz nicht eingeschränkt ist?
- Wissen alle Benutzer, wer zur Bedienung des Faxgerätes sonst noch berechtigt ist?

M 2.49 Beschaffung geeigneter Faxgeräte

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Beschaffungsstelle

Bei Neuanschaffungen von Faxgeräten sollte darauf geachtet werden, dass übliche Standardsicherheitsfunktionen implementiert sind wie:

- Austausch einer Teilnehmerkennung,
- Sendebericht,
- Journalführung.

Unter Beachtung des Preis-/Leistungsverhältnisses sind darüber hinaus folgende zusätzliche Sicherheitsfunktionen zu begrüßen:

- paßwortgeschützter Zugang,
- paßwortgeschützter Pufferspeicher,
- Einrichten einer geschlossenen Benutzergruppe,
- Ausschließen bestimmter Faxanschlüsse von Versendung oder Empfang.

Ergänzende Kontrollfragen:

- Werden bei der Neubeschaffung von Faxgeräten Sicherheitsfunktionen als Auswahlkriterien berücksichtigt?
- Wird bei der Beschaffung von Faxgeräten mit zusätzlichen Sicherheitsfunktionen die Angemessenheit und Wirtschaftlichkeit am Schutzbedarf ausgerichtet?

M 2.50 Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen

Verantwortlich für Initiierung: Leiter Innerer Dienst, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Fax-Verantwortlicher

Alle Fax-Verbrauchsgüter, aus denen Informationen über Faxtexte gewonnen werden könnten, wie z. B. Zwischenträgerfolien oder fehlerhafte Ausdrucke, sollten vor der Entsorgung vernichtet oder durch eine zuverlässige Fachfirma entsorgt werden.

Das gleiche gilt beim Austausch informationstragender Ersatzteile, wie z. B. photo-elektrische Trommeln.

Wartungsfirmen, die Faxgeräte periodisch warten oder reparieren, sind auf eine entsprechende Handhabung zu verpflichten und ggf. zu kontrollieren.

Ergänzende Kontrollfragen:

- Auf welche Weise wird nicht mehr benötigtes Fax-Verbrauchsmaterial entsorgt?
- Sind die Fax-Verantwortlichen auf die Schutzbedürftigkeit des zu entsorgenden Materials und die bestehenden Entsorgungsmöglichkeiten hingewiesen worden?

M 2.51 Fertigung von Kopien eingehender Faxsendungen

Verantwortlich für Initiierung: Fax-Verantwortlicher

Verantwortlich für Umsetzung: Benutzer

Ein Fax auf Thermopapier kann nach einiger Zeit stark verblassen oder schwarz werden. Daher sollten von Faxen auf Thermopapier, deren Informationsgehalt länger benötigt wird, Kopien auf Normalpapier erstellt werden.

Ergänzende Kontrollfragen:

- Gibt es Faxgeräte im Unternehmen/ der Behörde, die mit Thermopapier arbeiten?
- Werden wichtige eingehende Faxsendungen kopiert?

M 2.52 Versorgung und Kontrolle der Verbrauchsgüter

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter Innerer Dienst

Verantwortlich für Umsetzung: Innerer Dienst, Administrator, Benutzer

Viele im Büroalltag eingesetzte Geräte wie Fax, Drucker, etc. sind auf bestimmte Verbrauchsgüter (z. B. Papier, Toner, Datensicherungsbänder) angewiesen, um funktionieren zu können. Daher muss die Versorgung mit diesen Verbrauchsgütern vor Ort sichergestellt sein. Es sollten klare und eindeutige Regelungen existieren, welche Verbrauchsgüter von wem nachgefüllt bzw. bestellt werden sollten.

Bestimmte Ressourcen dürfen nicht von jedem Mitarbeiter nachgefüllt oder beschafft werden, sondern nur von autorisierten Personen, beispielsweise sehr teure Produkte oder technisch komplexe Komponenten.

Alle Benutzer sollten informiert sein, wer zu benachrichtigen ist, wenn Verbrauchsgüter nachbeschafft oder aufgefüllt werden müssen. Für jede Sorte von Verbrauchsmaterial sollte jemand benannt werden, der für Versorgung und Kontrolle verantwortlich ist. Dieser ist dafür verantwortlich

- regelmäßig zu prüfen, ob ausreichende Vorräte vorhanden sind und vor Ort nachgefüllt werden muss,
- die Beschaffungsstelle rechtzeitig zu benachrichtigen, wenn Verbrauchsmaterial nachbestellt werden muss.

Die Versorgung mit Verbrauchsgütern ist von der Beschaffungsstelle ausreichend sicherzustellen.

Ergänzende Kontrollfragen:

- Ist die Zuständigkeit für den Nachschub an Versorgungsgütern geregelt?
- Fehlt häufig Verbrauchsmaterial?

M 2.53 Abschalten des Faxgerätes außerhalb der Bürozeiten

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Brandschutzbeauftragter

Verantwortlich für Umsetzung: Fax-Verantwortlicher

Um die Brandgefahr, die von Faxgeräten immer ausgehen kann, zu reduzieren, sollten Geräte, die außerhalb der Arbeitszeit nicht benötigt werden (Abteilungs-Faxgerät, persönliches Gerät) zum Dienstschluss abgeschaltet werden. Damit kann auch erreicht werden, dass eingehende Faxsendungen nicht unkontrolliert längere Zeit im Faxgerät verbleiben. Realisierbar ist die Abschaltung auf einfache Weise durch Zeitschaltuhren, die die Stromversorgung des Gerätes auf die üblichen Bürozeiten einschränken.

Für später eingehende Sendungen kann ein anderer (möglichst ständig kontrollierter) Fax-Anschluss benannt werden oder bei modernen TK-Anlagen eine Anrufumleitung eingerichtet werden.

Gleichzeitig kann mit dem Abschalten des Faxgerätes die Überlastung des Gerätes aufgrund eines technischen Versagens oder aufgrund beabsichtigter Massenfaxsendungen außerhalb der Bürozeit verhindert werden.

Das Abschalten sollte unterbleiben, wenn für die Verfügbarkeit des Gerätes besondere Anforderungen bestehen, die bei den Ausweichlösungen nicht umgesetzt werden können.

Ergänzende Kontrollfragen:

- Welche Faxgeräte müssen auch außerhalb der Bürozeiten aktiv sein?
- Werden die anderen Geräte ausgeschaltet?
- Besteht die Möglichkeit einer Anrufweiterleitung?

M 2.54 Beschaffung geeigneter Anrufbeantworter

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Haustechnik, Beschaffungsstelle

Diese Maßnahme ist bei der Neubeschaffung von Anrufbeantwortern zu beachten. Sollten vorhandene Geräte den Sicherheitsansprüchen nicht genügen, ist eine Neuanschaffung oder die Abschaltung dieser Geräte in Erwägung zu ziehen.

Bei der Beschaffung von Anrufbeantwortern sollten unter Beachtung der Wirtschaftlichkeit einige Kriterien beachtet werden, um Gefährdungen möglichst auszuschließen:

- Zur Sicherstellung einwandfreier fernmeldetechnischer Funktionen müssen die Geräte eine BZT-Zulassung (Postzulassung) besitzen.
- Bei ganz oder teilweise digital speichernden Geräten empfiehlt es sich, solche auszuwählen, die eine Notstromversorgung durch Batterien oder vom Benutzer wechselbare Akkumulatoren bieten. Bei fest eingebauten Akkumulatoren wird bei einem Austausch der Einsatz eines Servicetechnikers notwendig, was zu einem längeren Ausfall des Anrufbeantworters führen kann.
- Aufgrund unterschiedlicher Güte der Nachrichtenaufzeichnung (z. B. bei analoger oder digitaler Aufzeichnung) sollte vor der Beschaffung die Aufzeichnungsqualität getestet werden.
- Ganz oder teilweise digital speichernde Anrufbeantworter sollten mit einer Anzeige der Batteriekapazität sowie einem deutlichem Warnzeichen (evtl. auch akustisch) ausgestattet sein, um verminderte Batterieleistung rechtzeitig anzeigen zu können.
- Bei Anrufbeantwortern, die eine einzige Kassette sowohl für Aufzeichnungen als auch für den Ansagetext verwenden, entstehen durch Bandspulvorgänge Wartezeiten. Es sollte abgewogen werden, ob diese Wartezeiten in Kauf genommen werden können.
- Die Bedienungsfreundlichkeit des Anrufbeantworters sollte beachtet werden. Ergonomische und übersichtliche Tastenanordnung, Funktionstasten ohne Doppelbelegungen und für jedermann verständliche Bedienungsanleitungen sind vorteilhaft.
- Die Fernabfrage sollte nach Möglichkeit mechanisch oder elektronisch deaktivierbar, der Sicherungscode zumindest drei- bis vierstellig und frei programmierbar sein. Eine zusätzliche Sperrschaltung, die den Anrufbeantworter nach drei vergeblichen Versuchen die Verbindung unterbrechen lässt, bietet einen erhöhten Schutz. Hieraus ergeben sich zumindest ein höherer Zeitaufwand und höhere Telefonkosten für den potentiellen Angreifer. Besser noch sind Geräte, bei denen die Fernabfragefunktionen nach drei vergeblichen Versuchen vollkommen gesperrt werden und nur noch am Gerät selbst wieder aktivierbar sind. Auch Sperrzeiten, die nach jedem Fehlversuch verlängert werden, sind sinnvoll.

Ergänzende Kontrollfragen:

- Sind obige Hinweise der Beschaffungsstelle bekannt?

M 2.55 Einsatz eines Sicherungscodes

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Verfügt der Anrufbeantworter über Fernabfragemöglichkeiten und einen Sicherungscode, so ist anzustreben, dass die Fernabfrage nur mittels eines individuell gewählten, geheim zu haltenden Sicherungscodes aktiviert werden kann. Insbesondere ist ein evtl. werkseitig eingestellter Code zu ändern. Der Sicherungscode ist wie ein Passwort zu hinterlegen (siehe hierzu M 2.22 *Hinterlegen des Passwortes*) und auch regelmäßig zu ändern.

Bei der Bedienung des Anrufbeantworters mittels Fernabfragegerät sollte darauf geachtet werden, dass sich kein Fremder in der Nähe aufhält, der die Eingabe der Codes beobachten oder erlauschen könnte.

Ergänzende Kontrollfragen:

- Wurden die Benutzer über den korrekten Umgang mit der Fernabfrage unterrichtet?

M 2.56 Vermeidung schutzbedürftiger Informationen auf dem Anrufbeantworter

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Da sich zurzeit Anrufbeantworter nicht vollständig gegen Missbrauch absichern lassen, sollte die Aufzeichnung schutzbedürftiger Informationen vermieden werden oder sogar in Bereichen, in denen typischerweise schutzbedürftige Informationen ausgetauscht werden, der Einsatz von Anrufbeantwortern überdacht werden. Im Ansagetext sollte daher darauf hingewiesen werden, dass keine schutzbedürftigen Informationen auf dem Anrufbeantworter hinterlassen werden sollten.

Ergänzende Kontrollfragen:

- Werden Personen, die schutzbedürftigen Informationen aufsprechen, über die damit verbundenen Risiken aufgeklärt?
- Sind Anrufbeantworter in Bereichen installiert, in denen häufig schutzbedürftige Informationen anfallen?

M 2.57 Regelmäßiges Abhören und Löschen aufgezeichneter Gespräche

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Die im Anrufbeantworter gespeicherten Gespräche sollten regelmäßig abgehört und gelöscht werden. Ist das Löschen bei analog aufzeichnenden Geräten nicht möglich, sollte das Magnetband an den Anfang zurückgespult werden, damit die Aufzeichnung neuer Gespräche gespeicherte alte Nachrichten überschreibt.

M 2.58 Begrenzung der Sprechdauer

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Zur Verhinderung von vorzeitiger Füllung des Speichermediums, sollte die maximale Sprechdauer pro Anruf auf 2-4 Minuten begrenzt werden, wenn das Gerät eine solche Einstellung erlaubt.

M 2.59 Auswahl eines geeigneten Modems in der Beschaffung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer, Administrator, Beschaffungsstelle

Bei der Beschaffung eines Modems sind folgende Punkte zu beachten:

- **Modem-Zulassung**

  Ein Modem, dass in Deutschland an das öffentliche Telekommunikationsnetz angeschlossen werden soll, muss eine BZT-Zulassung (früher ZZF-Zulassung, davor FTZ-Zulassung, im allgemeinen Sprachgebrauch auch Post-Zulassung genannt) haben. Hinweis: Entgegen der Angaben in vielen Modem-Handbüchern muss die Inbetriebnahme eines zugelassenen Modems nicht mehr der Telekom gemeldet werden.

- **Bauweise**

  Ein internes Modem bietet den Vorteil, dass die Modem-Konfiguration nur über den Rechner, in dem es eingebaut ist, geändert werden kann. Verfügt der Rechner über Zugangs- oder Zugriffsschutzmechanismen, können sie zum Schutz der Modem-Konfigurationsdaten eingesetzt werden. Gleichzeitig kann damit die Nutzung des Modems auf autorisierte Personen beschränkt werden. Manipulationen am Modem sind durch den Einbau im Rechner erschwert. Bei vernetzten Systemen, die nicht über derartige Schutzmechanismen verfügen (einige Peer-to-Peer-Netze), besteht der Nachteil eines internen Modems darin, dass das Modem unkontrolliert von allen Arbeitsplätzen genutzt werden kann.

  Ein externes Modem kann nach Nutzung verschlossen aufbewahrt werden. Es bietet außerdem den Vorteil, dass es üblicherweise über diverse Anzeigen sowie den Modem-Lautsprecher über den aktuellen Status informieren kann. Über den Modem-Lautsprecher kann auch gehört werden, ob von extern eine Verbindung aufgebaut wird oder ob eine Applikation unaufgefordert versucht, Informationen über die Installation und die System-Konfiguration an den Hersteller zu übertragen. Ein weiterer Vorteil eines externen Modems ist, dass es unabhängig vom IT-System nur für die jeweilige Datenübertragung eingeschaltet werden kann und somit z. B. sichergestellt werden kann, dass die letzte Verbindung getrennt worden ist und dass keine Verbindung von außerhalb aufgebaut werden kann. Nachteilig ist, dass ein externes Modem zur Manipulation der Konfigurationsdaten oder zum Auslesen gespeicherter Passwörter einfach an ein nicht geschütztes IT-System angeschlossen werden kann.

  PCMCIA-Modems bieten aufgrund der Baugröße den Vorteil, dass sie nach Nutzung einfach verwahrt werden können. Eine sichere Aufbewahrung verhindert, dass sie zur Manipulation an ungeschützte Rechner angeschlossen werden.

- **Übertragungsgeschwindigkeit**

  Je höher die Übertragungsgeschwindigkeit eines Modems ist, desto geringer sind die Kosten für die Übertragung großer Datenmengen aufgrund der Zeiteinsparung.

  Zunächst ist zu klären, welche Übertragungsgeschwindigkeiten für den gewünschten Einsatzzweck notwendig ist. Ausreichend sind z. B. bei ASCII-Terminalemulation 2400 bit/sec, bei Faxübertragung 9600 bit/sec, bei Datex-J (T-Online) zurzeit 14400 bit/sec. Für Datenübertragung großen Ausmaßes sind die aktuell größtmöglichen Übertragungsgeschwindigkeiten einzusetzen. Übertragungsgeschwindigkeiten von mehr als 2400 bit/sec erschweren darüber hinaus das Abhören erheblich.

  Anschließend muss bei Geschwindigkeiten über 9600 bit/sec überprüft werden, ob die Schnittstelle des IT-Systems, an dem das Modem betrieben werden soll, höhere Geschwindigkeiten zulässt.

  Bei der Auswahl des Modems sollte beachtet werden, dass die Leistungsmerkmale, die für die tatsächlich erreichte Übertragungsgeschwindigkeit ausschlaggebend sind, genormt sind. Dies sind zum einen Normen für die Übertragungsgeschwindigkeit wie V.32bis für 14400 bit/sec und zum anderen Protokolle zur Übertragungsoptimierung durch Datenkompression und Fehlerkorrektur wie MNP 5 oder V.24bis.

- **Befehlssatz**

  Die meisten Modems arbeiten heute nach dem herstellerabhängigen Hayes-Standard (auch AT-Standard genannt). Aufgrund der weiten Verbreitung dieses Standards kann bei Einsatz eines Modems, das diesen Standard beherrscht, davon ausgegangen werden, dass die Kommunikation mit anderen Modems meist problemlos möglich ist. Bei der Anschaffung von Modems der neuesten Generation sollte bedacht werden, dass die versprochenen hohen Übertragungsraten oftmals nur erreicht werden können, wenn Geräten desselben Herstellers auf beiden Seiten eingesetzt werden.

- **Handbuch**

  Ein gut lesbares und ausführliches Handbuch ist zur schnellen Installation und bestmöglichen Konfiguration eines Modems wichtig.

- **Sicherheitsmechanismen**

  Es gibt vielfältige Sicherheitsmechanismen, die in Modems integriert sein können wie Passwortmechanismus oder Callback-Funktion. Einige Modems bieten sogar die Möglichkeit, die übertragenen Daten zu verschlüsseln.

  Die Anschaffung eines Modems mit Verschlüsselungsoption ist vorteilhaft, wenn regelmäßig Übertragungen großer Datenmengen innerhalb einer Organisation mit verstreuten Liegenschaften durchgeführt werden sollen. Diese Online-Verschlüsselung bedingt einen geringeren organisatorischen Aufwand als das Verschlüsseln der Daten mittels Zusatzprodukten. Generelle Aussagen zur Sicherheit der eingesetzten Algorithmen können nicht gemacht werden. Für den IT-Grundschutz bietet der DES-

Algorithmus bei entsprechendem Schlüsselmanagement ausreichende Sicherheit.

Die vielfach angebotene Callback-Funktion bietet unter Sicherheitsgesichtspunkten den Vorteil, dass auf einfache Weise unautorisierte Anrufer abgewiesen werden können (siehe auch M 5.30 *Aktivierung einer vorhandenen Callback-Option*).

Ergänzende Kontrollfragen:

- Sind IT-Benutzer oder die Beschaffungsstelle über diese Hinweise informiert?

M 2.60 Sichere Administration eines Modems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer, Administrator

Der sichere Einsatz eines Modems bedingt einige administrative Maßnahmen:

- Die Telefonnummer eines Modem-Zugangs darf nur den Kommunikationspartnern bekanntgegeben werden, um den Zugang vor Einwählversuchen zu schützen. Sie darf nicht im Telefonverzeichnis der Organisation erscheinen.
- Ist ein Modem in einen Netzserver integriert, können Benutzer von ihren Arbeitsplatzrechnern auf das Modem zugreifen. Dann darf ein Zugriff auf die Kommunikationssoftware nur den Benutzern möglich sein, die für die Datenübertragung berechtigt sind (siehe auch M 2.42 *Festlegung der möglichen Kommunikationspartner*).
- Außerdem müssen regelmäßig die Einstellungen des Modems und der Kommunikationssoftware überprüft werden sowie die durchgeführten Datenübertragungen protokolliert werden.
- Es muss sichergestellt sein, dass das Modem die Telefonverbindung unterbricht, sobald der Benutzer sich vom System abmeldet. Bei einem Standalone-System kann dies dadurch realisiert sein, dass das Modem nur solange mit dem Telefonnetz verbunden ist, wie es für die Datenübertragung eingesetzt wird, und es anschließend ausgeschaltet bzw. von der Leitung getrennt wird. Bei einem im Netzserver integrierten Modem muss dies über die Konfiguration sichergestellt werden. Ein externes Modem kann einfach ausgeschaltet werden. Außerdem müssen alle Benutzer darauf hingewiesen werden, dass nach der Datenübertragung auch das Kommunikationsprogramm zu beenden ist.
- Es muss außerdem darauf geachtet werden, dass nach einem Zusammenbruch der Modem-Verbindung der externe Benutzer automatisch vom IT-System ausgeloggt wird. Andernfalls kann der nächste Anrufer unter dieser Benutzer-Kennung weiterarbeiten, ohne sich einzuloggen.

Ergänzende Kontrollfragen:

- Wurden die gewählten Einstellungen daraufhin getestet, ob eine unbefugte Nutzung des Modems wirksam verhindert ist?
- Wird die Modemverbindung getrennt, wenn der Benutzer sich abmeldet?
- Wird der Benutzer abgemeldet, wenn die Modemverbindung getrennt wird?

M 2.61 Regelung des Modem-Einsatzes

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Es ist festzulegen:

- wer der Verantwortliche für den sicheren Betrieb des Modems ist (beispielsweise im Stand-alone Einsatz der IT-Benutzer, in vernetzten Systemen der Administrator),
- wer das Modem benutzen darf,
- in welchen Fällen vertrauliche Informationen bei der Übertragung verschlüsselt werden sollten,
- in welchen Fällen durchgeführte Datenübertragungen zu protokollieren sind (z. B. bei Übermittlung personenbezogener Daten). Bietet die Kommunikationssoftware Protokollierungsfunktion an, sollte diesen im sinnvollen Rahmen genutzt werden.

Alle Login-Vorgänge, ob erfolgreich oder erfolglos, müssen protokolliert werden. Korrekt eingegebene Passwörter sollten nicht mitprotokolliert werden, es ist aber zu überlegen, die bei erfolglosen Login-Versuchen eingegebenen Passwörter mitzuprotokollieren, um Passwort-Attacken zu entdecken.

Indizien für Passwort-Attacken können z. B. sein: häufige erfolglose Login-Versuche für einen Benutzer, erfolglose Login-Versuche immer vom selben Anschluss, Versuche sich auf verschiedene Benutzernamen anzumelden während einer Verbindung oder von einem Anschluss.

Nach dem Verbindungsaufbau muss dem Anrufenden ein Anmelde-Prompt angezeigt werden. Dabei sollte darauf geachtet werden, dass vor der erfolgreichen Anmeldung möglichst wenig Informationen über das angewählte IT-System weitergegeben werden. Es sollte weder die Art der eingesetzten Hardware noch des Betriebssystems gegeben werden. Der Anmelde-Prompt sollte den Namen des IT-Systems und/oder der Organisation enthalten, einen Hinweis, dass alle Verbindungen protokolliert werden und eine Eingabeaufforderung für Benutzername und Passwort. Bei erfolglosen Anmeldeversuchen darf keine Ursache angezeigt werden (falscher Benutzername, falsches Passwort).

Trennung Dial-In / Dial-Out

Für ein- bzw. abgehende Verbindungen sollten getrennte Leitungen und Modems benutzt werden. Ein Anrufer sollte keine Möglichkeit haben, sich über das angewählte IT-System wieder nach außen verbinden zu lassen. (Wenn dies für Außendienstmitarbeiter unbedingt notwendig ist, muss dem eine starke Authentisierung vorangehen, z. B. über Chipkarten.) Ansonsten besteht die Gefahr, dass Hacker den Zugang missbrauchen, zum einen um teure Fernverbindungen aufzubauen und zum anderen um ihre Spuren zu verwischen.

Beim Callback sollte für den Rückruf ein anderes Modem oder eine andere Leitung benutzt werden, als das anrufende Modem benutzt hat (siehe auch M 5.44 *Einseitiger Verbindungsaufbau*).

Ergänzende Kontrollfragen:

- Sind allen für die Kommunikation zugelassenen Mitarbeitern die diesbezüglichen Regelungen bekannt?

M 2.62 Software-Abnahme- und Freigabe-Verfahren

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT

Der Einsatz von IT zur Aufgabenbewältigung setzt voraus, dass die maschinelle Datenverarbeitung soweit wie möglich fehlerfrei arbeitet, da die Kontrolle der Einzelergebnisse in den meisten Fällen nicht mehr zu leisten ist. Im Zuge eines Software-Abnahme-Verfahrens wird deshalb überprüft, ob die betrachtete Software fehlerfrei arbeitet, das heißt, ob die Software die erforderliche Funktionalität zuverlässig bereitstellt und ob sie darüber hinaus keine unerwünschten Nebeneffekte hat. Mit der anschließenden Freigabe der Software durch die fachlich zuständige Stelle wird die Erlaubnis erteilt, die Software zu nutzen. Gleichzeitig übernimmt diese Stelle damit auch die Verantwortung für das IT-Verfahren, dass durch die Software realisiert wird.

Bei der Software-Abnahme unterscheidet man sinnvollerweise zwischen Software, die selbst oder im Auftrag entwickelt wurde, und Standardsoftware, die nur für den speziellen Einsatzzweck angepasst wird.

Abnahme von selbst- oder im Auftrag entwickelter Software

Bevor der Auftrag zur Software-Entwicklung intern oder extern vergeben wird, muss die Anforderungsdefinition für die Software erstellt sein, aus der dann das Grob- und Feinkonzept für die Realisierung entwickelt wird. Anhand dieser Dokumente erstellt die fachlich zuständige Stelle, nicht die für die Software-Entwicklung zuständige Stelle, im allgemeinen einen Abnahmeplan.

Üblicherweise werden hierzu Testfälle und die erwarteten Ergebnisse für die Software erarbeitet. Anhand dieser Testfälle wird die Software getestet und der Abgleich zwischen berechnetem und erwartetem Ergebnis wird als Indiz für die Korrektheit der Software benutzt.

Zur Entwicklung der Testfälle und zur Durchführung der Tests ist folgendes zu beachten:

- die Testfälle werden von der fachlich zuständigen Stelle entwickelt,
- für Testfälle werden keine Daten des Wirkbetriebs benutzt,
- Testdaten, insbesondere wenn sie durch Kopieren der Wirkdaten erstellt werden, dürfen keine vertraulichen Informationen beinhalten; personenbezogene Daten sind zu anonymisieren oder zu simulieren,
- die Durchführung der Tests darf keine Auswirkungen auf den Wirkbetrieb haben; nach Möglichkeit sollte ein logisch oder physikalisch isolierter Testrechner benutzt werden.

Eine Abnahme ist zu verweigern, wenn:

- Schwerwiegende Fehler in der Software festgestellt werden,
- Testfälle auftreten, in denen die erwarteten Ergebnisse nicht mit den berechneten übereinstimmen,

- Benutzerhandbücher oder Bedienungsanleitungen nicht vorhanden oder von nicht ausreichender Qualität sind und
- Dokumentation der Software nicht vorhanden oder nicht ausreichend ist.

Die Ergebnisse der Abnahme sind schriftlich festzuhalten. Die Dokumentation des Abnahmeergebnisses sollte umfassen:

- Bezeichnung und Versionsnummer der Software und ggf. des IT-Verfahrens,
- Beschreibung der Testumgebung,
- Testfälle und Testergebnisse und
- Abnahmeerklärung.

Abnahme von Standardsoftware

Wird Standardsoftware beschafft, so sollte auch diese einer Abnahme und einer Freigabe unterzogen werden. In der Abnahme sollte überprüft werden, ob

- die Software frei von Computer-Viren ist,
- die Software kompatibel zu den anderen eingesetzten Produkten ist,
- die Software in der angestrebten Betriebsumgebung lauffähig ist und welche Parameter zu setzen sind,
- die Software komplett einschließlich der erforderlichen Handbücher ausgeliefert wurde und
- die geforderte Funktionalität erfüllt wird.

Freigabe-Verfahren

Ist die Abnahme der Software erfolgt, muss die Software für die Nutzung freigegeben werden. Dazu ist zunächst festzulegen, wer berechtigt ist, Software freizugeben. Die Freigabe der Software ist schriftlich festzulegen und geeignet zu hinterlegen.

Die Freigabeerklärung sollte umfassen:

- Bezeichnung und Versionsnummer der Software und ggf. des IT-Verfahrens,
- Bestätigung, dass die Abnahme ordnungsgemäß vorgenommen wurde,
- Einschränkungen für die Nutzung (Parametereinstellung, Benutzerkreis,...),
- Freigabedatum, ab wann die Software eingesetzt werden darf und
- die eigentliche Freigabeerklärung.

Falls IT-technisch möglich muss verhindert werden, dass Software nach der Freigabe verändert oder manipuliert werden kann. Andernfalls ist dies durch eine Regelung festzulegen.

Auch nach intensiven Abnahmetests kann es vorkommen, dass im laufenden Einsatz Fehler in der Software festgestellt werden. Für diesen Fall ist festzu-

legen, wie in einem solchen Fehlerfall verfahren werden soll (Ansprechpartner, Fehlerbeseitigungsablauf, Beteiligung der fachlich zuständigen Stelle, Wiederholung der Abnahme und Freigabe, Versionskontrolle).

Für weiterführende Erklärungen siehe Baustein B 1.10 *Standardsoftware*.

Ergänzende Kontrollfragen:

- Gibt es für sämtliche eingesetzte Software eine Abnahme- und Freigabebestätigung?
- Werden Fehler auch ohne Beteiligung der fachlich zuständigen Stelle beseitigt?
- Kann im Einsatz befindliche Software unerkannt manipuliert werden?

M 2.63 Einrichten der Zugriffsrechte

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Verantwortliche der einzelnen IT-Anwendungen, Administrator

Arbeiten mit einem IT-System mehrere Benutzer, so muss durch eine ordnungsgemäße Administration der Zugriffsrechte sichergestellt werden, dass die Benutzer das IT-System nur gemäß ihren Aufgaben nutzen können.

Vorausgesetzt sei, dass von den Fachverantwortlichen die Zugangs- und Zugriffsberechtigungen für die einzelnen Funktionen festgelegt wurden (siehe M 2.7 *Vergabe von Zugangsberechtigungen* und M 2.8 *Vergabe von Zugriffsrechten*). Anschließend werden die Benutzer des IT-Systems den einzelnen Funktionen zugeordnet. Die Ergebnisse sind schriftlich zu dokumentieren.

Der Administrator muss dann das IT-System so konfigurieren, dass diese Benutzer Zugang zum IT-System erhalten und mit den ihnen zugewiesenen Zugriffsrechten nur ihre Aufgaben wahrnehmen können. Bietet das IT-System keine Möglichkeit, Zugriffsrechte zuzuweisen (z. B. beim DOS-PC mit mehreren Benutzern), so ist ein Zusatzprodukt zu diesem Zweck einzusetzen (siehe z. B. M 4.41 *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*).

Lässt das IT-System es zu, so sind die sinnvoll einsetzbaren Protokollfunktionen zur Beweissicherung durch den Administrator zu aktivieren. Dazu gehören erfolgreiche und erfolglose An- und Abmeldevorgänge, Fehlermeldungen des Systems, unerlaubte Zugriffsversuche.

Für den Vertretungsfall muss der Administrator vorab kontrollieren, ob der Vertreter vom Fachverantwortlichen autorisiert ist. Erst dann darf er die erforderlichen Zugriffsrechte im akuten Vertretungsfall einrichten.

Ergänzende Kontrollfragen:

- Werden die vom Administrator eingerichteten Zugriffsrechte sporadisch überprüft?
- Liegt eine Dokumentation vor, welche Rechtestruktur im IT-System realisiert ist?

M 2.64 Kontrolle der Protokolldateien

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Verantwortliche der einzelnen IT-Anwendungen, Revisor

regelmäßige Auswertung der Protokollierung durch Revisor

Die Protokollierung sicherheitsrelevanter Ereignisse ist als Sicherheitsmaßnahme nur wirksam, wenn die protokollierten Daten in regelmäßigen Abständen durch einen Revisor ausgewertet werden. Ist es personell oder technisch nicht möglich, die Rolle eines unabhängigen Revisors für Protokolldateien zu implementieren, kann ihre Auswertung auch durch den Administrator erfolgen. Für diesen Fall bleibt zu beachten, dass damit eine Kontrolle der Tätigkeiten des Administrators nur schwer möglich ist. Das Ergebnis der Auswertung sollte daher dem IT-Sicherheitsbeauftragten, dem IT-Verantwortlichen oder einem anderen besonders zu bestimmenden Mitarbeiter vorgelegt werden.

Löschung/Archivierung der Protokolldateien

Die regelmäßige Kontrolle dient darüber hinaus auch dem Zweck, durch die anschließende Löschung der Protokolldaten ein übermäßiges Anwachsen der Protokolldateien zu verhindern. Je nach Art der Protokolldaten kann es sinnvoll sein, diese auf externen Datenträgern zu archivieren.

Da Protokolldateien in den meisten Fällen personenbezogene Daten beinhalten, ist sicherzustellen, dass diese Daten nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet werden (siehe § 14 Abs. 4 BDSG und M 2.110 *Datenschutzaspekte bei der Protokollierung*). Der Umfang der Protokollierung und die Kriterien für deren Auswertung sollte dokumentiert und innerhalb der Organisation abgestimmt werden.

Fristen für Löschung bzw. Aufbewahrung

Aus verschiedenen gesetzlichen Regelungen können sich einerseits Mindestaufbewahrungsfristen, aber andererseits auch Höchstaufbewahrungsfristen an Protokolldaten ergeben. So kann durch datenschutzrechtliche Regelungen eine Löschung erforderlich sein (siehe dazu auch M 2.110 *Datenschutzaspekte bei der Protokollierung*).

Für bestimmte Protokolldaten gelten aber unter Umständen gesetzliche Mindestaufbewahrungsfristen, z. B. wenn sie Aufschluss über betriebswirtschaftliche Vorgänge geben. Diese Fristen müssen auf jeden Fall eingehalten werden. Vor der Löschung von Protokolldaten ist daher sorgfältig zu prüfen, ob entsprechende Rechtsvorschriften zu beachten sind und ggf. welche Aufbewahrungsfristen sich daraus ergeben. Hierbei sollte die Rechtsabteilung beteiligt werden.

Die nachfolgenden Auswertungskriterien dienen als Beispiele, die Hinweise auf eventuelle Sicherheitslücken, Manipulationsversuche und Unregelmäßigkeiten erkennen lassen:

- Liegen die Zeiten des An- und Abmeldens außerhalb der Arbeitszeit (Hinweis auf Manipulationsversuche)?
- Häufen sich fehlerhafte Anmeldeversuche (Hinweis auf den Versuch, Passwörter zu erraten)?
- Häufen sich unzulässige Zugriffsversuche (Hinweis auf Versuche zur Manipulation)?

- Gibt es auffällig große Zeitintervalle, in denen keine Protokolldaten aufgezeichnet wurden (Hinweis auf eventuell gelöschte Protokollsätze)?
- Ist der Umfang der protokollierten Daten zu groß (eine umfangreiche Protokolldatei erschwert das Auffinden von Unregelmäßigkeiten)?
- Gibt es auffällig große Zeitintervalle, in denen anscheinend kein Benutzerwechsel stattgefunden hat (Hinweis darauf, dass das konsequente Abmelden nach Arbeitsende nicht vollzogen wird)?
- Gibt es auffallend lange Verbindungszeiten in öffentliche Netze hinein (siehe G 4.25 *Nicht getrennte Verbindungen*)?
- Wurde in einzelnen Netzsegmenten oder im gesamten Netz eine auffällig hohe Netzlast oder eine Unterbrechung des Netzbetriebes festgestellt (Hinweis auf Versuche, die Dienste des Netzes zu verhindern bzw. zu beeinträchtigen oder auf eine ungeeignete Konzeption bzw. Konfiguration des Netzes)?

Bei der Auswertung der Protokolldateien sollte besonderes Augenmerk auf alle Zugriffe gelegt werden, die unter Administratorkennungen durchgeführt wurden.

Wenn regelmäßig umfangreiche Protokolldateien ausgewertet werden müssen, ist es sinnvoll, ein Werkzeug zur Auswertung zu benutzen. Dieses Werkzeug sollte wählbare Auswertungskriterien zulassen und besonders kritische Einträge (z. B. mehrfacher fehlerhafter Anmeldeversuch) hervorheben.

Das oben Gesagte gilt analog auch für die Erhebung von Auditdaten, da es sich dabei im Prinzip nur um die Protokollierung sicherheitskritischer Ereignisse handelt.

Ergänzende Kontrollfragen:

- Wer wertet die Protokolldateien aus? Findet das Vier-Augen-Prinzip Anwendung?
- Können die Aktivitäten des Administrators ausreichend kontrolliert werden?
- Wird das IT-Sicherheitsmanagement bei Auffälligkeiten unterrichtet?

M 2.65 Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Revisor, Administrator, IT-Sicherheitsmanagement

Mittels Protokollauswertung oder durch Stichproben ist in angemessenen Zeitabständen zu überprüfen, ob die Benutzer des IT-Systems sich regelmäßig nach Aufgabenerfüllung abmelden oder ob mehrere Benutzer unter einer Kennung arbeiten.

Sollte festgestellt werden, dass tatsächlich mehrere Benutzer unter einer Kennung arbeiten, sind sie auf die Verpflichtung zum Abmelden nach Aufgabenerfüllung hinzuweisen. Gleichzeitig sollte der Sinn dieser Maßnahme erläutert werden, die im Interesse des einzelnen Benutzers liegt.

Stellt sich heraus, dass die An- und Abmeldevorgänge zu zeitintensiv sind und trotz Aufforderung nicht akzeptiert werden, sollten alternative Maßnahmen diskutiert werden wie zum Beispiel:

- Das IT-System kann für bestimmte Zeitintervalle einem Benutzer zugeordnet werden, so dass in dieser Zeit andere Benutzer das IT-System nicht nutzen dürfen. Dies setzt voraus, dass der Arbeitsprozess dementsprechend zeitlich variabel ist.
- Es können zusätzliche IT-Systeme angeschafft werden, mit denen die quasiparallele Arbeit an einem IT-System vermieden werden kann. Zu beachten ist, dass zwar die Anschaffungskosten für die zusätzlichen IT-Systeme anfallen, aber andererseits die Anschaffungskosten für PC-Sicherheitsprodukte entfallen können.
- Sollten sich die Datenbestände der einzelnen Benutzer separieren lassen (beispielsweise Benutzer A bearbeitet die Daten A-L, Benutzer B die Daten M-Z), so können dafür unterschiedliche Zugriffsrechte eingeräumt werden. Will ein Benutzer dann mit seinen Daten arbeiten, muss er sich zuvor beim System anmelden, da seine Kollegen kein Zugriffsrecht auf diese Daten besitzen.

Ergänzende Kontrollfragen:

- Wie häufig wird der ordnungsgemäße Benutzerwechsel geprüft?
- Gibt es Akzeptanzprobleme bezüglich des Benutzerwechsels?
- Lassen sich die Datenbestände separieren?

M 2.66 Beachtung des Beitrags der Zertifizierung für die Beschaffung

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Beschaffungsstelle

Bei der Beschaffung von IT-Produkten und IT-Systemen muss frühzeitig festgelegt werden, ob die bloße Zusicherung des Herstellers oder Vertreibers über implementierte Sicherheitsfunktionen als ausreichend vertrauenswürdig anerkannt werden kann. Insbesondere bei einem hohen oder sehr hohen Schutzbedarf kann die Vertrauenswürdigkeit der Produkte in Hinblick auf IT-Sicherheit nur dadurch gewährleistet werden, dass unabhängige Prüfstellen die Produkte untersuchen und bewerten (evaluieren).

Allgemein anerkannte Grundlage dieser Evaluierungen bilden seit 1991 die europaweit harmonisierten "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)" und das Evaluationshandbuch ITSEM und seit 1998 die weltweit angestimmten "Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik" / Common Criteria (CC). In Deutschland führen das BSI selbst und vom BSI akkreditierte Prüfstellen solche Evaluationen durch. Bei positivem Evaluationsergebnis und bei Einhaltung der Rahmenbedingungen von ITSEC und ITSEM bzw. der Common Criteria wird für das untersuchte Produkt oder System vom BSI als Zertifizierungsstelle ein Sicherheitszertifikat erteilt.

Aus dem dazugehörenden Zertifizierungsreport geht hervor, welche Funktionalität mit welcher Prüftiefe untersucht wurde und welche Bewertung vorgenommen wurde. Dabei reichen die Prüftiefe von Evaluationsstufe E 1 (geringste Prüftiefe) bis Evaluationsstufe E 6 (höchste Prüftiefe) bei den ITSEC bzw. von Vertrauenswürdigkeitsstufe EAL 1 (geringste Prüftiefe) bis Vertrauenswürdigkeitsstufe EAL 7 (höchste Prüftiefe) bei den CC. Dabei entspricht die Evaluationsstufe E 1 der ITSEC in etwa der Vertrauenswürdigkeitsstufe EAL 2 der CC usw. Zusätzlich wird die geprüfte Mechanismenstärke der Implementation der Sicherheitsfunktionen angegeben, die ein Maß darstellt für den Aufwand, den man zum Überwinden der Sicherheitsfunktionen aufbringen muss. ITSEC und CC unterscheiden hier die Mechanismenstärken niedrig, mittel und hoch. Darüber hinaus werden Hinweise gegeben, welche Randbedingungen beim Einsatz des Produktes beachtet werden müssen.

Stehen bei der IT-Beschaffung mehrere Produkte mit angemessenem Preis-/Leistungsverhältnis zur Auswahl, so kann ein eventuell vorhandenes Sicherheitszertifikat als Auswahlkriterium positiv berücksichtigt werden. Hierbei sollten Sicherheitszertifikate insbesondere dann berücksichtigt werden, wenn der evaluierte Funktionsumfang die Mindestfunktionalität (weitestgehend) umfasst und die Mechanismenstärke dem Schutzbedarf entspricht (siehe M 4.41 *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*). Je höher dann die im Zertifikat angegebene Prüfungstiefe ist, desto mehr Vertrauen in Wirksamkeit und Korrektheit der Sicherheitsfunktionen kann dem Produkt entgegengebracht werden.

Die Zertifizierungsstellen geben regelmäßig Übersichten heraus, welche Produkte ein Zertifikat erhalten haben. Eine Zusammenstellung der vom BSI zertifizierten IT-Produkte und -Systeme kann beim BSI angefordert werden: **BSI 7148** - BSI-Zertifikate. Weiterhin veröffentlicht das BSI neu erteilte Zertifikate in der Zeitschrift KES, Zeitschrift für Kommunikations- und EDV-Sicherheit. Diese Informationen lassen sich ebenfalls vom BSI-Server abrufen.

Ergänzende Kontrollfragen:

- Sind die IT-Beschaffungsstellen/-ämter über den Beitrag der Evaluation/Zertifizierung unterrichtet worden?
- Sind für die Beschaffungsstelle/-ämter aktuelle Übersichten über zertifizierte Produkte verfügbar?
- Werden von der Beschaffungsstelle die relevanten Zertifizierungsreports angefordert?

M 2.67 Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Bevor mit der eigentlichen Konfiguration und Installation von Peer-to-Peer-Diensten begonnen werden kann, müssen zuerst einige grundlegende Überlegungen angestellt werden:

Werden Peer-to-Peer-Dienste wirklich benötigt?

Zunächst muss geklärt werden, welche Dienstleistung das jeweilige Betriebssystem erbringen und in welchem Rahmen es diesbezüglich eingesetzt werden soll. Insbesondere ist zu klären, ob überhaupt Peer-to-Peer-Funktionalitäten, d. h. die Freigabe von Ressourcen, wie Verzeichnisse oder Drucker, auf einem Arbeitsplatz-Computer, verwendet werden sollen.

Dies soll anhand einiger **Beispiele** veranschaulicht werden:

- Das IT-System wird für eine Arbeitsgruppe von typischerweise drei bis fünf Benutzern eingesetzt, bei denen jeder alle Rechte besitzen sollte. An jedem Arbeitsplatz soll die komplette Peer-to-Peer-Funktionalität unterstützt werden.
- Das IT-System wird für eine größere Arbeitsgruppe eingesetzt, in der unterschiedliche Rechte vergeben werden können. Die Peer-to-Peer-Funktionalität soll aufgrund konkreter Anforderungen in eingeschränkter Form realisiert werden.
- Das IT-System wird in einem servergestützten Netz eingesetzt, bei dem auf die Peer-to-Peer-Funktionalität zum Austausch von Daten in der Regel verzichtet werden kann. Einzelne Drucker sollen jedoch über Peer-to-Peer-Funktionalität gemeinsam benutzt werden können.
- Das IT-System wird in einem servergestützten Netz eingesetzt, in dem keine Peer-to-Peer-Funktionalität vorgesehen ist. Dann sind alle Peer-to-Peer-Dienste zu deaktivieren. In diesem Fall kann die Betrachtung der folgenden Punkte entfallen, doch sollte dann die Maßnahme M 5.37 *Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz* beachtet werden.

Hinweis:

Servergestützte Netze bieten wesentlich weitgehendere Sicherheitsfunktionalitäten als Peer-to-Peer-Netze. Darüber hinaus entstehen durch die Verwendung von Peer-to-Peer-Diensten in servergestützten Netzen zusätzliche Sicherheitsprobleme. **Deshalb sollte bei servergestützten Netzen auf die Verwendung von Peer-to-Peer-Funktionalitäten verzichtet werden.**

Sofern Peer-to-Peer-Dienste verwendet werden sollen, müssen anschließend diese Überlegungen in eine Sicherheitsstrategie übersetzt werden.

Dabei zeigt sich, dass je nach bereits vorhandener Systemumgebung und Organisationsstruktur sowie der vorzusehenden Restriktionen an die Peer-to-Peer-Funktionalitäten, ein mehr oder weniger großer Aufwand bei der Entwicklung einer dazu passenden Sicherheitsstrategie notwendig ist.

Es wird nachfolgend eine methodische Vorgehensweise aufgezeigt, mittels derer eine umfassende Sicherheitsstrategie für den Einsatz von Peer-to-Peer-Diensten entwickelt werden kann. Da jedoch Peer-to-Peer-Dienste in verschiedenen Konfigurationen eingesetzt werden können, ist für die jeweilige Ausprägung individuell zu entscheiden, welche der beschriebenen Schritte anzuwenden sind.

In der Sicherheitsstrategie sollte aufgezeigt werden, wie Peer-to-Peer-Dienste sicher installiert, administriert und betrieben werden. Nachfolgend werden die einzelnen Entwicklungsschritte einer solchen Strategie vorgestellt:

1. Definition der Peer-to-Peer-Netzstruktur

Eine Peer-to-Peer-Netzstruktur wird definiert durch die Festlegung,

- welche Rechner als "Fileserver" (sie dürfen Verzeichnisse freigeben),
- welche Rechner als "Druckserver" (sie dürfen Drucker freigeben),
- welche Rechner als "Applikationsserver" für bestimmte IT-Anwendungen (Bei WfW sind das z. B. *Mail, Schedule+*, *Fax.* Sie sollten ständig verfügbar sein.) und
- welche Rechner nur als Clients (sie können sich nur mit anderen Rechnern verbinden)

fungieren sollen. Dabei ist darauf zu achten, dass die Kapazität der "Server" den jeweiligen Anforderungen hinsichtlich Geschwindigkeit und Plattenspeicherplatz genügt. Außerdem sollte auch die Anzahl der "Server" auf das notwendige Maß beschränkt werden. Darüber hinaus sollten keine Applikationen auf "Server" ausgelagert werden, bei denen ständig große Datenmengen über das Netz übertragen werden müssen, da dies zu Netzüberlastungen führen kann.

2. Regelung der Verantwortlichkeiten

Peer-to-Peer-Dienste sollten mittels eines geschulten **Administrators** nebst Stellvertreter sicher betrieben werden. Diese allein dürfen Sicherheitsparameter der Peer-to-Peer-Funktionalitäten verändern. Sie sind z. B. dafür zuständig, auf eventuellen "Applikationsservern" oder "Fileservern" den entsprechenden **Verantwortlichen** Administrationsrechte und -werkzeuge zur Verfügung zu stellen, damit diese die Freigabe der von anderen benötigten Verzeichnisse bzw. Anwendungen vornehmen können.

Administratoren benennen

Auch in einem servergestützten Netz, in dem zusätzlich Peer-to-Peer-Funktionalitäten zugelassen werden sollen, müssen explizit Peer-to-Peer-Administratoren ernannt werden, die aber mit den Netzadministratoren identisch sein dürfen.

Die Verantwortlichkeiten der einzelnen **Benutzer** beim Einsatz von Peer-to-Peer-Diensten sind unter Schritt 7 dargestellt.

3. Einschränkung der Freigabemöglichkeiten

Windows für Workgroups:

Mit dem Administrationswerkzeug ADMINCFG.EXE für WfW können die folgenden Möglichkeiten für jeden WfW-Rechner einzeln zugelassen oder gesperrt werden:

- Freigabe von Verzeichnissen,
- Freigabe von Druckern,
- Restriktionen für das WfW-Anmeldepasswort (Ablaufzeit, Mindestlänge etc.),
- Freigabe von Netz-DDE (z. B. für den Datenaustausch über die Ablagemappe oder das Telefonieren unter WfW).

Die Datei ADMINCFG.EXE gehört zwar zum Lieferumfang von WfW, wird aber nicht standardmäßig auf den Rechnern installiert. Eine Dokumentation erfolgt nur in den Anleitungen für Systemverwalter (siehe M 4.45 *Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW*).

Es ist festzulegen, auf welchen Rechnern dieses Administrationswerkzeug installiert werden soll.

Dieses Programm verfügt über eine Passwortabfrage, mit der die eingestellte Konfiguration geschützt wird. Jeder, der Zugriff auf dieses Programm hat, kann versuchen, das Passwort der jeweiligen Konfigurationsdatei herauszufinden und dann die Freigabeoptionen zu ändern.

Sinnvollerweise sollte es daher nur dem Administrator und seinem Stellvertreter zur Verfügung gestellt werden. Darüber hinaus ist es unter WfW möglich, die Konfigurationsdateien zentral auf einem Server abzulegen, und zwar entweder für jeden Benutzer einzeln, für Gruppen oder für alle Benutzer gemeinsam. Weitere Informationen hierzu finden sich im *WfW Resource Kit, Addendum for Operating System Version 3.11*. Dies hat den Vorteil, Änderungen für mehrere WfW-Benutzer gleichzeitig vornehmen zu können, insbesondere wenn das Passwort der Konfigurationsdatei(en) geändert werden soll.

Hinweis: Eine durch ein Passwort geschützte Konfiguration bietet nur eingeschränkte Sicherheit, da sie einem vorsätzlichen Angriff kaum standhält. Die Einschränkung der WfW-Funktionalität beugt damit in erster Linie dem unbeabsichtigten Fehlverhalten der Benutzer vor.

Windows 95:

Die Möglichkeit zur Freigabe von Verzeichnissen bzw. Druckern lässt sich unter Windows 95 für einzelne Rechner und/oder Benutzer durch entsprechende Einträge in deren Profile einschränken (siehe auch M 4.58 *Freigabe von Verzeichnissen unter Windows 95*).

Windows NT/2000:

Unter Windows NT/2000 ist die Möglichkeit der Freigabe von Verzeichnissen auf Administratoren bzw. Hauptbenutzer eingeschränkt, so dass hier einem Missbrauch durch Endbenutzer vorgebeugt ist. Ob und ggf. welche Ressourcen freigegeben werden sollen, ist bei der Planung des Netzes im Detail fest-

zulegen (siehe M 2.94 *Freigabe von Verzeichnissen unter Windows NT* und M 4.149 *Datei- und Freigabeberechtigungen unter Windows*).

Unix bzw. Linux:

Auf IT-Systemen unter Unix oder Linux können Peer-to-Peer-Dienste durch eine Reihe von Mechanismen bereitgestellt werden. Die wichtigsten Beispiele sind NFS-Shares, SAMBA und durch den Daemon *inetd* bereitgestellte Dienste. Durch geeignete Rechtevergabe (siehe auch M 4.19 *Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen*) muss sichergestellt werden, dass Benutzer die systemweiten Konfigurationsdaten (beispielsweise */etc/inetd.conf*) nicht modifizieren können. Anderenfalls besteht die Gefahr, dass Benutzer zusätzliche privilegierte Dienste aktivieren, wodurch Sicherheitslücken entstehen können (siehe auch M 5.72 *Deaktivieren nicht benötigter Netzdienste*).

Bestimmte Netzdienste können unter Unix bzw. Linux auch ohne Supervisor-Rechte gestartet werden, in der Regel jedoch mit eingeschränkter Funktionalität. Dies kann nur dadurch verhindert werden, dass dem Benutzer der Zugriff auf die entsprechenden Daemons verweigert wird. Auch auf Entwicklungswerkzeuge (z. B. Compiler) sollten Benutzer nur dann zugreifen können, wenn sie sie zwingend benötigen (siehe auch M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*).

4. Festlegung einer Namenskonvention

Eindeutige Namen für Rechner und Benutzer vergeben

Um eine Maskerade zu erschweren, sollten eindeutige Namen für die Rechner, Benutzergruppen und die Benutzer verwendet werden. Diese Namen sind allen Benutzern bekannt zu geben. Erfolgt nun eine Anmeldung unter einem Namen, den es nach der Konvention nicht geben kann, z. B. indem er einem bestehenden nur ähnlich ist, wird eine Maskerade offensichtlich. Eine Anmeldung unter einem bereits angemeldeten Rechnernamen wird von WfW abgewiesen, jedoch ist eine Maskerade unter einem zugelassenen Namen dann möglich, wenn der betreffende Anwender nicht angemeldet ist.

Unter Windows 95 ist durch die Systemrichtlinien sicherzustellen, dass die Benutzer weder Rechner- noch Benutzernamen selbstständig ändern können. Dazu sollte für Standardbenutzer der Zugriff auf die Systemsteuerungsoption *Netzwerk* deaktiviert werden (siehe auch M 2.103 *Einrichten von Benutzerprofilen unter Windows 95*).

Unter Windows NT/2000 sind nur die vom Administrator definierten Benutzer zugelassen und es können nur Administratoren den Rechnernamen ändern. Allerdings können Benutzer versuchen, sich über die Option *Verbinden Als* unter *Netzlaufwerk verbinden* unter anderem Benutzernamen anzumelden.

Namenskonventionen für Freigabenamen

Zusätzlich können Namenskonventionen für die Freigabenamen von Verzeichnissen oder Druckern eingeführt werden. Sollen keine Rückschlüsse auf den Inhalt des Verzeichnisses möglich sein, sind entsprechende Pseudonyme zu verwenden. Soll eine unter Windows freigegebene Ressource nicht als solche erkennbar sein, ist dem Freigabenamen das Zeichen "$" anzuhängen. Letzteres empfiehlt sich immer dann, wenn Verzeichnisse nur zum bilateralen Austausch von Informationen zwischen zwei Anwendern freigegeben werden.

Bei korrekter Rechtevergabe können Benutzer von IT-Systemen unter Unix oder Linux weder die IP-Adresse noch den Rechnernamen ändern. Ähnlich wie unter Windows NT/2000 können sie jedoch bei der Anmeldung an einem anderen IT-System einen beliebigen Benutzernamen wählen.

5. Festlegung freizugebender Verzeichnisse bzw. Drucker und Vergabe der Zugriffsrechte

Für die "Applikationsserver" ist festzulegen, welche Verzeichnisse (z. B. das Post-Office-Verzeichnis AGPO unter dem WfW-Programm *Mail*) für den Betrieb freizugeben sind. Für die "Fileserver" sind diejenigen Verzeichnisse auszuwählen, die den Benutzern zur Verfügung gestellt werden sollen. Unter WfW und Windows 95 können beliebige Benutzer Ressourcen für den Netzzugriff freigeben, unter Windows NT/2000 ist dies nur den Administratoren bzw. Hauptbenutzern erlaubt.

Dabei muss zwischen zwei Zugriffsmodellen unterschieden werden:

- der Sicherheit auf Freigabeebene (Share Level Security), bei der die Zugriffe auf freigegebene Ressourcen über Passwörter kontrolliert werden, und
- der Sicherheit auf Benutzer-Ebene (User Level Security), bei der die Zugangs- und Zugriffskontrolle eines Server-Betriebssystems genutzt werden.

WfW unterstützt nur das erste dieser Modelle, Windows NT/2000 (als Client) das zweite, während Windows 95 über die Registerkarte *Zugriffssteuerung* der Systemsteuerungsoption *Netzwerk* die Auswahl zwischen beiden Modellen gestattet.

Bei Verwendung der Sicherheit auf Freigabeebene sind für die freigegebenen Verzeichnisse Zugriffsrechte (Lese- oder Lese-/Schreibrecht) zu definieren und geeignete Passwörter auszuwählen.

Zugriff hat, wer das Passwort kennt!

Durch die gezielte Weitergabe dieser Passwörter an einzelne Benutzer werden nunmehr die Zugriffsrechte im Peer-to-Peer-Netz vergeben. Diese Passwörter sind nur soweit erforderlich bekannt zu geben, da die Rücknahme der Freigabe für eine einzelne Person nur durch einen aufwendigen Passwortwechsel für alle anderen noch berechtigten Benutzer vorgenommen werden kann.

Bei Verwendung der Sicherheit auf Benutzer-Ebene unter Windows NT/2000 und Windows 95 werden die Zugriffsrechte dagegen explizit einzelnen Benutzern und/oder Gruppen zugewiesen, so dass in diesem Fall die Eingabe von Passwörtern entfällt. Dies setzt die Einbindung der Clients in eine Arbeitsgruppe bzw. eine Domäne zusammen mit wenigstens einem Windows NT/2000-System voraus. Die Verwendung der Sicherheit auf Freigabeebene ist in diesem Fall zu vermeiden, da sie einen wesentlich geringeren Schutz bietet. Anschließend ist zu entscheiden, ob die Verzeichnisse automatisch beim Start des jeweiligen Servers freigegeben und ob sie automatisch beim Start des zugreifenden Rechners verbunden werden sollen.

Das zuvor Gesagte gilt analog für die Freigabe von Druckern.

Ressourcen und Protokolle festlegen

Unter Unix oder Linux ist nicht nur festzulegen, welche Ressourcen (z. B. Verzeichnisse oder Drucker) im Netz zur Verfügung gestellt werden sollen, sondern auch, über welche Protokolle der Zugriff erfolgen soll. Dateien oder Verzeichnisse können unter Unix beispielsweise via FTP, NFS oder SAMBA für die gemeinsame Nutzung bereitgestellt werden. Letzteres erlaubt auch Windows-Systemen den Zugriff auf die Ressourcen, ohne dass dort zusätzliche Software-Komponenten installiert werden müssten. Gängige Methoden zur Bereitstellung von Druckdiensten unter Unix sind das LPR-Protokoll und SAMBA.

Unter Unix unterstützen alle gängigen Netzdienste eine benutzerspezifische Zugriffskontrolle. Diese sollte aktiviert und genutzt werden, sofern nicht alle Benutzer im Netz unbeschränkten Zugriff auf die Ressourcen haben sollen. Beim Einsatz von SAMBA sollte die Einstellung *security=share* auf jeden Fall vermieden werden (siehe auch M 5.82 *Sicherer Einsatz von SAMBA*).

6. Passwortwechselstrategie

Windows für Workgroups:

Im WfW-Netz werden eine Reihe von Passwörtern gebraucht: die Anmeldepasswörter, das Passwort für den Aufruf von ADMINCFG.EXE und die Passwörter für die verschiedenen Rechte freigegebener Verzeichnisse, Drucker und Ablagemappen. Die Anmeldepasswörter und das Passwort für den Aufruf von ADMINCFG.EXE sollten regelmäßig gewechselt werden (siehe auch M 2.11 *Regelung des Passwortgebrauchs*). Eine maximale Gültigkeitsdauer dieser Passwörter ist daher festzulegen. Damit auch der Wechsel des ADMINCFG.EXE-Passwortes einfach möglich ist, können die zugehörigen Konfigurationsdateien zentral auf einem Server hinterlegt werden. Da ein Wechsel der Freigabe-Passwörter mit erheblichem organisatorischen Aufwand (siehe Nr. 5) verbunden sein kann, ist vorab festzulegen, wie oft diese gewechselt und wie die neuen Passwörter den Betroffenen bekannt gegeben werden sollen.

Windows 95:

Unter Windows 95 hängt die Anzahl der zu verwendenden Passwörter davon ab, ob als Zugriffsmodell die Sicherheit auf Benutzer-Ebene oder die Sicherheit auf Freigabeebene verwendet wird. Im ersten Fall werden, analog zur Situation bei Windows NT/2000, nur die Anmeldepasswörter zu den Rechnern benötigt, die Ressourcen für den Netzzugriff freigegeben haben. Dagegen werden im zweiten Fall, ähnlich wie bei WfW, auch Passwörter für den Zugriff auf freigegebenen Ressourcen benötigt. Eigene Passwörter zur Verwaltung der Peer-to-Peer-Funktionalität entfallen, da diese hier über Benutzerprofile gesteuert wird.

Zugriffsschutz auf Benutzer-Ebene

Der Zugriffsschutz auf Benutzer-Ebene basiert auf den Benutzerlisten, die auf Windows NT/2000 oder Novell Netware Servern geführt werden, und kann daher auch nur in solchen Netzen realisiert werden. Dieses Zugriffsmodell bietet die größere Sicherheit und sollte daher vorzugsweise eingesetzt werden, wenn trotz einer Vernetzung über Windows NT/2000 oder Novell Netware Server Peer-to-Peer-Funktionalitäten eingesetzt werden sollen.

Windows NT/2000:

Unter Windows NT/2000 erfolgt die Verwaltung der Peer-to-Peer-Funktionalität unter der Kontrolle der allgemeinen Zugangs- und Zugriffskontrolle, so dass hier keine eigenen Passwörter für diese Verwaltungstätigkeiten erforderlich sind. Zur Verwaltung der Zugangspasswörter der betreffenden Benutzer sollten die Vorgaben der Maßnahme M 2.11 *Regelung des Passwortgebrauchs* berücksichtigt werden.

Unix bzw. Linux:

inkonsistente Passwort-Datenbanken

Werden Ressourcen unter Unix oder Linux über mehr als ein Protokoll im Netz zur Verfügung gestellt, so werden dabei u. U. unterschiedliche Passwort-Datenbanken verwendet (z. B. NIS, */etc/passwd* und *smb.passwd*). Diese sollten entweder manuell oder mit Hilfe geeigneter Administrations-Tools synchronisiert werden. Inkonsistente Inhalte in den Passwort-Datenbanken führen möglicherweise zu Verwirrung bei den Benutzern und sollten daher vermieden werden.

7. Verantwortlichkeiten für Benutzer im Peer-to-Peer-Netz

Neben der Wahrnehmung der Peer-to-Peer-Managementaufgaben (siehe Nr. 2) müssen weitere Verantwortlichkeiten festgelegt werden. Es ist festzulegen, welche Verantwortung die einzelnen Benutzer der Peer-to-Peer-Dienste übernehmen müssen. Dies können zum Beispiel Verantwortlichkeiten sein für

- die Auswertung der Protokolldateien auf den einzelnen Rechnern,
- die Vergabe von Zugriffsrechten,
- das Hinterlegen und den Wechsel von Passwörtern und
- die Durchführung von Datensicherungen.

8. Schulung

Abschließend muss festgelegt werden, welche Peer-to-Peer-Benutzer zu welchen Punkten geschult werden müssen. Erst nach ausreichender Schulung kann der Wirkbetrieb aufgenommen werden.

Die so entwickelte Sicherheitsstrategie ist zu dokumentieren und im erforderlichen Umfang den Benutzern der Peer-to-Peer-Dienste mitzuteilen.

Ergänzende Kontrollfragen:

- Wird die Sicherheitsstrategie an Veränderungen im Einsatzumfeld angepasst?

M 2.68 Sicherheitskontrollen durch die Benutzer beim Einsatz von Peer-to-Peer-Diensten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Da beim Einsatz von Peer-to-Peer-Diensten die wesentlichen Sicherheitseigenschaften lediglich dezentral kontrolliert werden können, obliegt es dem einzelnen Benutzer, solche Sicherheitskontrollen durchzuführen. In geeigneten Abständen sollten daher von den Benutzern folgende Kontrollen durchgeführt werden:

- **Kontrolle aktiver Verbindungen**: Es sollte überprüft werden, welcher Rechner aktuell Zugriff auf den eigenen Rechner hat und wie die Art des Zugriffs erfolgt. Hierzu kann
  - unter WfW das Programm *Netzwerkmonitor* in der Programmgruppe *Netzwerk*,
  - unter Windows 95 das optional installierbare Programm *Netzwerkmonitor* in der Programmgruppe *Zubehör\Systemprogramme*,
  - unter Windows NT die Systemsteuerungsoption *Server* und
  - unter Windows 2000 das MMC-Snap-in *Freigegebene Ordner* (*Sitzungen* und *Geöffnete Dateien*)

  verwendet werden.

Beispiel:

Erkennbar sind die vom Rechner *MUSTER* aufgebauten Verbindungen. Dabei bedeutet:

INFOS	Es wird auf das Verzeichnis *INFOS* schreibend zugegriffen.
TEMP	Es wird auf das Verzeichnis *TEMP* lesend zugegriffen.
HP$	Auf den lokalen Drucker mit dem Namen *HP$* wird zugegriffen.
CLIPSRV/SYSTEM	Eine Verbindung zur Ablagemappe wurde hergestellt.
CLIPSRV/$SEITE12	Auf die Seite mit Namen *SEITE12* der Ablagemappe wird zugegriffen.

Zeigt sich dabei, dass ein Rechner unberechtigt auf ein Verzeichnis oder den Drucker zugreift, ist die Freigabe rückgängig zu machen. Eventuelle Druckjobs können über den Druckmanager abgebrochen werden. Im Ereignisprotokoll (siehe nächste Grafik) werden die entsprechenden Aktionen dokumentiert. Zeigt sich, dass unberechtigt auf die Ablagemappe zugegriffen wird, ist ebenfalls zu trennen, jedoch empfiehlt es sich vorher mit der *Druck*-Taste den Fensterinhalt des *Netzwerkmonitors* in die Zwischenablage zu kopieren, da Zugriffe auf die Ablagemappe nicht dokumentiert werden.

- **Kontrolle der Protokolldaten**: Sind auf einem Rechner Ressourcen freigegeben, sollte das Ereignisprotokoll aktiviert und regelmäßig ausgewertet werden. Die entsprechenden Optionen finden sich

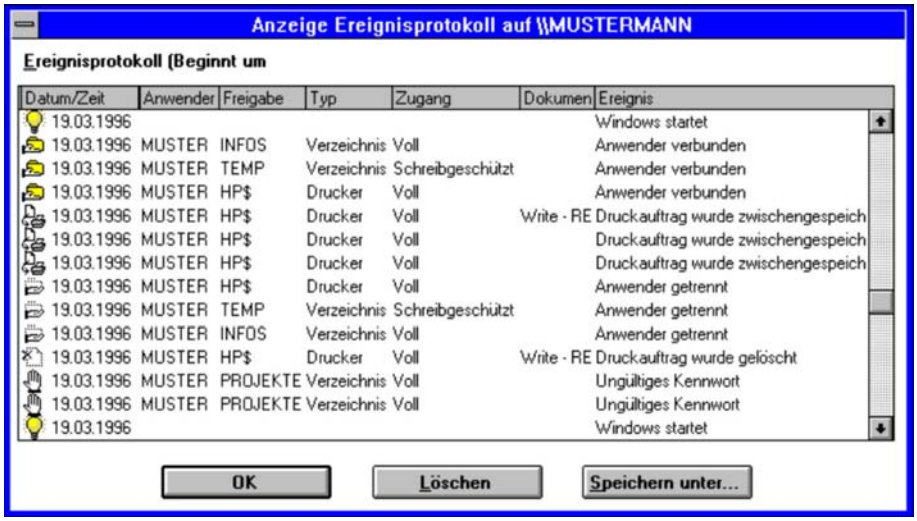
  - unter WfW in der Programmgruppe *Systemsteuerung* unter *Netzwerk* bzw. in der Programmgruppe *Netzwerk* unter *Netzwerkmonitor*,
  - unter Windows NT in der Programmgruppe *Verwaltung* unter *Benutzer-Manager* bzw. unter *Ereignisanzeige* und
  - unter Windows 2000 in den MMC-Snap-ins *Gruppenrichtlinien* und *Ereignisanzeige*.

  Windows 95 bietet standardmäßig keine Möglichkeit zur Ereignisprotokollierung. Daher sollte unter Windows 95 der *Netzwerkmonitor* offen gehalten werden, falls trotz dieser Schwachstelle die Peer-to-Peer-Funktionalitäten genutzt werden sollen.

Protokolle auswerten

Es sollte regelmäßig, beispielsweise wöchentlich, überprüft werden, ob sich unberechtigte Benutzer mit freigegebenen Verzeichnissen verbunden hatten, ob es fehlerhafte Versuche zum Verbinden freigegebener Verzeichnisse gab oder ob das System zu ungewöhnlichen Zeiten gestartet wurde. Da diese Protokolldaten auch personenbezogene Daten beinhalten, sind sie nach ihrer Auswertung, wenn die Notwendigkeit der Speicherung nicht mehr besteht, zu löschen.

Beispiel für ein mögliches Ereignisprotokoll:



- **Kontrolle automatisch freigegebener Ressourcen**: Sporadisch sollten WfW- und Windows 95-Benutzer überprüfen, welche ihrer Ressourcen automatisch nach dem Systemstart ohne ihre direkte Beteiligung freigegeben werden. Dies kann zum Beispiel dadurch erfolgen, dass sie nach Systemstart kontrollieren, welche Verzeichnisse, Drucker und Seiten der Ablagemappe dann freigegeben sind. Ggf. ist die Freigabe zurückzunehmen. Unerklärliche Unregelmäßigkeiten, wie die automatische Freigabe eines Verzeichnisses, das der Benutzer selbst nie freigegeben hat, sind dem Administrator zu melden. Es kann sich hier um Hinweise auf Trojanische Pferde handeln, die unbemerkt Verzeichnisse freigeben.

  Besteht Unsicherheit darüber, ob oder was freigegeben wurde, sollte unter WfW die Datei *shares.pwl* gelöscht werden, die die Einträge für die automatische Freigabe enthält. Unter Windows 95 sind die Freigaben mit Hilfe des Explorers zurückzunehmen. Dieses Problem stellt sich unter Windows NT/2000 nicht, da hier nur Administratoren bzw. Hauptbenutzer Ressourcen freigeben dürfen.

  WfW: Zugriffsrechte sind schwierig zu prüfen

  Eine Kontrolle der Rechtevergabe ist in einem Peer-to-Peer-Netz unter WfW nicht auf direktem Wege möglich, da die Kenntnis eines gültigen Passwortes gleichbedeutend mit dem Besitz des Rechtes ist. Lediglich durch einen aufwendigen Passwortwechsel kann eine konsistente Rechteverteilung sichergestellt werden.

Auf IT-Systemen unter Unix oder Linux sollten die Sicherheitskontrollen durch geeignete administrative Maßnahmen unterstützt und vereinfacht werden. Hierzu wird empfohlen, regelmäßig Informationen über die aktiven Netzverbindungen zu sammeln (beispielsweise unter Benutzung des Befehls *netstat*) und in einer Protokolldatei zu speichern. Es bietet sich an, diesen Vorgang mit Hilfe des *cron*-Daemons zu automatisieren. Um das Datenvolumen zu minimieren, sollten dabei irrelevante Informationen herausgefiltert werden. Je nach Kenntnisstand der Benutzer sollten die Protokolldaten dann entweder durch die Benutzer selbst kontrolliert oder in regelmäßigen Abständen dem Administrator zur Verfügung gestellt werden. In ähnlicher Weise kann mit anderen Protokolldateien verfahren werden, in denen beispielsweise fehlgeschlagene Login-Versuche oder andere sicherheitsrelevanten Ereignisse festgehalten werden.

Ergänzende Kontrollfragen:

- Werden Unregelmäßigkeiten dem Administrator bekannt gegeben?

M 2.69 Einrichtung von Standardarbeitsplätzen

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator

Ein Standardarbeitsplatz ist gekennzeichnet durch einheitliche Hardware und Software sowie deren Konfiguration. Die Planung und Einrichtung erfolgt üblicherweise unter den Aspekten der Aufgabenstellung, Zuverlässigkeit, Ergonomie, Geschwindigkeit und Wartbarkeit. Sie wird durch fachkundiges Personal durchgeführt. Die Einrichtung von Standardarbeitsplätzen ist in mehrfacher Hinsicht vorteilhaft:

IT-Sicherheit:

- Standardarbeitsplätze sind leichter in Sicherheitskonzepte einzubinden.
- Der Aufwand für die Dokumentation des IT-Bestandes wird reduziert.

IT-Management:

- Die Beschaffung größerer Stückzahlen gleicher Komponenten ermöglicht Preisvorteile.
- Der Einsatz nicht zulässiger Software ist einfacher festzustellen.
- Durch gleiche IT-Ausstattung entfallen "Neidfaktoren" zwischen den einzelnen Benutzern.

IT-Nutzer:

- Bei Gerätewechsel ist keine erneute Einweisung in die IT-Konfiguration erforderlich, Ausfallzeiten werden somit minimiert.
- Bei Fragen zu Hard- und Software können sich Anwender gegenseitig helfen.

Systemadministration bei Installation und Wartung:

- Eine gewissenhaft geplante und getestete Installation kann fehlerfrei und mit geringem Arbeitsaufwand installiert werden.
- Die einheitliche Arbeitsumgebung erleichtert den Benutzerservice (Wartung, Support und Pflege).

Schulung:

- Die Teilnehmer werden in dem Umfeld geschult, das sie am Arbeitsplatz vorfinden.

Ergänzende Kontrollfragen:

- Werden Abweichungen vom Standardarbeitsplatz begründet?
- Werden die Begründungen regelmäßig überprüft?
- Welche Aspekte werden bei Planung und Einrichtung von Standardarbeitsplätzen berücksichtigt?

M 2.70 Entwicklung eines Konzepts für Sicherheitsgateways

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Die Kopplung von lokalen Netzen mit globalen Netzen wie dem Internet führt zu einem neuen Informationsangebot. Die lokale Vernetzung von Rechnersystemen sorgt dafür, dass von jedem Arbeitsplatzrechner aus auf die vielfältigen Informationen zugegriffen werden kann.

Diese Netzkopplung lässt aber auch neue Gefährdungen entstehen, da prinzipiell nicht nur ein Datenfluss von außen in das zu schützende Netz stattfinden kann, sondern auch ein Datenabfluss in die andere Richtung. Darüber hinaus gefährdet die Möglichkeit, von einem entfernten Rechner aus (z. B. aus dem Internet) Befehle auf Rechnern im lokalen Netz ausführen zu lassen, die Integrität und die Verfügbarkeit der lokalen Rechner und dadurch indirekt auch die Vertraulichkeit der lokalen Daten.

Ein zu schützendes Teilnetz sollte daher nur dann an ein nicht-vertrauenswürdiges Netz angeschlossen werden, wenn dies unbedingt erforderlich ist. Dies gilt insbesondere für Anschlüsse an das Internet, das aufgrund der hohen Nutzerzahl das wohl am wenigsten vertrauenswürdige existierende Netz darstellt. Dabei ist auch zu prüfen, inwieweit das zu schützende Netz in Teilnetze segmentiert werden muss, weil bestimmte Rechner oder Bereiche des zu schützenden Netzes überhaupt nicht oder nur bedingt ans Internet angeschlossen werden sollten, und ob für die Kopplung mit dem Internet nicht ein Stand-alone-System ausreicht (siehe M 5.46 *Einsatz von Stand-alone-Systemen zur Nutzung des Internets* und Baustein B 3.210 *Internet-PC*).

Um die Sicherheit des zu schützenden Netzes zu gewährleisten, muss ein geeignetes Sicherheitsgateway eingesetzt werden. Damit ein Sicherheitsgateway effektiven Schutz bieten kann, müssen folgende grundlegende Bedingungen erfüllt sein:

Das Sicherheitsgateway muss

- auf einer umfassenden Sicherheitsrichtlinie aufsetzen,
- im IT-Sicherheitskonzept der Organisation eingebettet sein,
- korrekt installiert und
- korrekt administriert werden.

Der Anschluss an ein nicht-vertrauenswürdiges Netz darf erst dann erfolgen, wenn überprüft worden ist, dass mit dem gewählten Sicherheitsgateway-Konzept sowie den personellen und organisatorischen Randbedingungen alle Risiken beherrscht werden können.

Es gibt verschiedene Arten, Sicherheitsgateways zu realisieren. Um festzustellen, welches Konzept für den Einsatzzweck am besten geeignet ist, muss zunächst geklärt werden, welche Sicherheitsziele durch das Sicherheitsgateway erfüllt werden sollen.

Beispiele für Sicherheitsziele sind:

- Schutz des vertrauenswürdigen (internen) Netzes gegen unbefugten Zugriff aus dem nicht-vertrauenswürdigen Netz,
- Schutz der lokal übertragenen und gespeicherten Daten gegen Angriffe auf deren Vertraulichkeit oder Integrität,
- Schutz der lokalen Netzkomponenten gegen Angriffe auf deren Verfügbarkeit (Insbesondere gilt dies auch für Informationsserver, die Informationen aus dem internen Bereich für die Allgemeinheit zu Verfügung stellen.),
- Verfügbarkeit der Informationen des externen Netzes im zu schützenden internen Netz, (die Verfügbarkeit dieser Informationen muss aber gegenüber dem Schutz der lokalen Rechner und Informationen zurückstehen!),
- Schutz vor Angriffen, die auf IP-Spoofing beruhen, die Source-Routing Option, das Protokoll ICMP oder Routing-Protokolle missbrauchen,
- Schutz vor Angriffen durch neue sicherheitsrelevante Softwareschwachstellen. (Da die Anzahl der potentiellen Angreifer und deren Kenntnisstand bei einer Anbindung an das Internet als sehr hoch angesehen werden muss, ist dieses Sicherheitsziel von besonderer Bedeutung.)
- Schutz vor ungewünschtem Datenabfluss

Auf den Sicherheitszielen aufbauend muss eine Sicherheitsrichtlinie erarbeitet werden, in der Aufgaben und Anforderungen an das Sicherheitsgateway festgelegt werden. Diese Sicherheitsrichtlinie muss in die IT-Sicherheitsstrategie der jeweiligen Organisation eingebettet sein und daher mit dem IT-Sicherheitsmanagement abgestimmt werden.

Entscheidungen dokumentieren

Die Entscheidungen, die bei der Erarbeitung der Sicherheitsrichtlinie für das Sicherheitsgateway getroffen wurden, sollten - ebenso wie die Gründe für diese Entscheidungen - nachvollziehbar dokumentiert werden.

Die Umsetzung der Sicherheitsrichtlinie für das Sicherheitsgateway erfolgt dann durch die Realisierung des Sicherheitsgateways, durch geeignete Auswahl von Hardware-Komponenten, Paketfilter und Application-Level-Gateway und die sorgfältige Festlegung und Einrichtung von Filterregeln.

Die Begriffe Paketfilter und Application-Level-Gateway sind für die weiteren Abschnitte wichtig und werden daher kurz erläutert, um Missverständnisse zu vermeiden:

Paketfilter

- *Paketfilter* sind IT-Systeme mit spezieller Software, die die Informationen anhand der Header-Daten der unteren Schichten (Transportschicht oder Verbindungsschicht) des OSI-Modells filtern und anhand spezieller Regeln Pakete weiterleiten oder verwerfen (siehe M 2.74 *Geeignete Auswahl eines Paketfilters*). Paketfilter treffen ihre Entscheidungen beispielsweise anhand von Quell- und Ziel-Adressen oder -Ports eines Paketes, ohne den Inhalt zu berücksichtigen.

Application-Level-Gateway

- Ein *Application-Level-Gateway* ist ein IT-System, das die Informationen der Anwendungsschicht (das heisst, den tatsächlichen Inhalt (die Nutzdaten) eines Paketes oder mehrerer zusammengehöriger Pakete) filtert und anhand spezieller Regeln Verbindungen oder auch bestimmte Kommandos verbieten oder erlauben kann (siehe M 2.75 *Geeignete Auswahl eines Application-Level-Gateways*). Während Paketfilter auf Schicht 3 und 4 des OSI-Modells arbeiten, arbeiten Gateways auf Schicht 7. Ein Application-Level-Gateway ist im Allgemeinen auf einem IT-System implementiert, das ausschließlich für diese Aufgabe eingesetzt wird und dessen Befehlsumfang auf das Notwendigste reduziert ist.

Damit ein Sicherheitsgateway einen wirkungsvollen Schutz eines Netzes gegen Angriffe von außen darstellt, müssen einige grundlegende Voraussetzungen erfüllt sein:

- Die gesamte Kommunikation zwischen den beteiligten Netzen muss über das Sicherheitsgateway geführt werden. Dafür muss sichergestellt sein, dass das Sicherheitsgateway die einzige Schnittstelle zwischen den beiden Netzen darstellt. Es müssen Regelungen getroffen werden, dass keine weiteren externen Verbindungen unter Umgehung des Sicherheitsgateways geschaffen werden dürfen.
- Ein Sicherheitsgateway darf ausschließlich als schützender Übergang zum internen Netz eingesetzt werden. Daher dürfen auf einem Sicherheitsgateway selbst nur die dafür erforderlichen Dienste verfügbar sein und keine weiteren Dienste, wie z. B. ein Webserver, angeboten werden. Wie Informationsserver und andere Komponenten, die auf eigenen Systemen laufen, geeignet in ein Sicherheitsgateway integriert werden können, wird in einer Reihe eigener Maßnahmen für verschiedene Systeme beschrieben, siehe beispielsweise M 4.223 *Integration von Proxy-Servern in das Sicherheitsgateway* oder M 5.115 *Integration eines Webservers in ein Sicherheitsgateway*.
- Die Administration der Komponenten des Sicherheitsgateways darf nur über einen gesicherten Zugang möglich sein, also z. B. über eine gesicherte Konsole, eine verschlüsselte Verbindung oder ein separates Netz (Administrationsnetz). Eine Konsole sollte in einem Serverraum aufgestellt sein (siehe B 2.4 *Serverraum*).
- Ein Sicherheitsgateway baut auf Sicherheitsrichtlinie auf, die für das zu schützende Netz definiert wurde, und gestattet nur die dort festgelegten Verbindungen. Diese Verbindungen müssen gegebenenfalls sehr detailliert (bis hin zu einer individuellen Angabe von IP-Adresse, Dienst, Zeit, Richtung und Benutzer getrennt) festgelegt werden können.
- Für die Konzeption und den Betrieb eines Sicherheitsgateways muss geeignetes Personal zur Verfügung stehen. Der zeitliche Aufwand für den Betrieb eines Sicherheitsgateways darf nicht unterschätzt werden. Alleine die Auswertung der angefallenen Protokolldaten nimmt oft viel Zeit in Anspruch. Der Administrator muss fundierte Kenntnisse der eingesetzten IT-Komponenten besitzen und entsprechend geschult werden.

- Die Benutzer des lokalen Netzes sollten durch den Einsatz eines Sicherheitsgateways möglichst wenig Einschränkungen hinnehmen müssen.

Sicherheitsgateways haben auch Grenzen

Ein Sicherheitsgateway kann das interne Netz vor vielen Gefahren beim Anschluss an das Internet schützen, aber nicht vor allen. Beim Aufbau eines Sicherheitsgateways und der Erarbeitung einer Sicherheitsrichtlinie sollte man sich daher die Grenzen eines Sicherheitsgateways verdeutlichen:

- Es werden Protokolle überprüft, nicht die übertragenen Informationen. Eine Protokollprüfung bestätigt beispielsweise, dass eine E-Mail mit ordnungsgemäßen Befehlen zugestellt wurde, kann aber keine Aussagen zum eigentlichen Inhalt der E-Mail machen.
- Die Filterung von aktiven Inhalten ist unter Umständen nur teilweise erfolgreich, da eventuell nicht alle verschiedenen Möglichkeiten zur Einbettung von aktiven Inhalten erkannt werden.
- Sobald ein Benutzer eine Kommunikation über ein Sicherheitsgateway herstellen darf, kann er über das verwendete Kommunikationsprotokoll beliebige andere Protokolle tunneln. Damit könnte ein Innentäter einem Externen den Zugriff auf interne Rechner ermöglichen oder selbst unerlaubte Protokolle nutzen. Die unberechtigte Nutzung von Tunnel-Verfahren ist meist nur schwer feststellbar.
- Eine Einschränkung der Internet-Zugriffe auf festgelegte Webserver ist praktisch unmöglich, da viele Webserver auch über Proxies nutzbar sind. Daher kann eine Sperrung bestimmter IP-Adressen leicht umgangen werden.
- Software zum Filtern anhand von Web-Adressen ("URLs") ist häufig noch unausgereift. Beispielweise ist es möglich, dass nicht alle Arten der Adressierung erfasst werden. Das folgende Beispiel mit dem BSI-Webserver soll aufzeigen, welche Möglichkeiten zur Adressierung vorhanden sind. Die Liste ist bei weitem nicht vollständig, da einzelne Buchstaben auch durch Escape-Sequenzen dargestellt werden können.

  www.bsi.bund.de

  www.bsi.de

  194.95.176.226

  3261051106

  Zudem können URL-Filter durch Nutzung von "Anonymizern" umgangen werden.
- Die Filterung von Spam-Mails ist noch nicht ausgereift. Kein SMTP-Proxy kann zweifelsfrei feststellen, ob eine E-Mail vom Empfänger erwünscht ist oder nicht. Spam-Mails dürften frühestens dann verschwinden, wenn die Absender von E-Mails zweifelsfrei nachweisbar sind. Dies ist aber mit dem herkömmlichen Protokoll SMTP alleine nicht realisierbar.
- Sicherheitsgateways schützen nicht vor allen Denial-of-Service-Angriffen. Wenn ein Angreifer z. B. die Anbindung zum Provider lahmlegt, hilft auch das beste Sicherheitsgateway nicht. Außerdem gibt es immer wieder Fehler

in der Implementierung von Protokollen auf Endgeräten, die von Sicherheitsproxies nicht abfangen werden können.

- Ein Sicherheitsgateway kann zwar einen Netzübergang sichern, er hat aber keinen Einfluss auf die Sicherheit der Kommunikation innerhalb der Netze!
- Auch die speziell unter Sicherheitsaspekten entwickelten Komponenten von Sicherheitsgateways können trotz großer Sorgfalt Programmierfehler enthalten.
- Sicherheitsgateways können nur begrenzt gegen eine absichtliche oder versehentliche Fehlkonfiguration der zu schützenden Clients und Server schützen.
- Eingebaute Hintertüren in der verwendeten Software können eventuell auch durch ein Sicherheitsgateway hindurch ausgenutzt werden. Im Extremfall kann die Software des Sicherheitsgateways selbst Hintertüren enthalten.
- Die korrekte Konfiguration der Komponenten des Sicherheitsgateways ist oft sehr anspruchsvoll. Fehler in der Konfiguration können zu Sicherheitslücken oder Ausfällen führen.
- Ist die Dokumentation der technischen Ausstattung des Sicherheitsgateways durch den Hersteller mangelhaft, so begünstigt dies Fehler bei Konfiguration und Administration.
- Wenn die Komponenten des Sicherheitsgateways falsch dimensioniert sind, kann die Verfügbarkeit beeinträchtigt werden. Wird beispielsweise der Rechner, auf dem ein HTTP-Sicherheitsproxy läuft, zu schwach dimensioniert (zu wenig Arbeitsspeicher, zu langsamer Prozessor), so kann dies die Geschwindigkeit des Internetzugriffes stark beeinträchtigen.
- Es kann nicht verhindert werden, dass Angreifer die Komponenten des Sicherheitsgateways mit Hilfe von Schwachstellenscannern analysieren.
- Ein Sicherheitsgateway kann nicht gegen die bewusste oder unbewusste Missachtung von Sicherheitsrichtlinien und -konzepten durch die Anwender schützen.
- Ein Sicherheitsgateway schützt nicht vor dem Missbrauch freigegebener Kommunikation durch Innentäter ("Insider-Angriffe").
- Ein Sicherheitsgateway schützt nicht vor Social Engineering.
- Werden mobile Endgeräte (Laptop, PDA etc.), die von Mitarbeitern auch extern benutzt werden, an das interne Netz angeschlossen, so kann auf diese Weise Schadsoftware (Viren, Würmer, Trojaner) in das vertrauenswürdige Netz eingeschleppt werden.
- Ein Sicherheitsgateway schützt auch nicht davor, dass Schadprogramme auf Austauschmedien, z. B. CD-ROM, Diskette, USB-Stick in das vertrauenswürdige Netz eingeschleppt werden.

Ergänzende Kontrollfragen:

- Sind die Sicherheitsziele für das Sicherheitsgateway dokumentiert?
- Ist die Sicherheitsrichtlinie für das Sicherheitsgateway mit der allgemeinen Sicherheitsstrategie abgestimmt?

M 2.71 Festlegung einer Policy für ein Sicherheitsgateway

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Die Policy des Sicherheitsgateways bestimmt das Verhalten des Sicherheitsgateways. Sie definiert, welche Informationen, Dienste und Protokolle das Sicherheitsgateway wie behandelt und wer sie nutzen darf. Die Policy ist nicht zu verwechseln mit der Sicherheitsrichtlinie für das Sicherheitsgateway, in der Vorgaben für den sicheren Betrieb des Sicherheitsgateway selbst gemacht werden.

Kommunikationsanforderungen

Für die Erstellung einer Policy muss als erstes festgelegt werden, welche Arten der Kommunikation mit dem äußeren Netz zugelassen werden. Bei der Festlegung der Kommunikationsanforderungen müssen speziell die folgenden Fragen beantwortet werden:

- Welche Informationen dürfen durch das Sicherheitsgateway nach außen hindurch- bzw. nach innen hereingelassen werden?
- Welche Informationen soll das Sicherheitsgateway verdecken (z. B. die interne Netzstruktur oder die Benutzernamen)?
- Welche Authentisierungsverfahren sollen innerhalb des zu schützenden Netzes bzw. für das Sicherheitsgateway benutzt werden (z. B. Einmalpasswörter oder Chipkarten)?
- Welche Zugänge werden benötigt (z. B. nur über einen Internet-Service-Provider oder auch über einen Modem-Pool)?
- Welcher Datendurchsatz ist zu erwarten?

Auswahl der Dienste

Aus den Kommunikationsanforderungen wird dann abgeleitet, welche Dienste im zu sichernden Netz erlaubt werden.

Es muss unterschieden werden zwischen denjenigen Diensten, die für die Benutzer im zu schützenden Netz und denjenigen, die für externe Benutzer zugelassen werden.

Wenn zum Beispiel E-Mail empfangen werden soll (was im allgemeinen die Minimalanforderung ist) muss das Protokoll SMTP vom Sicherheitsgateway durchgelassen werden können.

In der Policy muss explizit festgelegt werden, welche Dienste für welche Benutzer und/oder Rechner zugelassen werden sollen und für welche Dienste Vertraulichkeit und/oder Integrität gewährleistet werden müssen. Es sollten nur die Dienste zugelassen werden, die unbedingt notwendig sind. Alle anderen Dienste müssen verboten werden. Dies muss auch die Voreinstellung sein: Alle Dienste, für die noch keine expliziten Regeln festgelegt wurden, dürfen nicht zugelassen werden.

Für jeden erlaubten Dienst muss festgelegt werden, welche Funktionen des verwendeten Protokolls genutzt werden dürfen und welche unterbunden

werden sollen (z. B. der "PORT"-Befehl von FTP zur Verhinderung von aktivem FTP) und welche der übertragenen Nutzdaten gefiltert werden sollen (z. B. zur Kontrolle auf Computer-Viren).

Es muss festgelegt werden, zu welchen Wochentagen und Tageszeiten die bereitgestellten Dienste genutzt werden können.

Für kurzzeitige Änderungen (z. B. für Tests) oder neue Dienste sollten Ausnahmeregelungen vorgesehen werden.

Es sind Forderungen an die Filter zu stellen, und zwar einmal an die Paketfilter, die die Header-Informationen der Dienste der Schichten 3 und 4 des OSI-Schichtenmodells (IP, ICMP, ARP, TCP und UDP) verwenden, sowie an die Sicherheitsproxies, die die Informationen der Dienste der Anwendungsschicht (z. B. Telnet, FTP, SMTP, DNS, NNTP, HTTP) verwenden. Einen Überblick, was für einen sicheren Einsatz der einzelnen Protokolle und Dienste zu beachten ist, gibt M 5.39 *Sicherer Einsatz der Protokolle und Dienste*. Darauf aufbauend müssen Filterregeln formuliert werden (siehe M 2.76 *Auswahl und Einrichtung geeigneter Filterregeln*).

Organisatorische Regelungen

Neben der sorgfältigen Aufstellung und Umsetzung der Filterregeln sind darüber hinaus folgende organisatorische Regelungen erforderlich:

- Es müssen Verantwortliche sowohl für den Entwurf als auch für die Umsetzung und das Testen der Filterregeln benannt werden. Es muss geklärt werden, wer befugt ist, die Filterregeln z. B. für Tests neuer Dienste zu verändern.
- Es muss festgelegt werden, welche Informationen protokolliert werden und wer die Protokolle auswertet. Es müssen sowohl alle korrekt aufgebauten als auch die abgewiesenen Verbindungen protokolliert werden. Die Protokollierung muss den datenschutzrechtlichen Bestimmungen entsprechen.
- Die Benutzer müssen über ihre Rechte, insbesondere auch über den Umfang der Nutzdaten-Filterung umfassend informiert werden.
- Es ist empfehlenswert, den Benutzern eine Dokumentation zur Verfügung zu stellen, aus der hervorgeht, welche Dienste in welchem Umfang genutzt werden können und ob dabei besondere Dinge zu beachten sind.
- Angriffe auf das Sicherheitsgateway sollten nicht nur erfolgreich verhindert, sondern auch schnell erkannt werden können. Angriffe können über die Auswertung der Protokolldateien erkannt werden. Das Sicherheitsgateway sollte aber auch in der Lage sein, aufgrund von vordefinierten Ereignissen, wie z. B. häufigen fehlerhaften Passworteingaben auf einem Application-Level-Gateway oder Versuchen, verbotene Verbindungen aufzubauen, Warnungen auszugeben oder evtl. sogar Aktionen auszulösen.
- Es ist zu klären, welche Aktionen bei einem Angriff gestartet werden, ob z. B. der Angreifer verfolgt werden soll oder ob die Netzverbindungen nach außen getrennt werden sollen. Da hiermit starke Eingriffe in den Netzbetrieb verbunden sein können, müssen Verantwortliche bestimmt sein, die entscheiden können, ob ein Angriff vorliegt und die entsprechende

Maßnahmen einleiten. Die Aufgaben und Kompetenzen für die betroffenen Personen und Funktionen müssen eindeutig festgelegt sein.

Folgende Fragen müssen bei der Festlegung der Policy geklärt werden:

- Welcher Schaden kann im zu schützenden Netz verursacht werden, wenn das Sicherheitsgateway überwunden wird? Da es keine absolute Sicherheit geben kann, muss entschieden werden, ob der maximal auftretende Schaden tragbar ist oder ob zusätzliche Maßnahmen ergriffen werden müssen.
- Welche Restrisiken existieren bei einem ordnungsgemäßen Betrieb des Sicherheitsgateways? Dies sind z. B. Schwachstellen in den benutzten Geräten und Betriebssystemen.
- Wie schnell wird ein Angriff auf das Sicherheitsgateway bemerkt?
- Welche Protokoll-Informationen sind auch nach einem erfolgreichen Angriff noch verfügbar?
- Sind die Benutzer bereit, die Einschränkungen durch das Sicherheitsgateway zu akzeptieren?

Entscheidungen und Gründe dokumentieren

In der Policy müssen die getroffenen Entscheidungen dokumentiert werden. Darüber hinaus ist es wichtig, dass auch die für die Entscheidungen relevanten Informationen und Entscheidungsgründe so dokumentiert sind, dass sie zu einem späteren Zeitpunkt (etwa bei der Revision der Policy) nachvollzogen werden können. Diese Hintergrundinformationen brauchen nicht direkt in der Policy selbst enthalten zu sein, sondern es ist eher empfehlenswert, sie in einem eigenen Dokument festzuhalten.

Ergänzende Kontrollfragen:

- Welche Protokolle und Dienste sollen über das Sicherheitsgateway genutzt werden?
- Ist dokumentiert, nach welchen Kriterien die zu nutzenden Dienste ausgewählt wurden?
- Sind die Zuständigkeiten für den Betrieb und die Überwachung des Sicherheitsgateways geregelt?

M 2.72 Anforderungen an eine Firewall

Die Maßnahme ist mit Version November 2004 entfallen.

M 2.73 Auswahl geeigneter Grundstrukturen für Sicherheitsgateways

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Nachdem eine Sicherheitsrichtlinie für das Sicherheitsgateway festgelegt worden ist, muss entschieden werden, mit welchen Komponenten das Sicherheitsgateway realisiert werden soll. Dafür ist eine geeignete Anordnung auszuwählen.

Grundlegende Strukturen von Sicherheitsgateways

Im Wesentlichen bieten sich zwei sinnvolle Grundstrukturen an, die als Anhaltspunkt zum Aufbau eines Sicherheitsgateways dienen können. Die grundlegenden Strukturen werden im Folgenden erläutert.

1. Paketfilter - Application-Level-Gateway - Paketfilter (P-A-P)

Bei dieser Grundstruktur werden ein Paketfilter, ein Application-Level-Gateway (ALG) und ein weiterer Paketfilter "hintereinander geschaltet", so dass jeglicher Datenverkehr alle drei Komponenten überqueren muss. In der folgenden Abbildung sind beispielhaft einige Möglichkeiten zur Einrichtung von "Demilitarisierten Zonen" (DMZ) eingezeichnet, in denen weitere Komponenten des Sicherheitsgateways in einer geschützten Umgebung betrieben werden können.

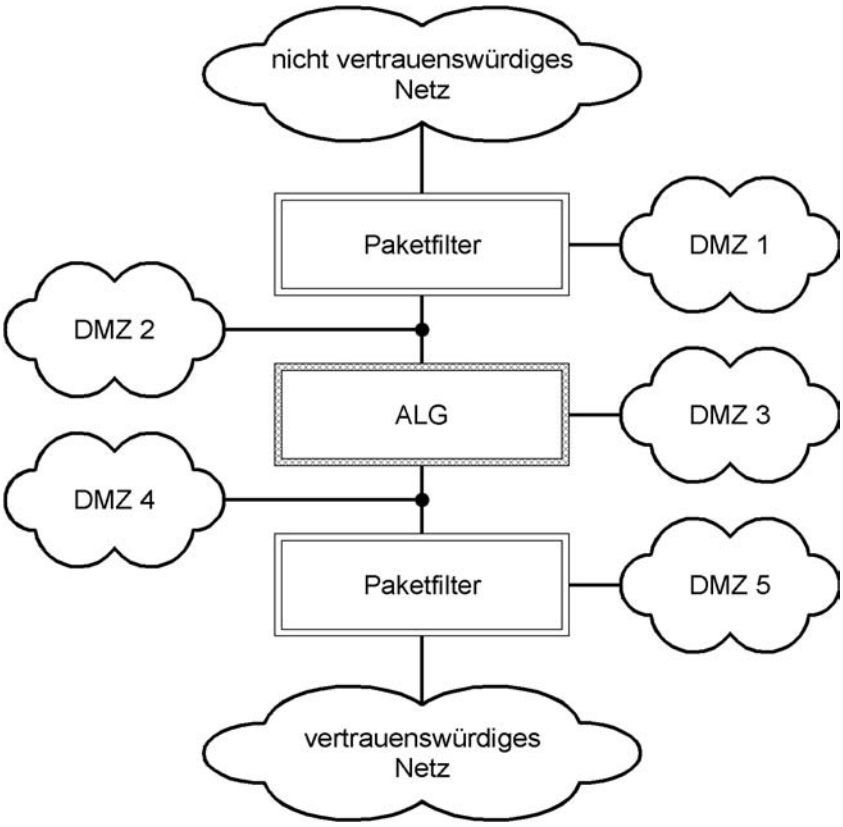


Abbildung 1: Mehrstufiger Aufbau bestehend aus Paketfilter - ALG - Paketfilter

Der Einsatzbereich für diesen Typ von Sicherheitsgateways ist vor allem die Trennung zweier Netze, falls sich das Maß der Vertrauenswürdigkeit dieser Netze erheblich unterscheidet (z. B. Trennung des Internets von einem Intranet), oder Trennung zweier Teilnetze des internen Netzes mit deutlich unterschiedlichen Sicherheitsanforderungen.

Bei den beiden Paketfiltern braucht es sich nicht notwendigerweise um dedizierte IT-Systeme (Rechner oder Appliances) zu handeln. Falls die eingesetzten Router eine integrierte Paketfilter-Funktionalität besitzen, so können die Router die Funktion des Paketfilters im Sicherheitsgateway mit übernehmen.

Die Möglichkeiten der Paketfilter-Funktionalität in Routern sind jedoch oft eingeschränkt, so dass in bestimmten Einsatzszenarien ein dedizierter Paketfilter erforderlich sein kann.

2. Nur Paketfilter

Die einfachste Grundstruktur eines Sicherheitsgateways besteht ausschließlich aus einem Paketfilter.

Das Grundproblem bei der Filterung der Kommunikation alleine mit einem Paketfilter liegt darin, dass die Entscheidung darüber, ob ein Zugriff erlaubt oder abgewiesen werden soll, anhand der leicht zu fälschenden Daten aus den Headern der verschiedenen IP-basierten Protokolle gefällt wird.

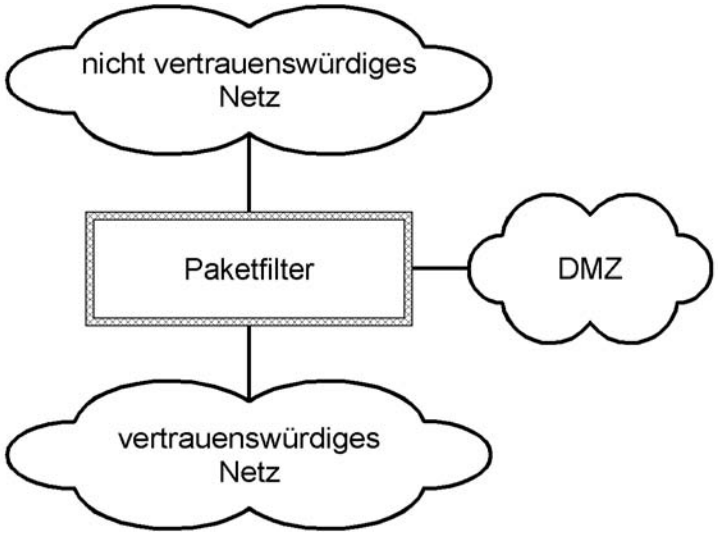


Abbildung 2: Einstufiger Aufbau bestehend aus einem Paketfilter.

Einsatzbereiche sind deshalb vor allem:

1. Trennung zweier Netze, falls sich das Maß der Vertrauenswürdigkeit dieser Netze nur wenig voneinander unterscheidet (z. B. Trennung des Internets von einem Intranet mit nur geringem Schutzbedarf).
2. Trennung zweier organisationsinterner Netze.
3. Privater Bereich (Schutz des "heimischen" Rechners beim Zugriff auf das Internet)

Die Verwendung eines zusätzlichen IP-Proxys kann verhindern, dass Informationen des IP-Headers, wie beispielsweise die IP-ID oder die TTL ("Time-To-Live"), das vertrauenswürdige Netz verlassen. Mittels der IP-ID kann trotz NAT-Funktion die Anzahl der Rechner in einem vertrauenswürdigen Netz bestimmt werden und die TTL lässt Rückschlüsse auf verwendete Betriebssysteme zu. Über Paketfilterregeln oder entsprechendes Routing muss sichergestellt werden, dass der IP-Proxy nicht umgangen werden kann.

Vor- und Nachteile der Grundstrukturen

Prinzipiell ist der oben dargestellte P-A-P-Aufbau zur Erzielung eines hohen Sicherheitsniveaus in allen Anwendungszusammenhängen zu empfehlen. Wird auf Komponenten dieses Aufbaus verzichtet, so ist dies stets mit Sicherheitseinbußen verbunden.

In der folgenden Tabelle werden Vor- und Nachteile bzw. Einsatzumgebungen sowohl für den P-A-P-Aufbau, als auch für einen einzelnen Paketfilter beschrieben.

Paketfilter - ALG - Paketfilter (P-A-P)	**Paketfilter**
- Kann als Grundlage Sicherstellung eines hohen Sicherheitsniveau dienen. - Hohe Komplexität aufgrund der Verwendung mehrerer Module. - Nicht in jedem Anwendungszusammenhang einsetzbar. Beispielsweise kann IPSEC-Verkehr nicht über einen TCP/IP-Proxy geleitet werden. - Einfache Erweiterungsmöglichkeiten, z. B. kann ein Virenscanner oder ein Spam-Filter ohne großen Aufwand an das ALG angeschlossen werden. - Die Ausnutzung von Sicherheitslücken in Client-Software kann teilweise verhindert werden. - Umfangreiche Protokollierungsmöglichkeiten.	- Kein hohes Sicherheitsniveau, höchstens für normalen Schutzbedarf ausreichend. - Gegenüber einem P-A-P-Aufbau relativ einfache Administration. - Geringe Investitionskosten (kostenlose Software unter verschiedenen Betriebssystemen vorhanden). - Keine wesentliche Einschränkung des maximalen Datendurchsatzes am Netzübergang. - Einfache, grundlegende Absicherung. - Integration auf einem zu schützenden Rechner theoretisch möglich (z. B. kann ein Web-Server gleichzeitig als Paketfilter genutzt werden). Bereitstellung neuer Dienste gegenüber P-A-P-Aufbau stark vereinfacht.

Tabelle 1: Vor- und Nachteile des P-A-P Aufbaus und von Paketfiltern

Auf dem Application-Level-Gateway laufen so genannte Proxy-Prozesse (oft auch Proxy-Server genannt), die den Verbindungsaufbau zum Zielrechner durchführen, nachdem eine Authentisierung des Benutzers stattgefunden hat, und die Daten gemäß den Informationen der Anwendungsschicht filtern. Verbindungen, für die keine Proxy-Prozesse existieren, sind nicht möglich.

Rechner, auf denen einzelne Komponenten des Sicherheitsgateways realisiert werden, müssen so eingerichtet werden, dass nur die unbedingt notwendigen Programme auf ihnen laufen (Minimalsystem). Die eingesetzten Programme müssen richtig konfiguriert sind und alle bekannten Schwachstellen müssen beseitigt werden.

Werden zur Erzielung eines hohen Sicherheitsniveaus mehrere Systeme hintereinander geschaltet, so ist es dringend zu empfehlen, diese Systeme auf verschiedenen Systemen zu realisieren (z. B. mit unterschiedlichen Betriebssystemen). Dadurch wird verhindert, dass ein Angreifer das Sicherheitsgateway besonders leicht überwinden kann, indem er auf allen beteiligten Systemen die gleiche Sicherheitslücke ausnutzt.

Hinweise zur Auswahl einer Grundstruktur

Die Frage, welcher Typ eines Sicherheitsgateways eingesetzt werden soll, ist einerseits davon abhängig, wie groß der Unterschied der Vertrauenswürdigkeit der zu trennenden Netze ist (d. h. "wie wenig vertrauenswürdig" das nicht-vertrauenswürdige Netz ist), und andererseits davon, wie hoch der Schutzbedarf des Netzes ist, das durch das Sicherheitsgateway geschützt werden soll.

Sonderfall Internet

Das Internet ist in diesem Zusammenhang das am wenigsten vertrauenswürdige Netz. Soll das eigene Netz mit dem Internet verbunden werden, so sollte grundsätzlich der mehrstufige P-A-P-Aufbau gewählt werden. Nur in Ausnahmefällen kann davon abgewichen werden, beispielsweise bei sehr kleinen Netzen, bei denen ein mehrstufiges Sicherheitsgateway einen unverhältnismäßig hohen Aufwand bedeuten würde, oder wenn das eigene Netz nur einen geringen Schutzbedarf hat. Auch in solchen Fällen muss jedoch mindestens ein Paketfilter eingesetzt werden, der besonders sorgfältig zu konfigurieren ist.

Falls das weniger vertrauenswürdige Netz "nur in geringem Maße nicht-vertrauenswürdig" ist, brauchen die Netze nicht durch ein mehrstufiges Sicherheitsgateway getrennt zu werden. In diesem Fall ist ein sorgfältig konfigurierter Paketfilter meist ausreichend.

Nur in geringem Maße nicht-vertrauenswürdige Netze können beispielsweise folgende Netztypen darstellen:

- andere (organisations-) interne Netze
- Netze ohne Verbindung zum Internet
- Netze mit Verbindung zum Internet, die ihrerseits durch besondere Sicherheitsmaßnahmen (z. B. durch ein eigenes Sicherheitsgateway) vom Internet abgeschottet sind

Folgende Tabelle fasst die Empfehlungen zusammen:

Einsatzgebiet	**Empfohlener Aufbau**
Trennung zweier Teilnetze des internen Netzes mit gleichem Schutzbedarf	Paketfilter. Bei normalem Schutzbedarf genügt ein Router mit integrierter Paketfilter-Funktion.
Trennung zweier Teilnetze des internen Netzes mit unterschiedlichem Schutzbedarf (insbesondere: Teilnetz mit hohem Schutzbedarf und Teilnetz mit normalem Schutzbedarf)	Mindestens Paketfilter. Falls vom weniger vertrauenswürdigen Netz aus auf einen Dienst im Netz mit hohem Schutzbedarf zugegriffen werden soll, dann ist es empfehlenswert, diesen Zugriff über ein ALG abzusichern.
Trennung eines Teilnetzes mit besonderen Sicherheitsanforderungen von einem anderen internen Netz	Mehrstufiger Aufbau aus Paketfilter - ALG - Paketfilter. Zusätzlich ist in diesem Fall eine ergänzende Sicherheitsbetrachtung notwendig. Der mehrstufige Aufbau kann hier nur als Grundlage für sehr hohe Sicherheit dienen. In der Regel werden zusätzliche Maßnahmen notwendig sein, für die aber keine allgemeinen Empfehlungen möglich sind.
Trennung des eigenen Netzes vom Internet	Grundsätzlich mehrstufiger Aufbau aus Paketfilter - ALG - Paketfilter. In Ausnahmefällen (sehr kleines Netz, kein hoher Schutzbedarf) kann ein Paketfilter (beispielsweise in Verbindung mit einem NAT-Router) ausreichend sein. Zumindest für Dienste wie E-Mail und HTTP wird der Einsatz eines entsprechenden Proxyservers dringend empfohlen. Bei normalem Schutzbedarf kann gegebenenfalls auf den inneren Paketfilter verzichtet werden. Falls kein P-A-P-Aufbau gewählt wird, wird eine zusätzliche Risikobetrachtung dringend empfohlen.

Tabelle 2: Empfehlungen für Grundstrukturen

Andere Strukturen

Neben den bisher beschriebenen Strukturen sind weitere Strukturen möglich, die meist aus einem Verzicht auf Komponenten des P-A-P-Aufbaus resultieren. Dies ist jedoch immer mit Einbußen bei der Sicherheit verbunden.

Verzicht auf Paketfilter ist nicht sinnvoll

Gelegentlich wird beispielsweise auf den "inneren" Paketfilter verzichtet, der das ALG vom vertrauenswürdigen (bzw. internen) Netz trennt. Da einerseits die meisten Router bereits eine integrierte Paketfilter-Funktionalität bieten und angesichts der vergleichsweise geringen Kosten für einen entsprechend ausgestatteten Rechner gibt es jedoch kaum schlüssige Gründe, auf einen der Paketfilter zu verzichten.

Appliances

Verschiedene Hersteller bieten Sicherheitsgateways als Appliances an. Dabei handelt es sich um vorkonfigurierte Geräte, die zwar teilweise aus normalen Rechner-Komponenten aufgebaut sind und unter einem darauf angepassten herkömmlichen Betriebssystem laufen, aber nur für einen genau vorgegebenen Einsatzzweck (hier: Paketfilter bzw. ALG) hergestellt und konfiguriert wurden. Die Bandbreite der angebotenen Geräte reicht von reinen Paketfiltern bis zu mehrstufigen Lösungen, die in einem Gerät mehrere Komponenten eines Sicherheitsgateway integrieren.

Gegenüber einem Aufbau des Sicherheitsgateways aus "normalen" Rechnern, die (in Eigenregie oder durch einen Dienstleister) entsprechend konfiguriert werden, bieten Appliances oft den Vorteil einer einfacheren Konfiguration. Dem steht jedoch meist der Nachteil gegenüber, dass die Konfiguration weniger flexibel ist und weniger Möglichkeiten zur Anpassung an individuelle Bedürfnisse bietet.

Appliances, die mehrere Funktionen (z. B. Paketfilter und ALG) unter einer Betriebssysteminstallation betreiben, haben gegenüber einer Realisierung des Sicherheitsgateways durch drei getrennte Systeme den weiteren Nachteil, dass ein Angreifer nur die Sicherheitsmechanismen eines einzigen Betriebssystems überwinden muss, um das Sicherheitsgateway komplett zu kompromittieren. Dieser Aspekt muss bei der Planung des Sicherheitsgateways mit berücksichtigt werden. Soll trotzdem ein entsprechendes Gerät eingesetzt werden, so können gegebenenfalls zusätzliche Sicherheitsmaßnahmen erforderlich werden, um das angestrebte Sicherheitsniveau zu erreichen.

Dokumentation

Die Entscheidung für eine bestimmte Struktur sollte zusammen mit den Gründen, die für die Entscheidung ausschlaggebend waren, nachvollziehbar dokumentiert werden.

Ergänzende Kontrollfragen:

- Welche Struktur wurde für das Sicherheitsgateway ausgewählt? Sind die Entscheidungsgründe dokumentiert?

M 2.74 Geeignete Auswahl eines Paketfilters

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Funktionen eines Sicherheitsgateways auf Transport- und Netzwerkebene werden von den so genannten Paketfiltern übernommen. Aufgabe eines Paketfilters ist es, Datenpakete anhand der Informationen in den Header-Daten der UDP/IP- bzw. TCP/IP-Schicht (z. B. IP-Adresse und Portnummer) zu verarbeiten. Diese Entscheidung trifft der Paketfilter anhand den vom Administrator vorgegebenen Filterregeln. Vielfach bieten die Paketfilter auch eine Möglichkeit zur "Network Address Translation" (NAT), bei der die Absender-Adressen von IP-Paketen durch eine IP-Adresse des Paketfilters ersetzt wird. Dadurch wird die Netzstruktur des zu schützenden Netzes verdeckt.

Die Filterregeln werden für jedes eintreffende Datenpaket sequentiell abgearbeitet. Sobald eine Regel auf ein Paket zutrifft, bricht in der Regel die Überprüfung ab und die betreffende Regel wird auf dieses Paket angewendet.

Paketfilter lassen sich anhand der Filtermöglichkeiten weiter unterteilen.

Statische Paketfilter

Paketfilter, die eine Entscheidung anhand der Header-Daten der UDP/IP- und TCP/IP-Schichten (z. B. anhand der IP-Quelladresse, der IP-Zieladresse und der TCP-Flags) treffen, werden statische Paketfilter genannt.

Dynamische Paketfilter/Stateful Inspection

Dynamische Paketfilter (oder auch Paketfilter mit "Stateful Inspection" genannt) erweitern die Funktionalität der statischen Paketfilter um die Möglichkeit zur Betrachtung des Kommunikationkontextes. Dynamische Paketfilter können auch bei verbindungslosen Protokollen (wie z. B. UDP) eine Entscheidung treffen, ob ein eintreffendes Paket die Antwort auf eine Anfrage ist oder ob dieses Paket zu einer Kommunikationsinitiierung gehört. Zudem ist es möglich, Dienste sicher bereitzustellen, die nicht mit festen Portnummern verbunden sind, da auch hier Pakete unabhängig von Portnummern immer dann weitergeleitet werden, wenn es vorher eine passende Anfrage aus dem vertrauenswürdigen Netz gab.

Ein dynamischer Paketfilter speichert für eine bestimmte Zeitspanne die Quell-IP-Adresse und die Quell-Portnummer ausgehender Pakete. Eintreffende IP-Pakete werden nur dann weitergeleitet, wenn deren Ziel-IP-Adresse und Ziel-Portnummern noch im Speicher vorhanden sind, das heißt, wenn vorher eine Anfrage vom vertrauenswürdigen Netz aus gestartet wurde und die festgelegte Wartezeit noch nicht überschritten wurde.

Paketfilter mit Stateful Inspection stellen zudem meist die Möglichkeit zur Betrachtung der übertragenen Daten auf der Anwendungsebene bereit.

Realisierungsformen von Paketfiltern

1. Einrichtung eines Rechners als Paketfilter unter Nutzung eines Betriebssystems, das die notwendigen Funktionalitäten bereitstellt

Vorteile	Nachteile
Je nach verwendetem Betriebssystem relativ geringe Investitionskosten.	- Evtl. lange Ausfallzeiten bei Defekten, da u. U. das Betriebssystem aufgrund ausgetauschter Hardware neu installiert oder konfiguriert werden muss. - Relativ hoher Aufwand zur Konfiguration als Minimalsystem (im Vergleich zu einem Router mit Paketfilterfunktion). - Know-How-Aufbau notwendig zur Konfiguration als Minimalsystem. - Die Hardware von PC-Systemen ist oft anfälliger als die Hardware von Appliances, da letztere z. B. meist keine Festplatten oder Lüfter enthalten. - Die Administrationskosten sind in der Regel höher als bei Appliances, da Konfigurationsoberflächen meist nicht zur Verfügung stehen. - Die Komplexität ist oft höher als bei Appliances.

Tabelle 1: Einrichten eines Rechners als Paketfilter

2. Einrichtung von Filterregeln auf einem Router

Vorteile	Nachteile
- Keine Investitionskosten, falls ein Router schon vorhanden ist. - Im Vergleich zu rechnerbasierten Paketfiltern besteht eine geringe Ausfallwahrscheinlichkeit, da Router in der Regel eine bessere Verfügbarkeit aufweisen.	- Die Erweiterungsmöglichkeiten von Routern sind oft eingeschränkt. - Die Konfiguration ist evtl. schwieriger als bei Appliances oder rechnerbasierten Paketfiltern. - Keine Kontrolle über die Sicherheitsfunktionen des Routers durch organisationsinternes Personal, falls dieser bei einem Dienstleister aufgestellt ist und von diesem administriert wird.

Tabelle 2: Vor- und Nachteile der Einrichtung von Filterregeln auf einem Router

3. Verwendung einer Appliance

Vorteile	Nachteile
- Geringer Zeitaufwand nötig bis zur Inbetriebnahme. - Vereinfachte Konfiguration der bereitgestellten Funktionen (ggf. über Web-Oberfläche) - Einfache Konfiguration, da Appliances oft Administrationsoberflächen anbieten. - Appliances unterstützen oft automatische Updates. - Im Vergleich zu rechnerbasierten Paketfiltern eher geringere Ausfallwahrscheinlichkeit, da Appliances oft weniger "bewegliche Teile" enthalten (z. B. Festplatte oder Lüfter) als normale Rechner.	- Geringe Erweiterungsmöglichkeiten der proprietären Hard- und Software. - Lange Ausfallzeiten, falls das Gerät im Fehlerfalle oft zum Hersteller gesandt werden muss, falls keine entsprechenden Wartungsverträge geschlossen wurden. Gegebenenfalls muss deshalb ein Ersatzgerät beschafft werden, das als "Cold Standby" vorgehalten wird. - Wenig Informationen zur sicheren Konfiguration und zum sicheren Betrieb zu speziellen Produkten erhältlich (über die Informationen des Herstellers hinaus). Dies ist besonders dann problematisch, wenn der Hersteller den Support einstellt. - Bestimmte Appliances besitzen u. U. eine geringe Verbreitung. In diesem Fall existieren evtl. wenig Berater bzw. Dienstleister zur Administration.

Tabelle 3: Verwndung einer Appliance

Anforderungen an Paketfilter

Bei allen drei Realisierungsformen lässt sich gegebenenfalls die Paketfilterkonfiguration aus den Einstellungen eines eventuell vorhandenen ALGs automatisch ableiten. Dies besitzt zum einen den Vorteil des geringen Konfigurationsaufwandes, zum anderen den Nachteil der geringeren Sicherheit, da eine Fehlkonfiguration des ALGs automatisch eine Fehlkonfiguration des Paketfilters bewirkt.

Vor der Beschaffung sollte überprüft werden, welche der folgenden Anforderungen das ALG erfüllt. Je nach Anwendungszusammenhang kann dabei auf einige Anforderungen verzichtet werden, d. h. es muss eine Bewertung der aufgelisteten Anforderungen im Anwendungszusammenhang erfolgen.

Folgende Möglichkeiten sollten vom Paketfilter unterstützt werden:

1. Weiterleiten oder Verwerfen von Paketen anhand
   - der Quell-IP- und Ziel-IP-Adresse einzelner Rechner oder Netze
   - des Quell- und Zielports
   - des ICMP-Typs
   - aller TCP-Flags (URG, ACK, PSH, RST, SYN, FIN). Mit Hilfe des ACK-Bits kann beispielsweise zwischen Paketen zum Verbindungsaufbau und Paketen im Rahmen einer etablierten Verbindung unterschieden werden. Durch Kontrolle der anderen Bits können IP-Pakete mit unsinnigen Kombinationen von TCP-Flags abgelehnt werden
   - der IP-Optionen.
2. Unterstützung der Aktionen
   - Weiterleiten des Pakets ("allow")
   - Verwerfen des Pakets ("deny & drop")
   - Verwerfen des Pakets und Meldung an den Absender ("deny & reject")
3. Erstellung von Filterregeln getrennt für jede Schnittstelle des Paketfilters
4. Getrennte Filterung kommender und gehender Pakete
5. Unveränderbare Festlegung der Reihenfolge zur Abarbeitung der Filterregeln
6. Protokollierung von IP-Adresse, Dienst, Zeit und Datum für jedes Paket, aber auch eingeschränkt auf bestimmte Pakete
7. Im Falle, dass ein Router als Paketfilter eingesetzt wird, muss das dynamische Routing so konfigurierbar sein, dass Routing-Pakete (z. B. RIP), die das zu schützende Netz betreffen, nur an dem Interface zugelassen werden, das auch mit dem zu schützenden Netz verbunden ist.
8. Schutz vor IP-Spoofing
9. Falls nur ein Paketfilter ohne ALG als Sicherheitsgateway eingesetzt wird, müssen zusätzlich folgende Funktionen unterstützt werden:
   - Port-Forwarding (auch oft "Destination NAT" genannt)
   - Network Address Translation (NAT). Auch Unterstützung für:
     - Ersetzen der IP-ID
     - Ersetzen der TTL
   - Stateful Inspection

Die Anforderungen an den Paketfilter und die Gründe, die für die getroffene Auswahl ausschlaggebend waren, sollten nachvollziehbar dokumentiert werden.

Ergänzende Kontrollfragen:

- Welche Anforderungen an den Paketfilter wurden festgelegt?
- Welche Formen von Paketfiltern (Rechner, Router, Appliance) werden eingesetzt? Sind die Gründe für die Auswahl dokumentiert?

M 2.75 Geeignete Auswahl eines Application-Level-Gateways

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Die Funktionen eines Sicherheitsgateways auf Anwendungsebene werden von den so genannten Application-Level-Gateways (ALG) übernommen. Implizit nehmen ALGs auch Funktionen auf den Schichten 1-3 wahr. ALGs werden oft auch Sicherheitsproxies genannt, im Folgenden wird aber abkürzend der Begriff "Proxy" verwendet. Proxies unterbrechen den direkten Datenstrom zwischen Quelle und Ziel. Bei einer Kommunikation zwischen Client und Server über einen Proxy hinweg nimmt der Proxy die Anfragen des Clients entgegen und leitet sie an den Server weiter. Bei einem Verbindungsaufbau in umgekehrter Richtung, also vom Server zum Client, verfährt der Proxy analog. Sämtliche Kommunikationsbeziehungen zwischen den beiden Rechnern verlaufen in diesem Fall also mittelbar über den Proxy.

Einige Vor- und Nachteile von Sicherheitsproxies werden in der folgenden Tabelle zusammengestellt:

Vorteile von Proxies

- Oft geringere Anzahl von Programmierfehlern als in den vom Proxy geschützten Client- bzw. Serverdienstprogrammen.
- Filterung einzelner Protokollbefehle (z. B. bei HTTP der Befehl POST) in Abhängigkeit von der Parametrisierung der Befehle, der Zeit und des Benutzer möglich.
- Entfernung unerwünschter Inhalte in den übertragenen Daten.
- Abwehr von Angriffen, die auf fehlerhaften Header-Daten beruhen.
- Ersetzung der Absender-Adresse eines weitergeleiteten IP-Pakets durch die IP-Adresse der Netzschnittstelle, über die das Paket den Proxy verlässt. Dadurch werden IP-Adressen des vertrauenswürdigen Netzes verheimlicht. Im DNS braucht zudem nur eine IP-Adresse eingetragen werden.
- Erzwingen einer starken Authentisierung möglich.
- Umfangreiche Protokollierungsmöglichkeiten. Für jede Verbindung auf der Anwendungsebene kann protokolliert werden:
  - Benutzeridentifikation
  - IP-Adresse des Quell- und Zielrechners
  - Portnummern
  - Zeit und Datum

In Abhängigkeit vom Dienst können weitergehende Informationen protokolliert werden (z. B. URL bei HTTP).

Nachteile von Proxies

- Verringerung des maximalen Datendurchsatzes.
- Längere Antwortzeiten (Latenzzeiten) beim Abruf von Informationen.

Eventuell Einschränkung der Funktionalität der Clientprogramme (z. B. durch Filterung aktiver Inhalte

Transparente und nicht-transparente Proxies

Proxies können in zwei verschiedenen Betriebarten arbeiten, dem sogenannten transparenten und dem nicht-transparentem Modus. Ein transparenter Proxy braucht den Clients nicht mitgeteilt zu werden. Er liest alle im Netz befindlichen IP-Pakete mit und entscheidet anhand von IP-Adresse und Portnummer, welche davon in ein anderes Netz weitergeleitet werden sollen. Bei Verwendung eines nicht-transparenten Proxies hingegen muss dessen IP-Adresse und Portnummer in der Client-Software (z. B. dem Webbrowser) eingetragen werden, um eine Verbindung über den Proxy hinweg zu ermöglichen.

Vor der Beschaffung sollte überprüft werden, welche der folgenden Anforderungen das ALG erfüllt. Je nach Anwendungszusammenhang kann dabei auf einige Anforderungen verzichtet werden.

Die aufgelisteten Anforderungen müssen im Anwendungszusammenhang bewertet werden. Wenn ein bestimmtes Protokoll nicht genutzt wird, braucht das ALG keine Unterstützung für das Protokoll zu bieten. Unterstützt das ALG Protokolle, die nicht genutzt werden, so sollte die Möglichkeit bestehen, das betreffende Protokoll zu deaktivieren.

Wurde für einige der im folgenden aufgeführten Protokolle in der Policy des Sicherheitsgateway festgelegt, dass sie nicht erlaubt sein sollen, so brauchen Sie natürlich auch nicht unterstützt zu werden.

Die die Kriterien der Bewertung und die getroffenen Entscheidungen müssen nachvollziehbar dokumentiert werden.

Allgemein

1. Unterstützung der wichtigsten verwendeten Protokolle (beispielsweise Telnet, FTP, SMTP, NNTP, HTTP und HTTPS) auf Anwendungsschicht. Für die Nutzung anderer Dienste sollten generische Proxies für TCP- und UDP vorhanden sein.
2. Die Proxies des Application-Level-Gateways sollten transparent betrieben werden können.
3. Es sollte ein eigener MTA auf dem ALG integriert werden können, um gegebenenfalls mehrere MTAs in verschiedenen vertrauenswürdigen Netzen bedienen zu können.
4. Es sollte eine Schnittstelle zum Anbinden von externen Analyseprogrammen zum Auffinden von Schadsoftware (z. B. Virensuchprogramme) vorhanden sein.
5. Die Kommunikation mit einem Directory-Dienst für die Authentisierung der Anwender sollte unterstützt werden.

6. Für jedes unterstützte Protokoll muss eine Filterung nach den in M 2.76 *Auswahl und Einrichtung geeigneter Filterregeln* spezifizierten Kriterien möglich sein. Insbesondere müssen die Filterregeln benutzerabhängig formulierbar sein, und es muss möglich sein, mehrere Benutzer zu einer Gruppe zusammenzufassen.
7. Eine Filterung in Abhängigkeit von Inhalten sollte unterstützt werden, damit eine zentrale Virenprüfung und das Blockieren aktiver Inhalte möglich ist (siehe G 5.23 *Computer-Viren* bzw. G 5.88 *Missbrauch aktiver Inhalte*).
8. Bei dem Einsatz eines Application-Level-Gateways sollte keine Änderung der Software im zu schützenden Netz oder im externen Netz nötig sein.
9. Für jede aufgebaute und abgewiesene Verbindung auf der Anwendungsschicht muss eine Protokollierung von IP-Adresse des Quell- und Zielrechners, Portnummern, Zeit, Datum und der zutreffenden Regel durchgeführt werden, wobei auch Einschränkungen auf bestimmte Verbindungen möglich sein müssen.
10. Die übertragene Datenmenge sollte protokolliert werden können.
11. Die Uhrzeit des Verbindungsaufbaus und des Verbindungsabbaus sollten protokolliert werden können.

Im Folgenden werden spezifischere Anforderungen für einige häufig genutzte Protokolle zusammengestellt:

HTTP:

12. Filtern anhand der Request-Methode, z. B. GET, HEAD, PUT oder CONNECT
13. Sperren von Web-Seiten bzw. Web-Sites anhand der URL
14. Filtern anhand des MIME-Types
15. Entfernen von aktiven Inhalten und Cookies aus Web-Seiten
16. Filtern anhand von HTTP-Header-Daten
17. Filtern der folgenden Header-Felder sollte möglich sein:
    - Referrer
    - Via
    - From
    - Server
18. Filtern von "Web-Bugs"
19. Erzwingen einer starken Authentisierung am Proxy
20. Accounting zur Feststellung der von einen Nutzer abgerufenen Datenmenge
21. Unterstützung zur Signaturprüfung von signierten aktiven Inhalten
22. Protokollierung der abgerufenen Web-Seite

23. Protokollierung der Nutzung von gesperrten Request-Methoden

HTTPS:

24. Temporäre Entschlüsselung des Datenverkehrs, um das Entfernen aktiver Inhalte aus Web-Seiten, die mittels HTTPS abgerufen werden, zu ermöglichen. Temporäre Entschlüsselung bedeutet, dass übermittelte Daten erst entschlüsselt, nach der Filterung auf aktive Inhalte aber wieder verschlüsselt werden.
25. Protokollierung der abgerufenen Web-Seite
26. Benachrichtigung des Administrators bei automatischem Update abgelaufener oder ungültiger Zertifikate

SMTP:

27. Entfernen von aktiven Inhalten aus HTML-E-Mails
28. Filtern anhand des MIME-Types
29. Filtern anhand der Absender- und Empfängeradresse
30. Filtern anhand der IP-Adresse des MTAs
31. Kontrolle auf Mail-Relaying anhand des Domain-Namens
32. Überprüfung auf Zustellbarkeit der E-Mail anhand des Domain-Namens
33. Entfernung bedenklicher E-Mailanhänge anhand der Dateiendung. Zu blockierende Anhänge sollen frei vorgegeben werden können.
34. Erkennung von Spam-Mails mit Hilfe einer Kombination verschiedener Filter-Verfahren.
35. Erkannte Spam-Mails sollten wie folgt behandelt werden können:
    - Löschen
    - Isolierung ("Quarantäne")
    - Markieren
36. Erkannte E-Mails mit nicht spezifikationskonformen Headern ("Bad-Mails"), sollten wie folgt behandelt werden können:
    - Löschen
    - Isolierung ("Quarantäne")
    - Markieren
37. Bereitstellung einer Schnittstelle, die die Anbindung eines Spam-Filters ermöglicht.
38. Blockieren von (ausgehenden) E-Mails aufgrund der Erkennung von Schlüsselwörtern
39. Protokollierung der E-Mail-Adressen des Absenders und des Adressaten
40. Protokollierung des Erfolgs bzw. des Fehlschlagens der E-Mail-Weiterleitung
41. Möglichkeit zur Einrichtung eines

- Mail-Relay (Weiterleitung von einem MTA im vertrauenswürdigen Netz zu einem MTA im nicht-vertrauenswürdigen Netz)
- Mail-Server (Möglichkeit zum Abruf mit POP3 oder IMAP und zur Weiterleitung mit SMTP)

FTP (passiv und aktiv):

42. Filterung anhand von FTP-Befehlen (z. B. GET, PUT, PASV, PORT)
43. Nutzerbasierte Freigabe bzw. Sperrung von FTP-Befehlen
44. Restriktionen anhand des Dateinamens (z. B. Sperrung von *.exe)
45. Erzwingen einer starken Authentisierung am Proxy
46. Protokollierung der Nutzung von gesperrten Request-Methoden
47. Protokollierung des Benutzernamens im Falle einer Authentisierung und des Dateinamens

NNTP:

48. Filtern anhand der Request-Methode, z. B. ARTICLE, BODY, HEAD und STAT
49. Protokollierung der Nutzung von gesperrten Request-Methoden
50. Entfernen von aktiven Inhalten und Cookies aus Web-Seiten
51. Erzwingen einer starken Authentisierung am Proxy
52. Gezielte Sperrung einzelner Foren

Telnet:

53. Erzwingen einer starken Authentisierung am Proxy
54. Protokollierung des Benutzernamens im Falle einer Authentisierung

POP:

55. Filtern anhand der Request-Methode, z. B. STAT, LIST, RETR oder DELE
56. Entfernen von aktiven Inhalten und Cookies aus HTML-E-Mails
57. Protokollierung der Nutzung von gesperrten Request-Methoden

UDP- und TCP-Relays:

58. Erzwingen einer starken Authentisierung am Proxy
59. Protokollierung des Benutzernamens im Falle einer Authentisierung

IP-Relay:

60. Der Aufbau von VPNs über das Application-Level-Gateway sollte mittels IP-Relays unterstützt werden.

DNS:

61. Bereitstellung einer integrierten Lösung bestehend aus öffentlichem und privatem DNS-Server

62. Sichere Abschottung des DNS-Proxies vom Rest des Betriebssystems des ALGs

Klartextprotokolle wie Telnet und FTP sollten nach Möglichkeit nicht mehr in öffentlichen Netzen benutzt werden und durch sicherere Alternativen (SSH / SCP) ersetzt werden. Auch im internen Netz sollten sie nur dann noch verwendet werden, wenn aus zwingenden Gründen ein Umstieg auf SSH oder ein anderes sicheres Protokoll nicht möglich ist.

Auch POP sollte nach Möglichkeit allenfalls noch intern verwendet werden. Sollen von einem externen Mailserver (etwa bei einem Provider) E-Mails abgerufen werden, so sollte der Variante "POP über SSL" der Vorzug gegeben werden. In diesem Fall ist allerdings ein SSL-Proxy (analog zum HTTPS-Proxy) nötig, der die verschlüsselte Verbindung am Sicherheitsgateway unterbricht und es so ermöglicht, E-Mails zentral auf Viren und andere schädliche Inhalte zu prüfen.

Ergänzende Kontrollfragen:

- Welche Protokolle unterstützt das ausgewählte ALG? Können nicht genutzte Protokolle deaktiviert werden?
- Wurde die Auswahl und Bewertung der Anforderungen an das ALG dokumentiert?
- Erfüllen die eingesetzten Proxies die aufgeführten Anforderungen?

M 2.76 Auswahl und Einrichtung geeigneter Filterregeln

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Das Aufstellen und die notwendige Aktualisierung der Filterregeln für ein Sicherheitsgateway ist keine einfache Aufgabe. Der Administrator muss dafür fundierte Kenntnisse der eingesetzten Protokolle besitzen und entsprechend geschult werden.

Beim **Aufstellen der Filterregeln** sollten folgende Punkte beachtet werden:

- Grundsätzlich sollte die "Whitelist" Strategie verwendet werden, das heißt die Regeln sollten so formuliert werden, dass alle Zugänge, die nicht explizit erlaubt werden, verboten sind.
- Falls es Bedarf für eine benutzerspezifische Authentisierung gibt, muss geklärt werden, welche Benutzer aus dem internen Netz welche Dienste verwenden dürfen und welche Authentisierungsverfahren eingesetzt werden sollen.
- Alle Rechner im inneren Netz müssen berücksichtigt werden.
- Es muss festgelegt werden, welche Dienste zu welchen Zeiten zur Verfügung stehen sollen. Wenn eine Organisation festgelegte Arbeitszeiten hat, Mitarbeiter z. B. nur zwischen 7.00 und 19.00 Uhr anwesend sein können, so sollte es außerhalb der üblichen Arbeitszeiten auch nicht möglich sein, Verbindungen aufzubauen.

zeitliche Beschränkungen

Die Filterregeln sollten in einer Tabelle zusammengefasst werden, deren eine Achse die Ziel-IP-Adressen und deren andere Achse die Quell-IP-Adressen enthält. Die Einträge enthalten dann die erlaubten Portnummern, dabei ist die obere der Quell-, die untere der Zielport. Paketfilter können die Überprüfung der Pakete unter anderem unmittelbar nach dem Empfang oder unmittelbar vor der Weiterleitung durchführen. Normalerweise sollte die erste Variante gewählt werden. Außerdem müssen die Paketfilter so konfiguriert werden, dass als Absenderadresse nur die Nummern der an dem Interface angeschlossenen Rechner zugelassen werden ("Ingress-Filterung"). Adressen, die mit den anderen Interfaces verknüpft sind, dürfen nicht durchgelassen werden. Dies verringert die Gefahr von IP-Spoofing Angriffen.

Beispiel:

Die folgende Tabelle enthält Filterregeln für das interne Interface eines Paketfilters zwischen einem internen Netz und dem Zwischennetz, das sich zwischen dem internen und dem externen Paketfilter befindet und die Verbindungen zwischen diesen kontrolliert.

Die Einträge enthalten die erlaubten Verbindungen, dabei bezeichnet der obere Eintrag den Quellport und der untere Eintrag den Zielport.

Quellsystem	**Zielsystem**	**Quellport**	**Zielport**
Interner Mailserver	Externer Mailserver im Zwischennetz	TCP > 1023	TCP: 25
Interner DNS-Server	Externer DNS-Server im Zwischennetz	TCP : 53	UDP: 53
IT-System mit der IP-Adresse 192.168.0.5	Appl.-Level-Gateway im Zwischennetz	TCP > 1023	TCP: 20,21
IT-System mit der IP-Adresse 192.168.0.7	Appl.-Level-Gateway im Zwischennetz	TCP > 1023	TCP: 23
IT-System mit dem IP-Adressbereich 192.168.0.*	Appl.-Level-Gateway im Zwischennetz	TCP > 1023	TCP: 22,80
IT-System mit dem IP-Adressebereich 192.168.1.*	Appl.-Level-Gateway im Zwischennetz	TCP > 1023	TCP: 80

Tabelle 1: Filterregeln für das interne Interface eines Paketfilters

Der Verbindungsaufbau zwischen den nicht aufgeführten Systemen, wie beispielsweise zwischen internem Mailserver und externem DNS-Server, muss unterdrückt werden. Alle nicht aufgelisteten Portnummern sind zu blocken. Sofern weitere Dienste oder Kommunikationsbeziehungen benötigt werden, muss die Tabelle 1 entsprechend ergänzt werden.

Dies bedeutet beispielsweise, dass der interne Mailserver mit TCP von einem Port mit einer Portnummer > 1023 auf Port 25 (SMTP) des externen Mailservers im Zwischennetz zugreifen darf. Ports mit einer Portnummer > 1023 werden auch als unprivilegierte Ports bezeichnet, im Gegensatz zu Ports mit niedrigeren Portnummern, die als privilegierte oder "well-known Ports" bezeichnet werden, da die Dienste hinter diesen Portnummern von der "Internet Assigned Numbers Authority" (IANA) zugewiesen sind.

Diese Tabelle muss dann in entsprechende Filterregeln umgesetzt werden. Dies ist häufig nicht einfach und muss deshalb sehr genau kontrolliert werden.

Ggf. können die Filterregeln mit Hilfe von Tools umgesetzt werden, die über Bedienoberflächen die Modellierung des Netzes und der zugehörigen Filterregeln erleichtern. Durch regelmäßige Tests muss überprüft werden, dass alle Filterregeln korrekt umgesetzt worden sind. Insbesondere muss sichergestellt werden, dass nur die Dienste zugelassen werden, die in der Sicherheitsrichtlinie vorgesehen sind.

Für die Regeln eines Application-Level-Gateways sind analoge Tabellen zu erstellen und in die entsprechenden Filterregeln umzusetzen.

Beispiel:

Benutzername	Dienst	Befehl	Authentisierung
Frau Beispiel	FTP	..., RETR, STOR	Einmalpasswort
Herr Mustermann	FTP	..., RETR	Chipkarte

Tabelle 2: Tabelle für die Regeln eines Application-Level-Gateways

Die Benutzerin Frau Beispiel darf (unter anderem) die Befehle RETR und STOR des Dienstes FTP benutzen, d. h. sie darf über FTP Dateien laden und senden, während Herr Mustermann nur Dateien laden darf.

Ergänzende Kontrollfragen:

- Besitzen die Administratoren die notwendigen Kenntnisse, um die Filterregeln zu formulieren?
- Wurde die Tabelle der erlaubten IP- und Port-Kombinationen erstellt?
- Wurde die Umsetzung der Tabelle in Filterregeln überprüft? Entsprechen die Filterregeln den in der Tabelle formulierten Anforderungen?
- Wurden die Regeln des Application-Level-Gateways entsprechend formuliert und umgesetzt?

M 2.77 Integration von Servern in das Sicherheitsgateway

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Neben Installation und Betrieb des Sicherheitsgateways müssen oft auch Server sicher angeordnet werden. Dazu gehören z. B. Informationsserver für die Bereitstellung von Informationen an interne oder externe Benutzer, Mailserver und DNS-Server.

Für die Anordnung von Servern ist zu unterscheiden, ob diese im zu schützenden Netz, im Netz zwischen den beiden Paketfiltern (im Folgenden nur noch "Zwischennetz" genannt) oder auf der externen Seite des Sicherheitsgateways angesiedelt werden sollen.

Externe Zugänge

Externe Zugänge zum vertrauenswürdigen Netz, beispielsweise mit SSH über einen Modem-Pool, sollten wie Zugänge aus dem nicht-vertrauenswürdigen Netz behandelt werden. Dies lässt sich erreichen, indem z. B. ein Terminalserver mit angeschlossenen Modems auf die externe Seite des Sicherheitsgateways gestellt wird, so dass ein Zugang von dort nur über SSH zum internen Rechner durchgeführt werden kann.

Keine Zugänge am Sicherheitsgateway vorbei

Es müssen klare Regelungen darüber getroffen werden, dass keine externen Zugänge unter Umgehung des Sicherheitsgateways geschaffen werden dürfen. Diese Regelungen müssen allen Mitarbeitern bekanntgemacht werden. Es muss sichergestellt werden, dass sowohl das IT-Sicherheitsmanagement als auch der Administrator des Sicherheitsgateways rechtzeitig über entsprechende Pläne unterrichtet wird, um eine Einbettung in das IT-Sicherheitskonzept und die Sicherheitsrichtlinie des Sicherheitsgateways zu gewährleisten.

Weitere Informationen zur Behandlung externer Zugänge finden sich auch im Baustein B 4.4 *Remote Access*.

Anordnung von Informationsservern

Server, die der Bereitstellung von Informationen für externe Benutzer dienen, sollten generell "möglichst nahe" am nicht-vertrauenswürdigen Netz platziert werden (z. B. hinter dem externen Paketfilter) und wie andere im nicht-vertrauenswürdigen Netz vorhandene Server betrachtet werden. Die Platzierung "möglichst weit außen" erschwert bei einer Kompromittierung des Informationsservers den Zugriff auf das vertrauenswürdige Netz, da der Angreifer noch mehrere Komponenten des Sicherheitsgateways überwinden muss. Ihre Verwaltung sollte entweder nur lokal oder über speziell abgesicherte und gegebenenfalls sogar zeitlich begrenzte Zugänge vom vertrauenswürdigen Netz aus erfolgen.

Da Informationsserver, die Informationen für externe Benutzer anbieten, wie Rechner des nicht vertrauenswürdigen Netzes behandelt werden sollten, sollte durch Filterregeln und gegebenenfalls durch eine entsprechende Konfiguration des Servers sichergestellt werden, dass von einem solchen Server aus keine

Verbindungen ins vertrauenswürdige Netz hinein möglich sind, sondern nur vom vertrauenswürdigen Netz aus zum Server.

Beispielsweise sollten für einen Webserver, dessen Administration vom vertrauenswürdigen Netz aus über eine SSH-Verbindung erfolgt, keine SSH-Verbindungen erlaubt werden, die vom Server ausgehen, sondern nur Verbindungen, die vom vertrauenswürdigen Netz zum Server gehen.

Getrennte Server für Intranet und externes Netz

Gibt es Daten, die nur für die Benutzer des vertrauenswürdigen Netzes erreichbar sein sollen (etwa einen Intranet-Webserver), so sollten diese möglichst nicht auf einem Server gespeichert werden, der auch Dienste für externe Benutzer anbietet. In diesem Fall wird empfohlen, weitere Informationsserver im Zwischennetz einzusetzen, die von außen nicht erreichbar sind und gegen Angriffe von innen durch den Paketfilter geschützt werden.

Falls die Daten, die nur für interne Benutzer erreichbar sein sollen einen hohen Schutzbedarf bezüglich der Vertraulichkeit haben, so darf der entsprechende Informationsserver nicht im gleichen Zwischennetz angesiedelt werden, wie Informationsserver für externe Benutzer. In diesem Fall muss eine eigene DMZ für die betreffenden Server eingerichtet werden.

Für folgende Informationsserver werden in eigenen Maßnahmen Hinweise zur Integration in ein Sicherheitsgateway gegeben:

- Webserver (siehe M 5.115 *Integration eines Webservers in ein Sicherheitsgateway*)
- E-Mailserver (siehe M 5.116 *Integration eines E-Mailservers in ein Sicherheitsgateway*)
- Datenbankserver (siehe M 5.117 *Integration eines Datenbank-Servers in ein Sicherheitsgateway*)
- DNS-Server (siehe M 5.118 *Integration eines DNS-Servers in ein Sicherheitsgateway*)
- Webanwendung mit Web-, Applikations- und Datenbankserver (siehe M 5.119 *Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway*)

Ergänzende Kontrollfragen:

- Werden Daten, die nur für interne Benutzer verfügbar sein sollen, von Daten für externe Benutzer getrennt?
- Sind Server mit sensiblen Daten, die nur für interne Benutzer zugänglich sein sollen, in einer eigenen DMZ angesiedelt?

M 2.78 Sicherer Betrieb eines Sicherheitsgateways

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Für einen sicheren Betrieb eines Sicherheitsgateways sind die umgesetzten Sicherheitsmaßnahmen regelmäßig auf ihre korrekte Einhaltung zu überprüfen. Insbesondere müssen die für den Betrieb des Sicherheitsgateways getroffenen organisatorischen Regelungen regelmäßig/sporadisch auf ihre Einhaltung überprüft werden. Es sollte in regelmäßig kontrolliert werden, ob neue Zugänge unter Umgehung des Sicherheitsgateways geschaffen wurden.

Filterregeln testen

Durch regelmäßige Tests muss außerdem überprüft werden, dass alle Filterregeln korrekt umgesetzt worden sind. Dabei ist zu testen, dass nur die Dienste zugelassen werden, die in der Policy des Sicherheitsgateways erlaubt sind.

Falls nachträgliche Änderungen der Policy erforderlich sind, müssen diese streng kontrolliert werden und insbesondere auf Seiteneffekte überprüft werden.

Die bei der Beschaffung an Paketfilter bzw. an Application-Level-Gateways gestellten Forderungen sind umzusetzen. Sie sind regelmäßig zu aktualisieren und auf Vollständigkeit zu prüfen.

Die Default-Einstellung der Filterregeln und die Anordnung der Komponenten muss sicherstellen, dass alle Verbindungen, die nicht explizit erlaubt sind, blockiert werden. Dies muss auch bei einem völligen Ausfall der Komponenten des Sicherheitsgateways gelten.

Es muss die Regel **"Alles was nicht ausdrücklich erlaubt ist, ist verboten"** realisiert sein. So darf z. B. ein Benutzer, der keinen Eintrag in einer Access-Liste hat, keine Möglichkeit haben, Dienste des Internets zu benutzen.

Darüber hinaus sind die folgenden Punkte zu beachten:

- Alle Geräte (Rechner, Router oder Appliances), die Bestandteil eines Sicherheitsgateways sind, müssen besonders sorgfältig und sicher konfiguriert werden.

  Besonders sorgfältige Konfiguration der Komponenten

- Auf den eingesetzten Komponenten dürfen nur Programme vorhanden sein, die für die Funktionsfähigkeit des Sicherheitsgateways nötig sind. Der Einsatz dieser Programme muss ausführlich dokumentiert und begründet werden. Beispielsweise sollten Dienste deaktiviert und Treiber entfernt werden, die nicht benötigt werden. Treiber sollten nach Möglichkeit auch aus dem Betriebssystem-Kern entfernt werden. Das Verbleiben von Software muss dokumentiert und begründet werden.

- Um ein Mitlesen oder Verändern der Authentisierungsinformationen zu verhindern, dürfen Administratoren und Revisoren nur über einen vertrauenswürdigen Pfad auf das Sicherheitsgateway zugreifen, beispielsweise direkt über die Konsole, über eine verschlüsselte Verbindung oder über ein separates Administrationsnetz (Out-of-Band Management).

  Sicherer Zugriff

- Es muss dafür gesorgt werden, dass die Betriebssysteme und Programme auf den Komponenten des Sicherheitsgateways jederzeit auf einem sicheren Patch-Stand sind. Die Systemadministratoren müssen sich daher

  Sicherer Patch-Stand!

regelmäßig über bekannt gewordene Software-Schwachstellen informieren und sicherheitskritische Patches besonders sorgfältig zeitnah installieren (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*, M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*, sowie M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*).

Regelmäßige Integritätstests

- Es müssen in regelmäßigen Abständen Integritätstests der eingesetzten Software durchgeführt werden (siehe auch M 4.93 *Regelmäßige Integritätsprüfung*). Im Fehlerfall muss das Sicherheitsgateway abgeschaltet werden.
- Das Sicherheitsgateway muss auf sein Verhalten bei einem Systemabsturz getestet werden. Insbesondere sollte kein automatischer Neustart möglich sein und es muss möglich sein, die Access-Listen auf einem schreibgeschützten Medium zu speichern.

  Die Access-Listen sind die wesentlichen Daten für den Betrieb des Sicherheitsgateways sind. Daher muss durch einen entsprechenden Schutz sichergestellt werden, dass auch dann keine alten oder fehlerhaften Access-Listen benutzt werden, falls es einem Angreifer gelingt, einen Neustart des Sicherheitsgateways oder einzelner Komponenten zu verursachen.
- Bei einem Ausfall des Sicherheitsgateways muss sichergestellt sein, dass in dieser Zeit keine Netzverbindungen aus dem zu schützenden Netz heraus oder zu diesem aufgebaut werden können (siehe auch M 2.302 *Sicherheitsgateways und Hochverfügbarkeit* und M 6.94 *Notfallvorsorge bei Sicherheitsgateways*).
- Beim Wiedereinspielen von gesicherten Datenbeständen muss darauf geachtet werden, dass für den sicheren Betrieb des Sicherheitsgateways relevante Dateien wie Access-Listen, Passwortdateien oder Filterregeln auf dem aktuellsten Stand sind.

Ergänzende Kontrollfragen:

- Sind die Komponenten des Sicherheitsgateways sicher konfiguriert?
- Wie wird sichergestellt, dass die Betriebssysteme und Programme, die auf den Komponenten des Sicherheitsgateways eingesetzt werden, stets auf einem sicheren Patch-Stand sind?
- Auf welchem Weg greifen Administratoren oder Revisoren auf das Sicherheitsgateway bzw. die Komponenten zu?
- In welchen Abständen finden Integritätsprüfungen statt?
- Was geschieht bei einem Absturz oder Neustart des Sicherheitsgateways?

M 2.79 Festlegung der Verantwortlichkeiten im Bereich Standardsoftware

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Leiter IT, Leiter Organisation

Vor der Einführung von Standardsoftware müssen eine Reihe von Verantwortlichkeiten geregelt werden. Beispielhaft seien die Verantwortlichkeiten genannt für die Erstellung eines Anforderungskataloges, die Vorauswahl von Produkten, das Testen und Freigeben und die Installation.

Nachfolgend wird zum Vergleich aufgezeigt, wie diese Verantwortlichkeiten sinnvoll verteilt werden können. Da jedoch die Bezeichnungen in den meisten Organisationen voneinander abweichen, werden vorab einige Instanzen anhand ihrer Aufgaben definiert, denen anschließend die einzelnen Verantwortlichkeiten zugeordnet werden können:

- Die **Fachabteilung** ist der Anwender der Standardsoftware. Sie äußert ihren Bedarf an neuer Software und gibt damit den Anstoß zu deren Beschaffung. Sie wird bei Vorauswahl und Test beteiligt, um die Anforderungen der Anwender einzubringen.
- Die **Behörden-/Unternehmensleitung** ist verantwortlich für die Freigabe von Standardsoftware. Diese Verantwortung wird meist an den **Leiter der Fachabteilung** delegiert, womit nach Freigabe die Verantwortung für den korrekten Einsatz der Standardsoftware auf die Fachabteilung übergeht.
- Der **IT-Bereich** hat die Aufgabe, IT-Lösungen für die Erfüllung der Aufgaben der Fachabteilung bereitzustellen und den sicheren und zuverlässigen Betrieb der IT zu gewährleisten.
- Die **Beschaffungsstelle** muss die Interoperabilität und Kompatibilität der zu beschaffenden Standardsoftware sowie die Einhaltung von Hausstandards und gesetzlichen Vorschriften sicherstellen. Oft gibt es in den einzelnen Fachabteilungen IT-Koordinatoren, die Teile der Aufgaben der Beschaffungsstelle für die Fachabteilung beratend wahrnehmen und evtl. auch die Haushaltsmittel der Fachabteilung koordinieren.
- Der **Haushalt** ist verantwortlich für das Rechnungswesen, die IT-Budgetverwaltung und für die Bereitstellung der benötigten Haushaltsmittel.
- Der **IT-Sicherheitsbeauftragte** muss überprüfen, ob mit den eingesetzten oder zu beschaffenden Produkte ein angemessenes IT-Sicherheitsniveau gewährleistet werden kann. Im Rahmen des IT-Sicherheitsmanagements (siehe Baustein B 1.0 *IT-Sicherheitsmanagement*) muss er die IT-Sicherheit im laufenden Betrieb sicherstellen.
- Der **Datenschutzbeauftragte** muss die Einhaltung der datenschutzrechtlichen Bestimmungen und eines ausreichenden Schutzes personenbezogener Daten gewährleisten.

- Der **Personal- bzw. Betriebsrat** muss in vielen Fällen bei der Auswahl neuer Standardsoftware beteiligt werden, insbesondere wenn damit größere Änderungen im Arbeitsablauf verbunden sind oder wenn die zu beschaffende Software zur Leistungskontrolle geeignet ist (siehe M 2.40 *Rechtzeitige Beteiligung des Personal-/Betriebsrates*).

Im Gesamtprozess "Standardsoftware" muss für jeden einzelnen Schritt festgelegt werden, welche der zuvor beschriebenen Instanzen für die Durchführung verantwortlich sind und welche Instanzen dabei beteiligt werden müssen. Eine mögliche sinnvolle Verantwortungsverteilung ist zur Orientierung in nachfolgender Tabelle zusammengefasst:

	verantwortlich	**zu beteiligen**
Erstellung des Anforderungskatalogs	Fachabteilung, IT-Bereich	Beschaffungsstelle, Haushälter, IT-Sicherheitsbeauftragter, Datenschutzbeauftragter, Personal- oder Betriebsrat
Vorauswahl eines geeigneten Produktes	Beschaffungsstelle	IT-Bereich, Fachabteilung
Testen	Fachabteilung und IT-Bereich	IT-Sicherheitsbeauftragter, Datenschutzbeauftragter, Personal- oder Betriebsrat
Freigabe	Behörden-/Unternehmensleitung evtl. delegiert an Leiter Fachabteilung	-
Beschaffung	Beschaffungsstelle	Haushalt
Sicherstellen der Integrität der Software	IT-Bereich	-
Installation und Konfiguration	IT-Bereich	-
Versionskontrolle und Lizenzverwaltung	IT-Bereich	-
Deinstallation	IT-Bereich	-
Kontrolle des IT-Betriebs	IT-Sicherheitsbeauftragter	-

Die getroffenen Zuordnungen sind verbindlich festzuschreiben und deren Einhaltung ist periodischen Kontrollen zu unterziehen.

Ergänzende Kontrollfragen:

- Welche Regelungen sind in Kraft?
- Sind alle Mitarbeiter über bestehende Richtlinien und über deren Kontrolle unterrichtet?
- Werden alle relevanten Stellen (z. B. Personalrat, Haushalt, Datenschutzbeauftragter, ...) entsprechend ihrer Funktion beteiligt?

M 2.80 Erstellung eines Anforderungskatalogs für Standardsoftware

Verantwortlich für Initiierung: Leiter Fachabteilung

Verantwortlich für Umsetzung: Fachabteilung, Leiter IT

Zur Lösung einer Aufgabe, die mit IT bearbeitet wird, bietet der Markt meist eine Vielzahl gleichartiger Standardsoftwareprodukte an. In ihrer Grundfunktionalität vergleichbar, unterscheiden sie sich jedoch in Kriterien wie Anschaffungs- und Betriebskosten, Zusatzfunktionalitäten, Kompatibilität, Administration, Ergonomie und IT-Sicherheit.

Anforderungskatalog

Für die Auswahl eines geeigneten Produktes muss daher zunächst ein Anforderungskatalog erstellt werden. Der Anforderungskatalog sollte u. a. zu den folgenden Punkten Aussagen enthalten:

- **Funktionale Anforderungen**, die das Produkt zur Unterstützung der Aufgabenerfüllung der Fachabteilung erfüllen muss. Die für die Fachaufgabe relevanten Einzelfunktionalitäten sollten hervorgehoben werden.

  Verkürzte Beispiele:

  - Textverarbeitung mit den Zusatzfunktionen Einbinden von Graphiken, Makro-Programmierung, Rechtschreibprüfung und Silbentrennung. Makro-Programmierung muss abschaltbar sein, Rechtschreibprüfung muss in Englisch, Französisch und Deutsch verfügbar sein. Die spezifizierten Textformate müssen im- und exportiert werden können.
  - Datenbank (Front-End und Back-End) für Multi-User-Betrieb mit Unterstützung der Standardabfragesprache SQL und graphischer Bedienoberfläche
  - Terminplaner zur Koordinierung und Kontrolle von Terminen der Abteilungsangehörigen mit integrierter Terminabstimmung, automatischem Versand von Einladungen und Aufgaben- und Prioritäten-Listen, Schnittstelle zum hausinternen Mailprogramm

- **IT-Einsatzumgebung**, diese wird einerseits beschrieben durch die Rahmenbedingungen, die durch die vorhandene oder geplante IT-Einsatzumgebung vorgegeben werden, und andererseits durch die Leistungsanforderungen, die durch das Produkt an die Einsatzumgebung vorgegeben werden.

  Verkürzte Beispiele:

  - Vorgegebene IT-Einsatzumgebung: Unter Novell 3.11 vernetzter PC, 80486-Prozessor, 8 MB Hauptspeicher, 500 MB Festplattenkapazität, Diskettenlaufwerk, CD-ROM-Laufwerk, MS-DOS 6.0, Produkt darf maximal 50 MB der Festplatte belegen, es muss unter Windows 3.11 laufen und netztauglich sein.

  - Leistungsanforderungen: Das Textverarbeitungsprogramm X benötigt 16 MB Festplattenplatz, läuft auf einem PC ab 80386-Prozessor, 8 MB Hauptspeicher, Windows 3.11.

- **Kompatibilitätsanforderungen** zu anderen Programmen oder IT-Systemen, also Migrationsunterstützung und Aufwärts- und Abwärtskompatibilität.

  Verkürzte Beispiele:

  - Datenbestände aus der vorhandenen Datenbank XYZ müssen übernommen werden können.
  - Die Funktionen A, B, C müssen bei Versionswechseln erhalten bleiben.
  - Der Datenaustausch mit dem Unix-System XYZ muss möglich sein.

- **Performanceanforderungen** beschreiben die erforderlichen Leistungen hinsichtlich Durchsatz und Laufzeitverhalten. Für die geforderten Funktionen sollten möglichst genaue Angaben über die maximal zulässige Bearbeitungszeit getroffen werden.

  Verkürzte Beispiele:

  - Die maximale Antwortzeit bei Ausführung von Funktion X darf 2 Sekunden nicht überschreiten.
  - Die Verschlüsselungsrate sollte auf einem 486 DX 33 mindestens 60 KB/sec betragen.
  - Andere gleichzeitig verarbeitete Prozesse dürfen durch das Produkt maximal um 30% verlangsamt werden.

- **Interoperabilitätsanforderungen**, d. h. die Zusammenarbeit mit anderen Produkten über Plattformgrenzen hinweg muss möglich sein.

  Verkürzte Beispiele:

  - Versionen des Textverarbeitungsprogramms sollen für Windows-, Unix- und Macintosh-Plattformen verfügbar sein. Dokumente sollen auf einem Betriebssystem erstellt und auf einem anderen weiterverarbeitet werden können.
  - Das Textverarbeitungsprogramm muss mit dem eingesetzten Mailprogramm zusammenarbeiten können.

- **Zuverlässigkeitsanforderungen** betreffen die Stabilität des Produktes, also Fehlererkennung und Toleranz sowie Ausfall- und Betriebssicherheit.

  Verkürzte Beispiele:

  - Fehleingaben des Benutzers müssen erkannt werden und dürfen nicht zum Programmabbruch oder Systemabsturz führen.
  - Die Datenbank muss über Mechanismen verfügen, die es erlauben, bei einem Systemabbruch mit Zerstörung der Datenbank alle Transaktionen zu rekonstruieren (Roll-Forward).

- **Konformität zu Standards**, dies können internationale Normen, De-facto-Standards oder auch Hausstandards sein.

  Verkürzte Beispiele:

  - Das Produkt muss der EU-Bildschirmrichtlinie 90/270/EWG entsprechen.
  - Die Implementation eines Token-Ring-LANs muss konform sein zur Norm ENV 41110.
  - Das Produkt muss dem X/Open-Standard entsprechen.

- **Einhaltung von internen Regelungen und gesetzlichen Vorschriften** (z. B. ausreichender Datenschutz bei der Verarbeitung personenbezogener Daten)

  Verkürzte Beispiele:

  - Das Produkt muss den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme genügen.
  - Da personenbezogene Daten verarbeitet werden, müssen die Bestimmungen des Bundesdatenschutzgesetzes mit den implementierten Funktionen erfüllt werden können.

- **Anforderungen an die Benutzerfreundlichkeit**, die durch die leichte Bedienbarkeit, Verständlichkeit und Erlernbarkeit gekennzeichnet ist, also insbesondere durch die Güte der Benutzeroberfläche sowie die Qualität der Benutzerdokumentation und der Hilfefunktionen.

  Verkürzte Beispiele:

  - Eine Online-Hilfefunktion muss implementiert sein.
  - Die Benutzeroberfläche muss so gestaltet sein, dass ungelernte Kräfte innerhalb von zwei Stunden in die Benutzung eingewiesen werden können.
  - Die Benutzerdokumentation und die Benutzeroberfläche sollten in der Landessprache vorliegen.

- **Anforderungen an die Wartbarkeit** ergeben sich für den Anwender hauptsächlich aus der Fehlerbehandlung des Produktes.

  Verkürzte Beispiele:

  - Der Administrationsaufwand darf nicht zu hoch sein.
  - Der Anbieter muss eine Hotline für Fragen anbieten.
  - Das Produkt muss einfach zu installieren und zu konfigurieren sein.
  - Das Produkt muss einfach zu deinstallieren sein.

- die **Obergrenze der Kosten**, die durch die Beschaffung dieses Produktes verursacht würden, werden vorgegeben. Dabei müssen nicht nur die unmittelbaren Beschaffungskosten für das Produkt selber einbezogen werden, sondern auch Folgekosten, wie z. B. eine Aufrüstung der Hardware, Personalkosten oder notwendige Schulungen.

Verkürzte Beispiele:

- Das Produkt darf maximal 15.000,- Euro kosten.
- Die Schulungskosten dürfen 2.000,- Euro nicht überschreiten

- Aus den **Anforderungen an die Dokumentation** muss hervorgehen, welche Dokumente in welcher Güte (Vollständigkeit, Verständlichkeit) erforderlich sind.

  Verkürzte Beispiele:

  - Die Benutzerdokumentation muss leicht nachvollziehbar und zum Selbststudium geeignet sein. Die gesamte Funktionalität des Produktes ist zu beschreiben.
  - Die Systemverwalterdokumentation muss Handlungsanweisungen für mögliche Fehler enthalten.

- Bezüglich der **Softwarequalität** können Anforderungen gestellt werden, die von Herstellererklärungen über das eingesetzten Qualitätssicherungsverfahren, über ISO 9000 ff. Zertifikate bis hin zu unabhängigen Softwareprüfungen nach ISO 12119 reichen.

  Verkürzte Beispiele:

  - Der Software-Herstellungsprozess des Herstellers muss nach ISO 9000 zertifiziert sein.
  - Die Funktionalität des Produktes muss unabhängig gemäß ISO 12119 überprüft worden sein.

- Sollen durch das Produkt IT-Sicherheitsfunktionen erfüllt werden, sind sie in Form von **Sicherheitsanforderungen** zu formulieren (siehe M 4.42 *Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung*). Dies wird nachfolgend noch ausführlich erläutert.

Sicherheitsanforderungen

Abhängig davon, ob das Produkt Sicherheitseigenschaften bereitstellen muss, können im Anforderungskatalog Sicherheitsfunktionen aufgeführt werden. Typische Sicherheitsfunktionen, die hier in Frage kommen, seien kurz erläutert. Weitere Ausführungen findet man in den ITSEC.

- **Identifizierung und Authentisierung**

  In vielen Produkten wird es Anforderungen geben, diejenigen Benutzer zu bestimmen und zu überwachen, die Zugriff auf Betriebsmittel haben, die vom Produkt kontrolliert werden. Dazu muss nicht nur die behauptete Identität des Benutzers festgestellt, sondern auch die Tatsache nachgeprüft werden, dass der Benutzer tatsächlich die Person ist, die er zu sein vorgibt. Dies geschieht, indem der Benutzer dem Produkt Informationen liefert, die fest mit dem betreffenden Benutzer verknüpft sind.

- **Zugriffskontrolle**

  Bei vielen Produkten wird es erforderlich sein sicherzustellen, dass Benutzer und Prozesse, die für diese Benutzer tätig sind, daran gehindert

werden, Zugriff auf Informationen oder Betriebsmittel zu erhalten, für die sie kein Zugriffsrecht haben oder für die keine Notwendigkeit zu einem Zugriff besteht. Desgleichen wird es Anforderungen bezüglich der unbefugten Erzeugung oder Änderung (einschließlich Löschung) von Informationen geben.

- **Beweissicherung**

  Bei vielen Produkten wird es erforderlich sein sicherzustellen, dass über Handlungen, die von Benutzern bzw. von Prozessen im Namen solcher Benutzer ausgeführt werden, Informationen aufgezeichnet werden, damit die Folgen solcher Handlungen später dem betreffenden Benutzer zugeordnet werden können und der Benutzer für seine Handlungen verantwortlich gemacht werden kann.

- **Protokollauswertung**

  Bei vielen Produkten wird sicherzustellen sein, dass sowohl über gewöhnliche Vorgänge als auch über außergewöhnliche Vorfälle ausreichend Informationen aufgezeichnet werden, damit durch Nachprüfungen später festgestellt werden kann, ob tatsächlich Sicherheitsverletzungen vorgelegen haben und welche Informationen oder sonstigen Betriebsmittel davon betroffen waren.

- **Unverfälschbarkeit**

  Bei vielen Produkten wird es erforderlich sein sicherzustellen, dass bestimmte Beziehungen zwischen unterschiedlichen Daten korrekt bleiben und dass Daten zwischen einzelnen Prozessen ohne Änderungen übertragen werden.

  Daneben müssen auch Funktionen bereitgestellt werden, die es bei der Übertragung von Daten zwischen einzelnen Prozessen, Benutzern und Objekten ermöglichen, Verluste, Ergänzungen oder Veränderungen zu entdecken bzw. zu verhindern, und die es unmöglich machen, die angebliche oder tatsächliche Herkunft bzw. Bestimmung der Datenübertragung zu ändern.

- **Zuverlässigkeit**

  Bei vielen Produkten wird es erforderlich sein sicherzustellen, dass zeitkritische Aufgaben genau zu dem Zeitpunkt durchgeführt werden, zu dem es erforderlich ist, also nicht früher oder später, und es wird sicherzustellen sein, dass zeitunkritische Aufgaben nicht in zeitkritische umgewandelt werden können. Desgleichen wird es bei vielen Produkten erforderlich sein sicherzustellen, dass ein Zugriff in dem erforderlichen Moment möglich ist und Betriebsmittel nicht unnötig angefordert oder zurückgehalten werden.

- **Übertragungssicherung**

  Dieser Begriff umfasst alle Funktionen, die für den Schutz der Daten während der Übertragung über Kommunikationskanäle vorgesehen sind:

  - Authentisierung

- Zugriffskontrolle
- Datenvertraulichkeit
- Datenintegrität
- Sende- und Empfangsnachweis

Einige dieser Funktionen werden mittels kryptographischer Verfahren realisiert.

Über die ITSEC hinaus können weitere Sicherheitsanforderungen an Standardsoftware konkretisiert werden.

- **Datensicherung**

  An die Verfügbarkeit der mit dem Produkt verarbeiteten Daten werden hohe Anforderungen gestellt. Unter diesen Punkt fallen im Produkt integrierte Funktionen, die Datenverlusten vorbeugen sollen wie die automatische Speicherung von Zwischenergebnissen oder die automatische Erstellung von Sicherungskopien vor der Durchführung größerer Änderungen.

- **Verschlüsselung**

  Verschlüsselung dient der Wahrung der Vertraulichkeit von Daten. Bei vielen Produkten wird es erforderlich sein, Nutzdaten vor einer Übertragung oder nach der Bearbeitung zu verschlüsseln und sie nach Empfang oder vor der Weiterverarbeitung zu entschlüsseln. Hierzu ist ein anerkanntes Verschlüsselungsverfahren zu verwenden. Es ist sicherzustellen, dass die zur Entschlüsselung benötigten Parameter (z. B. Schlüssel) in der Weise geschützt sind, dass kein Unbefugter Zugang zu diesen Daten besitzt.

- **Funktionen zur Wahrung der Datenintegrität**

  Für Daten, deren Integritätsverlust zu Schäden führen kann, können Funktionen eingesetzt werden, die Fehler erkennen lassen oder sogar mittels Redundanz korrigieren können. Meist werden Verfahren zur Integritätsprüfung eingesetzt, die absichtliche Manipulationen am Produkt bzw. den damit erstellten Daten sowie ein unbefugtes Wiedereinspielen von Daten zuverlässig aufdecken können. Sie basieren auf kryptographischen Verfahren (siehe M 5.36 *Verschlüsselung unter Unix und Windows NT* und M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*).

- **Datenschutzrechtliche Anforderungen**

  Wenn mit dem Produkt personenbezogene Daten verarbeitet werden sollen, sind über die genannten Sicherheitsfunktionen hinaus zusätzliche spezielle technische Anforderungen zu stellen, um den Datenschutzbestimmungen genügen zu können.

Stärke der Mechanismen

Sicherheitsfunktionen werden durch Mechanismen umgesetzt. Je nach Einsatzzweck müssen diese Mechanismen eine unterschiedliche Stärke besitzen, mit der sie Angriffe abwehren können. Die erforderliche Stärke der Mecha-

nismen ist im Anforderungskatalog anzugeben. Nach ITSEC unterscheidet man drei verschiedene Mechanismenstärken:

- **niedrig**: bietet Schutz gegen zufällige unbeabsichtigte Angriffe, z. B. Bedienungsfehler.
- **mittel**: bietet Schutz gegen Angreifer mit beschränkten Gelegenheiten oder Betriebsmitteln.
- **hoch**: kann nur von Angreifern überwunden werden, die über sehr gute Fachkenntnisse, Gelegenheiten und Betriebsmitteln verfügen, wobei ein solcher erfolgreicher Angriff als normalerweise nicht durchführbar beurteilt wird.

Beispiele für Anforderungen zu Sicherheitseigenschaften

Nachfolgend werden für einige wichtige Sicherheitsfunktionen Beispiele genannt, aus denen typische Anforderungen an Sicherheitseigenschaften deutlich werden.

Soll das Produkt über einen **Identifizierungs- und Authentisierungsmechanismus** verfügen, können beispielsweise folgende Anforderungen gestellt werden:

- Der Zugang darf ausschließlich über eine definierte Schnittstelle erfolgen. Dabei kann z. B. ein Anmeldemechanismus zum Einsatz kommen, der eine eindeutige Benutzer-Kennung und ein Passwort verlangt. Wird beim Zugang zum IT-System bereits die Identität des Benutzers sichergestellt, ist eine anonyme Passworteingabe ausreichend. Andere Möglichkeiten sind Verfahren, die auf dem Besitz bestimmter "Token" beruhen, wie z. B. einer Chipkarte.
- Das Zugangsverfahren selbst muss die sicherheitskritischen Parameter, wie Passwort, Benutzer-Kennung, usw., sicher verwalten. So dürfen aktuelle Passwörter nie unverschlüsselt auf den entsprechenden IT-Systemen gespeichert werden.
- Das Zugangsverfahren muss definiert auf Fehleingaben reagieren. Erfolgt zum Beispiel dreimal hintereinander eine fehlerhafte Authentisierung, ist der Zugang zum Produkt zu verwehren oder alternativ sind die zeitlichen Abstände, nach denen ein weiterer Zugangsversuch erlaubt wird, sukzessiv zu vergrößern.
- Das Zugangsverfahren muss das Setzen bestimmter Minimalvorgaben für die sicherheitskritischen Parameter zulassen. So sollte die Mindestlänge eines Passwortes sechs Zeichen, die Mindestlänge einer PIN drei Ziffern betragen. Ggf. ist auch die Syntax für Passwörter vorzugeben.

Soll das Produkt über eine **Zugriffskontrolle** verfügen, können beispielsweise folgende Anforderungen gestellt werden:

- Das Produkt muss verschiedene Benutzer unterscheiden können.
- Das Produkt muss je nach Vorgabe Ressourcen einzelnen autorisierten Benutzer zuteilen können und Unberechtigten den Zugriff gänzlich verwehren.

- Mittels einer differenzierten Rechtestruktur (lesen, schreiben, ausführen, ändern, ...) sollte der Zugriff geregelt werden können. Die für die Rechteverwaltung relevanten Daten sind manipulationssicher vom Produkt zu verwalten.

Soll das Produkt über eine **Protokollierung** verfügen, können folgende Anforderungen sinnvoll sein:

- Der Mindestumfang, den das Produkt protokollieren können muss, sollte parametrisierbar sein. Beispielsweise sollten folgende Aktionen protokollierbar sein:
  - bei Authentisierung: Benutzer-Kennung, Datum und Uhrzeit, Erfolg, ...,
  - bei der Zugriffskontrolle: Benutzer-Kennung, Datum und Uhrzeit, Erfolg, Art des Zugriffs, was wurde wie geändert, gelesen, geschrieben, ...,
  - Durchführung von Administratortätigkeiten,
  - Auftreten von funktionalen Fehlern.
- Die Protokollierung darf von Unberechtigten nicht deaktivierbar sein. Die Protokolle selbst dürfen für Unberechtigte weder lesbar noch modifizierbar sein.
- Die Protokollierung muss übersichtlich, vollständig und korrekt sein.

Soll das Produkt über eine **Protokollauswertung** verfügen, können folgende Anforderungen sinnvoll sein:

- Eine Auswertefunktion muss nach den bei der Protokollierung geforderten Datenarten unterscheiden können (z. B. "Filtern aller unberechtigten Zugriffe auf alle Ressourcen in einem vorgegebenen Zeitraum").

  Die Auswertefunktion muss auswertbare ("lesbare") Berichte erzeugen, so dass keine sicherheitskritischen Aktivitäten übersehen werden.

Soll das Produkt über Funktionen zur **Unverfälschbarkeit** verfügen, könnte beispielsweise folgende Anforderung gestellt werden:

- Ein Datenbank-Managementsystem muss über Möglichkeiten zur Beschreibung von Regeln bestimmter Beziehungen zwischen den gespeicherten Daten verfügen (z. B. referentielle Integrität). Außerdem müssen geeignete Mechanismen existieren, die verhindern, dass es durch Änderungen der Daten zu Verstößen gegen diese Regeln kommt.

Soll das Produkt über Funktionen zur **Datensicherung** verfügen, können beispielsweise folgende Anforderungen gestellt werden:

- Es muss konfigurierbar sein, welche Daten wann gesichert werden.
- Es muss eine Option zum Einspielen beliebiger Datensicherungen existieren.
- Die Funktion muss das Sichern von mehreren Generationen ermöglichen.

- Datensicherungen von Zwischenergebnissen aus der laufenden Anwendung sollen möglich sein.

Soll das Produkt über eine **Verschlüsselungskomponente** verfügen, sind folgende Anforderungen sinnvoll:

- Der implementierte Verschlüsselungsalgorithmus sollte - beim Einsatz in Behörden - vom BSI anerkannt sein. Hier empfiehlt sich eine individuelle Beratung durch das BSI. Außerhalb der Behörden ist bei mittlerem Schutzbedarf der DES geeignet.
- Das Schlüsselmanagement muss mit der Funktionalität des Produktes harmonieren. Dabei sind insbesondere grundsätzliche Unterschiede der Algorithmen zu berücksichtigen:
  - symmetrische Verfahren benutzen einen geheim zu haltenden Schlüssel für die Ent- und Verschlüsselung,
  - asymmetrische Verfahren benutzen einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten (geheim zu haltenden) für die Entschlüsselung.
- Das Produkt muss die sicherheitskritischen Parameter wie Schlüssel sicher verwalten. So dürfen Schlüssel (auch mittlerweile nicht mehr benutzte) nie ungeschützt, das heißt auslesbar, auf den entsprechenden IT-Systemen abgelegt werden.

Soll das Produkt über Mechanismen zur **Integritätsprüfung** verfügen, sind folgende Anforderungen sinnvoll:

- Das Produkt führt bei jedem Programmaufruf einen Integritätscheck durch.
- Bei der Datenübertragung müssen Mechanismen eingesetzt werden, mit denen absichtliche Manipulationen an den Adressfeldern und den Nutzdaten erkannt werden können. Daneben darf die bloße Kenntnis der eingesetzten Algorithmen ohne spezielle Zusatzkenntnisse nicht ausreichen, unerkannte Manipulationen an den obengenannten Daten vorzunehmen.

Werden personenbezogene Daten mit dem Produkt verarbeitet, können beispielsweise folgende **datenschutzrechtlichen Anforderungen** gestellt werden:

- Das Produkt darf keine freie Abfrage für Datenauswertungen zulassen. Die Auswertungen von Datensätzen müssen auf bestimmte Kriterien einschränkbar sein.
- Es muss parametrisierbar sein, dass für bestimmte Dateien Änderungen, Löschungen oder Ausdrucke von personenbezogenen Daten nur nach dem Vier-Augen-Prinzip möglich sind.
- Die Protokollierung muss parametrisierbar sein, so dass aufgezeichnet werden kann, wer wann an welchen personenbezogenen Daten welche Änderungen vorgenommen hat.
- Die Übermittlung personenbezogener Daten muss durch geeignete Stichprobenverfahren festgestellt und überprüft werden können (BDSG, § 10). Die Art der Stichprobe muss sich individuell einstellen lassen.

- Das Produkt muss das Löschen von personenbezogenen Daten ermöglichen. Ersatzweise muss das Sperren personenbezogener Daten möglich sein, um ihre weitere Verarbeitung oder Nutzung einzuschränken bzw. zu verhindern.

Bewertungsskala

Um einen Vergleich verschiedener Produkte im Sinne einer Nutzwertanalyse durchführen zu können, müssen Kriterien vorhanden sein, wie die Erfüllung der einzelnen Anforderungen gewertet wird. Dazu ist es erforderlich, vorab die Bedeutung der einzelnen Anforderungen für die angestrebte IT-gestützte Aufgabenerfüllung quantitativ oder qualitativ zu bewerten.

Diese Bewertung kann beispielsweise in drei Stufen vorgenommen werden. In der ersten Stufe wird festgelegt, welche im Anforderungskatalogs geforderten Eigenschaften **notwendig** und welche **wünschenswert** sind. Wenn eine notwendige Eigenschaft nicht erfüllt ist, wird das Produkt abgelehnt (so genanntes K.O.-Kriterium). Das Fehlen einer wünschenswerten Eigenschaft wird zwar negativ gewertet, dennoch wird aber das Produkt aufgrund dessen nicht zwingend abgelehnt.

Als zweite Stufe wird die **Bedeutung** der geforderten wünschenswerte Eigenschaft für die Aufgabenerfüllung angegeben. Dies kann z. B. quantitativ mit Werten zwischen 1 für niedrig und 5 für hoch erfolgen. Notwendige Eigenschaften müssen nicht quantitativ bewertet werden. Ist dies aber aus rechnerischen Gründen erforderlich, müssen sie auf jeden Fall höher bewertet werden als jede wünschenswerte Eigenschaft (um die Bedeutung einer notwendigen Eigenschaft hervorzuheben, kann sie z. B. mit 10 bewertet werden).

In der dritten Stufe wird ein **Vertrauensanspruch** für die Korrektheit Aufgabenerfüllung der geforderten Eigenschaften angegeben (z. B. mit Werten zwischen 1 für niedrig und 5 für hoch). Anhand des Vertrauensanspruchs wird später entschieden, wie eingehend die Eigenschaft getestet wird. Der Vertrauensanspruch der Sicherheitsmechanismen muss entsprechend ihrer Mechanismenstärke bewertet werden, beispielsweise kombiniert man

- Mechanismenstärke niedrig mit Vertrauensanspruch 1
- Mechanismenstärke mittel mit Vertrauensanspruch 3
- Mechanismenstärke hoch mit Vertrauensanspruch 5

Diese Orientierungswerte müssen im Einzelfall verifiziert werden.

Beispiele:

Auszugsweise sollen für einige typische Standardsoftwareprodukte Sicherheitsanforderungen erläutert werden:

Textverarbeitungsprogramm:

Notwendige Sicherheitseigenschaften:

- Automatische Datensicherung im laufenden Betrieb von Zwischenergebnissen

Wünschenswerte Sicherheitseigenschaften:

- Passwortschutz einzelner Dateien
- Verschlüsselung einzelner Dateien
- Makro-Programmierung muss abschaltbar sein

Dateikompressionsprogramm:

Notwendige Sicherheitseigenschaften:

- Im Sinne der Datensicherung dürfen nach Kompression zu löschende Dateien erst dann vom Kompressionsprogramm gelöscht werden, wenn die Kompression fehlerfrei abgeschlossen wurde.
- Vor der Dekomprimierung einer Datei muss deren Integrität überprüft werden, damit z. B. Bitfehler in der komprimierten Datei erkannt werden.

Wünschenswerte Sicherheitseigenschaften:

- Passwortschutz komprimierter Dateien

Terminplaner:

Notwendige Sicherheitseigenschaften:

- Eine sichere Identifikation und Authentisierung der einzelnen Benutzer muss erzwungen werden, z. B. über Passwörter.
- Eine Zugriffskontrolle für die Terminpläne der einzelnen Mitarbeiter ist erforderlich.
- Zugriffsrechte müssen für Einzelne, Gruppen und Vorgesetzte getrennt vergeben werden können.
- Eine Unterscheidung zwischen Lese- und Schreibrecht muss möglich sein.

Wünschenswerte Sicherheitseigenschaften:

- Eine automatisierte Datensicherung in verschlüsselter Form ist vorzusehen.

Reisekostenabrechnungssystem:

Notwendige Sicherheitseigenschaften:

- Eine sichere Identifikation und Authentisierung der einzelnen Benutzer muss erzwungen werden, z. B. über Passwörter.
- Eine Zugriffskontrolle muss vorhanden und auch für einzelne Datensätze einsetzbar sein.
- Zugriffsrechte müssen für Benutzer, Administrator, Revisor und Datenschutzbeauftragter getrennt vergeben werden können. Eine Rollentrennung zwischen Administrator und Revisor muss durchführbar sein.

- Datensicherungen müssen so durchgeführt werden können, dass sie verschlüsselt abgelegt werden und nur von Berechtigten wiedereingespielt werden können.
- Detaillierte Protokollierungsfunktionen müssen verfügbar sein.

Wünschenswerte Sicherheitseigenschaften:

- Ein optionaler Integritätscheck für zahlungsrelevante Daten sollte angeboten werden.

Beispiel für eine Bewertungsskala:

Eine Fachabteilung will für Datensicherungszwecke ein Komprimierungsprogramm beschaffen. Nach der Erstellung eines Anforderungskataloges könnten die dort spezifizierten Eigenschaften wie folgt bewertet werden:

Eigenschaft	notwendig	wünschenswert	Bedeutung	Vertrauensanspruch
korrekte Kompression und Dekompression	X		10	5
Erkennen von Bitfehlern in einer komprimierten Datei	X		10	2
Löschung von Dateien nur nach erfolgreicher Kompression	X		10	3
DOS-PC, 80486, 8 MB	X		10	5
Windows-tauglich		X	2	1
Durchsatz bei 50 MHz über 1 MB/s		X	4	3
Kompressionsrate über 40% bei Textdateien des Programms XYZ		X	4	3
Online-Hilfefunktion		X	3	1
Maximale Kosten 50.- Euro pro Lizenz	X		10	5
Passwortschutz für komprimierte Dateien (Mechanismenstärke hoch)		X	2	5

Ergänzende Kontrollfragen:

- Wer wird bei der Erstellung des Anforderungskatalogs beteiligt?
- Wer entscheidet, ob ein Produkt Sicherheitsfunktionen beinhalten muss?
- Gibt es einheitliche Vorgaben, wie eine Nutzwertanalyse aufgebaut sein muss?

M 2.81 Vorauswahl eines geeigneten Standardsoftwareproduktes

Verantwortlich für Initiierung: Beschaffungsstelle

Verantwortlich für Umsetzung: Beschaffungsstelle, Leiter IT, Fachabteilung

Die Vorauswahl eines Standardsoftwareproduktes orientiert sich an dem durch die Fachabteilung und den IT-Bereich aufgestellten Anforderungskatalog. Zunächst sollte die für die Vorauswahl zuständige Stelle eine Marktanalyse durchführen, bei der anhand des Anforderungskatalogs eine tabellarische Marktübersicht erarbeitet werden sollte. In dieser Tabelle sollten für die in Frage kommenden Produkte Aussagen zu den im Anforderungskatalog festgehaltenen Punkten gemacht werden.

Die Marktübersicht sollte vom IT-Bereich erarbeitet werden, sie kann anhand von Produktbeschreibungen, Herstelleraussagen, Fachzeitschriften oder Händlerauskünften erstellt werden. Alternativ ist eine Ausschreibung möglich und teilweise vorgegeben. Der Anforderungskatalog ist Grundlage einer Ausschreibung, so dass anhand der eingehenden Angebote eine vergleichbare Marktübersicht erstellt werden kann.

Anschließend müssen die in der Marktübersicht erfassten Produkte bzgl. der Vorgaben des Anforderungskatalogs bewertet werden. Hierzu kann die in M 2.80 *Erstellung eines Anforderungskatalogs für Standardsoftware* erarbeitete Bewertungsskala eingesetzt werden. Anhand der vorliegenden Informationen wird festgestellt, welche der geforderten Eigenschaften des Produktes vorhanden sind. Fehlen dem Produkt notwendige Eigenschaften, wird es verworfen. Über die Bewertung der Bedeutung der einzelnen Eigenschaften jedes Produktes kann eine Summe ermittelt werden. Anhand dieser Summen kann nun eine Hitliste für die Produkte aus der Vorauswahl erstellt werden.

Beispiel:

Die im Anforderungskatalog geforderten und bewerteten Eigenschaften für ein Komprimierungsprogramm werden nun wie folgt gewichtet:

Eigenschaft	Notwendig/ Wünschenswert	Bedeutung	Produkt 1	Produkt 2	Produkt 3	Produkt 4
korrekte Kompression und Dekompression	N	10	j	j	j	j
Erkennen von Bitfehlern in einer komprimierten Datei	N	10	j	j	K.O.	j
Löschung von Dateien nur nach erfolgreicher Kompression	N	10	j	j	j	j
DOS-PC, 80486, 8 MB	N	10	j	j	j	j
Windows-tauglich	W	2	n	j	j	j
Durchsatz bei 50 MHz über 1 MB/s	W	4	j	j	j	n
Kompressionsrate über 40% bei Textdateien des Programms XYZ	W	4	j	j	n	n
Online-Hilfefunktion	W	3	n	n	n	j
Maximale Kosten 50.- Euro pro Lizenz	N	10	j	j	j	j
Passwortschutz für komprimierte Dateien (Mechanismenstärke hoch)	W	2	j	j	n	j
Bewertung		65 (=Max.)	60	62	K.O.	57

Als Ergebnis ergibt sich, dass Produkt 3 herausfällt, da eine notwendige Eigenschaft nicht gegeben ist. Ansonsten wird die Hitliste angeführt von Produkt 2, gefolgt von Produkt 1 und 4.

Die erstellte Hitliste zusammen mit der Marktübersicht sollte dann der Beschaffungsstelle vorgelegt werden, damit dieser überprüfen kann, inwieweit die dort aufgeführten Produkte den internen Regelungen und gesetzlichen Vorgaben entsprechen. Dabei muss die Beschaffungsstelle auch darauf achten, dass die anderen Stellen, deren Vorgaben eingehalten werden müssen, wie der Datenschutzbeauftragte, der IT-Sicherheitsbeauftragte oder der Personal- bzw. Betriebsrat, rechtzeitig beteiligt werden.

Es muss entschieden werden, wie viele und welche Kandidaten der Hitliste getestet werden sollen. Sinnvollerweise sollten die ersten zwei oder drei

Spitzenkandidaten ausgewählt werden und daraufhin getestet werden, ob sie die wichtigsten Kriterien des Anforderungskatalogs auch tatsächlich erfüllen. Dies ist insbesondere für die notwendigen Anforderungen wichtig. Hierfür sollten Testlizenzen beschafft werden und, wie in M 2.82 *Entwicklung eines Testplans für Standardsoftware* und M 2.83 *Testen von Standardsoftware* beschrieben, Tests durchgeführt werden.

Neben den Kriterien des Anforderungskatalogs können für die Entscheidung noch die folgenden Punkte berücksichtigt werden:

- **Referenzen**

  Kann der Hersteller oder Vertreiber für sein Produkt Referenzinstallationen angeben, so können die dort gemachten Erfahrungen hinterfragt und in die Produktbeurteilung einbezogen werden.

  Liegen externe Testergebnisse oder Qualitätsaussagen für das zu testende Softwareprodukt vor (z. B. Testergebnisse in Fachzeitschriften, Konformitätstests nach proprietären Standards, Prüfungen und Zertifikate nach einschlägigen Standards und Normen wie ISO 12119), so sollten auch diese Ergebnisse bei der Vorauswahl berücksichtigt werden.

- **Verbreitungsgrad des Produktes**

  Bei einem hohen Verbreitungsgrad hat der einzelne Anwender wenig oder keinen Einfluss auf den Hersteller des Produkts, wenn es um die Behebung von Fehlern oder die Implementation bestimmter Funktionalitäten geht. Er kann aber davon ausgehen, dass das Produkt weiterentwickelt wird. Oft gibt es externe Tests, die durch den Hersteller beauftragt oder von Fachzeitschriften durchgeführt wurden. Bei Produkten mit hohem Verbreitungsgrad ist im allgemeinen mehr über Schwachstellen bekannt, so dass der Anwender davon ausgehen kann, dass die wesentlichen Schwachstellen bereits bekannt sind, bzw. dass das Wissen über Schwachstellen schnell verbreitet wird und er nach dem Bekanntwerden Abhilfe schaffen kann.

  Bei einem niedrigen Verbreitungsgrad kann ein Anwender mehr Einfluss auf den Hersteller nehmen. Externe Tests liegen im allgemeinen nicht vor, da sie für Produkte kleiner Hersteller zu aufwendig und zu teuer sind. Produkte mit niedrigem Verbreitungsgrad enthalten meist nicht mehr oder weniger Schwachstellen als solche mit hohem Verbreitungsgrad. Nachteil ist hier, dass diese evtl. nicht so schnell bekannt werden und damit behoben werden können. Wenn es sich aber um Sicherheitslücken handelt, sind diese aber wahrscheinlich auch potentiellen Angreifer nicht bekannt bzw. keine lohnenden Angriffsziele.

- **Wirtschaftlichkeit / Kosten für Kauf, Betrieb, Wartung, Schulung**

  Vor der Entscheidung für ein Produkt sollte immer die Frage stehen, ob die Kosten für das Produkt in einem angemessenen Verhältnis zu dem damit erzielbaren Nutzen stehen. In die unmittelbaren Anschaffungskosten sind darüber hinaus alle Folgekosten für Betrieb, Wartung und Schulung einzubeziehen. Dazu muss z. B. geklärt werden, ob die vorhandene Hardware-Plattform aufgerüstet werden muss oder ob für Installation und Betrieb Schulungen erforderlich sind.

Ist dann die Kaufentscheidung für ein Produkt gefallen, sollte der Kauf natürlich beim günstigsten Anbieter getätigt werden. Dieser hat sich evtl. schon bei der Marktsichtung herauskristallisiert.

Ergänzende Kontrollfragen:

- Welche Regelungen sind in Kraft?
- Bietet die ausgewählte Software alle im Anforderungskatalog zusammengestellten Funktionen?
- Ist das Produkt kompatibel zu der aktuellen IT-Infrastruktur?
- Welche Folgekosten sind beispielsweise für Schulung und Programmpflege zu erwarten?
- Sind Installation und Betrieb durch vorhandenes Personal möglich, wird zusätzlicher Personalaufwand erforderlich oder muss externe Fachkompetenz verpflichtet werden?

M 2.82 Entwicklung eines Testplans für Standardsoftware

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Leiter Fachabteilung, Leiter IT

Die im nachfolgenden beschriebene Vorgehensweise beim Testen orientiert sich an den Standardwerken DIN ISO/IEC 12119 "Software-Erzeugnisse, Qualitätsanforderungen und Prüfbestimmungen", Vorgehensmodell für die Planung und Durchführung von IT-Vorhaben (V-Modell) und dem Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM), die als weiterführende Literatur empfohlen werden.

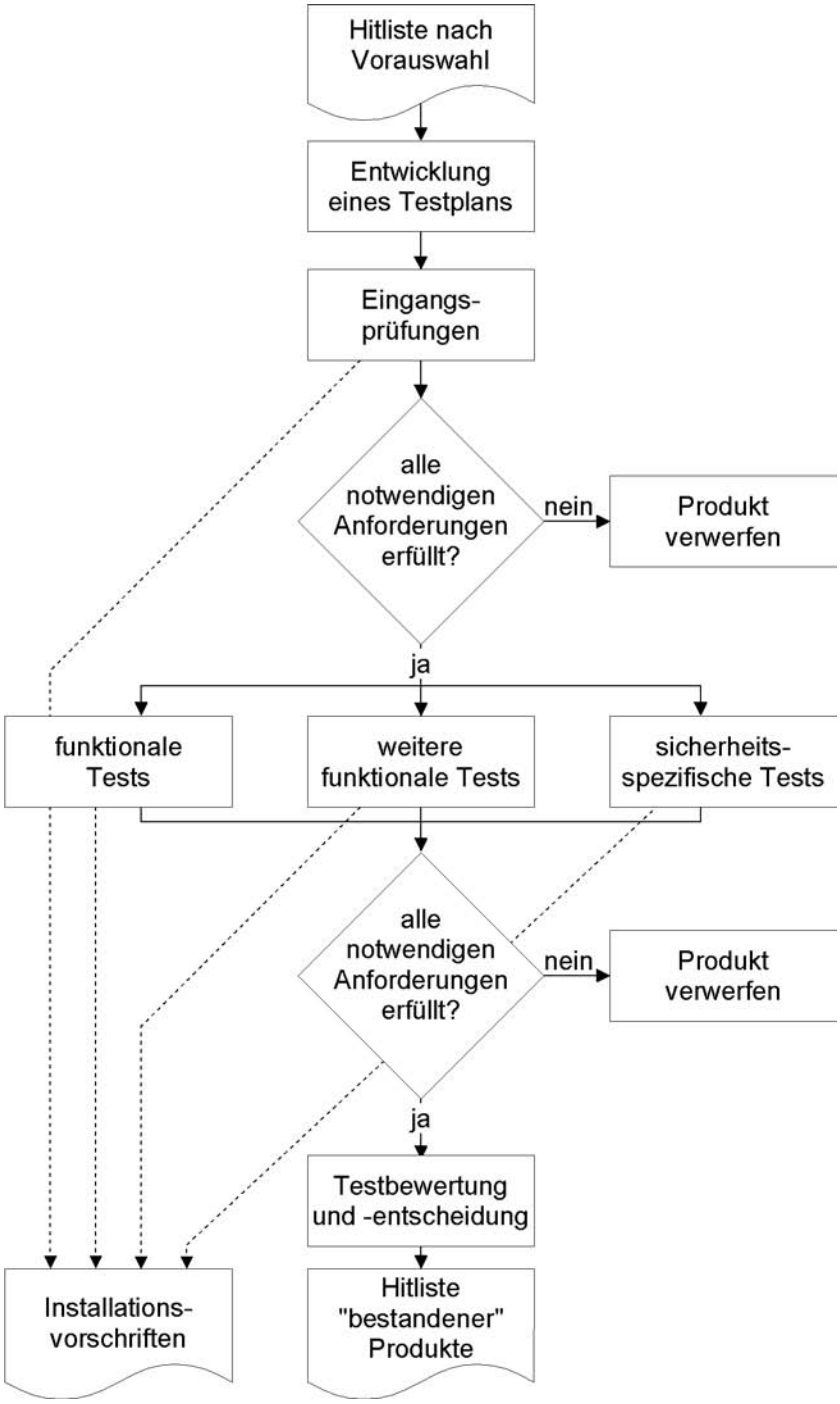
Vor der Entscheidung für ein geeignetes Standardsoftwareprodukt müssen die nach der Vorauswahl (siehe M 2.81 *Vorauswahl eines geeigneten Standardsoftwareproduktes*) in die engere Wahl gezogenen Produkte als Testlizenz beschafft und ausreichend getestet werden. War es aufgrund zeitlicher Beschränkungen, institutionsinterner Beschaffungsempfehlungen (Einhaltung von Hausstandards) oder anderen Gründen nicht möglich, dass Produkt vor der Beschaffung zu testen, müssen auf jeden Fall Tests vor der endgültigen Inbetriebnahme durchgeführt werden. Die Ergebnisse dieser Tests liefern dann die Grundlage für die Installationsvorschriften und anderer Freigabe-Bedingungen.

Obwohl bereits bei der Vorauswahl eine Überprüfung der notwendigen Anforderungen an das Produkt aufgrund der Herstelleraussagen stattgefunden hat, kann man nicht davon ausgehen, dass diese Anforderungen auch im gewünschten Maße erfüllt werden. Vielmehr muss nun durch systematisches Testen die Eignung und Zuverlässigkeit des Produktes auf Grundlage des Anforderungskataloges überprüft werden, um das geeignetste Produkt auszuwählen.

Dabei bietet es sich an, das Testen in vier Bereiche einzuteilen:

- Eingangsprüfungen (Prüfung auf Computer-Viren, Lauffähigkeit in der gewünschten IT-Einsatzumgebung, ...),
- funktionale Tests (Überprüfung der funktionalen Anforderungen),
- Tests weiterer funktionaler Eigenschaften (Überprüfung von Kompatibilität, Performance, Interoperabilität, Konformität mit Regelungen oder Gesetzen, Benutzerfreundlichkeit, Wartbarkeit, Dokumentation), und
- sicherheitsspezifische Tests (Überprüfung der Sicherheitsanforderungen).

Das prinzipielle Vorgehen beim Testen von Standardsoftware zeigt die folgende Abbildung.



Anhand der bei der Vorauswahl erstellten Hitliste sind diejenigen Produkte auszuwählen, die getestet werden sollen. Anschließend wird ein **Testplan** entwickelt.

Dieser umfasst folgende Inhalte:

- Festlegung der Testinhalte anhand des Anforderungskataloges,
- Überprüfung von Referenzen,

- Festlegung des Gesamtprüfaufwandes,
- Zeitplanung einschließlich Prüfaufwand je Testinhalt,
- Festlegung der Testverantwortlichen,
- Testumgebung,
- Inhalt der Testdokumentation,
- Festlegung von Entscheidungskriterien.

Die einzelnen genannten Punkte werden nachfolgend erläutert.

Festlegung der Testinhalte anhand des Anforderungskataloges

Aus dem Anforderungskatalog werden diejenigen Anforderungen ausgewählt, die überprüft werden sollen. Dies sollten insbesondere diejenigen Eigenschaften sein, die eine große Bedeutung oder einen hohen Vertrauensanspruch besitzen.

Überprüfung von Referenzen

Bei der Vorauswahl (siehe M 2.81 *Vorauswahl eines geeigneten Standardsoftwareproduktes*) wurden bereits erste Referenzen über die zu testenden Produkte eingeholt. Diese können ersatzweise herangezogen werden, wenn man der jeweiligen externen Testgruppe ausreichendes Vertrauen entgegenbringt.

Wurde für das Produkt ein Zertifikat nach den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) oder den Common Criteria (CC) vergeben, ist anhand des Zertifizierungsreportes zu prüfen, inwieweit die dort dokumentierten Testergebnisse berücksichtigt werden können.

Gegebenenfalls können dann eigene Test unterbleiben oder in geringerem Umfang stattfinden. Die frei werdenden Kapazitäten können auf andere Testinhalte verteilt werden.

Festlegung des Gesamtprüfaufwandes

Um den Aufwand für die Tests nicht ausufern zu lassen, sollte vorab der Gesamtprüfaufwand festgelegt werden, z. B. in Personentagen oder durch Fristsetzung.

Zeitplanung einschließlich Prüfaufwand je Testinhalt

Beim Testen mehrerer Produkte empfiehlt es sich, diese vergleichend zu testen. Das heißt, alle Produkte werden von einer Testgruppe bzgl. einer Anforderung des Anforderungskataloges getestet. Der Prüfaufwand ist damit für jede Anforderung des Anforderungskataloges festzulegen und wird damit automatisch gleichmäßig auf alle zu testenden Produkte verteilt. Der Prüfaufwand ergibt sich dabei aus Prüftiefe und Komplexität der Eigenschaft. Die Prüftiefe der jeweiligen Eigenschaften sollte sich zum einen an ihrem Vertrauensanspruch, das heißt an dem Vertrauen orientieren, das der Korrektheit dieser Eigenschaft entgegengebracht werden muss. Zum anderen muss aber

auch die Fehleranfälligkeit und Nutzungshäufigkeit der jeweiligen Eigenschaft berücksichtigt werden. Ausführlichere Informationen sind der Norm ISO 12119 zu entnehmen.

Hinweise:

- Für sicherheitsspezifische Anforderungen kann die Prüftiefe entsprechend der geforderten Mechanismenstärke zusätzlich relativiert werden.
- Der Prüfaufwand für die Eingangsprüfungen sollte gemessen an den anderen Tests gering sein.

Abschließend ist der Gesamtprüfaufwand entsprechend dem relativen Prüfaufwand der jeweiligen Eigenschaft auf die einzelnen Testabschnitte zu verteilen.

Festlegung der Testverantwortlichen

Für jeden Testinhalt ist nun festzulegen, welche Aufgaben durchzuführen sind und wer dafür verantwortlich ist. Insbesondere ist zu beachten, dass bei einigen Testinhalten der Personal- bzw. Betriebsrat, der Datenschutzbeauftragte und der IT-Sicherheitsbeauftragte zu beteiligen ist.

Testumgebung

Testen ist immer destruktiv, da vorsätzlich nach Fehlern gesucht wird. Aus diesem Grund muss das Testen immer in einer isolierten Testumgebung erfolgen.

Die Testumgebung sollte nach Möglichkeit ein genaues funktionales Abbild der Produktionsumgebung sein. In der Regel ist es jedoch nicht wirtschaftlich, die Produktionsumgebung in vollem Umfang nachzubilden.

Damit für die ausgewählten Produkte gleiche Randbedingungen gegeben sind, sollte eine Referenztestumgebung definiert werden. Für einzelne Tests kann diese weiter angepasst oder eingeschränkt werden.

Die für die einzelnen Prüfungen benötigten Ressourcen (Betriebsmittel, IT-Infrastruktur) sind zu spezifizieren. Es sollte im Detail beschrieben werden, wann und in welchem Umfang sie verfügbar sein müssen.

Wichtig ist, dass alle Betriebssysteme in allen im Produktionsbetrieb eingesetzten Versionen (Releases) in der Testumgebung zur Verfügung stehen. Die Intention ist dabei die Ermittlung von systembedingten Schwachstellen von Komponenten der Produktionsumgebung im Zusammenspiel mit dem zu installierenden Standardsoftwareprodukt. In Ausnahmefällen, wenn sich Aspekte verallgemeinern lassen, kann auf einzelne Komponenten verzichtet werden.

Folgende weitere Aspekte sind unbedingt zu beachten und helfen, eine sichere und geeignete Testumgebung aufzubauen:

- Die Computer-Virenfreiheit der Testumgebung ist durch ein aktuelles Virensuchprogramm sicherzustellen.

- Die Testumgebung muss frei sein von Seiteneffekten auf den Echtbetrieb. Um Wechselwirkungen von vornherein zu vermeiden, empfiehlt es sich, dedizierte IT-Systeme zu installieren.
- Die Zugriffsrechte müssen in der Testumgebung derart konfiguriert werden, wie sie dem Produktionsbetrieb entsprechen.
- Der Zutritt und Zugang zur Testumgebung muss geregelt sein.
- Es muss sichergestellt werden, dass das Produkt genau in der Testumgebung ermittelten Konfiguration in den Produktionsbetrieb übernommen wird. Daher ist in der Testumgebung ein geeignetes Verfahren zum Integritätsschutz einzusetzen (digitale Signaturen, Checksummen).
- Die Kosten für den Aufbau der Testumgebung müssen angemessen sein.

Nach Beendigung aller geplanten Tests ist zu entscheiden, ob die Testumgebung abgebaut werden soll. Ggf. sind weitere Tests auch nach der Beschaffung eines Produktes notwendig, so dass es eventuell wirtschaftlich ist, die Testumgebung vorzuhalten. Vor dem Abbau der Testumgebung sind die Testdaten zu löschen, falls sie nicht mehr benötigt werden (z. B. für eine spätere Installation). Druckerzeugnisse sind ordnungsgemäß zu entsorgen, Programme sind zu deinstallieren. Die Testlizenzen der nicht ausgewählten Produkte sind zurückzugeben.

Inhalt der Testdokumentation

Im Testplan ist vorzugeben, wie ausführlich die Testdokumentation zu erstellen ist. Hierbei sind die Aspekte der Nachvollziehbarkeit, Reproduzierbarkeit und Vollständigkeit zu berücksichtigen.

Die Testdokumentation muss Testpläne, -ziele, -verfahren und -ergebnisse enthalten und die Übereinstimmung zwischen den Tests und den spezifizierten Anforderungen beschreiben. Sämtliche Testaktivitäten sowie die getroffene Testbewertung (inklusive Entscheidungsargumentation) sind schriftlich festzuhalten. Dazu gehören im einzelnen

- Produktbezeichnung und Beschreibung,
- Testbeginn, -ende und -aufwand,
- Testverantwortliche,
- Konfiguration der Testumgebung,
- Beschreibung der Testfälle,
- Entscheidungskriterien, Testergebnisse und Argumentationsketten, und
- nicht erfüllte Anforderungen des Anforderungskataloges.

Der Testgruppe sollte eine Möglichkeit zur übersichtlichen Dokumentation und Protokollierung der Testaktivitäten und -ergebnisse zur Verfügung gestellt werden (z. B. Protokollierungstool, Formblätter o. Ä.).

Wird beim Testen ein automatisiertes Werkzeug verwendet, muss die Testdokumentation ausreichende Informationen über dieses Werkzeug und die Art

seines Einsatzes enthalten, damit die Entscheidung nachvollzogen werden kann.

Festlegung von Entscheidungskriterien

Bei der Bewertung der jeweiligen Testinhalte kann beispielsweise folgende dreistufige Skala verwendet werden:

Note	Entscheidungskriterien	
0	- oder -	Anforderungen sind nicht erfüllt. Es wurden nicht tolerierbare Fehler festgestellt, die sich nicht beheben lassen.
1	- oder -	Anforderungen sind erfüllt, aber es bestehen Vorbehalte (z. B. Funktion ist nur eingeschränkt geeignet). Es sind geringfügige Fehler festgestellt worden. Diese spielen nur eine untergeordnete Rolle, da sie tolerierbare Auswirkungen auf den Produktionsbetrieb haben oder da sie nur mit vernachlässigbarer Wahrscheinlichkeit vorkommen können.
2	- oder -	Anforderungen sind in vollem Umfang erfüllt. Fehler, die ggf. aufgetaucht sind, sind entweder zu beheben oder haben für den Betrieb keinerlei Bedeutung.

Tabelle: Bewertungsskala

Sind Fehler aufgetaucht, die nicht reproduziert werden können, hat der Prüfer zu entscheiden, welcher Kategorie (Note) der Fehler zuzuordnen ist.

Sind Fehler aufgetreten, die während des Tests behoben werden können, ist nach deren Behebung erneut im erforderlichen Umfang zu testen.

Beispiel:

Das Beispiel des Kompressionsprogramms aus M 2.81 *Vorauswahl eines geeigneten Standardsoftwareproduktes* wird hier fortgesetzt, um eine Möglichkeit zu beschreiben, den Prüfaufwand für jede Anforderung des Anforderungskataloges festzulegen. Hier wird der Prüfaufwand aus Prüftiefe und Komplexität abgeleitet. Der Vertrauensanspruch kennzeichnet den Bedarf an Vertrauen in die Eigenschaft.

Die Nutzungshäufigkeit, Fehleranfälligkeit und Komplexität einer Eigenschaft werden wie folgt bewertet:

- 1 bedeutet "niedrig",

- 2 bedeutet "mittel",
- 3 bedeutet "hoch".

Ein besonderer Fall ist gegeben, wenn eine unveränderbare Eigenschaft des Produktes betrachtet werden soll, die unabhängig von der Fehleranfälligkeit oder Nutzungshäufigkeit ist. Für diesen Fall wird der Wert 0 vergeben. Für das Beispiel des Kompressionsprogramms ergibt sich folgende Tabelle:

	Vertrauensanspruch	Fehleranfälligkeit	Nutzungshäufigkeit	Prüftiefe	Komplexität	Prüfaufwand	in %
korrekte Kompression und Dekompression	5	2	3	10	2	20	23
Erkennen von Bitfehlern in einer komprimierten Datei	2	2	1	5	2	10	11
Löschung von Dateien nur nach erfolgreicher Kompression	3	2	1	6	1	6	7
DOS-PC, 80486, 8 MB	5	0	0	5	1	5	6
Windows-tauglich	1	0	0	1	1	1	1
Durchsatz bei 50 MHz über 1 MB/s	3	1	2	6	1	6	7
Kompressionsrate über 40% für Textdateien des Programms XYZ	3	2	2	7	1	7	8
Online-Hilfefunktion	1	1	2	4	1	4	5
Maximale Kosten 50.- DM pro Lizenz	5	0	0	5	1	5	5
Passwortschutz für komprimierte Dateien (Mechanismenstärke hoch)	5	1	2	8	3	24	27

Tabelle: Beispiel für Kompressionsprogramm

In diesem Beispiel wurde der Prüfaufwand folgendermaßen definiert:

Prüfaufwand = Komplexität * Prüftiefe,

dabei ist

Prüftiefe = Vertrauensanspruch + Fehleranfälligkeit + Nutzungshäufigkeit

(Die Prozentzahlen für den Prüfaufwand in der letzten Spalte der Tabelle ergeben sich aus den für den Prüfaufwand errechneten Werten bei Division durch die Summe dieser Werte.)

Ein Beispiel für eine andere Methode, den Prüfaufwand zu berechnen und die Prüfergebnisse zu bewerten, findet sich in der Norm ISO 12119. Hier wird folgende Gewichtung der einzelnen Anforderungen vorgenommen: *Bewertung jedes Prüfinhaltes =(Komplexität+Fehleranfälligkeit) * (Benutzungshäufigkeit + Wichtigkeit)*.

Letztendlich muss der Testverantwortliche eine dem Produkt und der Institution adäquate Bewertungsmethode individuell festlegen.

Nach Erstellung des Testplans wird für jeden im Testplan spezifizierten Testinhalt ein Tester oder eine Testgruppe mit der Durchführung des ihr zugeteilten Tests beauftragt. Der Testplan ist der Testgruppe zu übergeben und die für die Einzeltests vorgegebenen Zeiten sind mitzuteilen.

Ergänzende Kontrollfragen:

- Sind alle für die Testdurchführung benötigten Formblätter und Checklisten erstellt?
- Wurden alle Aufgaben für das Testen zugeteilt?
- Wurden alle Prüfinhalte entsprechend den Vorgaben in Testfälle umgesetzt?

M 2.83 Testen von Standardsoftware

Verantwortlich für Initiierung: Leiter Fachabteilung, Leiter IT

Verantwortlich für Umsetzung: Tester

Das Testen von Standardsoftware lässt sich in die Abschnitte Vorbereitung, Durchführung und Auswertung unterteilen. In diesen Abschnitten sind folgende Aufgaben wahrzunehmen:

Testvorbereitung

- Festlegung der Testmethoden für die Einzeltests (Testarten, -verfahren und -werkzeuge)
- Generierung von Testdaten und Testfällen
- Aufbau der benötigten Testumgebung

Testdurchführung

- Eingangsprüfungen
- Funktionale Tests
- Tests weiterer funktionaler Eigenschaften
- Sicherheitsspezifische Tests
- Pilotanwendung

Testauswertung

Die einzelnen Aufgaben werden nachfolgend beschrieben.

Testvorbereitung

Festlegung der Testmethoden für die Einzeltests (Testarten, -verfahren und -werkzeuge)

Methoden zur Durchführung von Tests sind z. B. statistische Analyse, Simulation, Korrektheitsbeweis, symbolische Programmausführung, Review, Inspektion, Versagensanalyse. Hierbei muss beachtet werden, dass einige dieser Testmethoden nur bei Vorliegen des Quellcodes durchführbar sind. In der Vorbereitungsphase muss die geeignete Testmethode ausgewählt und festgelegt werden.

Es muss geklärt werden, welche Verfahren und Werkzeuge zum Testen von Programmen und zum Prüfen von Dokumenten eingesetzt werden. Typische Verfahren zum Testen von Programmen sind z. B. Black-Box-Tests, White-Box-Tests oder Penetrationstests. Dokumente können z. B. durch informelle Prüfungen, Reviews oder anhand von Checklisten kontrolliert werden.

Ein Black-Box-Test ist ein Funktionalitätstest ohne Kenntnis der internen Programmabläufe, bei dem z. B. das Programm mit allen Datenarten für alle Testfälle mit Fehlerbehandlung und Plausibilitätskontrollen durchlaufen wird.

Bei einem White-Box-Test handelt es sich um einen Funktionalitätstests unter Offenlegung der internen Programmabläufe, z. B. durch Quellcode-Überprüfung oder Tracing. White-Box-Tests gehen in der Regel über den IT-Grundschutz hinaus und können für Standardsoftware in der Regel nicht durchgeführt werden, da der Quellcode vom Hersteller nicht offengelegt wird.

Bei Funktionalitätstests soll der Nachweis erbracht werden soll, dass der Testinhalt der Spezifikation entspricht. Durch Penetrationstests soll festgestellt werden, ob bekannte oder vermutete Schwachstellen im praktischen Betrieb ausgenutzt werden können, beispielsweise durch Manipulationsversuche an den Sicherheitsmechanismen oder durch Umgehung von Sicherheitsmechanismen durch Manipulationen auf Betriebssystemebene.

Weiterhin ist die Art und Weise der Ergebnissicherung und -auswertung festzuschreiben, insbesondere im Hinblick auf die Wiederholbarkeit von Prüfungen. Es muss geklärt werden, welche Daten während und nach der Prüfung festzuhalten sind.

Generierung von Testdaten und Testfällen

Die Vorbereitung von Tests umfasst auch die Generierung von Testdaten. Methode und Vorgehensweise sind zuvor festzulegen und zu beschrieben.

Für jeden einzelnen Testinhalt muss eine dem Testaufwand angemessene Anzahl von Testfällen generiert werden. Jede der folgenden Kategorien ist dabei zu berücksichtigen:

Standardfälle sind Fälle, mit denen die korrekte Verarbeitung der definierten Funktionalitäten überprüft werden soll. Die eingehenden Daten nennt man **Normalwerte** oder **Grenzwerte**. Normalwerte sind Daten innerhalb, Grenzwerte sind Eckdaten des jeweils gültigen Eingabebereichs.

Fehlerfälle sind Fälle, in denen versucht wird, mögliche Fehlermeldungen des Programms zu provozieren. Diejenigen Eingabewerte, auf die das Programm mit vorgegebenen Fehlermeldungen reagieren soll, nennt man **Falschwerte**.

Ausnahmefälle sind Fälle, bei denen das Programm ausnahmsweise anders reagieren muss als bei Standardfällen. Es muss daher überprüft werden, ob das Programm diese Fälle als solche erkennt und korrekt bearbeitet.

Beispiele:

- Wenn die Eingabeparameter zwischen 1 und 365 liegen dürfen, sind Testläufe mit Falschwerten (z. B. 0 oder 1000), den Grenzwerten 1 und 365, sowie mit Normalwerten zwischen 1 und 365 durchführen.
- Ein Programm zur Terminplanung soll Feiertage berücksichtigen. Ein Sonderfall ist dann gegeben, wenn ein bestimmter Tag Feiertag in allen Bundesländern ist, außer in einem. Für dieses Bundesland und für diesen Tag muss das Programm dann differenziert reagieren.

Ist die Generierung von Testdaten zu aufwendig oder schwierig, können auch anonymisierte Echtdaten für den Test eingesetzt werden. Aus Gründen des

Vertraulichkeitsschutzes müssen Echtdaten unbedingt zuverlässig anonymisiert werden. Zu beachten bleibt, dass die anonymisierten Echtdaten u. U. nicht alle Grenzwerte und Ausnahmefälle abdecken, so dass diese gesondert erzeugt werden müssen.

Über die Testdaten hinaus sollten auch alle Arten möglicher Benutzerfehler betrachtet werden. Problematisch sind insbesondere alle Benutzerreaktionen, die im Programmablauf nicht vorgesehen und dementsprechend nicht korrekt abgewiesen werden.

Aufbau der benötigten Testumgebung

Die im Testplan beschriebene Testumgebung muss aufgebaut und die zu testenden Produkte dort installiert werden. Die eingesetzten Komponenten sind zu identifizieren und deren Konfiguration ist zu beschreiben. Treten bei der Installation des Produktes Abweichungen von der beschriebenen Konfiguration auf, so ist dies zu dokumentieren.

Testdurchführung

Die Durchführung der Tests muss anhand des Testplans erfolgen. Jede Aktion sowie die Testergebnisse müssen ausreichend dokumentiert und bewertet werden. Insbesondere wenn Fehler auftreten, sind diese derart zu dokumentieren, dass sie reproduziert werden können. Die für den späteren Produktionsbetrieb geeigneten Betriebsparameter müssen ermittelt und für die spätere Erstellung einer Installationsanweisung festgehalten werden.

Werden zusätzliche Funktionen beim Produkt erkannt, die nicht im Anforderungskatalog aufgeführt, aber trotzdem von Nutzen sein können, so ist hierfür mindestens ein Kurztest durchzuführen. Zeigt sich, dass diese Funktion von besonderer Bedeutung für den späteren Betrieb sind, sind diese ausführlich zu testen. Für den zusätzlich anfallenden Prüfaufwand ist ggf. eine Fristverlängerungen bei den Verantwortlichen zu beantragen. Die Testergebnisse sind in die Gesamtbewertung mit einzubeziehen.

Zeigt sich bei Bearbeitung einzelner Testinhalte, dass eine oder mehrere Anforderungen des Anforderungskataloges nicht konkret genug waren, sind diese gegebenenfalls zu konkretisieren.

Beispiel: Im Anforderungskatalog wird zum Vertraulichkeitsschutz der zu bearbeitenden Daten Verschlüsselung gefordert. Während des Testens hat sich gezeigt, dass eine Offline-Verschlüsselung für den Einsatzzweck ungeeignet. Daher ist der Anforderungskatalog hinsichtlich einer Online-Verschlüsselung zu ergänzen. (Eine Offline-Verschlüsselung muss vom Anwender angestoßen und die zu verschlüsselnden Elemente jeweils spezifiziert werden; eine Online-Verschlüsselung erfolgt transparent für den Anwender mit voreingestellten Parametern.)

Eingangsprüfungen

Vor allen anderen Tests sind zunächst die folgenden grundlegenden Aspekte zu testen, da ein Misserfolg bei diesen Eingangsprüfungen zu direkten Aktionen oder dem Testabbruch führt:

- Die Computer-Virenfreiheit des Produktes ist durch ein aktuelles Virensuchprogramm zu überprüfen.
- In einem Installationstest muss festgestellt werden, ob das Produkt für den späteren Einsatzzweck einfach, vollständig und nachvollziehbar zu installieren ist. Ebenfalls muss überprüft werden, wie das Produkt vollständig deinstalliert wird.
- Die Lauffähigkeit des Produktes ist in der geplanten Einsatzumgebung zu überprüfen; dies beinhaltet insbesondere eine Überprüfung der Bildschirmaufbereitung, der Druckerausgabe, der Mausunterstützung, der Netzfähigkeit, etc.
- Die Vollständigkeit des Produktes (Programme und Handbücher) ist zu überprüfen, z. B. durch einen Vergleich mit dem Bestandsverzeichnis, der Produktbeschreibung oder ähnlichem.
- Es sollten Kurztests von Funktionen des Programms durchgeführt werden, die nicht explizit in den Anforderungen erwähnt wurden, im Hinblick auf Funktion, Plausibilität, Fehlerfreiheit, etc.

Funktionale Tests

Die funktionalen Anforderungen, die im Anforderungskatalog an das Produkt gestellt wurden, sind auf folgende Aspekte zu untersuchen:

- *Existenz der Funktion* durch Aufruf im Programm und Auswertung der Programmdokumentationen.
- Fehlerfreiheit bzw. Korrektheit der Funktion

  Um die Fehlerfreiheit bzw. Korrektheit der Funktion sicherzustellen, sind je nach Prüftiefe bei der Untersuchung unterschiedliche Testverfahren wie Black-Box-Tests, White-Box-Tests oder simulierter Produktionsbetrieb anzuwenden.

  Die in der Vorbereitungsphase erstellten Testdaten und Testfälle werden im Funktionalitätstest eingesetzt. Bei den Funktionalitätstests ist es notwendig, die Testergebnisse mit den vorgegebenen Anforderungen zu vergleichen. Außerdem ist zu überprüfen, wie das Programm bei fehlerhaften Eingabeparametern oder fehlerhafter Bedienung reagiert. Die Funktion ist auch mit den Grenzwerten der Intervalle von Eingabeparametern sowie mit Ausnahmefällen zu testen. Diese müssen entsprechend erkannt und korrekt behandelt werden.
- Eignung der Funktion

  Die Eignung einer Funktion zeichnet sich dadurch aus, dass die Funktion

- tatsächlich die Aufgabe im geforderten Umfang und effizient erfüllt und
- sich leicht in die üblichen Arbeitsabläufe integrieren lässt.

Ist die Eignung der Funktion nicht offensichtlich, bietet es sich an, dies in einem simulierten Produktionsbetrieb, aber immer noch in der Testumgebung zu testen.

- Widerspruchsfreiheit

  Die Widerspruchsfreiheit der einzelnen Funktionen ist zu überprüfen und zwar jeweils zwischen Anforderungskatalog, Dokumentation und Programm. Eventuelle Widersprüche sind zu dokumentieren. Abweichungen zwischen Dokumentation und Programm sind so festzuhalten, dass sie bei einem späteren Einsatz des Produktes in den Ergänzungen zur Dokumentation aufgenommen werden können.

Tests weiterer funktionaler Eigenschaften

Die im Anforderungskatalog neben den funktionalen und den sicherheitsspezifischen Anforderungen spezifizierten weiteren funktionalen Eigenschaften sind ebenfalls zu überprüfen:

- Performance

  Das Laufzeitverhalten sollte für alle geplanten Konfigurationen des Produktes ermittelt werden. Um die Performance ausreichend zu testen, sind in der Regel Tests, in denen der Produktionsbetrieb simuliert wird oder auch Pilotanwendung bei ausgewählten Anwendern sinnvoll. Es muss festgestellt werden, ob die gestellten Performanceanforderungen erfüllt sind.

- Zuverlässigkeit

  Das Verhalten bei zufälligen oder mutwillig herbeigeführten Systemabstürzen ("Crash-Test") ist zu analysieren und es ist festzustellen, welche Schäden dabei entstehen. Es ist festzuhalten, ob nach Systemabstürzen ein ordnungsgemäßer und korrekter Wiederanlauf des Produktes möglich ist. Es ist ebenfalls zu überprüfen, ob ein direkter Zugriff auf Datenbestände unabhängig von der regulären Programmfunktion erfolgen kann. In vielen Fällen kann ein solcher Zugriff zu Datenverlusten führen und sollte dann vom Produkt verhindert werden. Ebenfalls sollte festgehalten werden, ob das Programm Möglichkeiten unterstützt, "kritische Aktionen" (z. B. Löschen, Formatieren) rückgängig zu machen.

- Benutzerfreundlichkeit

  Ob das Produkt benutzerfreundlich ist, ist in besonderem Maße vom subjektiven Empfinden der Testperson abhängig. Jedoch können bei der Beurteilung folgende Aspekte Anhaltspunkte liefern:

  - Technik der Menüoberflächen (Pull-Down-Menüs, Scrolling, Drag & Drop, etc.),

- Design der Menüoberflächen (z. B. Einheitlichkeit, Verständlichkeit, Menüführung),
- Tastaturbelegung,
- Fehlermeldungen,
- problemloses Ansprechen von Schnittstellen (Batchbetrieb, Kommunikation, etc.),
- Lesbarkeit der Benutzerdokumentation,
- Hilfefunktionen.

Die Analyse der Benutzerfreundlichkeit muss mögliche Betriebsarten des Produktes beschreiben, einschließlich des Betriebes nach Bedien- oder Betriebsfehlern, und ihre Konsequenzen und Folgerungen für die Aufrechterhaltung eines sicheren Betriebes.

- Wartbarkeit

  Der personelle und finanzielle Aufwand für die Wartung und Pflege des Produktes sollte während des Testens ermittelt werden. Dieser kann z. B. anhand von Referenzen wie anderen Referenzinstallationen oder Tests in Fachzeitschriften oder anhand des während des Testens ermittelten Installationsaufwandes geschätzt werden. Hierfür muss dokumentiert werden, wie viele manuelle Eingriffe während der Installation notwendig waren, um die angestrebte Konfiguration zu erreichen. Sind bereits Erfahrungen mit Vorgängerversionen des getesteten Produktes gesammelt worden, sollte hinterfragt werden, wie aufwendig deren Wartung war.

  Es sollte nachgefragt werden, inwieweit Support durch den Hersteller oder Vertreiber angeboten wird und zu welchen Konditionen. Wird vom Hersteller oder Vertreiber eine Hotline angeboten, sollte auch deren Erreichbarkeit und Güte betrachtet werden.

- Dokumentation

  Die vorliegende Dokumentation muss daraufhin überprüft werden, ob sie vollständig, korrekt und widerspruchsfrei ist. Darüber hinaus sollte sie verständlich, eindeutig, fehlerfrei und übersichtlich sein.

  Es muss weiterhin kontrolliert werden, ob sie für eine sichere Verwendung und Konfiguration ausreicht. Alle sicherheitsspezifischen Funktionen müssen beschrieben sein.

Darüber hinaus sind als weitere Punkte des Anforderungskatalogs zu testen:

- Kompatibilitätsanforderungen
- Interoperabilität
- Konformität zu Standards
- Einhaltung von internen Regelungen und gesetzlichen Vorschriften
- Softwarequalität

Sicherheitsspezifische Tests

Wurden sicherheitsspezifische Anforderungen an das Produkt gestellt, so sind zusätzlich zu den vorgenannten Untersuchungen auch folgende Aspekte zu untersuchen:

- Wirksamkeit und Korrektheit der Sicherheitsfunktionen,
- Stärke der Sicherheitsmechanismen und
- Unumgänglichkeit und Zwangsläufigkeit der Sicherheitsmechanismen.

Als Grundlage für eine Sicherheitsuntersuchung könnte beispielsweise das Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM) herangezogen werden, in dem viele der nachfolgend aufgezeigten Vorgehensweise beschrieben sind. Die weiteren Ausführungen dienen zur Orientierung und zur Einführung in die Thematik.

Zu Beginn muss durch funktionale Tests zunächst nachgewiesen werden, dass das Produkt die erforderlichen Sicherheitsfunktionen bereitstellt.

Anschließend ist zu überprüfen, ob alle erforderlichen Sicherheitsmechanismen im Anforderungskatalog genannt wurden, ggf. ist dieser zu ergänzen. Um die Mindeststärke der Mechanismen zu bestätigen oder zu verwerfen sind **Penetrationstests** durchzuführen. Penetrationstests sind nach allen anderen Tests durchzuführen, da sich aus diesen Tests Hinweise auf potentielle Schwachstellen ergeben können.

Durch Penetrationstests kann das Testobjekt oder die Testumgebung beschädigt oder beeinträchtigt werden. Damit solche Schäden keine Auswirkungen haben, sollten vor der Durchführung von Penetrationstests Datensicherungen gemacht werden.

Penetrationstests können durch Verwendung von Sicherheitskonfigurations- und Protokollierungstools unterstützt werden. Diese Tools untersuchen eine Systemkonfiguration und suchen nach gemeinsamen Schwachstellen wie etwa allgemein lesbaren Dateien und fehlenden Passwörtern.

Mit Penetrationstests soll das Produkt auf Konstruktionsschwachstellen untersucht werden, indem dieselben Methoden angewandt werden, die auch ein potentieller Angreifer zur Ausnutzung von Schwachstellen benutzen würde, wie z. B.

- Ändern der vordefinierten Befehlsabfolge,
- Ausführen einer zusätzlichen Funktion,
- Direktes oder indirektes Lesen, Schreiben oder Modifizieren interner Daten,
- Ausführen von Daten, deren Ausführung nicht vorgesehen ist,
- Verwenden einer Funktion in einem unerwarteten Kontext oder für einen unerwarteten Zweck,
- Aktivieren der Fehlerüberbrückung,

- Nutzen der Verzögerung zwischen dem Zeitpunkt der Überprüfung und dem Zeitpunkt der Verwendung,
- Unterbrechen der Abfolge durch Interrupts, oder
- Erzeugen einer unerwarteten Eingabe für eine Funktion.

Die Mechanismenstärken werden anhand der Begriffe Fachkenntnisse, Gelegenheiten und Betriebsmittel definiert, in der ITSEM werden diese näher erläutert. Beispielsweise können zur Bestimmung der Mechanismenstärke folgende Regeln angewandt werden:

- Kann der Mechanismus innerhalb von Minuten von einem Laien allein überwunden werden, dann kann er **nicht einmal als niedrig** eingestuft werden.
- Kann ein erfolgreicher Angriff von jedem bis auf einen Laien innerhalb von Minuten durchgeführt werden, dann ist der Mechanismus als **niedrig** einzustufen.
- Wenn für einen erfolgreichen Angriff ein Experte benötigt wird, der mit der vorhandenen Ausstattung Tage braucht, dann ist der Mechanismus als **mittel** einzustufen.
- Kann der Mechanismus nur von einem Experten mit Sonderausstattung überwunden werden, der dafür Monate braucht und eine geheime Absprache mit einem Systemverwalter treffen muss, dann ist er als **hoch** einzustufen.

Es muss sichergestellt werden, dass die durchgeführten Tests alle sicherheitsspezifischen Funktionen umfassen. Wichtig ist zu beachten, dass durch Testen immer nur Fehler oder Abweichungen von den Spezifikationen festgestellt werden können, niemals jedoch die Abwesenheit von Fehlern.

An einigen **Beispielen** sollen typische Untersuchungsaspekte aufgezeigt werden:

Passwortschutz:

- Gibt es vom Hersteller voreingestellte Passwörter? Typische Beispiele für solche Passwörter sind der Produktname, der Herstellername, "SUPERVISOR", "ADMINISTRATOR", "USER", "GUEST".
- Welche Datei ändert sich, wenn ein Passwort geändert wurde? Kann diese Datei durch eine alte Version aus einer Datensicherung ersetzt werden, um alte Passwörter zu aktivieren? Werden die Passwörter verschlüsselt gespeichert oder sind sie im Klartext auslesbar? Ist es möglich, in dieser Datei Änderungen vorzunehmen, um neue Passwörter zu aktivieren?
- Wird der Zugang tatsächlich nach mehreren fehlerhaften Passworteingaben gesperrt?
- Werden in Zeitschriften oder Mailboxen Programme angeboten, die die Passwörter des untersuchten Produkts ermitteln können? Für einige Standardapplikationen sind solche Programme erhältlich.

- Wenn Dateien mit Passwörtern geschützt werden, kann durch einen Vergleich einer Datei vor und nach der Passwortänderung die Stelle ermittelt werden, an der das Passwort gespeichert wird. Ist es möglich, an dieser Stelle Änderungen oder alte Werte einzugeben, um bekannte Passwörter zu aktivieren? Werden die Passwörter verschlüsselt gespeichert? Wie ist die Stelle belegt, wenn der Passwortschutz deaktiviert ist?
- Kann die Passwort-Prüfroutine unterbrochen werden? Gibt es Tastenkombinationen, mit denen die Passworteingabe umgangen werden kann?

Zugriffsrechte:

- In welchen Dateien werden Zugriffsrechte gespeichert und wie werden sie geschützt?
- Können Zugriffsrechte von Unberechtigten geändert werden?
- Können Dateien mit alten Zugriffsrechten zurückgespielt werden und welche Rechte benötigt man dazu?
- Können die Rechte des Administrators so eingeschränkt werden, dass er keinen Zugriff auf die Nutz- oder Protokolldaten erhält?

Datensicherung:

- Können erstellte Datensicherungen problemlos rekonstruiert werden?
- Können Datensicherungen durch ein Passwort geschützt werden? Wenn ja, können die oben dargestellten Untersuchungsansätze für Passwörter eingesetzt werden.

Verschlüsselung:

- Bietet das Produkt an, Dateien oder Datensicherungen zu verschlüsseln?
- Werden mehrere verschiedene Verschlüsselungsalgorithmen angeboten? Hierbei ist im allgemeinen folgende Faustregel zu beachten: "Je schneller ein in Software realisierter Verschlüsselungsalgorithmus ist, um so unsicherer ist er."
- Wo werden die zur Ver- oder Entschlüsselung genutzten Schlüssel gespeichert?

  Bei einer lokalen Speicherung ist zu untersuchen, ob diese Schlüssel passwortgeschützt oder mit einem weiteren Schlüssel überschlüsselt geschützt werden. Bei einem **Passwortschutz** sind die obigen Punkte zu berücksichtigen. Bei einer Überschlüsselung ist zu betrachten, wie der zugehörige Schlüssel geschützt wird.

  Dazu können folgende Punkte betrachtet werden: Welche Datei ändert sich, wenn ein Schlüssel geändert wurde? Durch den Vergleich dieser Datei vor und nach der Schlüsseländerung kann die Stelle ermittelt werden, an der dieser Schlüssel gespeichert wird. Ist es möglich, an dieser Stelle Änderungen vorzunehmen, um neue Schlüssel zu aktivieren, die dann vom Anwender genutzt werden, ohne dass dieser die Kompromittierung bemerkt?

- Gibt es vom Hersteller voreingestellte Schlüssel, die vor der erstmaligen Benutzung des Programms geändert werden müssen?
- Was passiert, wenn bei der Entschlüsselung ein falscher Schlüssel eingegeben wird?
- Wird nach der Verschlüsselung einer Datei die unverschlüsselte Variante gelöscht? Wenn ja, wird sie zuverlässig überschrieben? Wird vor der Löschung überprüft, ob die Verschlüsselung erfolgreich war?

Protokollierung:

- Wird der Zugriff auf Protokolldaten für Unbefugte verwehrt?
- Werden die zu protokollierenden Aktivitäten lückenlos aufgezeichnet?
- Hat der Administrator die Möglichkeit aufgrund seiner privilegierten Rechte, sich unberechtigt und unbemerkt Zugriff auf Protokolldaten zu verschaffen oder kann er die Protokollierung unbemerkt deaktivieren?
- Wie reagiert das Programm, wenn der Protokollierungsspeicher überläuft?

Darüber hinaus muss festgestellt werden, ob durch das neue Produkt Sicherheitseigenschaften an anderer Stelle unterlaufen werden. **Beispiel:** das zu testende Produkt bietet eine Schnittstelle zur Betriebssystemumgebung, das IT-System war aber vorher so konfiguriert, dass keine solchen Schnittstellen existierten.

Pilotanwendung

Nach Abschluss aller anderen Tests kann noch eine Pilotanwendung, also ein Einsatz unter Echtbedingungen, für notwendig gehalten werden.

Erfolgt der Test in der Produktionsumgebung mit Echtdaten, muss vorab durch eine ausreichende Anzahl von Tests die korrekte und fehlerfreie Funktionsweise des Programms bestätigt worden sein, um die Verfügbarkeit und Integrität der Produktionsumgebung nicht zu gefährden. Dabei kann das Produkt beispielsweise bei ausgewählten Benutzern installiert werden, die es dann für einen gewissen Zeitraum im echten Produktionsbetrieb einsetzen.

Testauswertung

Anhand der festgelegten Entscheidungskriterien sind die Testergebnisse zu bewerten, alle Ergebnisse zusammenzuführen und mit der Testdokumentation der Beschaffungsstelle bzw. Testverantwortlichen vorzulegen.

Anhand der Testergebnisse sollte ein abschließendes Urteil für ein zu beschaffendes Produkt gefällt werden. Hat kein Produkt den Test bestanden, muss überlegt werden, ob eine neue Marktsichtung vorgenommen werden soll, ob die gestellten Anforderungen zu hoch waren und geändert werden müssen oder ob von einer Beschaffung zu diesem Zeitpunkt abgesehen werden muss.

Beispiel:

Am Beispiel eines Kompressionsprogramms wird nun eine Möglichkeit beschrieben, Testergebnisse auszuwerten. Getestet wurden vier Produkte, die nach der dreistufigen Skala aus M 2.82 *Entwicklung eines Testplans für Standardsoftware* bewertet wurden.

Eigenschaft	Notwendig/ wünschenswert	Bedeutung	Produkt 1	Produkt 2	Produkt 3	Produkt 4
korrekte Kompression und Dekompression	N	10	2	2	j	0
Erkennen von Bitfehlern in einer komprimierten Datei	N	10	2	2	n	2
Löschung von Dateien nur nach erfolgreicher Kompression	N	10	2	2	j	2
DOS-PC, 80486, 8 MB	N	10	2	2	j	2
Windows-tauglich	W	2	0	2	j	2
Durchsatz bei 50 MHz über 1 MB/s	W	4	2	2	j	2
Kompressionsrate über 40%	W	4	2	1	n	0
Online-Hilfefunktion	W	3	0	0	n	2
Passwortschutz für komprimierte Dateien	W	2	2	1	n	2
Bewertung			100	98	K.O.	K.O.
Preisermittlung (maximale Kosten 50.- € pro Lizenz)			49,- €	25,- €		39,- €

Tabelle: Testplan für Standardsoftware

Produkt 3 war bereits in der Vorauswahl gescheitert und wurde daher nicht getestet.

Produkt 4 scheiterte in dem Testabschnitt "korrekte Kompression und Dekompression", weil die Erfüllung der Eigenschaft mit 0 bewertet wurde, es sich dabei aber um eine notwendige Eigenschaft handelt.

Bei der Berechnung der Bewertungspunktzahlen für die Produkte 1 und 2 wurden die Noten als Multiplikatoren für die jeweilige Bedeutungskennzahl benutzt und schließlich die Summe gebildet:

Produkt 1: 10*2+10*2+10*2+10*2+2*0+4*2+4*2+2*2 = 120

Produkt 2: 10*2+10*2+10*2+10*2+2*2+4*2+4*1+2*1 = 118

Nach der Testauswertung ist somit Produkt 1 auf dem ersten Platz, wird aber knapp gefolgt von Produkt 2. Die Entscheidung für ein Produkt hat jetzt die Beschaffungsstelle anhand der Testergebnisse und des daraus resultierenden Preis-/Leistungsverhältnisses zu treffen.

Ergänzende Kontrollfragen:

- Ist die benutzte Hardware- und Softwarekonfiguration konform zum Anforderungskatalog?
- Bieten Hersteller oder Vertreiber Unterstützung oder Wartungsdienste bei der Anwendung des Produktes?
- Sind in der Benutzerdokumentation alle für den Benutzer relevanten Funktionen vollständig und verständlich beschrieben?
- Enthalten die vorliegenden Dokumentationen Inhaltsverzeichnis, Stichwortverzeichnis und Seitenangaben?
- Sind alle geforderten Funktionen ausführbar und korrekt?
- Ist das Produkt in seiner Einsatzumgebung zuverlässig und robust? Können unter Grenzbelastungen oder bei Fehlbedienung Daten verfälscht oder zerstört werden?
- Werden unzulässige und nicht definierte Eingaben wie zulässige verarbeitet?
- Wurden Testdokumentationen entsprechend den Vorgaben angefertigt?

M 2.84 Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Leiter IT, Leiter Fachabteilung, Beschaffungsstelle

Nach Abschluss aller Tests müssen die Testergebnisse der Beschaffungsstelle vorgelegt werden. Die Entscheidung für ein Produkt hat jetzt die Beschaffungsstelle unter Beteiligung der Leiter der Fachabteilung und des IT-Bereichs aufgrund der Testergebnisse und des daraus resultierenden Preis-/Leistungsverhältnisses zu treffen. Hierbei ist insbesondere der Erfüllungsgrad der einzelnen Produkte gegenüber dem Anforderungskatalog in Relation zum Kaufpreis zu stellen. Auch sollten zusätzliche Funktionen der Produkte, die nicht im Anforderungskatalog aufgeführt wurden, aber dennoch für den Einsatz sinnvoll sind, bei der Entscheidung berücksichtigt werden.

Erstellen einer Installationsanweisung

Nach der Entscheidung für ein Produkt muss anschließend für das ausgewählte Produkt eine Installationsanweisung erstellt werden. Während des Testens wurde diejenige Konfiguration des Produktes ermittelt, die einen sicheren und effizienten Produktionsbetrieb erlaubt. Damit soll Benutzerfreundlichkeit, Ordnungsmäßigkeit und Sicherheit am Arbeitsplatz sichergestellt werden.

Um die geeignete Konfiguration des Produktes im Wirkbetrieb sicherzustellen, müssen bestimmte Parameter vorgegeben werden. Teilweise muss dies durch organisatorische Regelungen begleitet werden.

Für einige Eigenschaften eines Produktes wird im folgenden beispielhaft aufgezeigt, was im Rahmen einer Installationsanweisung vorgegeben werden kann.

Beispiel:

Benutzerfreundlichkeit:

- Mit dem Produkt sind die Treiber X, Y und Z (Bildschirm, Drucker, Maus, Netz) zu installieren, um eine für den Benutzer akzeptable Arbeitsumgebung zu schaffen (Bildschirm flimmerfrei, vernünftige Druckaufbereitung, etc.).
- Diejenigen Einstellungen, bei denen einzelne Funktionen die größte Verarbeitungsgeschwindigkeit haben, sind vorzugeben, wenn nicht andere Kriterien wie Sicherheit dagegen sprechen (die Größe der Auslagerungsdateien ist auf mindestens 10 MB festzusetzen, die Option Verifikation ist für die Datensicherung zu aktivieren, obwohl die Verifikation zusätzlichen Zeitaufwand erfordert).

Sicherheit:

- Die Parameter für Sicherheitsfunktionen sind voreinzustellen (z. B. die Mindestlänge von Passwörtern muss festgelegt werden (siehe dazu auch M 2.11 *Regelung des Passwortgebrauchs*), Datensicherungen sind täglich zu erstellen, die Protokollierung ist im vollen Umfang zu akti-

vieren, Zugriffsrechte auf personenbezogene Protokolldateien sind nur dem Datenschutzbeauftragten einzurichten, ...).

- Werden mehrere sicherheitsrelevante Verfahren unterstützt (z. B. Verschlüsselungsalgorithmus, Hashfunktionen), sind diejenigen auszuwählen, mit denen ein angemessenes Schutzniveau erreicht wird (zur Auswahl siehe M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*).

Funktion:

- Nur die Funktionen X, Y, und Z sind zu aktivieren, unerwünschte oder nicht benötigte Funktionen sind abzuschalten.
- Die Funktion der automatischen Datensicherung ist mit dem Parameter "alle 10 Minuten" zu aktivieren.

Organisation:

- Die Installation ist vom Administrator durchzuführen.
- Regelungen für den Betrieb müssen erlassen werden (z. B. Datensicherungen sind eigenverantwortlich vom Anwender durchzuführen, Passwörter müssen nach 30 Tagen gewechselt werden).

Randbedingungen:

- Die Konfiguration der Plattform, auf der das Standardsoftwareprodukt zum Einsatz kommen soll, muss insbesondere dann beschrieben und vorgegeben werden, wenn systembedingte Schwachstellen der Plattform damit beseitigt werden.

Ergänzende Kontrollfragen:

- Sind in der Installationsanweisung alle Angaben für eine erfolgreiche Installation enthalten?
- Sind Angaben enthalten, wie das Produkt wieder deinstalliert wird?

M 2.85 Freigabe von Standardsoftware

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Leiter Fachabteilung, Leiter IT

Vor der Übernahme der Standardsoftware in den Wirkbetrieb steht die formelle Freigabe. Verantwortlich für die Freigabe eines Produktes ist die Behörden- bzw. Unternehmensleitung, sie kann dies aber an die Leitung der Fachabteilung oder die Leitung des IT-Bereichs delegieren. Die Fachabteilung kann die durch Behörden- bzw. Unternehmensleitung vorgegebene Freigaberegelung durch eigene Restriktionen weiter einschränken. Der Einsatz nicht freigegebener Software ist zu untersagen (siehe M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*).

Der Freigabe geht immer der erfolgreiche Abschluss aller notwendigen Tests voraus (siehe M 2.83 *Testen von Standardsoftware*). Eine Freigabe darf nicht erfolgen, wenn während der Tests nicht tolerierbare Fehler, z. B. erhebliche Sicherheitsmängel, festgestellt wurden.

Für die Freigabe sind Installations- bzw. Konfigurationsvorschriften zu erarbeiten, deren Detaillierungsgrad davon abhängig ist, ob die Installation durch die Systemadministration oder den Benutzer vorgenommen werden soll. Die Installations- bzw. Konfigurationsvorschriften sind Ergebnisse der im Rahmen der Beschaffung durchgeführten Tests (siehe M 2.83 *Testen von Standardsoftware*). Wenn unterschiedliche Konfigurationen zulässig sind, muss die Auswirkung der einzelnen Konfigurationen auf die Sicherheit dargelegt werden. Insbesondere muss festgelegt werden, ob für alle oder nur einige Benutzer Einschränkungen der Produktfunktionalität oder der Zugriffsrechte vorzunehmen sind. Für die Festlegung dieser Randbedingungen sind der Personal- bzw. Betriebsrat, der Datenschutzbeauftragter sowie der IT-Sicherheitsbeauftragte rechtzeitig zu beteiligen.

Die Freigabe sollte in Form einer schriftlichen **Freigabeerklärung** erfolgen. In der Freigabeerklärung sollten Aussagen gemacht werden zu den folgenden Punkten:

- Programmname und Versionsnummer,
- Bezeichnung des IT-Verfahrens, in dem das Produkt eingesetzt werden soll,
- Bestätigung, dass die eingesetzten IT-Komponenten den fachlichen Anforderungen entsprechen,
- Datum der Freigabe, Unterschrift des Freigabe-Verantwortlichen,
- Unbedenklichkeitserklärung seitens IT-Sicherheitsbeauftragter, Datenschutzbeauftragter, Personal- bzw. Betriebsrat,
- vorgesehener Zeitpunkt des Einsatzes im Wirkbetrieb,
- für welche Benutzer das Produkt freigegeben wird,
- Installationsanweisung, insbesondere an welchen Arbeitsplätzen es mit welcher Konfiguration installiert wird,

- wer berechtigt ist, es zu installieren,
- wer Zugriff auf die Installationsdatenträger hat und
- welche Schulungen vor Nutzung des Produktes vorzunehmen sind.

Die Freigabeerklärung muss allen Beteiligten zur Kenntnis gegeben werden, insbesondere sollten bei der Freigabeinstanz, dem IT-Bereich, der Fachabteilung und ggf. beim IT-Anwender Kopien vorhanden sein.

Darüber hinaus ist organisatorisch zu regeln, dass die Freigabe und ggf. die notwendigen Tests wiederholt werden, wenn sich durch Versionswechsel oder Patches grundlegende Eigenschaften, insbesondere im Bereich der Sicherheitsfunktionen, geändert haben. Änderungen der genannten Art sind dem für die Freigabe des Produktes Verantwortlichen mitzuteilen.

Weiterhin kann festgelegt werden, welche Standardsoftware-Produkte, abhängig vom Einsatzort und -zweck, generell freigegeben werden. Voraussetzung ist, dass sie zumindest auf Computer-Viren geprüft, dass die Lizenzfragen geklärt und dass sie registriert sind. Beispiele hierfür wären:

- Demo-Versionen zu Testzwecken, die auf speziellen Rechnern zur Verfügung gestellt werden,
- Public-Domain-Software, die auf speziellen Servern installiert werden,
- Spielprogramme auf speziellen Rechnern, die in Pausenräumen aufgestellt werden.

Ergänzende Kontrollfragen:

- Wo werden die Freigabeerklärungen verwaltet und hinterlegt?
- Ist eine Installationsanweisung vorhanden?
- Ist sichergestellt, dass sämtliche Software der Freigabeprozedur unterzogen wird?

M 2.86 Sicherstellen der Integrität von Standardsoftware

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Leiter IT

Es ist sicherzustellen, dass die freigegebene Standardsoftware nur unverändert installiert werden kann. Damit soll verhindert werden, dass zwischenzeitlich gewollte oder ungewollte Veränderungen vorgenommen werden können, z. B. durch Computer-Viren, Bitfehler aufgrund technischer Fehler oder Manipulationen in Konfigurationsdateien.

Die Installation darf daher ausschließlich von Originaldatenträgern bzw. von nummerierten Kopien der Originaldatenträger erfolgen. Eine Alternative zur lokalen Installation von Datenträgern ist die Installation über ein lokales Netz von einer dafür freigegebenen Version. Dabei sollte sichergestellt sein, dass nur berechtigte Personen darauf Zugriff haben.

Von den Originaldatenträgern sollten, falls der Datenumfang (z. B. CD-ROM) es zulässt, Sicherungskopien angefertigt werden. Originaldatenträger und alle Kopien müssen vor unberechtigtem Zugriff geschützt aufbewahrt werden (siehe M 6.21 *Sicherungskopie der eingesetzten Software*). Die angefertigten Kopien sollten nummeriert und in Bestandsverzeichnisse aufgenommen werden. Kopien, die nicht mehr benötigt werden, sind zu löschen. Vor der Installation muss eine Computer-Virenprüfung durchgeführt werden.

Optional kann über die Originaldatenträger oder über eine während des Tests installierte Referenzversion eine Checksumme (siehe M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*) gebildet werden, anhand derer vor der Installation die Integrität der dafür eingesetzten Datenträger bzw. der in lokalen Netzen hinterlegten Versionen oder anhand derer die korrekte Installation überprüft werden kann. Darüber hinaus können installierten Programme zusätzlich zum Schutz vor unberechtigten Veränderungen der freigegebenen Konfiguration mit Checksummen versehen werden. Auf diese Weise können auch Infektionen mit bisher unbekannten Computer-Viren erkannt werden. Damit kann auch festgestellt werden, ob eine Vireninfektion vor oder nach der Installation stattgefunden hat.

Ergänzende Kontrollfragen:

- Auf welche Art wird die Integrität der Standardsoftware sichergestellt?
- Werden periodisch Kontrollen durchgeführt, um die Integrität der installierten Programme zu überprüfen?
- Werden Manipulationsversuche an Programmen und Daten festgestellt?

M 2.87 Installation und Konfiguration von Standardsoftware

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator

Die freigegebene Software wird entsprechend der Installationsanweisung auf den dafür vorgesehenen IT-Systemen installiert. Die Installationsanweisung beinhaltet neben den zu installierenden Programmen auch Konfigurationsparameter und die Einrichtung der Hardware- und Softwareumgebung.

Abweichungen von der Installationsanweisung bedürfen der Zustimmung der Freigabeinstanz.

Wenn die Benutzer die Software selbst installieren sollen, muss ihnen eine Installationsanweisung zur Verfügung gestellt werden, die eine selbständige Installation ermöglicht. Mindestens die Pilot-Installation durch einen ausgewählten typischen Benutzer sollte durch die IT-Abteilung begleitet werden, um die Verständlichkeit der Installationsanweisung zu überprüfen.

Da Standardsoftware für eine Vielzahl von Einsatzfelder entwickelt wird, enthält sie meist mehr Funktionen, als für die Erfüllung der Fachaufgabe benötigt werden. Damit es zu weniger Problemen und Fehlern bei der Arbeit mit der Software kommt, sollten nur die tatsächlich benötigten Funktionalitäten installiert werden. Funktionalitäten, die zu Sicherheitsproblemen führen können, dürfen nicht freigegeben werden.

Sowohl vor als auch nach der Installation von Software sollte eine vollständige Datensicherung durchgeführt werden. Die erste Datensicherung kann bei nachfolgenden Problemen während der Installation zur Wiederherstellung eines konsolidierten Aufsetzpunktes verwendet werden. Nach der erfolgreichen Installation sollte erneut eine vollständige Datensicherung durchgeführt werden, damit bei späteren Problemen wieder auf den Zustand nach der erfolgreichen Installation des Produktes aufgesetzt werden kann.

Die erfolgreiche Installation wird schriftlich an die für die Aufnahme des Wirkbetriebes zuständige Stelle gemeldet.

Optional kann die Installation durch den Einsatz eines sog. "Delta-Tools" begleitet werden, das alle Veränderungen in einer IT-Umgebung zwischen zwei bestimmbaren Zeitpunkten dokumentiert. Diese Dokumentation von Veränderungen ist insbesondere bei der Deinstallation der Software hilfreich.

Beim Einsatz eines neuen Produktes müssen evtl. Datenbestände übernommen werden, die mit einem Vorgängerprodukt erzeugt wurden. Hat sich bei den Tests gezeigt, dass es dabei zu Schwierigkeiten kommen kann, sind Hilfestellungen für die Benutzer zu erarbeiten oder die Übernahme von alten Datenbeständen ist zentral durch geschultes Personal durchzuführen.

Ergänzende Kontrollfragen:

- Welche Regelungen sind in Kraft?
- Welche Regelungen bestehen bezüglich möglicher Abweichungen von der Installationsanweisung?
- Wie wird der Erfolg einer Installation überprüft?

M 2.88 Lizenzverwaltung und Versionskontrolle von Standardsoftware

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Leiter IT, Leiter Organisation

Ohne eine geeignete Versionskontrolle und Lizenzkontrolle kommt es erfahrungsgemäß schnell zur Verwendung verschiedenster Versionen auf einem IT-System oder innerhalb einer Organisationseinheit, von denen evtl. einige ohne Lizenz benutzt werden.

Auf allen IT-Systemen einer Institution darf ausschließlich lizenzierte Software eingesetzt werden. Diese Regelung muss allen Mitarbeitern bekanntgemacht werden, die Administratoren der verschiedenen IT-Systeme müssen sicherstellen, dass nur lizenzierte Software eingesetzt wird. Dafür müssen sie mit geeigneten Werkzeugen zur Lizenzkontrolle ausgestattet werden.

Häufig werden in einer Institution verschiedene Versionen einer Standardsoftware eingesetzt. Im Rahmen der Lizenzkontrolle muss es auch möglich sein, einen Überblick über alle eingesetzten Versionen zu erhalten. Damit kann gewährleistet werden, dass alte Versionen durch neuere ersetzt werden, sobald dies notwendig ist, und dass bei der Rückgabe von Lizenzen alle Versionen gelöscht werden.

Darüber hinaus sind die verschiedenen Konfigurationen der installierten Software zu dokumentieren. Damit muss es möglich sein, sich einen Überblick zu verschaffen, an welchem IT-System welche sicherheitsrelevanten Einstellungen eines Standardsoftwareproduktes durch die Freigabe vorgegeben und welche tatsächlich installiert wurden. Damit kann z. B. schnell geklärt werden, an welchen Rechnern beim Produkt XYZ die Makro-Programmierung installiert worden ist und an welchen nicht.

Ergänzende Kontrollfragen:

- Welche Regelungen sind in Kraft?
- Sind verschiedene Versionen eines Standardsoftwareproduktes im Einsatz?

M 2.89 Deinstallation von Standardsoftware

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator

Bei der Deinstallation von Software müssen alle Dateien entfernt werden, die für den Betrieb der Software auf dem IT-System angelegt worden sind, und alle Einträge in Systemdateien, die bezüglich des Produktes vorgenommen wurden, gelöscht werden. Bei vielen Softwareprodukten werden während der Installation in diversen Verzeichnissen auf dem IT-System Dateien angelegt oder bestehende Dateien verändert. Häufig wird der Benutzer nicht einmal über alle bei der Installation durchgeführten Veränderungen am IT-System informiert.

Um eine vollständige Deinstallation durchführen zu können, ist es daher hilfreich, die bei der Installation durchgeführten Systemänderungen nachzuhalten, entweder manuell oder mit Hilfe von speziellen Tools. Wird dies nicht vorgenommen, kommt es erfahrungsgemäß dazu, dass eine Deinstallation nur rudimentär stattfindet oder dass sie unterlassen wird aus Furcht, wichtige Dateien bei der Deinstallation zu löschen.

Ergänzende Kontrollfragen:

- Werden Stichproben durchgeführt, ob bei einem Versionswechsel die Vorgängerversion vollständig deinstalliert wird?

M 2.90 Überprüfung der Lieferung

Verantwortlich für Initiierung: Leiter IT, Leiter Organisation

Verantwortlich für Umsetzung: Beschaffungsstelle

Nach Eingang einer Lieferung ist anhand der vorhandenen Unterlagen zu überprüfen,

- ob die Lieferung bestellt wurde,
- für wen sie bestimmt ist,
- ob Transportschäden zu erkennen sind,
- ob sie vollständig ist, d. h. ob einerseits alle bestellten Komponenten und andererseits alle gemäß Produktbeschreibung zum Lieferumfang des Produktes gehörenden Komponenten vorhanden sind.

Die Ergebnisse dieser Prüfungen sind in einem Wareneingangsverzeichnis zu dokumentieren, zusammen mit:

- Produktname und Version,
- Produktart, z. B. Textverarbeitung,
- Lieferumfang, also Beschreibung der einzelnen Komponenten inklusive Anzahl und Lieferform (Buch, Diskette, CD-ROM, ...),
- Lieferdatum,
- Lieferart,
- wer es in Empfang genommen hat,
- Aufbewahrungsort und
- an wen es weitergegeben wurde.

Für die Durchführung der funktionalen Tests, sowie die anschließende formelle Freigabe, die Installation und Konfiguration müssen die gelieferten Produkte an die IT-Abteilung weitergegeben werden.

Werden die Produkte nur vorübergehend eingesetzt oder zur Verfügung gestellt, z. B. im Rahmen von Tests, müssen zumindest die Seriennummer und andere produktspezifische Identifizierungsmerkmale in entsprechende Bestandsverzeichnissen vermerkt werden. Wenn die gelieferten Produkte für den dauerhaften Verbleib vorgesehen sind, sind sie mit eindeutigen Identifizierungsmerkmalen (z. B. gruppierte fortlaufende Inventarnummern) zu kennzeichnen. Anschließend müssen sie in ein Bestandsverzeichnis aufgenommen werden. Dieses muss Auskunft geben können über:

- Identifizierungsmerkmale,
- Beschaffungsquellen, Lieferzeiten,
- Verbleib,
- Freigabedatum,
- Installationsdatum und Konfigurationsbesonderheiten und

- Wartungsverträge, Wartungsintervalle.

Ergänzende Kontrollfragen:

- Welche Regelungen zum Wareneingang von informationstechnischen Produkten sind in Kraft?
- Wie wird verfahren, wenn unvollständige Lieferungen festgestellt werden?
- Sind schon häufiger unvollständige Lieferungen auffällig geworden?

M 2.91 Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Bevor mit der eigentlichen Konfiguration und Installation von Windows NT in einem Client-Server-Netz begonnen werden kann, müssen zuerst zwei grundlegende Überlegungen angestellt werden:

Zunächst muss geklärt werden, welche Dienstleistung das Betriebssystem erbringen und in welchem Rahmen es diesbezüglich eingesetzt werden soll.

Dies soll anhand einiger **Beispiele** veranschaulicht werden:

- Das System wird in einem servergestützten PC-Netz als Server für eine größere Arbeitsgruppe eingesetzt, in der unterschiedliche Rechte vergeben werden können. Ggf. sollen aufgrund konkreter Anforderungen zusätzlich Peer-to-Peer-Funktionalitäten in eingeschränkter Form realisiert werden. Beispielsweise sollen einzelne Drucker über Peer-to-Peer-Funktionalität gemeinsam benutzt werden können.
- Das System wird als Client in einem servergestützten PC-Netz mit Windows NT Servern eingesetzt, bei dem auf die Peer-to-Peer-Funktionalität zum Austausch von Daten verzichtet werden kann.
- Das System wird als Client in einem servergestützten PC-Netz mit Novell Netware Servern eingesetzt.
- Das System wird als Server in einem PC-Netz mit MS-DOS-, MS-Windows-, WfW- oder Windows 95-Clients eingesetzt.
- Das System wird als Server in einem Netz eingesetzt, in dem ausschließlich Windows NT-Clients vorhanden sind.

Durch die Verwendung von Peer-to-Peer-Funktionalitäten innerhalb eines Windows NT Netzes können zusätzliche Sicherheitsprobleme entstehen (siehe dazu auch Baustein B 5.1 *Peer-to-Peer-Dienste*). **Deshalb sollte auf die Verwendung von Peer-to-Peer-Funktionalitäten innerhalb von Windows NT Netzen verzichtet werden.** Peer-to-Peer-Funktionalitäten sollten höchstens als Übergangslösung eingeschränkt zugelassen werden, wenn z. B. WfW-Rechner oder nicht-netzfähige Drucker in das Windows NT-Netz eingebunden werden sollen.

Anschließend müssen diese Überlegungen in eine Sicherheitsstrategie übersetzt werden.

Dabei zeigt sich, dass je nach bereits vorhandener Systemumgebung und Organisationsstruktur sowie der ggf. vorzusehenden Restriktionen an eventuelle Peer-to-Peer-Funktionalitäten ein mehr oder weniger großer Aufwand bei der Entwicklung einer dazu passenden Sicherheitsstrategie notwendig ist.

Es wird nachfolgend eine methodische Vorgehensweise aufgezeigt, mittels derer eine umfassende Sicherheitsstrategie für ein Client-Server-Netz entwickelt werden kann. Da jedoch Windows NT in verschiedenen Konfigu-

rationen eingesetzt werden kann, ist für die jeweilige Ausprägung individuell zu entscheiden, welche der beschriebenen Schritte anzuwenden sind.

Festlegung einer Sicherheitsstrategie für ein Client-Server-Netz

In der Sicherheitsstrategie muss aufgezeigt werden, wie ein Client-Server-Netz für die jeweilige Organisation sicher aufgebaut, administriert und betrieben wird. Nachfolgend werden die einzelnen Entwicklungsschritte einer solchen Strategie vorgestellt:

1. Definition der Client-Server-Netzstruktur

Im ersten Schritt sind die logische Struktur des Client-Server-Netzes, insbesondere die Zuordnung der Server und der Netz-Domänen festzulegen (siehe M 2.93 *Planung des Windows NT Netzes*). Nach Möglichkeit sollte auf die Verwendung von Peer-to-Peer-Funktionalitäten verzichtet werden, da diese die Sicherheit des Client-Server-Netzes beinträchtigen können. Sofern sich dies jedoch nicht vermeiden lässt, sind verbindliche Regelungen für die Nutzung von Peer-to-Peer-Funktionalitäten zu treffen (siehe M 2.67 *Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste*).

2. Regelung der Verantwortlichkeiten

Ein Client-Server-Netz sollte von einem geschulten Netzadministrator nebst Stellvertreter sicher betrieben werden. Diese allein dürfen Sicherheitsparameter im Netz verändern. Sie sind z. B. dafür zuständig, auf den Servern den entsprechenden Verantwortlichen Administrationsrechte und -werkzeuge zur Verfügung zu stellen, damit diese die Vergabe von Datei- und Verzeichnisberechtigungen, die Freigabe der von anderen benötigten Verzeichnissen bzw. Anwendungen, den Aufbau von Benutzergruppen und -konten sowie die Einstellung der Systemrichtlinien für Benutzer, Zugriffskontrolle und Überwachung vornehmen können.

Die Verantwortlichkeiten der einzelnen Benutzer im Client-Server-Netz sind unter Schritt 11 dargestellt.

3. Festlegung von Namenskonventionen

Um die Verwaltung des Client-Server-Netzes zu erleichtern, sollten eindeutige Namen für die Rechner, Benutzergruppen und die Benutzer verwendet werden.

Zusätzlich sollten Namenskonventionen für die Freigabenamen von Verzeichnissen oder Druckern eingeführt werden (siehe M 2.67 *Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste*). Sollen keine Rückschlüsse auf den Inhalt eines freigegebenen Verzeichnisses möglich sein, sind entsprechende Pseudonyme zu verwenden. Soll eine freigegebene Ressource nicht als solche erkennbar sein, ist dem Freigabenamen das Zeichen "$" anzuhängen. Letzteres empfiehlt sich immer dann, wenn Verzeichnisse nur zum bilateralen Austausch von Informationen zwischen zwei Anwendern oder zum Zugriff auf Ressourcen, die nur einzelnen Benutzern bekannt sein sollen, freigegeben werden.

4. Festlegung der Regeln für Benutzerkonten

Vor der Einrichtung von Benutzerkonten sollten die Restriktionen, die für alle bzw. für bestimmte dieser Konten gelten sollen, festgelegt werden. Dies betrifft insbesondere die Regelungen für Passwörter und für die Reaktion des Systems auf fehlerhafte Login-Vorgänge. Die festgelegten Regelungen können mit Hilfe der Option "*Richtlinien*" des Benutzer-Managers umgesetzt werden (siehe M 4.48 *Passwortschutz unter Windows NT/2000/XP*).

5. Einrichtung von Gruppen

Zur Vereinfachung der Administration sollten Benutzerkonten, für die die gleichen Anforderungen gelten, zu Gruppen zusammengefasst werden. Benutzerrechte sowie Datei-, Verzeichnis- und Freigabeberechtigungen und ggf. weitere vordefinierte Funktionen werden dann den Gruppen und nicht einzelnen Benutzerkonten zugeordnet. Die Benutzerkonten erben die Rechte und Berechtigungen der Gruppen, denen sie angehören. So ist es z. B. denkbar, alle Mitarbeiter einer Abteilung in einer Gruppe zusammenzufassen. Eine Zuweisung von Benutzerrechten und -berechtigungen an einzelne Benutzer sollte nur erfolgen, wenn dies ausnahmsweise unumgänglich ist.

6. Festlegung der Benutzerrechte

Rechte gestatten einem Benutzer die Ausführung bestimmter Aktionen auf dem System. Sie beziehen sich auf das gesamte System, sind keinem speziellen Objekt zugeordnet und können die Berechtigungen für ein Objekt außer Kraft setzen, da ein Recht Vorrang vor allen Datei- und Verzeichnisberechtigungen hat. Wenn sich ein Benutzer bei einem Konto anmeldet, dem die gewünschten Rechte entweder direkt oder über die Gruppenmitgliedschaft erteilt wurden, kann er die entsprechenden Aktionen ausführen. Besitzt ein Benutzer nicht die geeigneten Rechte, so verhindert Windows NT jeden Versuch, die betreffenden Aktionen auszuführen.

Wie schon zuvor dargestellt, sollten Benutzerrechte möglichst nur Gruppen und nicht einzelnen Benutzern zugeordnet werden.

Windows NT legt bei der Installation Voreinstellungen fest, die in der Regel für einen sicheren und effizienten Betrieb ausreichend sind. Empfehlenswert erscheint jedoch, der Gruppe "Jeder" das Recht "*System herunterfahren*" und der Gruppe "Jeder" und ggf. der Gruppe "Gäste" das Recht "*Lokale Anmeldung*" zu entziehen (siehe M 4.50 *Strukturierte Systemverwaltung unter Windows NT*).

7. Festlegung der Vorgaben für Protokollierung

Windows NT stellt sehr ausführliche Möglichkeiten der Protokollierung sicherheitsrelevanter Ereignisse zur Verfügung, die bei vollständiger Nutzung in der Lage sind, das System weitgehend mit Auditing zu beschäftigen und dabei große Mengen an Plattenplatz zu verbrauchen. Dabei kann ein Spektrum von Ereignisarten aufgezeichnet werden, das sich von systemweiten Ereignissen, wie zum Beispiel dem Anmelden eines Benutzers bis hin zum Versuch eines Benutzers, eine bestimmte Datei zu lesen, erstreckt. Sowohl die erfolgreichen als auch die fehlgeschlagenen Versuche, eine Aktion durchzuführen, lassen sich aufzeichnen. Bei der Konfiguration der Protokollierung

ist jedoch zu beachten, dass ein Mehr an Protokollierung nicht unbedingt auch die Sicherheit des überwachten Systems erhöht. Protokolldateien, die nicht ausgewertet werden oder die aufgrund ihres Umfangs nur mit großem Aufwand auswertbar sind, führen nicht zu einer besseren Kontrolle der Systemabläufe, sondern sind letztlich nutzlos. Aus diesen Gründen sollte die Protokollierung so eingestellt werden, dass sie im Normalfall nur die wirklich bedeutsamen Ereignisse aufzeichnet (siehe M 4.54 *Protokollierung unter Windows NT*).

8. Regelungen zur Datenspeicherung

Es ist festzulegen, wo Benutzerdaten gespeichert werden (siehe M 2.138 *Strukturierte Datenhaltung*). So ist denkbar, dass Benutzerdaten nur auf einem Server abgelegt werden. Eine Datenspeicherung auf der lokalen Festplatte ist bei diesem Modell nicht erlaubt. Möglich ist aber auch, bestimmte Benutzerdaten nur auf der lokalen Festplatte abzulegen. Nach welcher Strategie verfahren werden soll, muss an den konkreten Umständen des Einzelfalles festgelegt werden. Eine generelle Empfehlung auszusprechen, ist nicht möglich.

9. Einrichtung von Projektverzeichnissen

Um eine saubere Trennung von Benutzer- und projektspezifischen Daten untereinander sowie von den Programmen und Daten des Betriebssystems durchzusetzen, sollte eine geeignete Verzeichnisstruktur festgelegt werden, mit der eine projekt- und benutzerbezogene Dateiablage unterstützt wird. So können beispielsweise zwei Hauptverzeichnisse \Projekte und \Benutzer angelegt werden, unter denen dann die Dateien und Verzeichnisse der Projekte bzw. Benutzer in jeweils eigenen Unterverzeichnissen abgelegt werden.

10. Vergabe der Zugriffsrechte

Für die Server ist festzulegen, welche Verzeichnisse und bei Nutzung von NTFS-Partitionen welche Dateien für den Betrieb freizugeben und welche Zugriffsrechte ihnen zuzuweisen sind (siehe M 4.53 *Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT*). Zusätzlich ist bei Nutzung von Peer-to-Peer-Funktionalitäten auf der Ebene der Clients zu entscheiden, welche Verzeichnisse für Netzzugriff freizugeben sind (siehe M 2.94 *Freigabe von Verzeichnissen unter Windows NT*).

Das zuvor gesagte gilt analog für die Freigabe von Druckern.

11. Verantwortlichkeiten für Administratoren und Benutzer im Client-Server-Netz

Neben der Wahrnehmung der Netzmanagement-Aufgaben (siehe Nr. 2) müssen weitere Verantwortlichkeiten festgelegt werden. Es ist festzulegen, welche Verantwortung die einzelnen Administratoren im Client-Server-Netz übernehmen müssen. Dies können zum Beispiel Verantwortlichkeiten sein für

- die Auswertung der Protokolldateien auf den einzelnen Servern oder Clients,
- die Vergabe von Zugriffsrechten,
- das Hinterlegen und den Wechsel von Passwörtern und

- die Durchführung von Datensicherungen.

Auch die Endbenutzer müssen in einem Client-Server-Netz bestimmte Verantwortlichkeiten übernehmen, sofern ihnen Rechte zur Ausführung administrativer Funktionen gegeben werden. In der Regel beschränken sich diese Verantwortlichkeiten jedoch auf die Vergabe von Zugriffsrechten auf die eigenen Dateien, sofern diese explizit festgelegt und nicht von Voreinstellungen des übergeordneten Verzeichnisses übernommen werden.

12. Schulung

Abschließend muss festgelegt werden, welche Benutzer zu welchen Punkten geschult werden müssen. Erst nach ausreichender Schulung kann der Wirkbetrieb aufgenommen werden. Insbesondere die Administratoren sind hinsichtlich der Verwaltung und der Sicherheit von Windows NT gründlich zu schulen.

Die so entwickelte Sicherheitsstrategie ist zu dokumentieren und im erforderlichen Umfang den Benutzern des Client-Server-Netzes mitzuteilen.

Ergänzende Kontrollfragen:

- Wird die Sicherheitsstrategie an Veränderungen im Einsatzumfeld angepasst?

M 2.92 Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die folgenden Punkte sollten auf der Ebene der Server in einem Windows NT Client-Server-Netz regelmäßig auf Einhaltung und Effektivität kontrolliert werden (siehe auch M 4.54 *Protokollierung unter Windows NT*):

- **System-Sicherheits-Einstellungen**

  Die korrekte Einstellung der sicherheitsrelevanten Einträge in der Registrierung, d. h. im wesentlichen die Einträge im Bereich *HKEY_LOCAL_MACHINE*, ist regelmäßig zu kontrollieren, indem die Einträge der Sicherheitsprotokolle, die sich auf die Registrierung beziehen, überprüft werden.

- **Benutzung von privilegierten Benutzerkonten**

  Die Benutzung privilegierter Benutzerkonten, also von Konten mit erweiterten Rechten und Berechtigungen wie etwa Administratoren, ist regelmäßig durch Überprüfung der Einträge im Sicherheitsprotokoll zu überprüfen. Ebenso ist das Protokoll auf Anmeldeversuche auf das Gastbenutzerkonto zu überprüfen.

- **Fehlgeschlagene Zugriffsversuche (Berechtigungsverstöße)**

  Sofern Zugriffe auf Dateien und/oder die Registrierung aufgezeichnet werden, ist das Sicherheitsprotokoll wöchentlich, bei Bedarf auch öfter, auf das Vorliegen fehlgeschlagener Zugriffsversuche zu überprüfen. Werden Berechtigungsverstöße festgestellt, ist die Ursache zu ermitteln.

- **Systemintegrität**

  Die Systemintegrität ist regelmäßig zu überprüfen; insbesondere sind die Daten der letzten Veränderung sowie die Zugriffsrechte auf die wichtigen Systemdateien zu überprüfen und mit den Werten, die unmittelbar nach der Installation des Systems sowie bei der jeweils vorherigen Überprüfung gegeben waren, zu vergleichen. Da diese Kontrolle mit Hilfe der von Windows NT gebotenen Möglichkeiten relativ aufwendig ist, sollten hier geeignete Zusatzwerkzeuge eingesetzt werden, beispielsweise das Shareware-Programm DumpACL oder das mit der Technischen Referenz (dem "Resource Kit") zu Windows NT ausgelieferte Dienstprogramm WinDiff, mit dem sich Inhalte von Verzeichnissen und Dateien vergleichen lassen.

- **Unbenutzte Benutzerkonten**

  Es ist sicherzustellen, dass die Konten ehemaliger Beschäftigter sofort deaktiviert und nach einer geeigneten Übergangszeit (ca. 1/2 Jahr) vom System gelöscht werden. Da die Zeit des letzten Anmeldens am System nicht angezeigt wird, sind zu diesem Zweck nach Möglichkeit alle Benutzerkonten mit einem Verfallsdatum einzurichten, das in gewissen Zeitabständen (z. B. jährlich) auf Antrag des Benutzers aktualisiert werden

muss. Inaktive, d. h. abgelaufene, Benutzerkonten sind zu löschen. Die Eigentümer sind vorab zu informieren. Die Liste der definierten Benutzer ist regelmäßig zu überprüfen, um sicherzustellen, dass nur aktive Beschäftigte auf dem System arbeiten.

- **Gruppenzugehörigkeit**

  Eine strukturierte Systemadministration setzt voraus, dass Systemrechte und Objektberechtigungen möglichst nicht an einzelne Benutzer, sondern an Benutzergruppen vergeben werden. Es ist sicherzustellen, dass bei Änderungen in den Beschäftigungsverhältnissen die Mitgliedschaft der einzelnen Benutzer in den Benutzergruppen den organisatorischen Vorgaben angepasst wird. Daher ist regelmäßig zu prüfen, ob die Mitgliedschaften der Benutzer in den verschiedenen Benutzergruppen noch dem aktuellen Stand entspricht. Weiterhin ist bei der Veränderung der Gruppenmitgliedschaft eines Benutzers zu prüfen, ob dies zu einer Anhäufung von Benutzerrechten führt. Insbesondere ist in regelmäßigen zu überprüfen, ob die Zuweisung von Sonderrechten an Gruppen oder einzelne Benutzer noch den aktuellen organisatorischen Vorgaben entsprechen.

- **Berechtigungskontrolle**

  Es ist sicherzustellen, dass die Eigentümer von Dateien und Verzeichnissen ihre Verpflichtung verstehen, anderen Benutzern nur dann Zugriff zu gewähren, wenn dies erforderlich ist. Mit dem Dateimanager bzw. Explorer ist regelmäßig zu überprüfen, dass auf sensitive Daten nicht zu weitgehende Berechtigungen vergeben wurden. Kritisch sind insbesondere Berechtigungen für die Gruppen "*Jeder*" und "*Gäste*" bzw. "*Domänen-Gäste*". Sofern temporäre Berechtigungen zum Einsatz kommen, ist sicherzustellen, dass dies nur dann geschieht, wenn es erforderlich ist, und dass diese Berechtigungen sorgfältig überwacht werden.

Es sind Prozeduren bzw. Verfahren zu entwickeln für den Fall, dass Abweichungen von den festgelegten Einstellungen auftreten. Diese Prozeduren müssen folgende Punkte enthalten:
- wer wird wann informiert,
- Begründung für die eventuelle Wahl abweichender Einstellungen und Angaben, ob hierdurch möglicherweise eine Sicherheitslücke entsteht,
- Schritte zur Behebung der Sicherheitslücke,
- Schritte zur Identifizierung der Ursache der Sicherheitslücke.

Die Durchführung der hier beschriebenen Kontrollen auf der Ebene von Clients sollte nur dann durchgeführt werden, wenn sichergestellt ist, dass damit keine unzulässigen Leistungskontrollen der Benutzer dieser Clients verbunden sind und wenn die datenschutzrechtlich korrekte Behandlung der Protokoll-Informationen gewährleistet werden kann.

Ergänzende Kontrollfragen:

- Werden Unregelmäßigkeiten dem Netzadministrator bekanntgegeben?
- Werden Abweichungen der Sicherheitseinstellungen vom zulässigen Wert unverzüglich korrigiert?
- Werden die möglichen Konsequenzen solcher Abweichungen analysiert?

M 2.93 Planung des Windows NT Netzes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Windows NT kann in einem Netz in verschiedenen Konfigurationen eingesetzt werden. Um die Vor- und Nachteile der einzelnen Einsatzarten abschätzen und nachvollziehen zu können, muss zunächst kurz auf das Sicherheitssystem von Windows NT eingegangen werden. Grundsätzlich behält das Betriebssystem die Kontrolle über alle Ressourcen. Ein Benutzer kann nur dann auf Ressourcen zugreifen, wenn er die dazu notwendigen Rechte und Berechtigungen hat. Der Zugang zum System ist nur über ein gültiges Benutzerkonto möglich, das mittels Passwort geschützt werden kann. Durch die Sicherheitskontenverwaltung (SAM - Security Account Manager) werden die Informationen über Benutzer- und Gruppenkonten in der Security Account Database, die häufig auch als SAM-Datenbank bezeichnet wird, verwaltet. Das Betriebssystem generiert bei der Anmeldung eines Benutzers für diesen unter Berücksichtigung der Eintragungen in der SAM-Datenbank ein Access-Token. Der Sicherheitskontrollmonitor (Security Reference Monitor) überprüft anhand dieses Tokens, ob der Benutzer die Berechtigung hat, auf bestimmte Objekte zuzugreifen, und ob er das Recht hat, die angeforderten Aktionen durchzuführen (beispielsweise eine Datei löschen oder das System herunterfahren).

Windows NT unterstützt die Arbeit im Netz mit folgenden Konzepten:

1. Arbeitsgruppen

Rechner können zu Arbeitsgruppen zusammengefasst werden und im Rahmen des Peer-to-Peer Konzeptes über das Netz Ressourcen gemeinsam nutzen (siehe dazu auch Baustein B 5.1 *Peer-to-Peer-Dienste*).

Jeder Rechner in einem solchen Netz kann gleichzeitig sowohl als Server als auch als Workstation benutzt werden. Realisiert wird dies durch Freigabe von Ressourcen auf den einzelnen Rechnern. Jede Windows NT Workstation, die in einer Arbeitsgruppe eingesetzt wird, verwaltet ihre eigene SAM-Datenbank und damit auch eigene Benutzer- und Gruppenkonten. Die Eintragungen in dieser Datenbank können von keinem anderen Rechner der Arbeitsgruppe benutzt werden. Dies hat zur Folge, dass eine zentrale Administration nicht möglich ist. Für den Zugriff auf freigegebene Ressourcen wird in der Regel ein Passwort benötigt.

Besonders nachteilig wirkt sich bei diesem Konzept aus, dass keine ausreichende Kontrolle über die Rechte der einzelnen Benutzer möglich ist. Die Einrichtung von Arbeitsgruppen sollte daher möglichst vermieden werden.

2. Netz mit dediziertem Server

Hierbei handelt es sich um ein Netz mit Client-Server-Struktur. Es wird dabei festgelegt, welche Rechner als Server und welche Rechner als Clients fungieren. Server können Verzeichnisse und/oder Drucker freigeben bzw. Anwendungen wie z. B. *Mail, Schedule+, Fax* global zur Verfügung stellen. Clients

können hingegen nur die von Servern zur Verfügung gestellten Ressourcen nutzen.

Ein NT-Rechner kann mit dem Betriebssystem "Windows NT Server" oder "Windows NT Workstation" betrieben werden. In kleinen Netzen kann auch eine Lizenzversion "Windows NT Workstation" als Server betrieben werden. Zu beachten ist aber, dass sich aufgrund der lizenzrechtlichen Einschränkung nicht mehr als 10 Benutzer gleichzeitig über das Netz auf diesem Rechner anmelden dürfen. Reicht dies nicht aus, muss Windows NT Server installiert werden. Auf Servern unter dem Betriebssystem Windows NT sollten generell keine normalen Benutzer arbeiten. Die Clients müssen nicht zwingend unter Windows NT betrieben werden.

Der Vorteil dieses Konzeptes liegt in der Zentralisierung der Datenhaltung und -verwaltung. Sofern in einem solchen Netz nur ein Server zum Einsatz kommt, ist für die Arbeit im Netz auch nur auf diesem Rechner je Benutzer ein Konto anzulegen. Für die Benutzung von Ressourcen oder Diensten des Servers über das Netz ist lediglich die Anmeldung des Benutzers an diesem einen Rechner notwendig. Für kleinere Netze kann der Einsatz dieses Konzeptes durchaus wirtschaftlich sinnvoll sein.

Sofern jedoch die Kapazität eines Servers nicht mehr ausreicht, um den jeweiligen Anforderungen hinsichtlich Geschwindigkeit und Plattenspeicherplatz zu genügen, nimmt der Verwaltungsaufwand erheblich zu, wenn ein oder mehrere Server dem Netz hinzugefügt werden. Sollen alle Benutzer das Recht erhalten, auf alle Server über das Netz zuzugreifen, müssen die Benutzerkonten auf jedem einzelnen Server eingerichtet und gepflegt werden.

3. Domänen-Konzept

Eine Domäne unter Windows NT ist eine Gruppe von Rechnern, die über eine gemeinsame Sicherheits- und Benutzerkontendatenbank (SAM-Datenbank) verfügt. Für den Benutzer bedeutet dies, dass er sich nur einmal an der Domäne anmelden muss. Danach stehen ihm sämtliche für ihn freigegebene Ressourcen zur Verfügung, unabhängig davon, auf welchem Server sich diese befinden.

Ein Server der Domäne unter dem Betriebssystem Windows NT Server dient als primärer Domänencontroller (PDC). Daneben kann die Domäne einen oder mehrere Backup Domänencontroller (BDC), Mitgliedsserver, d. h. Server ohne Domänencontrollerfunktionalität (siehe auch weiter unten) und Windows NT Workstations enthalten. Außerdem können zu einer Domäne Arbeitsstationen mit anderen Betriebssystemen wie z. B. Windows für Workgroups, Windows 95 oder MS-DOS gehören.

Die Entscheidung, ob ein Server als primärer Domänencontroller, als Backup Domänencontroller oder als Mitgliedsserver fungieren soll, muss vor der Installation getroffen werden, da später eine Änderung ohne Neuinstallation nicht mehr möglich ist. Zum besseren Verständnis soll zunächst näher auf die verschiedenen Serverarten einer Domäne eingegangen werden:

a) Primärer Domänencontroller (PDC)

Ein Server einer Windows NT Domäne muss zwingend als primärer Domänencontroller eingerichtet werden. Der Einsatz des Betriebssystems Windows NT Server ist zwingend, da die Workstation-Version diese Funktionalität nicht enthält. Auf dem PDC wird die zentrale Benutzerkontendatenbank (SAM-Datenbank) für die Domäne verwaltet. Alle Änderungen können nur an dieser Datenbank mit Hilfe des Benutzermanagers für Domänen durchgeführt werden. Außerdem werden die Benutzeranmeldungen vom primären Domänencontroller bearbeitet.

b) Backup Domänencontroller (BDC)

Andere Server der Domäne können als Backup Domänencontroller eingerichtet werden. Auch hier ist der Einsatz des Betriebssystems Windows NT Server zwingend. Auf jeden Backup Domänencontroller wird automatisch eine Read-only-Kopie der Benutzerdatenbank der Domäne repliziert. Die Synchronisation erfolgt regelmäßig. Auch Backup Domänencontroller können Benutzeranmeldungen für die Domäne bearbeiten. Dadurch ist es gerade bei einer großen Anzahl von Benutzern möglich, die durch die Benutzeranmeldungen entstehende Last auf mehrere Server zu verteilen.

Jede Domäne sollte möglichst über mindestens einen Backup Domänencontroller verfügen, um die Verwaltung der Domäne bei Ausfall des primären Domänencontrollers sicherzustellen. In einem solchen Fall ist es möglich, den Backup Domänencontroller zum primären Domänencontroller hochzustufen. Sofern kein Backup Domänencontroller eingerichtet wurde, kann einer Domäne durch Neuinstallation kein neuer primärer Domänencontroller hinzugefügt werden.

Wenn die Server der Domäne auf verschiedene über WAN-Verbindungen zusammengeschaltete Liegenschaften verteilt sind, sollte in jeder Liegenschaft wenigstens ein Backup Domänencontroller installiert sein.

c) Mitgliedsserver (Memberserver)

Hierbei handelt es sich um Server, die weder als primärer noch als Backup Domänencontroller eingerichtet wurden. Diese Server verfügen über keine Kopien der Benutzerkontendatenbank der Domäne. Die Benutzeranmeldung für die Domäne kann von einem solchen Server daher nicht bearbeitet werden.

Folgende Gründe sprechen dafür, einen Server als Mitgliedsserver in die Domäne einzufügen:

- Ein Server hat zeitkritische Aufgaben durchzuführen oder es müssen auf diesem Rechner umfangreiche Applikationen ausgeführt werden, so dass der Aufwand von Benutzeranmeldungen nicht akzeptabel ist.
- Ein Server soll in naher Zukunft in eine andere Domäne eingefügt werden. Dies ist dann einfacher möglich, als wenn er als Backup Domänencontroller konfiguriert wäre.

Wesentlicher Ansatz des Domänenkonzeptes ist es, dass alle Benutzerkonten für jede Domäne nur einmal definiert werden müssen. Die Verwaltung erfolgt in der zentralen Benutzerdatenbank auf dem primären Domänencontroller.

Für die Benutzer bedeutet dies, dass sie sich bei der Benutzeranmeldung nur gegenüber dieser Datenbank authentisieren müssen. Danach können sie auf alle Objekte und Ressourcen der Domäne zugreifen, sofern sie die entsprechenden Berechtigungen besitzen. Dabei spielt keine Rolle, auf welchem Server sich diese Objekte und Ressourcen befinden. Arbeitet der Benutzer auf einem Rechner unter dem Betriebssystem Windows NT Workstation, genügt die Benutzeranmeldung gegenüber der zentralen Benutzerdatenbank, um auch auf diesen Rechner Zugang zu erhalten.

Organisation von Domänen

Innerhalb eines Netzes können mehrere Domänen eingerichtet werden; jede muss dabei aber über einen eindeutigen Namen verfügen. Jede Domäne verwaltet ihre eigene zentrale SAM-Datenbank. Die jeweiligen Benutzer- und Gruppenkonten sind daher auch nur in der Domäne gültig, in der sie definiert wurden.

Es kann aber innerhalb eines Netzes die Notwendigkeit bestehen, dass Benutzer einer Domäne auf Ressourcen einer anderen Domäne zugreifen müssen. Hierzu gibt es den Mechanismus der Vertrauensbeziehungen zwischen Domänen.

Dabei unterscheidet man zwischen vertrauten Domänen (Trusted Domains) und vertrauenden Domänen (Trusting Domains). Den Benutzerkonten und globalen Gruppen der vertrauten Domäne können in der vertrauenden Domäne Rechte und Berechtigungen zugewiesen werden, wodurch auch der Zugriff auf freigegebene Ressourcen möglich wird.

Es sind folgende Domänen-Modelle möglich:

a) Single-Domänen-Modell

Dies ist das einfachste Domänen-Modell, da in einem Netz hierbei nur eine einzige Domäne existiert. Daher besteht nicht die Notwendigkeit, Vertrauensbeziehungen zu verwalten. Im gesamten Netz existiert hierbei nur eine einzige SAM-Datenbank, über die die Verwaltung erfolgt. Eine Abwandlung dieses Modells liegt vor, wenn in einem Netz mehrere Einzeldomänen eingerichtet wurden, zwischen denen keine Vertrauensbeziehungen definiert wurden. Hierbei verwaltet jede Domäne ihre eigene SAM-Datenbank und ihre eigenen Benutzer- und Gruppenkonten. Das Single-Domänen-Modell eignet sich besonders gut für Netze mit wenigen Benutzern (ca. 200 bis 300) und wenigen Computerkonten. Nachteilig ist bei diesem Modell, dass die Performance bei steigender Benutzer- und Gruppenanzahl abnimmt. Außerdem ist eine Gruppierung der Ressourcen nach Organisationseinheiten in dem Sinne, dass ein Server z. B. für eine Abteilung reserviert ist, nicht möglich.

b) Master-Domänen-Modell

Kennzeichen dieses Modells ist, dass ein Netz in mehrere Domänen eingeteilt wird, wobei eine Domäne zentral alle Benutzer- und Gruppenkonten verwaltet. Diese Domäne wird Master-Domäne genannt. In den anderen Domänen werden die Ressourcen zusammengefasst. Die Ressourcen-Domänen vertrauen dabei der Domäne mit den Benutzerkonten. Folgende Abbildung zeigt das Master-Domänen-Modell:

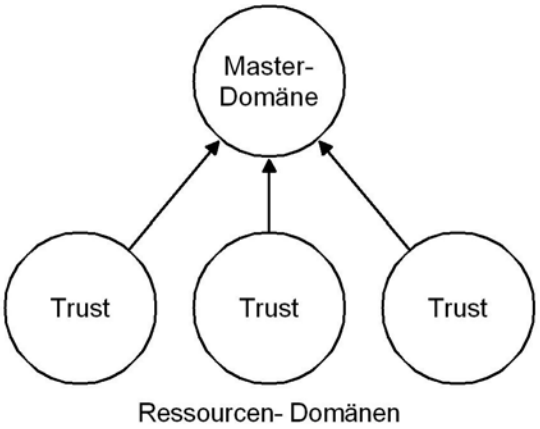


Abbildung: Master-Domänen-Modell

Dieses Domänen-Modell lässt sich nach Angaben von Microsoft bis zu einer Zahl von ca. 15.000 Benutzern einsetzen. Besonders geeignet ist dieses Modell, wenn eine Organisation aus mehreren Abteilungen besteht und alle Abteilungen ihre eigenen Ressourcen verwalten sollen, wobei die Benutzeradministration zentral erfolgt. Es ist bei diesem Domänen-Modell möglich, für die Administration der Ressourcen-Domänen jeweils einen eigenen Administrator zu benennen. Außerdem ist ein zentrales Sicherheitsmanagement möglich.

c) Multiple-Master-Domänen

Dieses Modell besteht aus mehreren Master-Domänen, die sich gegenseitig vertrauen. Die Benutzer- und Gruppenkonten werden in diesen Master-Domänen geführt. Darüber hinaus existieren Ressourcen-Domänen, die einseitig allen Master-Domänen vertrauen. Die folgende Abbildung zeigt das Modell der Multiple-Master-Domänen:

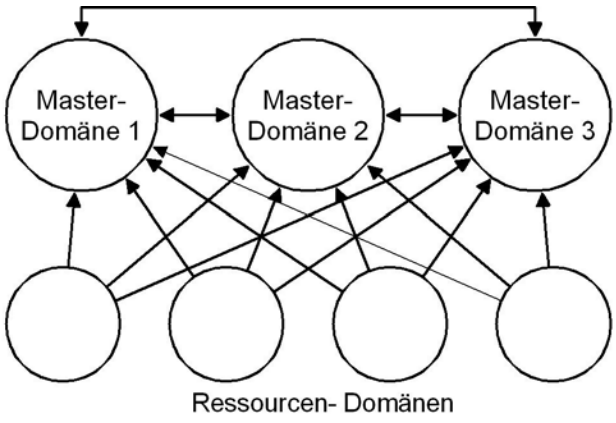


Abbildung: Multiple-Master-Domänen

Die explizite Vertrauensbeziehung zwischen Domäne 1 und Domäne 3 ist nötig, da Vertrauensstellungen nicht transitiv sind; d. h. vertrauen sich Domäne 1 und Domäne 2 sowie Domäne 2 und Domäne 3 gegenseitig, folgt nicht daraus, dass sich auch Domäne 1 und 3 gegenseitig vertrauen.

Multiple-Master-Domänen-Konzepte kommen häufig zum Einsatz, wenn die Benutzerzahl größer als 15.000 ist. Außerdem lässt es dieses Konzept zu, ein Netz nach Hauptabteilungen aufzuteilen und die Ressourcen durch die einzelnen Abteilungen verwalten zu lassen. Dazu wird je Hauptabteilung eine Master-Domäne eingerichtet. Die Benutzer einer Hauptabteilung erhalten ihre Benutzerkonten in der Master-Domäne. Die Ressourcen werden durch die Abteilungen in den Ressourcen-Domänen verwaltet. Auch ist es möglich, ein Netz nach Standorten zu organisieren. Hierbei wird für jeden Standort eine Master-Domäne und für jede Abteilung eine Ressourcen-Domäne eingerichtet. Dieses Domänen-Modell ist skalierbar, wobei die Größe einer Organisation keine Grenze setzt. Es besteht die Möglichkeit eines zentralen Sicherheitsmanagements, und globale Gruppen und Benutzerkonten brauchen organisationsweit nur einmal eingerichtet zu werden.

Es sei abschließend darauf hingewiesen, dass dieses Modell große Disziplin bei der Administration und sorgfältige Planung benötigt. Besondere Sorgfalt ist auf die Definition der Vertrauensbeziehungen zu legen. Außerdem muss zwingend verhindert werden, dass in den Ressourcen-Domänen Benutzerkonten eingerichtet werden.

d) Complete-Trust-Modell (Vertrauensverbund)

Bei diesem Modell bestehen gegenseitige Vertrauensbeziehungen zwischen allen Domänen eines Netzes. In jeder Domäne werden sowohl Ressourcen als auch Benutzer- und Gruppenkonten verwaltet. Ein Complete-Trust-Modell ist in folgender Abbildung dargestellt:

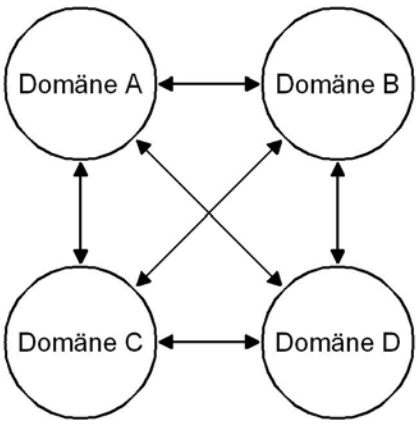


Abbildung: Complete-Trust-Modell

Bei diesem Modell ist es möglich, den Abteilungen einer Organisation sowohl die Verwaltung der Benutzerkonten als auch die Verwaltung der Ressourcen zu überlassen. Es wird keine zentrale Abteilung zur Verwaltung benötigt. Das Modell ist mit jeder Anzahl von Benutzern skalierbar. Dieses Modell hat aber auch erhebliche Nachteile. So ist die Kontrolle, ob die Sicherheitspolitik eingehalten wird, schwierig. Dies erschwert es, ein zentrales Sicherheitsmanagement aufzubauen. Außerdem ist es schwierig, die Tätigkeit der einzelnen Administratoren zu koordinieren. Wenn ein Netz sehr viele Domänen umfasst, sind sehr viele Vertrauensbeziehungen zu verwalten, was letztlich unübersichtlich ist.

Es können keine globalen Aussagen dazu gemacht werden, welches der beschriebenen Domänen-Modelle in einer Organisation Anwendung finden sollte. Dies kann nur in Abhängigkeit von der physischen und logischen Netzstruktur sowie der Verteilung von Daten, Anwendungen und Benutzern im Netz spezifisch festgelegt werden. Die Bestimmung der optimalen Domänenstruktur bedarf daher einer detaillierten Analyse, die für umfangreiche Netze aufwendig werden kann und ggf. durch Planungssoftware zu unterstützen ist.

Ergänzende Kontrollfragen:

- Ist die gewählte Netzstruktur einschließlich eventueller Vertrauensbeziehungen zwischen Domänen dokumentiert?
- Wird sie an Veränderungen im Einsatzumfeld angepasst?

M 2.94 Freigabe von Verzeichnissen unter Windows NT

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Unter Windows NT werden verschiedene Ebenen der Zugriffskontrolle auf Ressourcen unterschieden. Es gibt Zugriffsberechtigungen auf Freigabeebene und auf Verzeichnis- und Dateiebene (sog. NTFS-Berechtigungen). Die Zugriffsberechtigungen auf Verzeichnis- und Dateiebene stehen nur auf Datenträgern mit NTFS-Dateisystem zur Verfügung und werden ausführlich in M 4.53 *Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT* behandelt.

Die Freigabe von Verzeichnissen auf Servern ist notwendig, um Benutzern den Zugriff über das Netz auf diese Ressourcen zu ermöglichen. Ohne die Einrichtung einer entsprechenden Freigabe ist ein Netzzugriff auf ein Verzeichnis nicht möglich. Dies gilt selbst dann, wenn entsprechende NTFS-Berechtigungen vergeben wurden.

Es ist auf allen Rechnern unter dem Betriebssystem Windows NT, d. h. sowohl auf Domänencontrollern als auch auf Servern und Workstations (Clients) möglich, Verzeichnisse freizugeben. Üblicherweise sollten Verzeichnisse aber nur auf Domänencontrollern und Servern freigegeben werden. Verzeichnisfreigaben bzw. die Freigabe einzelner Laufwerke auf Workstations (Clients) erfolgen im Rahmen der Peer-to-Peer-Funktionalität (siehe M 5.37 *Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz*) und sollten die absolute Ausnahme bleiben, da dies zu unüberschaubaren Rechtestrukturen und ggf. sogar zum Unterlaufen der allgemeinen Sicherheitsvorgaben führen kann.

Ein Verzeichnis kann unter dem Betriebssystem Windows NT u. a. mit dem "Windows NT Explorer", über das Desktop-Symbol "Arbeitsplatz" oder mit dem Kommando "NET SHARE" freigegeben werden. Die Freigabe eines Verzeichnisses bezeichnet man auch als Einrichtung eines Shares. Im Windows NT Explorer oder im Desktop-Symbol "Arbeitsplatz" erfolgt die Freigabe eines Verzeichnisses über die Karte "Freigabe". Sie ist über den Menüpunkt "Eigenschaften" des Kontextmenüs erreichbar. Die Freigabe wird eingerichtet, indem die Option "Freigegeben als" angeklickt wird. Danach kann ein Freigabename mit einer maximalen Länge von 12 Zeichen eingegeben werden. Standardmäßig vergibt Windows NT den Namen des Verzeichnisses als Freigabenamen. Zur Erleichterung der Administration kann in dem Feld "Kommentar" eine kurze, prägnante Beschreibung zu der Freigabe eingegeben werden. Unter der Option "Benutzerbegrenzung" kann angegeben werden, wie viele Benutzer gleichzeitig auf die Freigabe zugreifen dürfen. Die standardmäßige Einstellung ist "Maximum erlaubt", d. h. die Anzahl ist nicht limitiert, und sollte beibehalten werden. Zur Lizenzkontrolle ist dieses Merkmal nur bedingt geeignet, da nur die Anzahl von Clients gezählt wird, die sich mit der Freigabe verbunden haben. Den Benutzern, die über das Netz auf diese Freigabe zugreifen sollen, muss eine entsprechende Freigabeberechtigung erteilt werden. Dies erfolgt über die Zugriffs-

kontrolliste, die nach Wahl des Feldes "Berechtigungen" durch das System geöffnet wird. Das Symbol des freigegebenen Verzeichnisses wird im "Windows NT Explorer" oder im Desktop-Symbol "Arbeitsplatz" mit einer Hand unterlegt, um anzuzeigen, dass es freigegeben wurde.

Das Recht, Verzeichnisse freizugeben sowie die Freigabeberechtigungen zu verwalten, haben nur Mitglieder der Gruppen "Administratoren" und "Server-Operatoren" auf Domänencontrollern bzw. Mitglieder der Gruppen "Administratoren" und "Hauptbenutzer" auf Windows NT-Workstations und Mitgliedsservern.

Unter Windows NT gibt es folgende Freigabeberechtigungen: "Kein Zugriff", "Lesen", "Ändern" und "Vollzugriff". Die Aktionen, die die einzelnen Freigabeberechtigungen ermöglichen, ergeben sich aus folgender Tabelle:

	Kein Zugriff	Lesen	Ändern	Voll-zugriff
Anzeigen von Unterverzeichnissen und Dateinamen		X	X	X
Anzeigen von Dateiinhalt und Dateiattributen		X	X	X
Programm ausführen		X	X	X
Wechsel in ein Unterverzeichnis		X	X	X
Einrichten von Unterverzeichnissen und Hinzufügen von Dateien			X	X
Ändern der Dateiattribute			X	X
Löschen von Unterverzeichnissen und Dateien			X	X
Zugriffsberechtigungen ändern (hat nur für Verzeichnisse Relevanz, die sich auf NTFS-Datenträgern befinden)				X
Besitzübernahme (hat nur für Verzeichnisse Relevanz, die sich auf NTFS-Datenträgern befinden)				X

Tabelle: Freigabeberechtigungen

Freigaben können nur für Verzeichnisse, nicht aber für Dateien definiert werden. Freigabeberechtigungen gelten nur für Zugriffe über das Netz, d. h. sie haben keine Bedeutung für Benutzer, die lokal an dem Rechner arbeiten dürfen, auf dem ein Verzeichnis freigegeben wurde. Außerdem gelten Freigabeberechtigungen nur in einheitlicher Form für alle Dateien und Unterverzeichnisse eines freigegebenen Verzeichnisses. Zwar ist es möglich, innerhalb eines freigegebenen Verzeichnisses auch ein Unterverzeichnis freizugeben und dabei auch abweichende Freigabeberechtigungen einzustellen, dies ist dann jedoch eine neue Freigabe mit folgenden Konsequenzen: Verbindet sich der Benutzer mit dem freigegebenen Verzeichnis, so gelten für ihn die dort festgelegten Freigabeberechtigungen für alle Dateien und

Unterverzeichnisse. Daran ändert sich auch nichts, wenn ein Unterverzeichnis gesondert freigegeben wurde. Verbindet sich der Benutzer hingegen direkt mit dem Unterverzeichnis, so gelten die dort eingerichteten Freigabeberechtigungen.

Beispiel: Gegeben sei folgende Verzeichnisstruktur: *D:\ABTEILUNG\REFERAT*. Eine Freigabe auf das Verzeichnis *ABTEILUNG* mit Berechtigung "Vollzugriff" und eine weitere Freigabe auf das Unterverzeichnis *REFERAT* mit Berechtigung "Lesen" werden eingerichtet. Verbindet sich der Benutzer mit dem Verzeichnis *D:\ABTEILUNG*, so kann er sowohl Dateien in diesem Verzeichnis, als auch Dateien im Unterverzeichnis *D:\ABTEILUNG\REFERAT* u. a. lesen, schreiben und löschen. Verbindet sich der Benutzer hingegen direkt mit dem Verzeichnis *D:\ABTEILUNG\REFERAT*, so kann er die in diesem Verzeichnis stehenden Verzeichnisse nur lesen. Sofern wie im vorstehenden Beispiel Restriktionen auf ein Unterverzeichnis gewünscht werden, kann dies nicht durch Freigabeberechtigungen sondern nur über die sog. NTFS-Berechtigungen erreicht werden (siehe M 4.53 *Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT*).

Wird ein Verzeichnis freigegeben, das sich auf einem NTFS-Datenträger befindet, gelten neben der Freigabeberechtigung auch die NTFS-Berechtigungen auf dieses Verzeichnis und die enthaltenen Dateien und Unterverzeichnisse. Dabei gilt die jeweils restriktivere Berechtigung. Besitzt ein Benutzer beispielsweise die Freigabeberechtigung "Lesen" für das freigegebene Verzeichnis, andererseits aber nur die NTFS-Berechtigung "Anzeigen" für dieses Verzeichnis, so ist sein Zugriffsrecht auf "Anzeigen" beschränkt. Über die NTFS-Berechtigung ist es daher möglich, Zugriffsrechte individuell auch auf Dateien und Unterverzeichnisse zu vergeben (näheres siehe M 4.53 *Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT*).

Freigabeberechtigungen durch Gruppenzugehörigkeiten sind kumulativ, d. h. ist ein Benutzer Mitglied in verschiedenen Gruppen, denen unterschiedliche Freigabeberechtigungen auf ein Verzeichnis eingeräumt wurden, so gilt für diesen Benutzer die weitestgehende Berechtigung. Von dieser Regel gibt es allerdings eine Ausnahme: Die Freigabeberechtigung "Kein Zugriff" dominiert alle anderen Freigabeberechtigungen.

Beispiel: Gegeben sei die Freigabe *D:\ERGEBNISSE*. Benutzer Meyer ist Mitglied der Gruppe A und der Gruppe B. Die Gruppe A erhält die Berechtigung "Lesen", die Gruppe B die Berechtigung "Vollzugriff" auf die o. g. Freigabe. In diesem Fall ist für den Benutzer Meyer die Freigabeberechtigung "Vollzugriff" maßgebend. Nimmt man den Benutzer Meyer noch in der Gruppe C auf, für die auf die Freigabe *D:\ERGEBNISSE* die Freigabeberechtigung "Kein Zugriff" vergeben wurde, so ist es dem Benutzer Meyer verwehrt, Zugriff über das Netz auf dieses Verzeichnis zu nehmen. Ist dies nicht gewünscht, kann der Administrator nur überprüfen, welchen Gruppen auf die Ressource die Freigabeberechtigung "Kein Zugriff" erteilt wurde und in welcher dieser Gruppen der betroffene Benutzer Mitglied ist. Der Benutzer ist dann aus der entsprechenden Gruppe zu entfernen.

Weiterhin ist zu beachten, dass Windows NT grundsätzlich die Wurzelverzeichnisse aller Platten sowie das Windows-Verzeichnis *%SystemRoot%* (in der Regel *C:\WINNT*) für administrative Zugriffe freigibt.

Dadurch besteht die Gefahr, dass

- jemand Administratorkennung und Passwort ausprobieren kann oder
- ein Administrator jederzeit unbemerkt auf Benutzerrechner zugreifen kann.

Falls diese Eigenschaft zur Erleichterung der Workstation-Betreuung gewünscht ist, ist zu überlegen, ob ein Administrator für alle von ihm betreuten Workstations dasselbe Administrator-Passwort verwenden soll. Dies lässt sich zwar leichter merken, führt aber dazu, dass ein Angreifer auf alle Workstations zugreifen kann, wenn er dieses eine Passwort herausgefunden hat.

Falls diese Zugriffsmöglichkeiten nicht gewünscht sind, z. B. weil der Administrator nicht auf lokale Benutzerdaten zugreifen können soll, sollte über den Benutzer-Manager, unter Richtlinien - Benutzerrechte das Recht "Zugriff auf diesen Computer vom Netz" für Administratoren gesperrt werden.

Die $-Freigaben können deaktiviert werden, sind aber beim nächsten Neustart des Systems wieder vorhanden, da sie automatisch angelegt werden. Mittels eines Registry-Schlüssels kann die Erstellung dieser Freigaben bei System-Start unterbunden werden. Bei System-Härtungen ist diese Anpassung der Registry sowie die Deaktivierung der Freigaben ADMIN$ und LAUFWERK$ oft empfehlenswert.

Windows NT vergibt bei jeder Freigabe standardmäßig die Freigabeberechtigung "Vollzugriff" für die Gruppe "Jeder". Dies ist insbesondere für Verzeichnisse, die sich auf Datenträgern ohne NTFS-Dateisystem befinden, nicht akzeptabel, da es hier außer den Freigabeberechtigungen keine andere Möglichkeit der Vergabe von Rechten und damit der Zugriffskontrolle gibt. Die Gruppe "Jeder" muss daher aus der Zugriffskontrolliste entfernt und durch die Gruppen und ggf. einzelnen Benutzer ersetzt werden, die auf das freigegebene Verzeichnis Zugriff nehmen sollen. Dabei sind dann auch entsprechende Freigabeberechtigungen zu vergeben.

Auch bei Verzeichnissen, die sich auf NTFS-Datenträgern befinden, sollte im Falle der Freigabe die Gruppe "Jeder" aus der Zugriffskontrolliste entfernt werden. Denkbar ist hier aber die Aufnahme der Gruppe "Benutzer" mit der Vergabe der Zugriffsberechtigung "Vollzugriff". Die individuelle Vergabe von Zugriffsberechtigungen auf das Verzeichnis bzw. auf enthaltene Dateien und Unterverzeichnisse erfolgt dann auf der Ebene der NTFS-Berechtigungen (siehe M 4.53 *Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT*).

Ergänzende Kontrollfragen:

- Ist dokumentiert, welche Verzeichnisse auf welchen Rechnern für den Netzzugriff freigegeben sind?
- Ist die Gruppe "Jeder" in den freigegebenen Verzeichnissen, die sich auf Datenträgern ohne NTFS-Dateisystem befinden, entfernt und durch die

Gruppen und ggf. einzelnen Benutzer, die auf das jeweilige freigegebene Verzeichnis über das Netz zugreifen dürfen, ersetzt worden?

- Werden die vorhandenen Freigaben an Veränderungen im Einsatzumfeld angepasst?

M 2.95 Beschaffung geeigneter Schutzschränke

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Beschaffungsstelle

Schutzschränke können ihren Inhalt gegen die Einwirkung von Feuer bzw. gegen unbefugten Zugriff schützen. Je nach angestrebter Schutzwirkung sind bei der Auswahl geeigneter Schutzschränke folgende Hinweise zu beachten:

- **Schutz gegen Feuereinwirkung:**

  Bei Datensicherungsschränken nach EN 1047-1 unterscheidet man bezüglich Schutz gegen Feuereinwirkung die Güteklassen S60 und S120. In diesen Güteklassen werden die Schutzschränke darauf geprüft, ob in ihnen bis zu einer Beflammungszeit von 60 bzw. 120 Minuten während eines normierten Testes für die geschützten Datenträger verträgliche Temperaturen erhalten bleiben. Durch Zusätze in der Klassifizierung werden die zu schützenden Datenträger bezeichnet. Die Kürzel bedeuten im einzelnen:

  P = Papierdokumente

  D = Datenträger mit Belastungsgrenzwert bis 70° C (z. B. Magnetbänder, Filme)

  DIS = Datenträger mit Belastungsgrenzwert bis 50° C (z. B. Disketten, Magnetbandkassetten einschließlich aller anderen Datenträger)

  Die Unterschiede zwischen den Klassen liegen in der Isolationsleistung, die bei DIS-Schränken am höchsten ist.

  Für den IT-Grundschutz sollten bei Schutz gegen Feuer Datensicherungsschränke der Güteklasse S60 ausreichend sein. Für die Verwendung als Serverschränke werden Datensicherungsschränke nach EN 1047-1 oder Datensicherungscontainer nach EN 1047-2 mit einer Klimaanlage angeboten.

  Bei Schutzschränken, die zum Schutz vor Feuer und Rauch dienen, sollte eine Vorrichtung zum automatischen Schließen der Türen im Brandfall vorgesehen werden. Die Schließung sollte lokal durch Rauchgasmelder und/oder extern durch ein Signal einer Brandmeldeanlage (soweit vorhanden) ausgelöst werden können.

- **Schutz gegen unbefugten Zugriff:**

  Der Schutzwert gegen unbefugten Zugriff wird neben der mechanischen Festigkeit des Schutzschrankes entscheidend durch die Güte des Schlosses beeinflusst. Für den IT-Grundschutz stehen Wertschutzschränke nach EN 1143-1 oder Sicherheitsschränke nach EN 14450 zur Verfügung. Sicherheitsschränke liegen im Widerstandswert unterhalb von Wertschutzschränken.

  Sind Zugriffsschutz und Brandschutz in Kombination erforderlich, so können Datensicherungsschränke verwendet werden, die sowohl die Anforderungen der EN 1143-1 als auch der EN 1047-1 erfüllen (sogenannte Duplexschränke).

Hilfestellung bei der Bewertung des Widerstandswertes verschiedener Schutzschränke gibt das VDMA-Einheitsblatt 24990, in dem Sicherheitsmerkmale

von Schutzschränken kurz beschrieben werden.

Bei der Auswahl von Schutzschränken ist auch die zulässige Deckenbelastung am Aufstellungsort zu berücksichtigen.

Nach diesen Auswahlkriterien für den Schutzwert des Schutzschrankes ist als nächstes die Ausstattung des Schrankes bedarfsgerecht festzulegen. Dazu sollte vor der Beschaffung eines Schutzschrankes festgelegt werden, welche Geräte bzw. welche Arten von Datenträgern in ihm aufbewahrt werden sollen. Die Innenausstattung des Schutzschrankes ist dieser Festlegung angemessen auszuwählen. Nachrüstungen sind in der Regel schwierig, da der Schutzwert des Schrankes und seine spezifische Zulassung beeinträchtigt werden können. Es sollte auch Raum für zukünftige Erweiterungen mit eingeplant werden.

In Serverschränken sollte außer für den Server und eine Tastatur auch Platz für einen Bildschirm und weitere Peripheriegeräte wie z. B. Bandlaufwerke vorgesehen werden, damit Administrationsarbeiten vor Ort durchgeführt werden können. Dazu ist zu beachten, dass die Ausstattung ergonomisch gewählt ist, damit Administrationsarbeiten am Server ungehindert durchgeführt werden können. So ist zum Beispiel ein ausziehbarer Boden für die Tastatur wünschenswert, der in einer Höhe angebracht wird, dass der Administrator seine Arbeiten sitzend durchführen kann. Je nach Nutzung des Schrankes können auch eine Klimatisierung und/oder eine USV-Versorgung erforderlich sein. Die entsprechenden Geräte sollten dann im Schrank mit untergebracht werden. Andernfalls muss zumindest eine Lüftung vorhanden sein. Die Ausstattung des Schrankes mit einem lokal arbeitenden Brandfrüherkennungssystem, das im Brandfall die Stromzufuhr der Geräte unterbricht (auf der Eingangs- **und** der Ausgangsseite der USV, sofern diese vorhanden ist), ist empfehlenswert.

Nicht im gleichen Schrank untergebracht werden sollten Backup-Datenträger und Protokolldrucker. Backup-Datenträger würden im Falle einer Beschädigung des Servers vermutlich ebenfalls beschädigt. Die Protokollierung der Aktionen am Server dient auch zur Kontrolle des Administrators. Es ist also nicht sinnvoll, ihm, gegebenenfalls sogar als Einzigem, Zugriff auf die Protokollausdrucke zu gewähren.

Ergänzende Kontrollfragen:

- Welche Schutzfunktionen soll der Schrank erfüllen?
- Werden diese durch den ausgewählten Schrank erfüllt?
- Welcher der genannten Güteklassen entspricht der Schutzschrank?
- Ist die Konsole des Servers nur für den Administrator zugänglich?
- Ist der Schutzschrank ausreichend dimensioniert?
- Wurden unautorisierte Änderungen am Schutzschrank durchgeführt?

M 2.96 Verschluss von Schutzschränken

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Generell sind Schutzschränke bei Nichtbenutzung zu verschließen. Werden Arbeiten, die ein Öffnen des Schutzschrankes erfordern, unterbrochen, so ist auch bei kurzfristigem Verlassen des Raumes der Schutzschrank zu verschließen. Bei Verwendung von Codeschlössern sind diese jedesmal zu verwerfen.

Ergänzende Kontrollfragen:

- Wird sporadisch überprüft, dass unbenutzte Schutzschränke verschlossen sind?

M 2.97 Korrekter Umgang mit Codeschlössern

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Werden Schutzschränke mit mechanischen oder elektronischen Codeschlössern verwendet, so muss der Code für diese Schlösser geändert werden:

- nach der Beschaffung,
- bei Wechsel des Benutzers,
- nach Öffnung in Abwesenheit des Benutzers,
- wenn der Verdacht besteht, dass der Code einem Unbefugten bekannt wurde und
- mindestens einmal alle zwölf Monate.

Der Code darf nicht aus leicht zu ermittelnden Zahlen (z. B. persönliche Daten, arithmetische Reihen) bestehen.

Die jeweils gültigen Codes von Codeschlössern sind aufzuzeichnen und gesichert zu hinterlegen (siehe M 2.22 *Hinterlegen des Passwortes* in analoger Anwendung). Zu beachten ist, dass eine Hinterlegung im zugehörigen Schutzschrank sinnlos ist.

Wenn der Schutzschrank neben einem Codeschloss ein weiteres Schloss besitzt, so ist abzuwägen, ob Code und Schlüssel gemeinsam hinterlegt werden, was im Notfall einen schnelleren Zugriff erlauben würde, oder getrennt hinterlegt werden, so dass es für einen Angreifer schwieriger ist, sich Zugriff zu verschaffen.

Ergänzende Kontrollfragen:

- Wird der Schlosscode nach den o. g. Ereignissen gewechselt?
- Wann wurde der Schlosscode zum letzten Mal gewechselt?
- Wird der Code der Codeschlösser hinterlegt?
- Wo und wie wird er hinterlegt?
- Wo werden evtl. vorhandene Reserveschlüssel zum Schrank aufbewahrt?

M 2.98 Sichere Installation von Novell Netware Servern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Im Vorfeld der Installation sowie bei der Einrichtung eines Novell Netware Servers sollten die folgenden Aspekte beachtet werden, um eine möglichst reibungslose und sichere Installation gewährleisten zu können.

Dokumentation der Installation

Die Installation von Novell Netware Servern sollte nachvollziehbar dokumentiert werden, damit im Vertretungsfall sowohl Außenstehende wie auch Neueinsteiger diese nach kurzer Einarbeitungszeit verstehen und nachvollziehen können.

In der Dokumentation sollte insbesondere die Parametrisierung des Servers (Netzeinbindung, Treiber), zusätzliche NLMs (Netware Loadable Modules, z. B. zur Datensicherung) und deren Konfiguration, sowie die eingespielten Patches aufgeführt werden. Weiterhin sollte die Installation und Einbindung zusätzlicher Hardware (z. B. Netzdrucker, Bandlaufwerke) ausführlich dokumentiert werden.

Desweiteren sollte die Dokumentation eine detaillierte Beschreibung der Server-Hardware und der installierten Peripheriegeräte (z. B. Netzdrucker) beinhalten. In Abhängigkeit der Komplexität des Novell-Netzes ist der Einsatz von Administrationstools für Dokumentations- und Revisionszwecke erstrebenswert.

Die zur Installation und Konfiguration eines Novell Netware Servers erforderliche Software sollte vollständig an einem gesicherten Ort hinterlegt werden, um im Bedarfsfall unnötige Verzögerungen zu vermeiden. Dies sollte insbesondere bei den aufzuspielenden Patches des Netzbetriebssystems, zusätzlichen NLMs sowie den einzusetzenden Treibern beachtet werden.

Das Laden des NLM-Utilities *SYS:SYSTEM\CONLOG.NLM* bewirkt, dass alle Meldungen, die am Monitor des Servers erscheinen, gleichzeitig in die Datei *SYS:ETC\CONSOLE.LOG* umgeleitet werden. Dieses NLM sollte bereits in der Startdatei *AUTOEXEC.NCF* geladen werden, um Fehler, die in der Startphase des Servers gemeldet werden, nachvollziehen zu können.

Hardwareausstattung

Bei der Festlegung der erforderlichen Hauptspeicherkapazität (RAM) von Novell Netware Servern ist neben der Festplattenkapazität, den eingesetzten Betriebssystemen der Novell Netware Clients auch die RAM-Speicherbelegung durch zusätzlich geladene NLMs zu berücksichtigen.

Hinsichtlich der Festplattenkapazität beim Einrichten einzelner Volumes auf einem Novell Netware Server ist insbesondere das SYS: Volume ausreichend zu dimensionieren, da alle Netware Prozesse standardmäßig auf diesem Volume ausgeführt werden. Eine zu kleine Dimensionierung des SYS: Volumes kann unter Umständen dazu führen, dass nach einer gewissen Betriebszeit temporäre Prozesse, wie z. B. Druckjobs, die Kapazitäten des Volumes

erschöpfen und somit einen vermeidbaren ABEND (Abnormal End - Absturz des Servers) hervorrufen.

Anforderungen an die Verfügbarkeit

Zur Erhöhung der Verfügbarkeit von Novell Netware Servern bzw. der gespeicherten Daten stellt das Netzbetriebssystem Novell Netware 3.x drei hierarchische Fehlertolerierungsstufen (System Fault Tolerance Level) zur Verfügung, die nachfolgend kurz aufgezeigt werden. Jede der hier aufgezeigten Fehlertolerierungsstufen beinhaltet dabei die Funktionalitäten der vorherigen Stufe.

- **SFT I (System Fault Tolerance I)**

  Novell Netware 3.x unterstützt standardmäßig SFT I. Hierbei werden Datenverluste aufgrund physikalischer Festplattenfehler verhindert. Nach einem Schreibzugriff auf eine Datei erfolgt ein Vergleich zwischen den veränderten Daten auf der Festplatte mit den Originaldaten, die sich noch im Arbeitsspeicher des Novell Netware Servers befinden. Ist dieses Ergebnis fehlerhaft, so wird der entsprechende Sektor der Festplatte als defekt markiert und für zukünftige Zugriffe gesperrt.

  Weiterhin werden die Daten des Arbeitsspeichers im Anschluss in dem zuvor beschriebenen Fehlerfall in den so genannten "Hot Fix Bereich" der Festplatte umgeleitet, für den Novell Netware standardmäßig zwei Prozent der Festplattenkapazität beansprucht.

- **SFT II (System Fault Tolerance II)**

  Die Fehlertolerierung der Stufe II (SFT II) kann auf zwei unterschiedliche Arten realisiert werden.

  - Disk Mirroring

    Beim Disk Mirroring werden an einen Festplattencontroller des Servers zwei identische Festplatten angeschlossen. Die zu speichernden Daten werden gleichzeitig auf beiden Festplatten gespeichert. Fällt eine der Festplatten durch einen Fehler aus, wird ohne Ausfallzeit und Datenverlust mit der zweiten Festplatte weitergearbeitet.

  - Disk Duplexing

    Beim Disk Duplexing werden zwei Festplatten und zwei Festplattencontroller von gleicher Art bzw. Größe im File Server installiert. Disk Duplexing gewährleistet somit eine Fortführung des Betriebes nicht nur beim Ausfall einer Festplatte, sondern auch beim Ausfall eines Festplattencontrollers.

- **SFT III (System Fault Tolerance III)**

  SFT III stellt die höchste Stufe der Toleranz gegen im Betrieb auftretende Hardware-Fehler dar. Zwei identische Novell Netware Server arbeiten hierbei gleichzeitig und parallel im Netz.

  Die beiden Novell Netware Server sind hierbei durch ein eigenes Hochgeschwindigkeitsnetz miteinander verbunden. Fällt einer der beiden Server

aus, so wird der Netzbetrieb, fast ohne Zeit- und Datenverlust, durch den zweiten Novell Netware Server weitergeführt.

Die Entscheidung, ob zusätzlich zur Stufe SFT I weitere Maßnahmen (SFT II, SFT III) ergriffen werden müssen, ist abhängig vom angestrebten Grad der Verfügbarkeit des Netzes.

Notstromversorgung

Durch den Einsatz einer Notstromversorgung (UPS=Unterbrechungsfreie Stromversorgung) können die Folgen eines plötzlichen Stromausfalles abgefangen werden. Novell Netware unterstützt den Einsatz geeigneter Geräte durch das so genannte UPS-Monitoring. Im Falle eines plötzlichen Stromausfalles wird der File Server am Ende der Überbrückungszeit der UPS geregelt heruntergefahren, d. h. die sich im Cache des Servers befindlichen Daten werden auf die Festplatten übertragen, Verbindungen zum Server ordnungsgemäß terminiert sowie die Serverprozesse geregelt beendet.

Ergänzende Kontrollfragen:

- Genügt die Dokumentation auch dem Vertretungsfall des Administrators?
- Wie wurde die Auswahl des SFT-Levels begründet?

M 2.99 Sichere Einrichtung von Novell Netware Servern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die im Lieferumfang von Novell Netware 3.x enthaltenen Sicherheitsfeatures sind nach dem erstmaligen Start der Datei *SERVER.EXE* nicht automatisch aktiviert, sondern müssen, jeweils einzeln durch die Systemadministration installiert und konfiguriert werden.

Mit Hilfe des Programms *SYS:PUBLIC\SETPASS.EXE* sollte der Supervisor nach dem erstmaligen Login sofort ein Passwort für diesen Account vergeben. Der standardmäßig vorhandene Guest-Account sollte ebenfalls mit einem Passwort versehen werden. Wird der Guest-Account im späteren Betrieb nicht benötigt, so sollte er entfernt werden.

Mittels DISABLE LOGIN (Serverkonsole) sollten während der Einrichtungsphase unautorisierte Login-Versuche unterbunden werden.

Mit Hilfe des Novell Utilities *SYS:PUBLIC\SYSCON.EXE* können im Anschluss, unter dem Menüpunkt **Supervisor Options** die meisten der Novell Sicherheitsmechanismen installiert und konfiguriert werden. Hierbei ist zu beachten, dass die unter **Default Time Restrictions** vorgenommenen Einstellungen nur dann für alle Accounts des Novell Netware Servers Gültigkeit haben, wenn diese Einstellungen vor der Einrichtung von Benutzern und Gruppen getroffen werden.

Nachfolgend werden sicherheitsrelevante Menüpunkte aufgeführt.

Default Account Balance/Restrictions

Mit Hilfe dieses Menüpunktes werden folgende Sicherheitseinstellungen auf dem Novell Netware Server aktiviert.

- **Account has Expiration Date**: Hiermit kann die Gültigkeitsdauer eines Accounts zeitlich limitiert werden. Da ein Account normalerweise auf Dauer angelegt ist, wird dieses Feature im Regelfall nur für einen Guest Account aktiviert.
- **Limit Concurrent Connections**: Hierdurch kann die Anzahl der gleichzeitigen Verbindungen eines Accounts zu dem Novell Netware Server limitiert werden. Im Regelfall sollte hierbei der Wert "Eins" gewählt werden.
- **Create Home Directory for User:** Optionale Erstellung eines persönlichen Verzeichnisses für jeden Benutzer. Es sollte die Option "Yes" gewählt werden.
- **Require Password:** Require Password installiert die Passwortabfrage für jeden Benutzer und bietet bei Aktivierung die Möglichkeit, Passwortregeln zu installieren. Für Require Password sollte die Option "Yes" gewählt werden.
- **Minimum Password Lenght:** Hierbei wird die erforderliche Mindestlänge eines Passwortes eingestellt. Die Mindestlänge eines Passwortes sollte

hierbei sechs Zeichen sein (siehe unter M 2.11 *Regelung des Passwortgebrauchs*). Wird die erforderliche Mindestlänge auf weniger als fünf Zeichen eingestellt, so wird dieses beim Ausführen von *SYS:\SYSTEM\SECURITY.EXE* angezeigt (siehe M 2.101 *Revision von Novell Netware Servern*).

- **Force Periodic Password Changes:** Durch die Einstellung "Yes" wird festgelegt, dass die Benutzer ihre Passwörter regelmäßig ändern müssen. Dies sollte der Regelfall sein.
- **Days Between Password Changes:** Unter diesem Menüpunkt wird die generelle Gültigkeitsdauer von Passwörtern festgelegt. Die Gültigkeitsdauer von Passwörtern muss für das jeweilige System festgelegt werden.

  Hinweis: Ist die Gültigkeitsdauer des Passwortes auf einen Wert eingestellt, der mehr als 60 Tage beträgt, so wird dieses durch das Novell Utility *SYS:SYSTEM\SECURITY.EXE* "beanstandet".
- **Limit Grace Logins:** Grace Logins ("Gnaden-Logins") sind die Logins, die nach Ablauf der Gültigkeitsdauer eines Passwortes erfolgen. Die Anzahl der Grace Logins sollte durch die Einstellung "Yes" grundsätzlich limitiert werden.
- **Grace Logins Allowed:** Die Anzahl der erlaubten Grace Logins sollte auf den Wert "Eins" eingestellt werden, damit ein Benutzer, dessen Passwort ungültig geworden ist, dieses sofort ändern muss.
- **Require Unique Passwords:** Die Aktivierung der Passworthistorie (REQUIRE UNIQUE PASSWORDS) hat zur Folge, dass die letzten neun Passwörter eines Accounts mit dem neu eingegebenen Passwort verglichen werden und bei Übereinstimmung das neue Passwort durch den Novell Netware Server zurückgewiesen wird.
- **Account Balance:** Novell Netware Accounting Funktion
- **Allow Unlimited Credit:** Novell Netware Accounting Funktion
- **Low Balance Limit:** Novell Netware Accounting Funktion

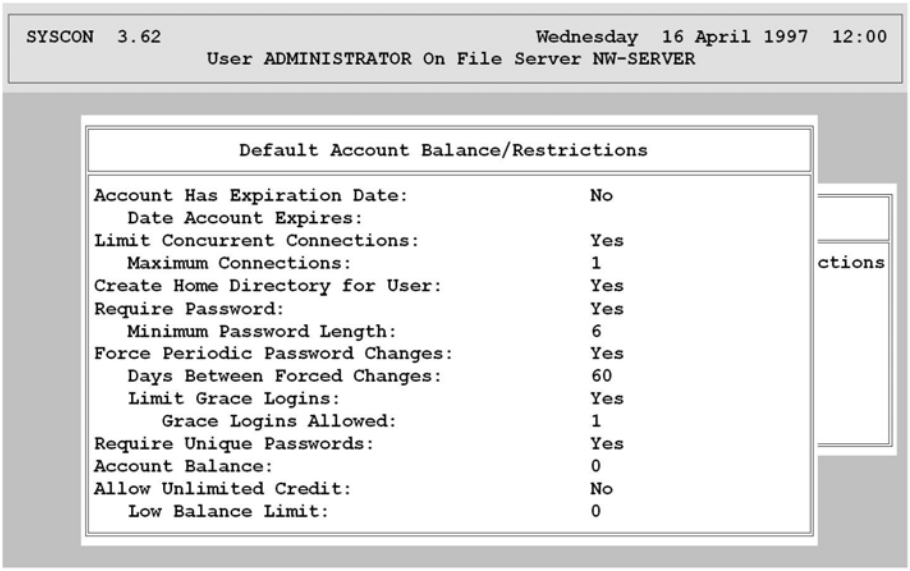


Abbildung 1: Menu *SYS:PUBLIC\SYSCON.EXE* "Default Account Balance/Restrictions"

Default Time Restrictions

Mit Hilfe der Time Restrictions werden die erlaubten Arbeitszeiten für Accounts auf einem Novell Netware Server definiert. Außerhalb der hier festgelegten Zeiten, die im Regelfall den üblichen Arbeitszeiten entsprechen sollten, ist es keinem Benutzer gestattet, sich am Novell Netware Server anzumelden.

Hinweis: Für die standardmäßig installierten Accounts Supervisor und Guest ist der Netware-Default-Wert (keine Zeitbeschränkungen) eingestellt. Es ist empfehlenswert, zumindest den Guest-Account mit Hilfe von *SYS:PUBLIC\SYSCON.EXE* (User Information - Time Restrictions) hinsichtlich der erlaubten Zugriffszeiten einzuschränken.

Nachträgliche Änderungen der "Default Time Restrictions" bei der Einrichtung bzw. Pflege von Benutzer Accounts haben keine Auswirkungen auf die erlaubten Zugangszeiten bereits eingerichteter Benutzer. Abweichende Zugangszeiten einzelner Benutzer müssen mit Hilfe von *SYS:\PUBLIC\SYSCON.EXE* (User Information - Time Restrictions) eingerichtet werden.

Edit System AUTOEXEC File

Durch die Server Startdatei *AUTOEXEC.NCF* werden die Parameter (z. B. Volumes, NLMs, zusätzliche Protokolle etc.) eines Novell Netware Servers konfiguriert.

Weiterhin können in der *AUTOEXEC.NCF* zusätzliche Sicherheitseinstellungen vorgenommen werden.

Das Novell Netware Konsolenkommando SECURE CONSOLE, das in die *AUTOEXEC.NCF* eingebunden sein sollte, bewirkt dabei, dass NLMs nur noch aus dem Serververzeichnis *SYS:SYSTEM* gestartet werden können, sowie die Deaktivierung des Novell Netware Debuggers. Weiterhin wird

durch SECURE CONSOLE das DOS aus dem Hauptspeicher des Novell Netware Servers entfernt, sowie die definierten Serversuchpfade außer Kraft gesetzt, die zudem nicht erneut definiert werden können.

File Server Console Operators

Mit Hilfe des Menu-Utilities *SYS:\PUBLIC\FCONSOLE.EXE* kann, ausgehend von einer Workstation, die begrenzte Kontrolle über einen Novell Netware Server übernommen werden.

Der File Server Operator, der neben der ausdrücklichen Berechtigung zur Nutzung von *SYS:\PUBLIC\FCONSOLE.EXE* keine weiteren Privilegien benötigt, kann hiermit Konsolennachrichten an die Benutzer versenden, den Novell Netware Server wechseln sowie den Server herunterfahren. Weiterhin können Statusanzeigen des Novell Netware Servers eingesehen und verändert werden (Datum, Uhrzeit, etc.) sowie Informationen zu den aktuellen Verbindungen eingesehen werden. Das Programm *SYS:\PUBLIC\FCONSOLE.EXE* kann standardmäßig durch den Supervisor bzw. einen äquivalenten Account aufgerufen werden. Andere Benutzer sollten auf diese Dateien keine Rechte besitzen.

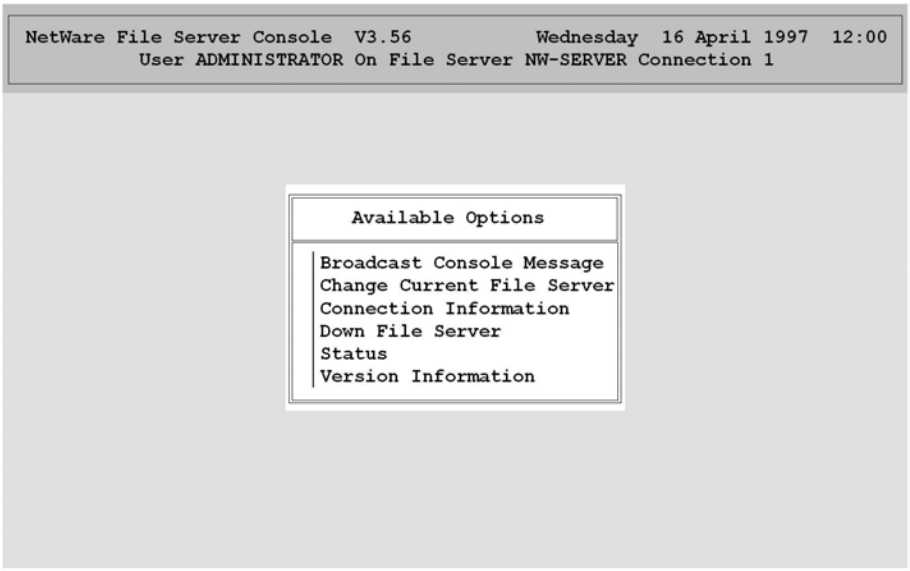


Abbildung 2: Menu *SYS:PUBLIC\FCONSOLE.EXE*

Intruder Detection/Lockout

Durch die Aktivierung des "Detect Intruders" werden unautorisierte Login-Versuche am Novell Netware Server erkannt und die hiervon betroffenen Accounts ggf. gesperrt.

Die Aktivierung des "Detect Intruders" sowie die weitere Parametrisierung dieses Menüpunktes beugt somit einer "Brute Force Attacke" unter Novell Netware vor.

Incorrect Login Attempts gibt hierbei die Anzahl der zulässigen Login Fehlversuche an; üblicherweise sollte hierbei der Wert "Drei" eingestellt werden.

Mit Hilfe von **Bad Login Count Retention Time** kann die zeitliche Zurückverfolgung von fehlgeschlagenen Login-Versuchen eines Accounts aktiviert werden. Übersteigt die Anzahl der Login-Fehlversuche eines Accounts innerhalb des definierten Zeitraumes den unter **Incorrect Login Attempts** eingestellten Wert, so wird der Benutzer Account auf dem Novell Netware Server gesperrt.

Der Menupunkt **Lock Account After Detection** sollte auf "Yes" eingestellt sein, um einen Account, der die Anzahl der ungültigen Login Versuche überschritten hat, zu sperren.

Der Zeitwert für **Length of Account Lockout** sollte keinesfalls zu gering gewählt werden (> 1 Stunde) um sicherzustellen, dass die Ursache für einen Intruder Lockout durch die Systemadministration und den betroffenen Benutzer aufgeklärt werden kann.

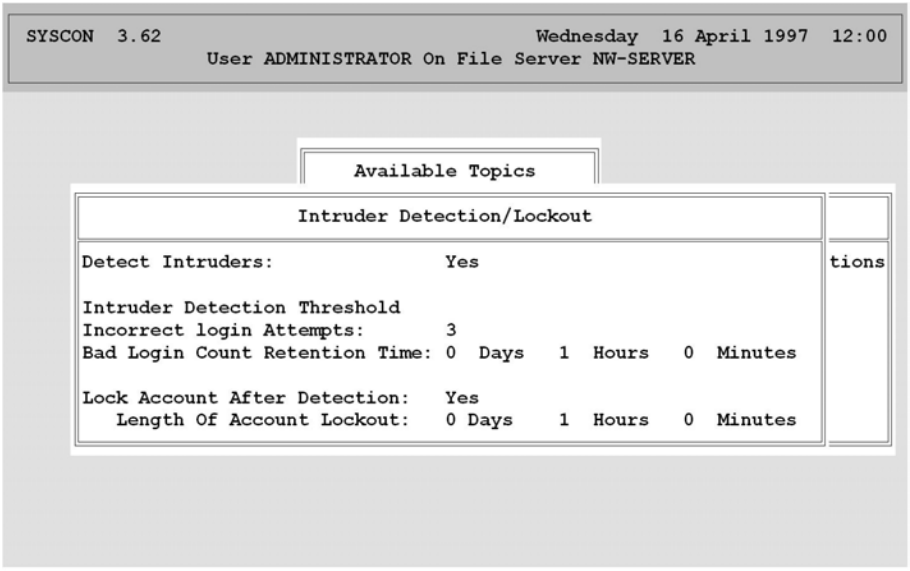


Abbildung 3: Menu *SYS:PUBLIC\SYSCON.EXE* "Supervisor Options - Intruder Detection Logout"

System Login Script

In dem System Login Script werden die Einstellungen vorgenommen, die für alle Benutzer nach deren Anmeldung auf dem Novell Netware Server existieren sollen. Das System Login Script wird, im Gegensatz zum User Login Script, für jeden Benutzer des Novell Netware Servers ausgeführt. Es ist daher sinnvoll, die Einstellungen, die für alle Benutzer des Novell Netware Servers gelten sollen, wie z. B. Laufwerkzuordnungen oder der Aufruf von externen Programmen, im System Login Script des Novell Netware Servers einzustellen.

Soll vermieden werden, dass ein Benutzer durch Verwendung des eigenen UER-Login-Scripts die Standardeinstellungen verändert, muss beim Verlassen des System-Login-Scripts der Befehl EXIT aufgenommen werden

Hinweis: Weiterhin ist für jeden Benutzer ein User-Login-Script zu erstellen. Dies ist erforderlich, da jeder Benutzer über das Zugriffsrecht "Create" im Verzeichnis *SYS:MAIL* verfügt. Einem Benutzer ohne User-Login-Script kann daher in seinem *SYS:MAIL*-Verzeichnis eine Datei *LOGIN* erzeugt werden, die Schadfunktionen ausführen kann.

View File Server Error Log

Das File Server Error Log ist das Fehlerprotokoll eines Novell Netware Servers. In ihm werden alle Fehler und Warnmeldungen des Servers gespeichert und können durch den Supervisor ausgewertet werden.

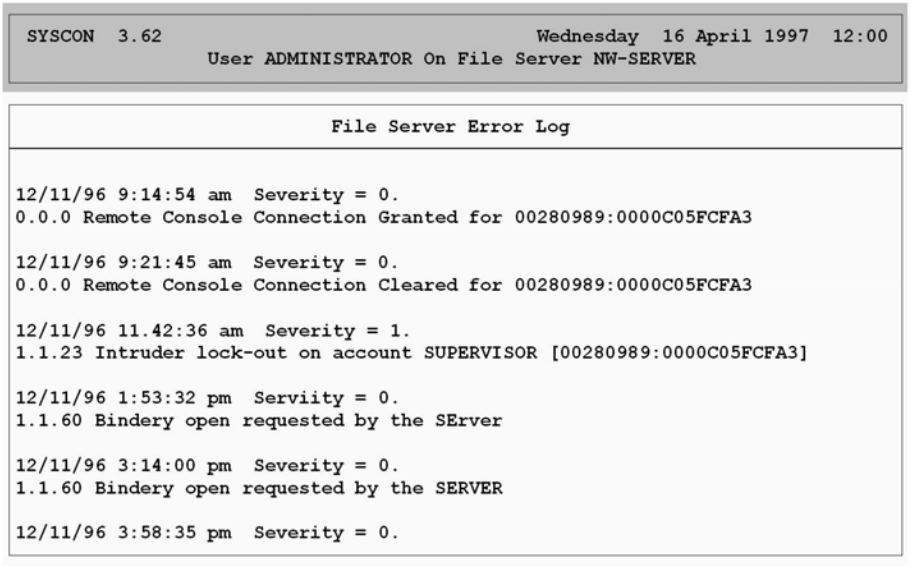


Abbildung 4: Menu *SYS:PUBLIC\SYSCON.EXE* "Supervisor Options - File Server Error Log"

Workgroup Managers

Ein Arbeitsgruppenverwalter (Workgroup Manager) ist ein eingeschränkter Supervisor Account, der das Recht zum Erstellen und Löschen von Bindery Objekten (Benutzer, Benutzergruppen, Druckerwarteschlangen) sowie deren Verwaltung hat. Die Rechte, die ein Arbeitsgruppenverwalter hierbei einsetzt bzw. an Benutzer und Benutzergruppen weitergeben darf, richten sich nach den durch den Supervisor zugestandenen Rechten.

Arbeitsgruppenverwalter können keine neuen Arbeitsgruppenverwalter oder einen Benutzer einrichten, dessen Sicherheitsstufe "Supervisor-äquivalent" ist, es sei denn, der Arbeitsgruppenverwalter verfügt über Supervisor-äquivalente Rechte.

Station Restrictions

Mit Hilfe des Menüpunktes Station Restrictions können die Netzadressen festgelegt werden, von denen aus sich ein Benutzer am Novell Netware Server anmelden darf. Informationen über die jeweilige Adresse einer Workstation im Netz lassen sich z. B. mit *SYS:PUBLIC\USERLIST.EXE /A* in Erfahrung bringen. Die Festlegung von erlaubten Netzadressen ist insbesondere für den Supervisor bzw. für äquivalente Accounts empfehlenswert. Dieses sollte jedoch vor Ort, je nach Gegebenheit, entschieden werden.

Standardisierte Einrichtung von Benutzern und Benutzergruppen

Neben der Einrichtung von Benutzern unter Einsatz des Menu-Utilities *SYS:PUBLIC\SYSCON.EXE* besteht zudem die Möglichkeit, Benutzer mit Hilfe der Utilities *SYS:\PUBLIC\MAKEUSER.EXE* und *SYS:\PUBLIC\USERDEF.EXE* einzurichten.

Diese eignen sich besonders für die gleichzeitige Einrichtung einer größeren Anzahl von Benutzern.

SYS:\PUBLIC\MAKEUSER.EXE erzeugt eine Art Batch-Datei, mit deren Hilfe mehrere Benutzer mit unterschiedlichen Rechten eingerichtet werden können.

SYS:\PUBLIC\USERDEF.EXE dient zur Einrichtung mehrerer Benutzer mit gleichen Rechten. Zu diesem Zweck wird eine Schablone (Template) erstellt, in der eingetragen wird, nach welchen Vorgaben die Benutzer einzurichten sind.

Diese Menu-Utilities sollten insbesondere in größeren Netzen aus Gründen einer vereinfachten und einheitlichen Administration eingesetzt werden.

M 2.100 Sicherer Betrieb von Novell Netware Servern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der sichere Betrieb eines Novell Netware Netzes setzt verschiedene Aktionen voraus, die nachfolgend beschrieben werden.

Vergabe von Zugriffsrechten auf Verzeichnisse und Dateien

Die Vergabe von Zugriffsrechten (Trustee Assignments) auf Verzeichnisse und Dateien von Novell Netware Servern spielt eine zentrale Rolle für die Sicherheit eines Novell Netware Servers.

Zugriffsrechte werden im Gegensatz zur Vergabe von Attributen einzelnen Benutzern bzw. Benutzergruppen zugewiesen.

Verzeichnisse und Dateien können über die Steuerung der Zugriffsrechte aufgabenbezogen zugewiesen werden. Hierdurch kann sichergestellt werden, dass Benutzergruppen bzw. Benutzer nur die Zugriffsrechte auf Verzeichnisse und Dateien haben, die sie zur Durchführung ihrer Aufgaben benötigen.

Aus Gründen der Übersichtlichkeit, einer vereinfachten Administration sowie einer verbesserten Revisionsfähigkeit sollte die Vergabe von Zugriffsrechten vorrangig über die Zuweisung von Rechten an Benutzergruppen erfolgen.

Um die versehentliche Freigabe von Verzeichnissen durch einen Benutzer zu verhindern, sollte die Systemadministration Benutzergruppen und Benutzern in den ihnen zugewiesenen Verzeichnissen die Rechte "Supervisory" (S) und "Access Control" (A) nicht erteilen.

Werden ausgewählten Verzeichnissen oder Dateien mit Hilfe von Netware-Attributen bestimmte Eigenschaften (z. B. schreibgeschützte Dateien) zugewiesen, so sollte beachtet werden, dass Benutzer, die das Zugriffsrecht "Modify (M)" auf die entsprechenden Verzeichnisse und Dateien besitzen, in der Lage sind, diese Attribute zu verändern. Daher sollte der Kreis der Benutzer mit diesem Zugriffsrecht eingeschränkt werden (s. u. Vergabe von Netware-Attributen auf Verzeichnisse und Dateien).

Vergabe von Netware-Attributen auf Verzeichnisse und Dateien

Neben der Benutzer- bzw. gruppenbezogenen Erteilung von Zugriffsrechten auf Verzeichnisse und Dateien kann durch die Vergabe von Netware-Attributen auf Verzeichnisse und Dateien die Datensicherheit erhöht werden. Attribute sind immer verzeichnis- bzw. dateibezogen, d. h. sie sind unabhängig von den zugewiesenen Zugriffsrechten und gelten für alle Benutzer einschließlich des Supervisors.

Benutzer, denen das Zugriffsrecht "Modify (M)" auf die in Frage kommenden Verzeichnisse und Dateien eingeräumt wurde, können die vergebenen Netware-Attribute ändern und somit jede Aktion, die sich aus ihren effektiven Rechten ergibt, ausführen.

Die Sicherheit durch den Einsatz von Netware-Attributen stellt sich somit als ein Subsystem in der Verzeichnis- und Dateisicherheit dar.

Bei der Vergabe von Netware-Attributen auf Verzeichnisse und Dateien sollten die folgenden Eigenschaften von Netware-Attributen beachtet werden.

- **Verzeichnis-Attribute:**

  Hidden (H): Das Verzeichnis wird als versteckt gekennzeichnet; es erscheint weder in einem Inhaltsverzeichnis unter DOS, noch kann es gelöscht oder kopiert werden.

  System (Sy): Das Verzeichnis (z. B. *SYS:SYSTEM\DELETED.SAV)* wird vom System benutzt; es erscheint ebenfalls nicht in einem Inhaltsverzeichnis unter DOS und kann weder kopiert noch gelöscht werden.

  Rename Inhibit (R): Das Verzeichnis kann nicht umbenannt werden.

  Delete Inhibit (D): Das Verzeichnis kann nicht gelöscht werden.

  Purge (P): Das Verzeichnis sowie die in ihm befindlichen Dateien werden beim Löschen sofort, auch physikalisch, gelöscht. Eine Wiederherstellung des Verzeichnisses mit Hilfe von *SYS:\PUBLIC\SALVAGE.EXE* ist nicht möglich.

- **Datei Attribute:**

  Read write (Rw): Auf die Datei ist sowohl Lese- wie auch Schreibzugriff möglich.

  Read only (Ro): Die Datei kann nur gelesen werden. Ein Schreibzugriff ist nicht möglich. Um Datenverluste bei einer gemeinsamen Benutzung zu vermeiden, sollten diese Dateien ebenfalls das Attribut "Shareable" (S) besitzen.

  Ausführbare Programmdateien (*.exe, *.com) sollten mit dem Attribut "Read only" versehen werden, um einem möglichen Befall durch Computer-Viren vorzubeugen.

  Shareable (S): Diese Dateien können von mehreren Benutzern gleichzeitig benutzt werden. Dateien, die mit dem Attribut "Shareable" versehen worden sind, sollten gleichzeitig das Attribut "Read Only" (RO) besitzen. Das Attribut "Shareable" ist nur relevant für Programme, die Dateien nicht netzfähig öffnen.

  Purge (P): Dateien mit dem Attribut "Purge" werden beim Löschen nicht nur logisch, sondern sofort physikalisch gelöscht. Dies hat zur Folge, dass die Datei nicht wiederhergestellt werden kann (*SYS:PUBLIC\SALVAGE.EXE*).

  In diesem Zusammenhang wird darauf hingewiesen, dass die physikalische Löschung von Dateien nicht nur durch das Netware-Attribut "Purge" erfolgen kann. Wenn das sichere Löschen von Verzeichnissen und Dateien gewünscht wird, dann kann hierzu das Netware Programm *SYS:PUBLIC\PURGE.EXE* eingesetzt werden.

  Transactional (T): Dateien mit diesem Attribut unterliegen der Transaktionskontrolle von Novell Netware. Als Transaktion wird hier eine zusammenhängende Folge von Veränderungen in einer oder mehreren

Dateien verstanden. Das Setzen dieses Attributes bewirkt, dass nur vollständig durchgeführte Transaktionen in den Datenbestand der Datei übernommen werden. Transaktionen, die unkorrekt abgebrochen wurden, werden von Novell Netware rückgängig gemacht.

Archive needed (A): Die so durch Novell Netware gekennzeichneten Dateien sind seit der letzten Datensicherung inhaltlich verändert oder neu auf dem Novell Netware Server aufgespielt worden. Datensicherungssoftware kann somit bei einer sequentiellen Datensicherung erkennen, dass die Datei erneut gesichert werden muss.

Copy Inhibit (C): Derartige Dateien können nicht kopiert werden. Dieses Netware-Attribut gilt allerdings nur für APPLE Macintosh Workstations.

Delete Inhibit (D): Die Datei kann nicht gelöscht werden.

Rename Inhibit (R): Die Datei kann nicht umbenannt werden.

Execute Only (X): Ausführbare Programmdateien (**.EXE*, **.COM*), die mit diesem Attribut versehen werden, können ausschließlich ausgeführt oder gelöscht werden. Ein Kopieren der Datei ist nicht möglich.

Hidden (H): Die Datei wird als versteckt gekennzeichnet. Sie erscheint nicht in einem Inhaltsverzeichnis unter DOS und kann weder kopiert noch gelöscht werden.

System (S): Die Datei (z. B. Bindery Dateien -*NET$OBJ.SYS*, *NET$PROP.SYS*, *NET$VAL.SYS)* wird vom Netzbetriebssystem verwendet; sie erscheint ebenfalls nicht in einem Inhaltsverzeichnis unter DOS und kann weder kopiert noch gelöscht werden.

Sicherung wichtiger Systemdateien

Die Server Startdateien *AUTOEXEC.NCF* und *STARTUP.NCF* sollten, in ihrer jeweils aktuellen Fassung, durch den Systemadministrator auf Diskette gesichert werden und vor unbefugtem Zugriff gesichert hinterlegt werden. Es ist sinnvoll, diese Dateien durch Kommentierungszeilen zu ergänzen, damit beim Auftreten von Problemen die jeweils eingestellten Parameter nachvollzogen werden können.

Weiterhin sollte die Bindery (*NET$OBJ.SYS*, *NET$PROP.SYS*, *NET$VAL.SYS*) eines Novell Netware Servers regelmäßig mit Hilfe des Programms *SYS:SYSTEM\BINDFIX.EXE* gesichert werden. Die gesicherte Bindery (*SYS:SYSTEM*.OLD*) sollte im Anschluss auf einen Datenträger gesichert und vor unbefugten Zugriff geschützt hinterlegt werden.

Nach der Ausführung von *SYS:SYSTEM\BINDFIX.EXE* sollte die Integrität der neuen Bindery auf jeden Fall getestet werden. Im Zweifelsfalle kann die alte Bindery durch *SYS:SYSTEM\BINDREST.EXE* wiederhergestellt werden.

Da die aktuelle Bindery während der Ausführung von *SYS:SYSTEM\BINDFIX.EXE* dem Zugriff der Benutzer entzogen wird, sollte aus Gründen der Betriebssicherheit bei der Sicherung der Bindery eines Novell Netware Servers außer dem Supervisor bzw. dem Supervisor-äqui-

valenten Benutzer kein Benutzer auf dem Novell Netware Server eingeloggt sein.

Eingeschränkte Nutzung des Supervisor Account bzw. eines Supervisor-äquivalenten Account

Der Account des Supervisors sollte bei der täglichen Administrationsarbeit nicht verwendet werden, sondern nur in Notfällen benutzt werden. Um dennoch die Systemadministration zu gewährleisten, sollte daher für jeden Benutzer mit der Netware-Sicherheitsstufe "Supervisor" ein Supervisor-äquivalenter Account eingerichtet werden, mit dem die Systemadministration normalerweise erfolgt. Werden die Administrationsarbeiten nicht hauptamtlich wahrgenommen, so sollten für die nicht-administrativen Aufgaben zusätzlich aufgabenbezogene Accounts eingerichtet werden.

Der Account des Supervisors bzw. eines Supervisor-äquivalenten Account sollte weiterhin nur auf hierzu definierten Workstations verwendet werden, da die Integrität anderer Workstations u. U. durch Benutzer manipuliert sein könnte.

Delegierung der Systemverwaltung

In größeren Netzen (mehrere Novell Netware Server oder verschiedene Liegenschaften) bzw. bei einer größeren Anzahl von Benutzern empfiehlt es sich, bestimmte Aufgaben der Systemadministration zu delegieren. Novell Netware 3.x bietet hierzu die Möglichkeit, Benutzer zu User-Account-Managern bzw. Workgroup-Managern zu bestimmen.

User-Account-Manager können die Benutzer und Gruppen verwalten, die ihnen vom Systemverwalter zugewiesen wurden. Dabei sind sie in der Lage, neben der Änderung der Benutzerdaten (Passwort, Benutzungszeiten usw.) alle Rechte, über die sie selbst verfügen, weiter zu geben. Des weiteren kann der User-Account-Manager einzelne Benutzer einer Gruppe zuweisen. Dabei müssen sowohl die Gruppen als auch die Benutzer vom entsprechenden User-Account-Manager verwaltet werden. Der User-Account-Manager ist nicht in der Lage neue Benutzer oder Gruppen einzurichten. Allerdings kann er ihm zugewiesene Benutzer oder Gruppen löschen.

Ein Workgroup-Manager hat alle Rechte eines User-Account-Managers. Darüber hinaus ist er in der Lage, neue Benutzer und Gruppen einzurichten. Eine weitere Aufgabe des Workgroup-Managers ist das Einrichten von Druckerwarteschlangen.

Nutzung von NCP-Paket-Signatur

Die Kommunikation eines Novell Netware Clients mit einem Novell Netware-Server wird durch das Netware Core Protokoll (NCP) gesteuert. Client und Server tauschen hierbei einzelne Pakete aus, in denen die Daten enthalten sind. Ein potentieller Angreifer kann diese Pakete mittels spezieller Programme (siehe G 5.58 *"Hacking Novell Netware"*) überwachen und die Datenpakete höher privilegierter Benutzer manipulieren.

Um dieser Bedrohung entgegenzuwirken, wurde die Paket-Signatur entwickelt. Bei der Anmeldung eines Benutzers am Server wird ein geheimer Schlüssel ermittelt. Wann immer die Workstation daraufhin eine Anfrage über

NCP an den Server sendet, wird diese mit einer Signatur versehen, die aus dem geheimen Schlüssel und der Signatur des vorherigen Pakets gebildet wird. Diese Signatur wird an das betreffende Paket angehängt und zum Server gesandt. Bevor die eigentliche Anfrage bearbeitet wird, verifiziert der Server die Paket-Signatur.

Durch die Option *Set NCP Packet Signature* -Wert- kann die Paket-Signatur am Server aktiviert werden.

Es sind folgende NCP-Paket-Signatur Level möglich:

Wert "0":	Es findet keine NCP-Paket-Signatur statt.
Wert "1":	Der Novell Netware Server arbeitet auf Anforderung des Clients mit der NCP-Paket-Signatur.
Wert "2":	Der Novell Netware Server fordert vom Client NCP-Paket-Signatur an. Sollte der Client dieses nicht realisieren können, so wird die Kommunikation zwischen Client und Novell Netware Server trotzdem zugelassen.
Wert "3":	Die NCP-Paket-Signatur ist zwingend vorgeschrieben.

Tabelle: NCP-Paket-Signatur Level

Zur Gewährleistung der IT-Sicherheit sollte die NCP-Paket-Signatur mit dem Wert "3" gewählt werden. Da sich jedoch die Netzlast beim Einsatz der NCP-Paket-Signatur um bis zu 30% erhöht, sollte im Vorfeld des Einsatzes geklärt werden, ob die Performance hierdurch nicht unzumutbar eingeschränkt wird.

Beschränkung des nutzbaren Festplattenspeichers

Mit Hilfe des Programms *SYS:PUBLIC\DSPACE.EXE* sollte der auf einem Volume oder einem Verzeichnis zur Verfügung stehende Festplattenspeicher limitiert werden, da erfahrungsgemäß die Inanspruchnahme des zur Verfügung stehenden Festplattenspeichers mit der Kapazität des Festplattenspeichers steigt.

Alternativ hierzu kann auch, soweit eingerichtet, die Kapazität des jeweiligen persönlichen Verzeichnis eines Benutzers beschränkt werden, wenn für die Arbeitsdaten eigene Verzeichnisse eingerichtet wurden.

Sperrung von nicht benötigten Programmen

Die meisten der unter *SYS:PUBLIC* bereitgestellten Novell Netware Programme werden durch die Netware-Benutzer im Regelfall nicht benötigt, da viele der Funktionen (Druckerkonfigurationen, Änderung des Passwortes, Laufwerkszuweisungen) durch die Client- Software gehandhabt werden können. Aus diesem Grund sowie der meist ungewohnten Handhabung der Novell Netware Dienstprogramme empfiehlt es sich, nicht benötigte Programme in das Verzeichnis *SYS:SYSTEM* zu verschieben. Insbesondere das Programm *SYS:PUBLIC\RENDIR.EXE* sollte wegen der erkannten Gefährdung (G 5.54 *Vorsätzliches Herbeiführen eines Abnormal End*) den Benutzern nicht zur Verfügung gestellt werden.

Keinesfalls sollten, wie oftmals beobachtet, die unter *SYS:SYSTEM* gespeicherten Programme in das Verzeichnis *SYS:PUBLIC* verlagert werden.

Information über Patches von Novell Netware

Im Verlauf der Entwicklung des Netzbetriebssystems Novell Netware 3.x haben sich diverse Schwachstellen bzw. Unzulänglichkeiten herausgestellt, die durch den Hersteller mit Hilfe von so genannten Patches größtenteils behoben wurden. Diese Patches werden durch den Hersteller im Internet zur Verfügung gestellt (http://www.novell.com, ftp.novell.com bzw. http://www.novell.de, ftp.novell.de). Informationen über die Funktionalität sowie das ggf. erforderliche Einspielen der zur Verfügung gestellten Patches können daher Schwachstellen im laufenden Produktionsbetrieb beseitigen. Insbesondere zusätzlich installierte Softwareprodukte, wie z. B. zur Datensicherung, erfordern oftmals einen bestimmten Patchlevel des Netzbetriebssystems. Hierbei ist jedoch zu beachten, dass die angebotenen Patches keineswegs blind aufgespielt werden sollten, sondern nur im Bedarfsfall ("never change a running system") sowie nach gründlicher Information.

Soweit vorhanden, sollten diese Patches zunächst auf einer Testkonfiguration ausgetestet werden.

Im Internet (Usenet) ist, neben den internationalen Diskussionsforen zum Thema Novell Netware (z. Z. comp.os.netware.announce, comp.os.netware.misc, comp.os.netware.security, bit.listserv.novell), für die deutschsprachigen Benutzer ein deutsches Novell Forum (z. Z. de.comp.sys.novell) vorhanden, in dem einige versierte Novelladminstratoren aktiv sind, die oftmals auch die schwierigsten Probleme zu lösen helfen. Außerdem werden zu den im Internet am häufigsten gestellten Fragen Dateien (so genannte FAQs - Frequently Asked Questions) zur Verfügung gestellt, die die häufigsten Probleme thematisieren und Lösungen anbieten.

Patches und Informationen über Novell Netware werden darüber hinaus auch über andere Anbieter von Netzdiensten, wie z. B. Compuserve, Fidonet und Mailboxen bereitgestellt.

Für die Richtigkeit und Vollständigkeit der jeweiligen Informationen in den Usenet Diskussionsforen sowie in den FAQs kann an dieser Stelle jedoch keine Garantie gegeben werden. Es sei darauf hingewiesen, dass eine vollständige Beschreibung des aufgetretenen Problems, sowie eine Beschreibung der jeweiligen Konfiguration des Netzes (Client, Server) besonders vorteilhaft bei der Hilfesuche im Internet (Usenet) ist.

Schwierigkeiten während des Netzbetriebes können darüber hinaus oftmals durch die Nachfrage bei dem Verkäufer des Netzbetriebssystems oder im Informationsaustausch mit Kollegen behoben werden; wobei auch hier die Problemlösung durch eine vollständige Konfigurationsbeschreibung erleichtert wird.

Prüfung auf Computer-Viren

Computer-Viren, die sich in den auf einem Novell Netware Server gespeicherten Programmen und Dateien befinden, können, aufgrund der zentralen Verteilung durch den Novell Netware Server an die Workstations, erhebliche Schäden im Netzverbund hervorrufen.

Aus diesem Grund sollten die Programme und Dateien eines Novell Netware Servers regelmäßig mit einem aktuellen Virensuchprogramm auf evtl. vorhandene Computer-Viren überprüft werden.

Zu diesem Zweck empfiehlt es sich einen speziellen Benutzer-Account auf dem Novell Netware Server einzurichten, der über die Zugriffsrechte "Read" (R) und "File Scan" (F) auf alle Dateien des Servers verfügt. Die Prüfung auf Computer-Viren sollte keinesfalls mit den Rechten des Supervisors, bzw. Supervisor-äquivalenten Rechten durchgeführt werden, da ein Computer-Viren-Checkprogramm, welches selbst mit einem Computer-Virus infiziert ist, diesen auf alle Programme und Dateien des Novell Netware Servers übertragen würde.

Die Benutzer bzw. Benutzergruppen sollten auf die Verzeichnisse und Dateien mit ausführbarem Programmcode lediglich die effektiven Rechte "Read" (R) und "File scan" (F) erhalten, zudem sollten ausführbare Programme mit dem Netware-Attribut "Read only" (RO) versehen werden.

M 2.101 Revision von Novell Netware Servern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die vollständige Revision eines Novell Netware 3.x Servers dürfte in der Praxis im Rahmen IT-Grundschutz kaum möglich sein. Folgende Revisionsansätze sollten dennoch beachtet werden:

Durch das Programm *SYS:SYSTEM\SECURITY.EXE* werden die Bindery-Dateien eines Novell Netware Servers auf die nachfolgenden Sicherheitsschwachstellen hin untersucht und die erkannten Schwachstellen aufgelistet.

No password assigned

Benutzer, die kein Passwort für das Login auf dem Novell Netware Server benötigen, werden aufgelistet.

Insecure passwords

Hierbei wird die Bindery des Novell Netware Servers auf mehrere Aspekte hin untersucht.

Zum einen werden die Benutzer angezeigt, deren Passwort gleich dem Anmeldenamen auf dem Novell Netware Server ist; weiterhin werden alle Benutzer aufgeführt, deren Passwort weniger als fünf Zeichen lang sein darf. Es wird weiterhin für jeden Benutzer geprüft, ob die Gültigkeitsdauer eines Passwortes mehr als 60 Tage beträgt und ob eine unbegrenzte Anzahl von "Frei-Anmeldungen" (Grace Logins) möglich ist.

Supervisor equivalence

SYS:SYSTEM\SECURITY.EXE überprüft die Bindery eines Novell Netware Servers dahingehend, ob Benutzer die Sicherheitsstufe "Supervisor" (Supervisor equivalence) auf dem Novell Netware Server haben, und führt diese auf.

Root directory privileges

Aufgrund der nach "unten" gerichteten Vererbung von Zugriffsrechten werden alle Benutzer eines Novell Netware Servers dahingehend geprüft, ob sie Zugriffsrechte im Hauptverzeichnis (Volume Ebene) haben.

Login scripts

Es werden alle Benutzer ermittelt, die über kein eigenes Login Script (User Login Script) verfügen.

Da alle Benutzer, um elektronische Nachrichten austauschen zu können, standardmäßig über das Zugriffsrecht "Create" in dem Verzeichnis *SYS:MAIL* verfügen, könnte ein "Angreifer" einem Benutzer, der über kein User Login Script verfügt, in dessen *SYS:MAIL* Verzeichnis eine Datei *LOGIN* (User-Login-Script) kopieren, mit dem dessen Novell Netware Umgebung verändert würde.

Excessive rights

Novell Netware 3.x stellt im Rahmen der Installation standardmäßig mehrere Verzeichnisse zur Verfügung (*SYS:SYSTEM, SYS:PUBLIC, SYS:LOGIN*). SYS:SYSTEM*SECURITY.EXE* überprüft die Bindery des Novell Netware Servers, ob Benutzer in diesen Verzeichnissen größere Rechte haben, als die standardmäßig vorgegebenen. Weiterhin werden die *SYS:MAIL* Verzeichnisse aller Benutzer auf das alleinige Verfügungsrecht (Ausnahme "Create" für die Gruppe "Everyone") des jeweiligen Inhabers geprüft.

Ergänzende Kontrollfragen:

- Wann wurde die letzte Revision durchgeführt?
- In welchen Intervallen erfolgt eine Revision?

M 2.102 Verzicht auf die Aktivierung der Remote Console

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Das Netzbetriebssystem Novell Netware ermöglicht mittels des Programmes *SYS:\SYSTEM\RCONSOLE.EXE* die Fernsteuerung der Novell Netware Serverkonsole durch eine Workstation. Der Novell Netware Server wird hierzu in der *AUTOEXEC.NCF* durch das Laden von *REMOTE.NLM* mit dem dazugehörenden Passwort und *RSPX.NLM* eingerichtet. Dabei muss vermieden werden, dass das Passwort im Klartext in der *AUTOEXEC.NCF* enthalten ist. Dazu kann nach Ausführen des Programms *REMOTE.NLM* der Befehl *REMOTE ENCRYPT* an der Serverkonsole eingegeben werden. Das dann abgefragte Passwort wird verschlüsselt und auf Wunsch mit dem dazugehörigen Befehl in der Datei *LDREMOTE.NCF* abgelegt. Der Befehl in der Datei *LDREMOTE.NCF* sieht z. B. wie folgt aus:

LOAD REMOTE -E 0613BB68060099

Netzanalyse-Tools, so genannte Sniffer, können die Daten, die zwischen der Workstation und dem Novell Netware Server ausgetauscht werden, auslesen und speichern. Hierzu gehört auch das verschlüsselte Passwort, welches zur Fernsteuerung des Novell Netware Servers eingegeben werden muss. Spezielle Software ist in der Lage, das verschlüsselte Passwort zu entschlüsseln. Unbefugte können hierdurch in die Lage versetzt werden, mittels der Fernsteuerung Zugriff auf die Konsole des Novell Netware Servers zu erlangen.

Um zudem zu verhindern, dass Remote-Sitzungen mit Netzanalyse-Tools aufgezeichnet und danach einfach wieder ins Netz eingespielt werden können, sollte darauf geachtet werden, dass Signaturen bei den RSPX-Paketen aktiviert sind. Dies kann überprüft werden, indem der Befehl *RSPX* an der Konsole des Servers ausgeführt wird. Die Antwort sollte wie folgt aussehen:

RSPX Packet Signatures:

All packets must contain signatures.

Sollten hier keine Signaturen aktiviert sein, kann dies durch den Befehl *RSPX SIGNATURES ON* veranlasst werden. Da diese Funktion erst ab Netware 3.12 unterstützt wird, sollte unbedingt auf die aktuelle Netware Version zurückgegriffen werden.

Soweit die örtlichen Gegebenheiten und die betrieblichen Abläufe dieses zulassen, sollte aus Sicherheitserwägungen auf die Fernsteuerung von Novell Netware Servern verzichtet werden.

Generell gilt jedoch, wenn C2-Sicherheit umgesetzt werden soll (siehe auch M 4.102 *C2-Sicherheit unter Novell 4.11*), dann darf das Programm *SYS:\SYSTEM\RCONSOLE.EXE* nicht eingesetzt werden.

M 2.103 Einrichten von Benutzerprofilen unter Windows 95

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Unter Windows 95 besteht die Möglichkeit, durch Einrichten von Benutzerprofilen eine Benutzertrennung durchzuführen. Diese Trennung dient jedoch (wenn nicht durch Systemrichtlinien eine Einschränkung erfolgt, siehe M 2.104 *Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95*) ausschließlich dazu, benutzerspezifische Einstellungen zu konservieren und damit für den jeweiligen Benutzer eine individuelle Arbeitsumgebung zu erhalten, die er nach seinen Bedürfnissen und Erfordernissen anpassen kann. Ein Windows 95-Anmeldepasswort wird erst nach Aktivieren der Benutzerprofile obligatorisch. Für dieses Passwort gelten im übrigen dieselben Überlegungen wie für WfW-Anmeldepasswörter (siehe M 4.46 *Nutzung des Anmeldepasswortes unter WfW und Windows 95*).

Die den Benutzer betreffenden Einstellungen werden in einem Verzeichnis *C:\WINDOWS\PROFILES\Benutzername* gespeichert.

Benutzerprofile sollten auf einem nicht vernetzten Windows 95-Rechner immer dann aktiviert werden, wenn unerfahrenen Benutzern das Navigieren unter Windows 95 erleichtert werden soll. Dies ist ebenfalls sinnvoll, wenn eine Benutzertrennung, wenn auch nicht unter Sicherheitsgesichtspunkten, so doch aus organisatorischen oder prinzipiellen Gründen gewünscht wird.

Dazu öffnet man die Programmgruppe *SYSTEMSTEUERUNG*, dann die Schaltfläche *KENNWÖRTER* und kann anschließend die Benutzerprofile aktivieren bzw. deaktivieren.

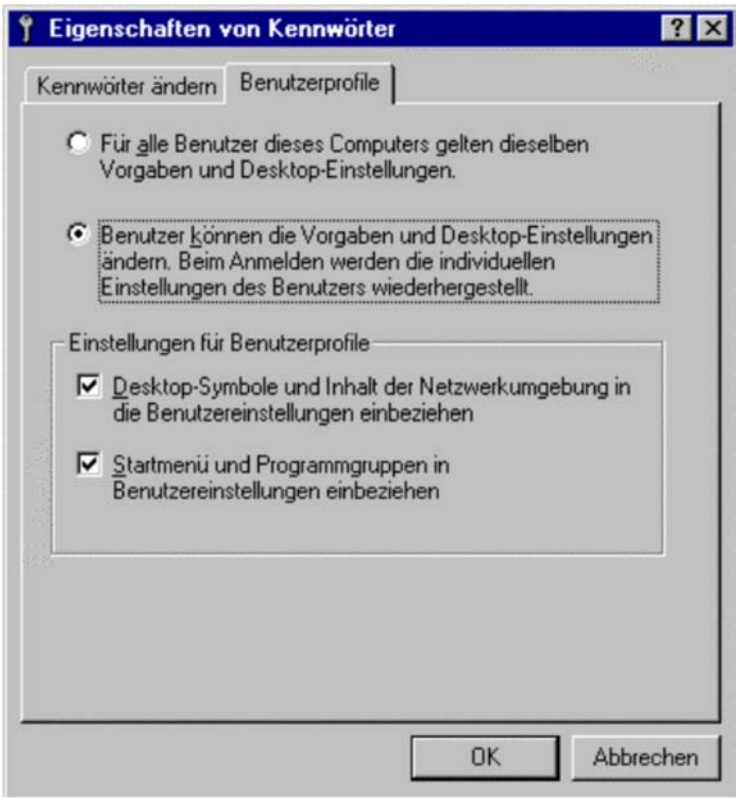


Abbildung: Maske Benutzerprofile

Hinweis: In Novell Netware- oder Windows NT-Netzen können verpflichtende Benutzerprofile angelegt werden, indem das entsprechende Profil in einem dem Benutzer zugeordneten Netzverzeichnis zugriffsgeschützt gespeichert wird. Dieses Profil hat den Namen *USER.MAN* und wird bei jeder Anmeldung am Server automatisch geladen (siehe M 4.51 *Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT*).

Ergänzende Kontrollfragen:

- Sollen an dem Windows 95 Rechner mehrere Benutzer arbeiten?
- Ist eine Benutzertrennung unter Sicherheitsgesichtspunkten oder aus organisatorischen bzw. prinzipiellen Gründen sinnvoll?

M 2.104 Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Soll unerfahrenen Benutzern das Navigieren unter Windows 95 erleichtert werden oder ist aus betrieblicher Sicht die Einschränkung bestimmter Ressourcen notwendig, so kann unter Windows 95 mit so genannten Systemrichtlinien die Benutzerumgebung benutzerspezifisch mit bestimmten Restriktionen versehen werden. Jedoch sollte berücksichtigt werden, dass Benutzer gegenüber dem IT-System möglicherweise eine abweisende Haltung einnehmen, wenn Einschränkungen nicht unmittelbar einsichtig sind. Eine Einschränkung sollte also nur dann erfolgen, wenn sie tatsächlich notwendig ist oder wenn sie vom Benutzer nicht bemerkt wird.

Sobald Systemrichtlinien aktiviert sind, wird beim Starten von Windows 95 überprüft, ob benutzerspezifische Einschränkungen für den aktuellen Benutzer eingerichtet wurden. Ist dies der Fall, werden diese geladen. Ist dies nicht der Fall, werden die Einschränkungen für den Standardbenutzer herangezogen. Im folgenden werden zunächst die prinzipiellen Einschränkungen beschrieben, die mit den **Systemrichtlinien** eingestellt werden können. Anschließend wird aufgezeigt, wie diese mittels des Systemrichtlinieneditors (*POLEDIT.EXE)* angelegt und aktiviert werden können.

Die wesentlichen mit Systemrichtlinien einzustellenden Restriktionen für einen nicht vernetzten Windows 95-Rechner sind:

- Der Zugriff auf die **Systemsteuerung** kann bezüglich der Optionen *ANZEIGE, NETZWERK, KENNWÖRTER, DRUCKEREINSTELLUNGEN* und *SYSTEM* eingeschränkt werden. Die jeweiligen Optionen können zum Teil vollständig deaktiviert oder auf einzelne Registerkarten beschränkt werden.

  Wesentlich bei diesen Optionen sind folgende Punkte:

  - Es können Vorgaben für Bildschirmfarben unter Ergonomiegesichtspunkten gemacht werden.
  - Es kann vorgesehen werden, eigene Kennwörter durch den Benutzer ändern zu lassen.
  - Druckerkonfiguration und Hardware-Einstellungen lassen sich fest vorgeben.

- Der Zugriff auf einzelne Funktionen der **Benutzeroberfläche** kann eingeschränkt werden. Beispielsweise können die Befehle *AUSFÜHREN*, *SUCHEN* und *BEENDEN* entfernt werden. Damit wird zum Beispiel verhindert, dass Benutzer nach sicherheitsrelevanten Dateien oder Programmen suchen und diese dann ggf. ausführen. Die Laufwerke lassen sich aus dem *ARBEITSPLATZ* und für den *EXPLORER* (dem früheren Dateimanager) ausblenden. Partitionen (Laufwerke) können dann ggf. nur noch

aus Anwendungen heraus gewechselt werden, da standardmäßig nur die Start-Partition (z. B. *C:*) zur Verfügung steht.

- Der **Programmstart** von ausführbaren Dateien kann eingeschränkt und die DOS-Eingabeaufforderung deaktiviert werden. Die für den einzelnen Benutzer erlaubten Anwendungen lassen sich explizit vorgeben (z. B. *WINWORD.EXE, EXCEL.EXE* und *EXPLORER.EXE*)

Zusätzlich kann für den Rechner gefordert werden, dass die Windows 95-Anmeldekennwörter sowohl aus Buchstaben als auch aus Sonderzeichen oder Zahlen bestehen müssen und welche Mindestlänge sie aufweisen sollen. Programme, die beim Systemstart ausgeführt werden sollen, lassen sich ebenfalls vorgeben.

Im folgenden wird in einzelnen Schritten gezeigt, wie Systemrichtlinien angelegt und aktiviert werden können und welche Restriktionen für einen nicht vernetzten Windows 95-Rechner Sicherheit bieten:

1. Anlegen einer Systemrichtliniendatei

Mit Hilfe des Systemrichtlinieneditors wird eine Systemrichtliniendatei erzeugt. Ihr Name ist zwar beliebig, jedoch wird an dieser Stelle der Einfachheit halber der Name *CONFIG.POL* gewählt. Dazu wird das Programm *POLEDIT.EXE* aufgerufen, eine neue Datei angelegt und diese unter dem Namen *CONFIG.POL* abgespeichert. Diese Datei enthält automatisch Einträge für den Standardbenutzer und den Standardcomputer, die im nächsten Schritt ggf. einzuschränken sind. Für den Administrator sind ebenfalls Einträge für den Computer und den Benutzer anzulegen (im Menü *BEARBEITEN* mit *BENUTZER HINZUFÜGEN* und *COMPUTER HINZUFÜGEN*), die im dritten Schritt zu spezifizieren sind.

Abbildung: Systemrichtlinien-Editor

2. Definition einer Richtlinie für den Standardbenutzer und Standardcomputer

Öffnet man mit dem Systemrichtlinieneditor die Einstellungen für den Standardbenutzer, so kann man menügeführt die entsprechenden sicherheitsrelevanten Einträge vornehmen.

Beispielsweise:

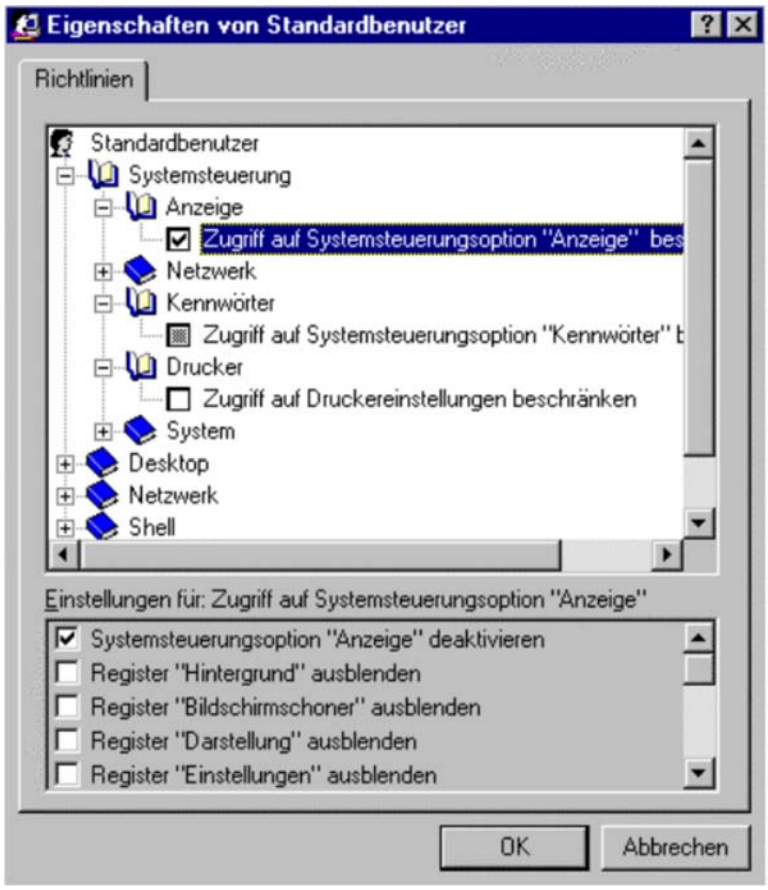


Abbildung: Maske Eigenschaften Standardbenutzer

Für einen **Standardbenutzer** sollten folgende Restriktionen eingestellt werden:

Systemsteuerung

- Der Zugriff auf die Registerkarte *BILDSCHIRMSCHONER* sollte dann deaktiviert werden, wenn der Benutzer die Bildschirmsperre nicht deaktivieren können soll. In diesem Fall ist ihm allerdings die Möglichkeit zu geben, das Bildschirmpasswort zu ändern. Dazu darf die *SYSTEMSTEUERUNG* (s. u.) nicht vollständig und bei der Option *KENNWÖRTER* die Registerkarte *KENNWORT ÄNDERN* nicht deaktiviert sein.
- Damit der Benutzer die Systemrichtlinien nicht deaktivieren kann, ist zwingend die Registerkarte *BENUTZERPROFILE* für die Systemsteuerungsoption *KENNWÖRTER* auszublenden.
- Die Einstellungen für die Hardware-Konfiguration sind vorzunehmen und der Zugriff auf die Register und Schaltflächen für die Systemsteuerungsoption *SYSTEM* maximal zu beschränken, damit fehlerhafte Konfigurationen durch den Benutzer vermieden werden, die die Verfügbarkeit oder Leistungsfähigkeit des Rechners einschränken können.

Shell-Zugriffsbeschränkungen

- Der Befehl *AUSFÜHREN* sollte deaktiviert werden, wenn verhindert werden soll, dass bestimmte Programme unter Angaben von Optionen gestartet werden können.
- Die *SYSTEM*- und *DRUCKERSTEUERUNG* kann vollständig deaktiviert werden, wenn man die Option *ORDNER UNTER "EINSTELLUNGEN" IM MENÜ "START" ENTFERNEN* aktiviert. Dies ist immer dann notwendig, wenn dem Benutzer jegliche Möglichkeit genommen werden soll, System- oder Druckereinstellungen zu ändern. Damit der Benutzer sein Bildschirmpasswort ändern kann, ist unter der Systemsteuerungsoption *ANZEIGE* die Registerkarte *BILDSCHIRMSCHONER* (siehe oben) freizugeben. Der Benutzer kann dann durch Klicken mit der rechten Maustaste auf den Desktop über *EIGENSCHAFTEN* auf die Bildschirmsperre zugreifen.
- Soll die Benutzung des *EXPLORERS* nicht erlaubt sein, so ist die Option *LAUFWERKE IM FENSTER "ARBEITSPLATZ" AUSBLENDEN* zu aktivieren, da der *EXPLORER* über den *ARBEITSPLATZ* gestartet werden kann, selbst wenn die Nutzung explizit verboten wurde.

System-Zugriffsbeschränkungen

- Die Option *PROGRAMME ZUM BEARBEITEN DER REGISTRIERUNG DEAKTIVIEREN* ist zu wählen.
  Hinweis: Diese Option betrifft nur den Registrierungseditor (*REGEDIT.EXE*). Mit dem Systemrichtlinien-Editor (*POLEDIT.EXE*) lässt sich die lokale Registrierung nach wie vor bearbeiten. Dieses Programm sollte daher von der Festplatte gelöscht werden.
- Es sollten nur zugelassene Anwendungen ausführbar sein.
  Es sind diejenigen Anwendungen, wie etwa *WINWORD.EXE*, *ACCESS.EXE*, *EXPLORER.EXE*, einzutragen, die der Benutzer ausführen können soll.
- Die MS-DOS-Eingabeaufforderung ist zu deaktivieren.
- Ggf. sind Single-Mode-Anwendungen für MS-DOS zu deaktivieren.
  Falls einige DOS-Anwendungen unter Windows 95 aufgerufen werden sollen, der Benutzer aber nicht auf die DOS-Ebene gelangen soll, ist die DOS-Eingabeaufforderung zu **aktivieren**, jedoch sind bei den zugelassenen Anwendungen für Windows nur diejenigen zu nennen, die benötigt werden. Die *COMMAND.COM* darf dann dort **nicht** genannt werden.

Für einen **Standardcomputer** sollten folgende Restriktionen eingestellt werden:

Netzwerk

- Unter *KENNWÖRTER* ist ein alphanumerisches Windows-Anmeldekennwort und eine Mindestlänge von sechs Zeichen zu fordern.
- Unter *UPDATE* ist *REMOTE-UPDATE* nicht zu deaktivieren, da sonst die Systemrichtlininen nicht geladen werden.

System

- Die *BENUTZERPROFILE* sind zu aktivieren.

3. Definition einer Richtlinie für den Administrator

In einer Richtlinie für den Administrator sollten keine der obigen Restriktionen gesetzt werden. Hierfür ist ein eigener Benutzer unter Windows 95 sowie ein Benutzer und Computer mittels Systemrichtlinien einzurichten, da sonst für ihn die über den Standardbenutzer eingestellten Einschränkungen gelten. Das dazugehörige Passwort darf nur dem Administrator und seinem Vertreter bekannt sein.

Diese Richtlinie ist ebenfalls in der Datei *CONFIG.POL* abzulegen.

4. Definition von Richtlinien für einzelne Benutzer basierend auf dem Standardbenutzer und Standardcomputer

Werden weitere Benutzer benötigt, deren Restriktionen sich von den unter 1. spezifizierten unterscheiden sollen, so sind analog zu 1. diese Richtlinien zusätzlich in der Datei *CONFIG.POL* einzurichten. Dazu kopiert man das Standardprofil, gibt diesem den Namen des betreffenden Benutzers und stellt die Restriktionen wie unter 1. für diesen Benutzer ein.

5. Aktivieren der Richtlinien

Beim Einrichten der Systemrichtlinien durch den Administrator ist besondere Vorsicht und Aufmerksamkeit geboten, da sehr leicht inkonsistente Systemzustände eingestellt werden können, die ein Arbeiten mit dem Rechner verhindern. Das Betriebssystem wäre neu zu installieren. Die Systemrichtlinien sollten also nur dann aktiviert werden, wenn die Richtlinien mit äußerster Sorgfalt definiert wurden.

Dazu öffnet der Administrator mit dem Systemrichtlinieneditor (*POLEDIT.EXE*) die lokale Registrierung und setzt dort für den *LOKALEN COMPUTER* unter der Option *NETZWERK-UPDATE* den Schalter *REMOTE-UPDATE*. Als Update-Modus muss *INTERAKTIV* gewählt werden. Der Pfad für die oben definierte *CONFIG.POL* ist ebenfalls anzugeben.

Die notwendigen Einstellungen können von besonders erfahrenen Administratoren auch mit dem Registrierungseditor (Programm *REGEDIT.EXE*) vorgenommen werden.

Darüber hinaus sind in der Programmgruppe *SYSTEMSTEUERUNG* mit der Schaltfläche *KENNWÖRTER* die Benutzerprofile zu aktivieren.

Ergänzende Kontrollfragen:

- Ist die Einschränkung der Benutzerumgebung aus betrieblicher Sicht notwendig?
- Ist die Einschränkung bestimmter Ressourcen notwendig?

M 2.105 Beschaffung von TK-Anlagen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Haustechnik, Beschaffungsstelle

Bei der Beschaffung neuer TK-Anlagen besteht die Möglichkeit, diese von vornherein so auszugestalten, dass im späteren Betrieb mit geringem personellen und organisatorischen Zusatzaufwand ein hohes Maß an Sicherheit erreicht werden kann. Hierfür muss in erster Linie auf

- das Vorhandensein geeigneter Funktionalitäten für die Anlagenadministration,
- ausreichende Protokollmechanismen und Auswerte-Tools sowie
- die Revisionsfähigkeit der TK-Anlage

geachtet werden. Für den Bereich der Bundesbehörden wurden entsprechende Anforderungen vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in Zusammenarbeit mit dem Zentralverband der Elektrotechnik- und Elektronikindustrie (ZVEI) erarbeitet und in der Broschüre

Sicherheitsanforderungen an TK-Anlagen

- Empfehlungen für den Bereich der Bundesbehörden -

zusammengefasst. Diese Empfehlungen sind aus Sicht des BSI auch auf andere Bereiche der Verwaltung und der Privatwirtschaft übertragbar.

M 2.106 Auswahl geeigneter ISDN-Karten in der Beschaffung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Beschaffungsstelle

Bei der Beschaffung von ISDN-Karten besteht die Möglichkeit, diese von vornherein so auszuwählen, dass im späteren Betrieb Sicherheitsfunktionalitäten nicht teuer hinzugekauft werden müssen. Erforderliche Sicherheitsfunktionalitäten sollten bereits auf der Karte vorhanden sein oder durch mitgelieferte Kommunikationssoftware und Treiberprogramme realisiert werden können.

Mögliche Kriterien für die Auswahl geeigneter ISDN-Karten sind:

- Fähigkeit zur Durchführung einer Authentisierung über PAP und CHAP (Password Authentikation Protocol und Challenge Handshake Authentication Protocol, RFC 1994),
- Vorhandensein eines Verschlüsselungsverfahrens (symmetrisch/asymmetrisch) in Hard- oder Software,
- Möglichkeit der Auswertung von CLIP-Rufnummern (Calling Line Identification Presentation) zur Authentisierung,
- Möglichkeit des Führens einer Rufnummerntabelle für das Durchführen eines Callbacks,
- Möglichkeit der Protokollierung nicht erfolgreicher Verbindungsaufbauten (Ablehnung aufgrund falscher Rufnummern- oder PAP/CHAP-Authentisierung).

Außerdem sind die ISDN-Karten auf Funktionalitäten hin zu untersuchen, die für einen sicheren Betrieb nicht vorhanden sein dürfen, oder falls sie dennoch vorhanden sind, zumindest durch Konfiguration eine Deaktivierung herbeigeführt werden kann. Hierzu zählt z. B. die "Remote-Control"-Funktionalität, die einen direkten Kommunikationsaufbau zum IT-System aus dem öffentlichen Netz zulässt.

Beachtet werden sollte, dass sowohl im Bereich der IT-Systeme, die mit ISDN-Karten ausgestattet werden sollen, als auch im Bereich der Netzkoppelelemente (z. B. ISDN-Router) ISDN-Karten mit möglichst gleichen Sicherheitsfunktionalitäten eingesetzt werden. Ist dies nicht gewährleistet, entfalten Sicherheitsfunktionalitäten, die auf beiden Seiten erforderlich sind, nicht die gewünschte Wirkung.

Ergänzende Kontrollfrage:

- Sind der Beschaffungsstelle diese ergänzenden Anforderungen an ISDN-Karten bekannt?

M 2.107 Dokumentation der ISDN-Karten-Konfiguration

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Je nach Einsatzgebiet ergeben sich für eine ISDN-Karte nahezu beliebig komplexe Konfigurationseinstellungen. Für das Sicherstellen eines geordneten Wiederanlaufs (z. B. nach Austausch einer ISDN-Karte oder deren Kommunikationssoftware) wird empfohlen, mindestens die folgenden Einstellungen zu dokumentieren:

- Typenbezeichnung der eingesetzten Karte und Seriennummer,
- Rufnummer(n) für den Kommunikationsaufbau und eine evtl. durchzuführende Authentisierung,
- Verwendetes D-Kanal-Protokoll (1TR6, EDSS-1 etc.),
- Verwendetes B-Kanal-Protokoll (X.25, PPP, TCP/IP, Bittransparent etc.),
- Stand der verwendeten CAPI-Version,
- Stand der verwendeten Treiber-Software,
- Art der Datenkompression, wenn verwendet,
- Art der Authentisierung (z. B. PAP/CHAP), wenn verwendet.

Beim Einsatz von Authentisierungsverfahren, die auf dem Besitz eines gemeinsamen Geheimnisses (z. B. Passwort) beruhen, kann auch dieses Geheimnis dokumentiert werden. Beachtet werden muss dann allerdings, dass die erstellte Dokumentation nur einem eingeschränkten Personenkreis zugänglich gemacht werden darf, um das Bekanntwerden des Geheimnisses zu verhindern.

Ergänzende Kontrollfrage:

- Sind in der Dokumentation Passwörter beschrieben? Wird die Dokumentation sicher aufbewahrt?

M 2.108 Verzicht auf Fernwartung der ISDN-Netzkoppelelemente

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der Verzicht auf Fernwartung ist eine wirkungsvolle Maßnahme, um Externe an Manipulationen an ISDN-Routern und IT-Systemen mit ISDN-Karten zu hindern.

Bei IT-Systemen mit ISDN-Karte sollte überprüft werden, ob die verwendete Kommunikationssoftware "Remote-Control"-Funktionalitäten bietet. Hierdurch kann das betreffende IT-System über das öffentliche ISDN angerufen werden, die ISDN-Karte nimmt den Anruf entgegen und der Anrufende bedient das IT-System so, als ob es "vor Ort" wäre. Diese Funktionalität ist zu deaktivieren.

Bei ISDN-Routern sollte die Fernwartung über reservierte Bandbreiten (oder reservierte ISDN-Rufnummern) deaktiviert werden, da hier i. d. R. eine nur über ein Passwort geschützte Verbindung zur Management Information Base des Routers hergestellt wird, in der nahezu alle Konfigurationseinstellungen vorgenommen werden können.

Ergänzende Kontrollfragen:

- Welche Gründe sprechen für und welche gegen den Verzicht der Fernwartung?
- Wurde die Entscheidung über die Fernwartung herbeigeführt?

M 2.109 Rechtevergabe für den Fernzugriff

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der externe Zugriff auf ein Unternehmensnetz muss hinsichtlich der eingeräumten Rechte auf das erforderlich Maß eingeschränkt werden. Über die in M 2.8 *Vergabe von Zugriffsrechten* beschriebenen Anforderungen ist weiterhin zu berücksichtigen, dass die Rechtevergabe für den Fernzugriff noch restriktiver zu handhaben ist.

Beispielsweise müssen für einen Telearbeitsplatz nicht zwingend Zugriffsrechte auf Verzeichnisse mit Software bestehen (siehe G 5.62 *Missbrauch von Ressourcen über abgesetzte IT-Systeme*).

Ergänzende Kontrollfrage:

- Wann wurden die für den Fernzugriff eingeräumten Rechte zuletzt überprüft?

M 2.110 Datenschutzaspekte bei der Protokollierung

Verantwortlich für Initiierung: Leiter IT, Datenschutzbeauftragter

Verantwortlich für Umsetzung: Administrator, Datenschutzbeauftragter

Unter Protokollierung beim Betrieb von IT-Systemen ist im datenschutzrechtlichen Sinn die Erstellung von manuellen oder automatisierten Aufzeichnungen zu verstehen, aus denen sich die Fragen beantworten lassen: "Wer hat wann mit welchen Mitteln was veranlasst bzw. worauf zugegriffen?" Außerdem müssen sich Systemzustände ableiten lassen: "Wer hatte von wann bis wann welche Zugriffsrechte?"

Art und Umfang von Protokollierungen hängen vom allgemeinen Datenschutzrecht und auch von bereichsspezifischen Regelungen ab.

Die Protokollierung der Administrationsaktivitäten entspricht einer Systemüberwachung, während die Protokollierung der Benutzeraktivitäten im wesentlichen der Verfahrensüberwachung dient. Dementsprechend finden sich die Anforderungen an die Art und den Umfang der systemorientierten Protokollierung überwiegend im allgemeinen Datenschutzrecht, während die verfahrensorientierte Protokollierung oft durch bereichsspezifische Regelungen definiert wird. Beispiele für verfahrensorientierte Protokollierung sind u. a. Meldegesetze, Polizeigesetze, Verfassungsschutzgesetze.

Mindestanforderungen an die Protokollierung

Bei der Administration von IT-Systemen sind die folgenden Aktivitäten vollständig zu protokollieren:

- **Systemgenerierung und Modifikation von Systemparametern**

  Da auf dieser Ebene in der Regel keine systemgesteuerten Protokolle erzeugt werden, bedarf es entsprechender detaillierter manueller Aufzeichnungen, die mit der Systemdokumentation korrespondieren sollten.

- **Einrichten von Benutzern**

  Wem von wann bis wann durch wen das Recht eingeräumt worden ist, das betreffende IT-System zu benutzen, ist vollständig zu protokollieren. Für diese Protokolle sollten längerfristige Aufbewahrungszeiträume vorgesehen werden, da sie Grundlage praktisch jeder Revisionsmaßnahme sind.

- **Erstellung von Rechteprofilen**

  Im Rahmen der Protokollierung der Benutzerverwaltung kommt es insbesondere auch darauf an aufzuzeichnen, wer die Anweisung zur Einrichtung bestimmter Benutzerrechte erteilt hat (siehe auch M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*).

- **Einspielen und Änderung von Anwendungssoftware**

  Die Protokolle repräsentieren das Ergebnis der Programm- und Verfahrensfreigaben.

- **Änderungen an der Dateiorganisation**

  Im Hinblick auf die vielfältigen Manipulationsmöglichkeiten, die sich bereits bei Benutzung der "Standard-Dateiverwaltungssysteme" ergeben, kommt einer vollständigen Protokollierung eine besondere Bedeutung zu (siehe z. B. Datenbankmanagement).

- **Durchführung von Datensicherungsmaßnahmen**

  Da derartige Maßnahmen (Backup, Restore) mit der Anfertigung von Kopien bzw. dem Überschreiben von Datenbeständen verbunden sind und häufig in "Ausnahmesituationen" durchgeführt werden, besteht eine erhöhte Notwendigkeit zur Protokollierung.

- **Sonstiger Aufruf von Administrations-Tools**

  Die Benutzung aller Administrations-Tools ist zu protokollieren, um feststellen zu können, ob Unbefugte sich Systemadministrator-Rechte erschlichen haben.

- **Versuche unbefugten Einloggens und Überschreitung von Befugnissen**

  Geht man von einer wirksamen Authentisierungsprozedur und sachgerechten Befugniszuweisungen aus, kommt der vollständigen Protokollierung aller "auffälligen Abnormalitäten" beim Einloggen und der Benutzung von Hard- und Software-Komponenten eine zentrale Bedeutung zu. Benutzer in diesem Sinne ist auch der Systemadministrator.

Bei der Verarbeitung von personenbezogenen Daten sind folgende Benutzeraktivitäten in Abhängigkeit von der Sensibilität der Verfahren bzw. Daten vollständig bzw. selektiv zu protokollieren:

- **Eingabe von Daten**

  Die so genannte Eingabekontrolle erfolgt grundsätzlich verfahrensorientiert (z. B. Protokollierung in Akten, soweit vorhanden, Protokollierung direkt im Datenbestand, sofern keine Akten geführt werden). Auch wenn man davon ausgeht, dass Befugnisüberschreitungen anderweitig protokolliert werden, dürfte eine vollständige Protokollierung von Dateneingaben als Regelfall angesehen werden müssen.

- **Datenübermittlungen**

  Nur soweit nicht gesetzlich eine vollständige Protokollierung vorgeschrieben ist, kann eine selektive Protokollierung als ausreichend angesehen werden.

- **Benutzung von automatisierten Abrufverfahren**

  In der Regel dürfte eine vollständige Protokollierung der Abrufe und der Gründe der Abrufe (Vorgang, Aktenzeichen etc.) erforderlich sein, um unbefugte Kenntnisnahme im Rahmen der grundsätzlich eingeräumten Zugriffsrechte aufdecken zu können.

- **Löschung von Daten**

  Die Durchführung der Löschung ist zu protokollieren.

- **Aufruf von Programmen**

  Dies kann erforderlich sein bei besonders "sensiblen" Programmen, die z. B. nur zu bestimmten Zeiten oder Anlässen benutzt werden dürfen. Deshalb ist in diesen Fällen eine vollständige Protokollierung angezeigt. Die Protokollierung dient auch der Entlastung der befugten Benutzer (Nachweis des ausschließlich befugten Aufrufs der Programme).

Zweckbindung bei der Nutzung von Protokolldaten

Protokolldaten unterliegen aufgrund der nahezu übereinstimmenden Regelungen im Datenschutzrecht des Bundes und der Länder einer besonderen engen Zweckbindung (z. B. § 14 Abs. 4 und § 31 BDSG, § 13 Abs. 5 HDSG). Sie dürfen nur zu den Zwecken genutzt werden, die Anlass für ihre Speicherung waren. Dies sind in der Regel die in einem Sicherheitskonzept festgelegten allgemeinen Kontrollen, die in den meisten Datenschutzgesetzen geforderte "Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden " (siehe z. B. § 18 Abs. 2 BDSG, § 8 Abs. 3 LDSG-SH) und die Kontrollen durch interne oder externe Datenschutzbeauftragte. Nur in Ausnahmefällen lassen die bereichsspezifischen Regelungen die Nutzung dieser Daten für andere Zwecke, z. B. zur Strafverfolgung, zu.

Aufbewahrungsdauer

Soweit nicht bereichsspezifische Regelungen etwas anderes vorsehen, richtet sich die Aufbewahrungsdauer der Protokolle nach den allgemeinen Löschungsregeln der Datenschutzgesetze. Maßstab ist die "Erforderlichkeit zur Aufgabenerfüllung". Gibt es keinen zwingenden Grund für das weitere Vorhalten von Protokolldateien, besteht eine Löschungspflicht (siehe z. B. § 20 Abs. 2 BDSG).

Als Anhaltspunkte können dienen:

- die Wahrscheinlichkeit, dass Unregelmäßigkeiten (noch) offenbar werden können und
- die Möglichkeit, die Gründe von Unregelmäßigkeiten anhand der Protokolle und anderer Unterlagen aufdecken zu können.

Erfahrungsgemäß sollte eine Frist von einem Jahr nicht überschritten werden.

Soweit Protokolle zum Zwecke gezielter Kontrollen angefertigt werden, kommen kürzere Speicherungsfristen in Betracht. In der Regel reicht eine Aufbewahrung bis zur tatsächlichen Kontrolle aus. Auch hier sind die bereichsspezifischen Vorschriften zu beachten.

Technische und organisatorische Rahmenbedingungen

Die Effektivität der Protokollierung und ihre Auswertung im Rahmen von Kontrollen hängt im entscheidenden Maße von den technischen und organisatorischen Rahmenbedingungen ab. In diesem Zusammenhang sollten folgende Aspekte Berücksichtigung finden:

- Es sollte ein Revisionskonzept erstellt werden, das den Zweck der Protokolle und deren Kontrollen sowie Schutzmechanismen für die Rechte der Mitarbeiter und der sonstigen betroffenen Personen klar definiert.
- Die Zwangsläufigkeit und damit die Vollständigkeit der Protokolle muss ebenso gewährleistet werden wie die Manipulationssicherheit der Einträge in Protokolldateien.
- Entsprechend der Zweckbindung der Datenbestände müssen wirksame Zugriffsbeschränkungen realisiert werden.
- Die Protokolle müssen so gestaltet sein, dass eine effektive Überprüfung möglich ist. Dazu gehört auch eine IT-Unterstützung der Auswertung.
- Die Auswertungsmöglichkeiten sollten vorab abgestimmt und festgelegt sein.
- Kontrollen sollten so zeitnah durchgeführt werden, dass bei aufgedeckten Verstößen noch Schäden abgewendet sowie Konsequenzen gezogen werden können. Kontrollen müssen rechtzeitig vor dem Ablauf von Löschungsfristen von Protokolldateien stattfinden.
- Kontrollen sollten nach dem 4-Augen-Prinzip erfolgen.
- Es sollte vorab definiert werden, welche Konsequenzen sich aus Verstößen ergeben, die durch die Kontrolle von Protokollen aufgedeckt werden.
- Die Mitarbeiter sollten darüber informiert sein, dass Kontrollen durchgeführt werden, ggf. auch unangekündigt.
- Für Routinekontrollen sollten automatisierte Verfahren (z. B. watch dogs) verwendet werden.
- Personal- bzw. Betriebsräte sollten bei der Erarbeitung des Revisionskonzeptes und bei der Festlegung der Auswertungsmöglichkeiten der Protokolle beteiligt werden.

M 2.111 Bereithalten von Handbüchern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Bei der Beschaffung von Informationstechnik, egal ob es sich um Hardware oder Software handelt, müssen die zugehörigen Handbücher und technischen Referenzen in ausreichender Anzahl mitbeschafft werden.

Im Lieferumfang von IT-Produkten ist zunehmend keine weiterführende Dokumentation mehr enthalten, sondern es werden neben Online-Hilfen nur noch Installationshilfen und einführende Texte mitgeliefert. Dieser eingeschränkte Umfang an Dokumentationshilfen ist insbesondere bei auftretenden Fehlern unzureichend. Es ist daher darauf zu achten, dass die erforderlichen Handbücher, technische Referenzen und Fehlerkataloge zusätzlich beschafft werden. Hierbei muss nicht ausschließlich auf die vom Hersteller angebotene Literatur zurückgegriffen werden.

Alle Handbücher zu einem IT-Produkt müssen jederzeit in der Anwendungsumgebung verfügbar sein. Beispielweise müssen die Handbücher zu einem Server-Betriebssystem bei diesem Server aufbewahrt werden, und nicht in einer evtl. geschlossenen Bibliothek. Bei der Notfallplanung ist der Zugriff auf diese Literatur einzuplanen (siehe M 6.3 *Erstellung eines Notfall-Handbuches*).

Ergänzende Kontrollfragen:

- Welche Handbücher gibt es zu den eingesetzten IT-Produkten?
- Wo werden die Handbücher verwahrt? Sind sie jederzeit verfügbar?

M 2.112 Regelung des Akten- und Datenträgertransports zwischen häuslichem Arbeitsplatz und Institution

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Mitarbeiter

Damit der Austausch von Akten und Datenträgern zwischen häuslichem Arbeitsplatz und Institution sicher vollzogen werden kann, ist eine Regelung über Art und Weise des Austauschs aufzustellen. Darin sollten zumindest folgende Punkte betrachtet bzw. geregelt werden:

- welche Akten/Datenträger über welchen Transportweg (Postweg, Kurier, Paketdienst, ...) ausgetauscht werden dürfen (siehe M 5.23 *Auswahl einer geeigneten Versandart für den Datenträger*),
- welche Schutzmaßnahmen sind beim Transport zu beachten. Beispiele dazu sind:
  - geschlossener Behälter,
  - Versandtasche,
  - Einschreiben,
  - Wertbrief,
  - Begleitschreiben und
  - Versiegelung.
- welche Akten/Datenträger nur persönlich transportiert werden dürfen.

Da Schriftstücke, Dokumente und Akten oftmals Unikate sind, muss bei der Auswahl eines geeigneten Aktenaustauschverfahrens beachtet werden, welchen Schaden der Verlust bedeuten würde. Hingegen kann beim Datenträgeraustausch vorab eine Datensicherung erfolgen.

Ergänzende Kontrollfragen:

- Sind betroffene Mitarbeiter darüber informiert, wie Akten- und Datenträger zu transportieren sind?

M 2.113 Regelungen für Telearbeit

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter Personal

Verantwortlich für Umsetzung: Personalabteilung, Vorgesetzte

Da es bisher kein "Telearbeitsgesetz" mit eigenständigen gesetzlichen Regelungen gibt, sollten einige Punkte entweder durch Tarifverträge, Betriebsvereinbarungen oder zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen Telearbeiter und Arbeitgeber geklärt werden. Darin sollten unter anderem die Punkte "Freiwilligkeit der Teilnahme an der Telearbeit", "Mehrarbeit und Zuschläge", "Aufwendungen für Fahrten zwischen Betrieb und häuslicher Wohnung", "Aufwendungen z. B. für Strom und Heizung", "Haftung (bei Diebstahl oder Beschädigung der IT, aber auch bei Arbeitsunfall oder Berufskrankheit)" und "Beendigung der Telearbeit" geklärt bzw. geregelt werden.

Im Sinne der IT-Sicherheit sollten zusätzlich folgende Punkte behandelt werden:

- **Arbeitszeitregelung:** die Verteilung der Arbeitszeiten auf Tätigkeiten in der Institution und am häuslichen Arbeitsplatz muss geregelt sein und feste Zeiten der Erreichbarkeit am häuslichen Arbeitsplatz müssen festgelegt werden.
- **Reaktionszeiten:** es sollte geregelt werden, in welchen Abständen aktuelle Informationen eingeholt werden (z. B. wie häufig E-Mails gelesen werden) und wie schnell darauf reagiert werden sollte.
- **Arbeitsmittel:** es kann festgeschrieben werden, welche Arbeitsmittel der Telearbeiter einsetzen kann und welche nicht genutzt werden dürfen (z. B. nicht freigegebene Software). So kann ein E-Mail-Anschluss zur Verfügung gestellt werden, aber die Nutzung von anderen Internet-Diensten wird untersagt. Weiterhin kann die Benutzung von Disketten (Gefahr von Computer-Viren) untersagt werden, wenn der Telearbeitsrechner dies nicht erfordert.
- **Datensicherung:** der Telearbeiter ist zu verpflichten, regelmäßig eine Datensicherung durchzuführen. Darüber hinaus sollte vereinbart werden, dass jeweils eine Generation der Datensicherung bei der Institution zur Unterstützung der Verfügbarkeit hinterlegt wird.
- **IT-Sicherheitsmaßnahmen:** der Telearbeiter ist zu verpflichten, die für die Telearbeit notwendigen IT-Sicherheitsmaßnahmen zu beachten und zu realisieren. Die umzusetzenden IT-Sicherheitsmaßnahmen sind dem Telearbeiter in schriftlicher Form zu übergeben.
- **Datenschutz:** der Telearbeiter ist auf die Einhaltung einschlägiger Datenschutzvorschriften zu verpflichten sowie auf die notwendigen Maßnahmen bei der Bearbeitung von personenbezogenen Daten am häuslichen Arbeitsplatz hinzuweisen.

- **Datenkommunikation:** es muss festgelegt werden, welche Daten auf welchem Weg übertragen bzw. welche Daten nicht oder nur verschlüsselt elektronisch übermittelt werden dürfen.
- **Aktentransport:** die Art und Absicherung des Aktentransports zwischen häuslichem Arbeitsplatz und Institution ist zu regeln.
- **Meldeweg:** der Telearbeiter ist zu verpflichten, IT-sicherheitsrelevante Vorkommnisse unverzüglich an eine zu bestimmende Stelle in der Institution zu melden.
- **Zutrittsrecht zum häuslichen Arbeitsplatz:** für die Durchführung von Kontrollen und für die Verfügbarkeit von Akten und Daten im Vertretungsfall kann ein Zutrittsrecht zum häuslichen Arbeitsplatz (ggf. mit vorheriger Anmeldung) vereinbart werden.

Ergänzende Kontrollfragen:

- Ist dem Telearbeiter der vereinbarte Rahmen seiner Tätigkeit bekannt?
- Wird dem Telearbeiter ein Informationsblatt darüber ausgehändigt?
- Wird dem Telearbeiter ein Merkblatt ausgehändigt, in dem die von ihm zu beachtenden IT-Sicherheitsmaßnahmen erläutert werden? Wann wurde das Merkblatt zuletzt aktualisiert?

M 2.114 Informationsfluss zwischen Telearbeiter und Institution

Verantwortlich für Initiierung: Vorgesetzte, Telearbeiter

Verantwortlich für Umsetzung: Vorgesetzte, Telearbeiter

Damit der Telearbeiter nicht vom betrieblichen Geschehen abgeschnitten wird, sollte der Vorgesetzte einen regelmäßigen Informationsaustausch zwischen dem Telearbeiter und den Arbeitskollegen ermöglichen. Dies ist wichtig, damit der Telearbeiter auch zukünftig über Planungen und Zielsetzungen in seinem Arbeitsbereich informiert ist, damit Frustrationen vermieden und ein positives Telearbeitsklima geschaffen wird und erhalten bleibt.

Die Beteiligung der Telearbeiter an Umlaufverfahren für Hausmitteilungen, einschlägige Informationen und Zeitschriften ist zu regeln. Dies stellt dann ein Problem dar, wenn der Telearbeiter ausschließlich zu Hause arbeitet. Eine Lösung wäre eventuell das Einscannen wichtiger Schriftstücke, um sie dann dem Telearbeiter per E-Mail zuzustellen. Zusätzlich ist der Telearbeiter über Änderungen von IT-Sicherheitsmaßnahmen zu unterrichten.

Weiterhin müssen die Arbeitskollegen über die Anwesenheits- und Erreichbarkeitszeiten und die E-Mail-Adresse bzw. Telefonnummer des Telearbeiters in Kenntnis gesetzt werden.

Folgende Punkte müssen darüber hinaus bei der Telearbeit geklärt werden:

- Wer ist Ansprechpartner bei technischen und/oder organisatorischen bei Problemen in der Telearbeit?
- Wem müssen Sicherheitsvorkommnisse mitgeteilt werden?
- Wie erfolgt die Aufgabenzuteilung?
- Wie erfolgt die Übergabe der Arbeitsergebnisse?

Treten technisch-organisatorische Probleme auf, müssen diese vom Telearbeiter unverzüglich der Institution gemeldet werden.

Ergänzende Kontrollfragen:

- Wie erfährt der Telearbeiter dienstliche Informationen?
- Wem meldet ein Telearbeiter Sicherheitsvorkommnisse?
- Gibt es einen Ansprechpartner (unabhängig vom Vorgesetzten) für die Telearbeiter?

M 2.115 Betreuungs- und Wartungskonzept für Telearbeitsplätze

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator, Telearbeiter

Für die Telearbeitsplätze muss ein spezielles Betreuungs- und Wartungskonzept erstellt werden, das folgende Punkte vorsieht:

- **Benennen von problembezogenen Ansprechpartnern für den Benutzerservice:** an diese Stelle wendet sich der Telearbeiter bei Software- und Hardware-Problemen. Der Benutzerservice versucht (auch telefonisch) kurzfristig Hilfestellung zu leisten bzw. leitet Wartungs- und Reparaturarbeiten ein.
- **Wartungstermine:** die Termine für vor Ort durchzuführende Wartungsarbeiten sollten frühzeitig bekanntgegeben werden, damit die Telearbeiter zu diesen Zeiten den Zutritt zum häuslichen Arbeitsplatz gewährleisten können.
- **Einführung von Standard-Telearbeitsrechnern:** es sollten alle Telearbeiter einer Institution einen definierten Standard-Telearbeitsrechner haben, damit Problemlösungen für den Benutzerservice erleichtert werden. Dies erleichtert ebenso den konzeptionellen und administrativen Aufwand für den Aufbau eines sicheren Telearbeitsrechners.
- **Fernwartung:** falls der Telearbeitsrechner über Fernwartung administriert und gewartet werden kann, sind die notwendigen Sicherheitsmaßnahmen sowie die erforderlichen online-Zeiten zu vereinbaren. Insbesondere ist ein Sicherungsverfahren festzulegen, um den Missbrauch eines Fernwartungszugangs zu verhindern (siehe M 5.33 *Absicherung der per Modem durchgeführten Fernwartung*).
- **Transport der IT:** es sollte aus Gründen der Haftung festgelegt werden, wer autorisiert ist, die IT zwischen Institution und häuslichen Arbeitsplatz des Telearbeiters zu transportieren.

Weitere Regelungen können der Maßnahme M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten* entnommen werden.

Ergänzende Kontrollfragen:

- Sind dem Telearbeiter die Ansprechpartner für Hard- und Softwareprobleme bekannt?
- Ist dem Benutzerservice die Konfiguration eines Standard-Telearbeitsrechners bekannt?
- Ist dem Benutzerservice die Adresse des Telearbeiters bekannt, damit er schnell vor Ort helfen kann?

M 2.116 Geregelte Nutzung der Kommunikationsmöglichkeiten

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Telearbeiter

Grundsätzlich verfügt ein Telearbeitsrechner über elektronische Kommunikationsmöglichkeiten. Im Sinne der IT-Sicherheit muss geregelt werden, auf welche Weise die vorhandenen Kommunikationsmöglichkeiten genutzt werden dürfen. Grundsätzlich sollte die private Nutzung der Kommunikationsmöglichkeiten untersagt werden.

Zu klären sind zumindest folgende Punkte:

- **Datenflusskontrolle**
  - Welche Dienste dürfen zur Datenübertragung genutzt werden?
  - Welche Dienste dürfen explizit nicht genutzt werden?
  - Welche Informationen dürfen an wen versendet werden?
  - Welcher Schriftverkehr darf über E-Mail abgewickelt werden?
  - Falls der Telearbeitsrechner ein Faxmodem besitzt oder wenn am Telearbeitsplatz ein Faxgerät vorhanden ist, so ist zu klären, welche Informationen per Fax an wen übermittelt werden dürfen.
  - Der elektronische Versand welcher Informationen bedarf der vorherigen Zustimmung der Institution?
- **Informationsgewinnung**
  - Welche elektronischen Dienstleistungen (Datenbankabfragen, elektronische Recherchen) dürfen vom Telearbeitsrechner aus in Anspruch genommen werden? Beispielsweise können aus der Art der Abfragen unter Umständen Rückschlüsse auf Unternehmensstrategien gezogen werden.
  - Welches Budget steht für elektronische Dienstleistungen zur Verfügung?
- **IT-Sicherheitsmaßnahmen**
  - Für welche Daten sollen welche Verschlüsselungsverfahren eingesetzt werden?
  - Für welche Daten ist eine Löschung nach erfolgreicher Übertragung notwendig? Dies kann beispielsweise für personenbezogene Daten gelten.
  - Von welchen Daten soll trotz der erfolgreichen Übertragung eine Kopie der Daten auf dem Telearbeitsrechner verbleiben?
  - Wird vor Versand oder nach Erhalt von Daten ein Computer-Viren-Check der Daten durchgeführt?

  - Für welche Datenübertragung eine Protokollierung erfolgen soll? Falls eine automatische Protokollierung nicht möglich sein sollte, ist festzulegen, ob und in welchem Umfang eine handschriftliche Protokollierung vorzusehen ist.

- **Internet-Nutzung**
  - Wird die Nutzung von Internet-Dienst generell verboten?
  - Welche Art von Daten darf aus dem Internet geladen werden? Werden Daten von fremden Servern geladen, so besteht die Gefahr, dass Computer-Viren importiert werden.
  - Welche Optionen dürfen im Internet-Browser aktiviert werden?
  - Welche Sicherungsverfahren sollen im Internet-Browser aktiviert werden?
  - Ist die Zustimmung der Institution erforderlich, wenn der Telearbeiter sich am Informationsaustausch mittels Newsgruppen beteiligen will? Ggf. ist eine anonyme Nutzung erforderlich.

- **Unterschriftenregelung**
  - Ist eine Unterschriftenregelung für die Kommunikation vorgesehen?
  - Werden gesetzkonforme digitale Signaturen eingesetzt?
  - Werden andere Authentisierungsverfahren für den Schriftverkehr genutzt?

Ergänzende Kontrollfragen:

- Ist der Telearbeiter über die Regelungen bzgl. der Nutzung der Kommunikationsmöglichkeiten informiert?
- Bestätigt der Telearbeiter die Belehrung über die Nutzung der Kommunikationsmöglichkeiten durch eine Unterschrift?

M 2.117 Regelung der Zugriffsmöglichkeiten des Telearbeiters

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Vorgesetzte

Verantwortlich für Umsetzung: Administrator, Vorgesetzte

Erfordert die Telearbeit den Zugriff auf die IT der Institution (zum Beispiel auf einen Server), muss zuvor festgelegt werden, welche Objekte (Daten, IT) der Telearbeiter tatsächlich für die Erfüllung seiner Aufgaben benötigt. Entsprechend sind die notwendigen Rechte wie Lese- und Schreibrechte auf diese Objekte zuzuweisen. Auf Objekte, die der Telearbeiter für seine Aufgabenwahrnehmung nicht braucht, sollte er auch nicht zugreifen können. Dies gilt sowohl für den Zugriff auf Daten wie auf in der Institution verfügbare IT. Damit soll erreicht werden, dass der Schaden, der aufgrund eines Hacker-Angriffs auf den Kommunikationsrechner entstehen kann, minimiert wird. Für die Erteilung der Zugangs- und Zugriffsrechte siehe M 2.7 *Vergabe von Zugangsberechtigungen* und M 2.8 *Vergabe von Zugriffsrechten*.

Ergänzende Kontrollfragen:

- Ist dem Administrator bekannt, auf welche Objekte der Telearbeiter zugreifen darf?
- Welche Voraussetzungen müssen vor einer Vergabe oder Änderungen von Zugriffsrechten erfüllt sein?
- Ist der Server so administriert, dass der Telearbeiter nur auf die erlaubten Objekte zugreifen kann?

M 2.118 Konzeption der sicheren E-Mail-Nutzung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Bevor E-Mailsysteme für die Nutzung freigeben werden, sollte festgelegt werden, für welchen Einsatzzweck und welche Informationen E-Mail vorgesehen ist. Abhängig davon, wofür E-Mail eingesetzt werden soll, unterscheiden sich auch die Ansprüche an Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit der zu übertragenden Daten sowie des eingesetzten E-Mail-Programms. Es muss geklärt werden, ob über E-Mail ausschließlich unverbindliche oder informelle Informationen weitergegeben werden sollen oder ob einige oder sogar alle der bisher schriftlich bearbeiteten Geschäftsvorfälle nun per E-Mail durchgeführt werden sollen. Bei letzterem ist zu klären, wie Anmerkungen an Vorgängen wie Verfügungen, Abzeichnungen oder Schlusszeichnungen, die bisher handschriftlich angebracht wurden, elektronisch abgebildet werden sollen.

Bei der Konzeption der E-Mail-Nutzung muss auch festgelegt werden, ob und wie kryptographische Sicherungsmechanismen zu implementieren sind (siehe dazu auch M 5.108 *Kryptographische Absicherung von E-Mail* und M 5.110 *Absicherung von E-Mail mit SPHINX (S/MIME)*).

Die Institution muss darauf aufbauend eine E-Mail-Richtlinie festlegen, in der folgende Punkte beschrieben sind:

- wer einen E-Mail-Anschluss erhält,
- die Regelungen, die von den E-Mail-Administratoren und den E-Mail-Benutzern zu beachten sind,
- bis zu welchem Anspruch an Vertraulichkeit oder Integrität Informationen per E-Mail versandt werden dürfen,
- welche Handbücher beschafft werden,
- wie die Benutzer geschult werden und
- wie jederzeit technische Hilfestellung für die Benutzer gewährleistet wird.

Durch organisatorische Regelungen oder durch die technische Umsetzung sind dabei insbesondere die folgenden Punkte zum ordnungsgemäßen Dateitransfer zu gewährleisten:

- Die E-Mail-Progamme der Benutzer müssen durch den Administrator so vorkonfiguriert sein, dass ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht werden kann (siehe auch M 5.57 *Sichere Konfiguration der Mail-Clients*).
- Die Übermittlung von Daten darf erst nach erfolgreicher Identifizierung und Authentisierung des Senders beim Übertragungssystem möglich sein.
- Die Benutzer müssen vor erstmaliger Nutzung von E-Mail in die Handhabung der relevanten Applikationen eingewiesen werden. Die organisationsinternen Benutzerregelungen zu Dateiübermittlung muss ihnen bekannt sein.

- Zur Beschreibung des Absenders werden bei E-Mails so oft genannte *Signatures* (Absenderangaben) an das Ende der E-Mail angefügt. Der Inhalt einer Signature sollte dem eines Briefkopfs ähneln, also Name, Organisationsbezeichnung und Telefonnummer und Ähnliches enthalten. Diese Signature darf jedoch weder mit einer Signatur im Sinne einer (eingescannten) Unterschrift noch mit einer elektronischen Signatur, die die Korrektheit und Authentizität des Textinhaltes belegt, verwechselt werden. Eine Signature sollte nicht zu umfangreich sein. Die Behörde bzw. das Unternehmen sollte einen Standard für die einheitliche Gestaltung von Signatures festlegen.
- Von den eingesetzten Sicherheitsmechanismen hängt es ab, bis zu welchem Vertraulichkeits- bzw. Integritätsanspruch Dateien per E-Mail versandt werden dürfen. Es sollte geregelt werden, ob und wann übertragene Dateien verschlüsselt bzw. digital signiert werden müssen (siehe auch M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*). Es ist zentral festzulegen, welche Applikationen für die Verschlüsselung bzw. den Einsatz von Digitalen Signaturen von den Benutzern zu verwenden sind. Diese müssen den Benutzern zur Verfügung gestellt werden, die wiederum in deren Anwendung unterwiesen werden müssen.
- Es sollte vor der Einführung elektronischer Kommunikationssysteme festgelegt werden, unter welchen Bedingungen ein- oder ausgehende E-Mails zusätzlich ausgedruckt werden müssen.
- Die Dateiübertragung kann (optional) dokumentiert werden. Für jede stattgefundene Übermittlung ist dann in einem Protokoll festzuhalten, wer wann welche Informationen erhalten hat. Bei der Übertragung personenbezogener Daten sind die gesetzlichen Vorgaben zur Protokollierung zu beachten.

E-Mails, die intern versandt werden, dürfen das interne Netz nicht verlassen. Dies ist durch entsprechende administrative Maßnahmen sicherzustellen. Beispielsweise sollte die Übertragung von E-Mails zwischen verschiedenen Liegenschaften einer Organisation über eigene Standleitungen und nicht über das Internet erfolgen.

Grundsätzlich sollten Nachrichten, die an interne Adressen verschickt wurden, nicht an externe Adressen weitergeleitet werden. Sollen hiervon Ausnahmen gemacht werden, sind alle Mitarbeiter darüber zu informieren. Beispielsweise kann für Außendienstmitarbeiter oder andere Mitarbeiter, die viel unterwegs sind, die E-Mail an externe Zugriffspunkte weitergeleitet werden.

Private Nutzung dienstlicher E-Mail-Zugänge

Es wird immer wieder diskutiert, ob und in wieweit dienstliche E-Mail-Zugänge für private Zwecke benutzt werden dürfen. Solange die private Nutzung sich in Grenzen hält, wird dies sogar von vielen Organisationen unterstützt, da die Mitarbeiter dadurch eine positivere Einstellung zu E-Mail bekommen. Generell empfiehlt es sich aber, hierzu in der E-Mail-Richtlinie zu vereinbaren, welche Spielregeln bei der E-Mail-Nutzung allgemein und auch hinsichtlich privater Nutzung einzuhalten sind.

Bei der Nutzung von E-Mail in Institutionen sollte auch festgelegt, welche E-Mail-Programme eingesetzt werden sollen. Neben unterschiedlicher

Funktionalität hat die Auswahl der E-Mail-Clients und -Server auch Einfluss auf die Benutzungsfreundlichkeit und den Administrationsaufwand, aber auch auf die Sicherheit der gesamten IT-Umgebung. Neben eigenständigen Client-Programmen kann auch auf Webmail zurückgegriffen werden.

Webmail

Als Webmail werden Angebote bezeichnet, bei denen über einen Browser auf webbasierte E-Mail-Dienste zugegriffen wird. Verschiedene Anbieter von Mailservern bieten entsprechende Erweiterungen entweder direkt in ihr Produkt integriert oder als Zusatzmodule an. Webmail hat den Vorteil, dass hierbei von jedem Rechner mit Internet-Anschluss weltweit auf die E-Mail-Postfächer zugegriffen werden kann, ohne dass hierfür in aufwendige Infrastruktur investiert werden muss. Es ist allerdings schwieriger als beim Transport über die internen E-Mail-Server, die organisationsweit gültigen Sicherheitsrichtlinien durchzusetzen, beispielsweise im Hinblick auf Virenschutz oder Verschlüsselung. Außerdem ist die Gefahr, dass vertrauliche E-Mails mitgelesen oder Passwörter abgehört werden, beim externen Zugriff auf Webmailzugänge wesentlich höher.

Webmail und Virenschutz

Bei der Nutzung von Webmail aus einem Behörden- bzw. Unternehmensnetz heraus muss unbedingt der Virenschutz beachtet werden. Bei aktuellen Virenwarnungen kann es einige Zeit in Anspruch nehmen, die neuen Virenschutz-Updates auf alle Clients aufzuspielen. In einer solchen Situation kann es sinnvoll sein, den Zugriff auf Webmail zumindest, solange zu verhindern, bis die Verantwortlichen für Virenschutz sicher sind, dass ein ausreichender Schutz besteht.

Der Umgang mit Webmail in der Behörde bzw. dem Unternehmen sollte daher geregelt sein. Hierbei gibt es mehrere Varianten:

- Organisationen können beschließen, die Nutzung von Webmail generell zu verbieten. Dies muss dann natürlich den Mitarbeitern bekannt gegeben werden. Das Verbot kann außerdem technisch durch Filterung bezüglich der bekannten Anbieter unterstützt werden, wobei man sich hier darüber klar sein sollte, dass Benutzer immer neue Wege finden können, um auf solche Dienste zuzugreifen.
- Es kann die Empfehlung ausgesprochen werden, Webmail für private E-Mails, die aus dem internen LAN verschickt werden sollen, zu nutzen. Damit kann vermieden werden, dass Mitarbeiter trotz entsprechender Verbote dienstliche E-Mail-Zugänge für private Zwecke nutzen - beispielsweise, weil es dringend oder einfach praktisch ist.
- Es gibt auch Organisationen, in denen Webmail offiziell für dienstliche E-Mails freigegeben ist. Die Gründe hierfür sind unterschiedlich. So gibt es z. B. eine Reihe kleinerer Organisationen, die keinen eigenen E-Mail-Server haben und Webmail für Kommunikation nach außen einsetzen. Webmail kann auch für Mitarbeiter praktisch sein, die auf Dienstreisen auf ihre E-Mail zugreifen müssen, für die aber kein Zugang über Remote Access eingerichtet ist. Ein weiterer Grund für die Nutzung von Webmail kann darin bestehen, dass die jeweilige Organisation bei bestimmten E-Mails nicht nach außen in Erscheinung treten will oder dass Webmail-Adressen dort angegeben werden, wo Spam erwartet wird, also bei bestimmten Downloads, Newsgruppen etc.

Wenn Webmail eingesetzt wird, sollten die Empfehlungen in M 5.96 *Sichere Nutzung von Webmail* beachtet werden.

Ergänzende Kontrollfragen:

- Existiert eine Sicherheitsrichtlinie für die E-Mail-Nutzung?
- An wen können sich die Benutzer bei Fragen zur E-Mail-Nutzung wenden?

M 2.119 Regelung für den Einsatz von E-Mail

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Sollen zwischen zwei oder mehreren Kommunikationspartnern Daten elektronisch ausgetauscht werden, so müssen diese zum ordnungsgemäßen Austausch folgende Punkte beachten:

- Die Adressierung von E-Mail muss eindeutig erfolgen, um eine fehlerhafte Zustellung zu vermeiden. Innerhalb einer Organisation sollten Adressbücher und Verteilerlisten gepflegt werden, um die Korrektheit der gebräuchlichsten Adressen sicherzustellen. Durch den Versand von Testnachrichten an neue E-Mailadressen ist die korrekte Zustellung von Nachrichten zu prüfen.
- Wenn eine E-Mail an mehrere Empfänger geschickt wird, sollten diese nicht so verschickt werden, dass jeder Empfänger die komplette Empfängerliste sehen kann. Dies ist nämlich nicht nur für die Empfänger lästig, sondern kann auch aus Datenschutzgründen unerwünscht sein und es könnte dadurch auch Spam verursacht werden.

  Ersatzweise könnte hierfür die E-Mail-Adressen statt unter "CC" unter "BCC" eingetragen oder auch Verteilerlisten benutzt werden. BCC steht für Blind Carbon Copy; hier eingetragene weitere Empfänger werden den anderen Empfänger nicht angezeigt.

  Hinweis: Es sollte überprüft werden, in welcher Form das eigene E-Mail-System diese E-Mails dann an die Empfänger weiterleitet. Bei einigen E-Mail-Systemen führt dies dazu, dass bei den Empfängern deren E-Mail-Adresse nicht im "TO:"-Feld steht, wie es häufig auch bei Spam der Fall ist. Besser ist in diesem Fall ein E-Mail-Programm, das eigene Verteilerlisten unterstützt und dann an jeden Empfänger eine **eigene** Mail schickt.
- Für alle nach außen gehenden E-Mails ist eine Signature zu verwenden.
- Die Betreffangabe (Subject) des Kommunikationssystems sollte immer ausgefüllt werden, z. B. entsprechend der Betreffangabe in einem Anschreiben.
- Die Korrektheit der durchgeführten Datenübertragung sollte überprüft werden. Die Empfängerseite sollte den korrekten Empfang überprüfen und der Senderseite bestätigen.
- Verwendung residenter Virenscanner für ein- bzw. ausgehende Dateien. Vor dem Absenden bzw. vor der Dateiübermittlung sind die ausgehenden Dateien explizit auf Computer-Viren zu überprüfen. Siehe auch M 5.109 *Einsatz eines E-Mail-Scanners auf dem Mailserver*.
- Erfolgt über die E-Mail noch eine Dateiübertragung, so sollten die folgenden Informationen an den Empfänger zusätzlich übermittelt werden:
  - Art der Datei (z. B. Excel-Datei, OpenOffice Text oder ähnliches),
  - Kurzbeschreibung des Inhalts der Datei,

- eventuell ein Hinweis, dass Dateien auf Computer-Viren überprüft sind,
- ggf. Art des verwendeten Packprogramms (z. B. Winzip, gzip)
- ggf. Art der eingesetzten Software für Verschlüsselung bzw. Digitale Signatur.

Jedoch sollte nicht vermerkt werden,

- welches Passwort für die eventuell geschützten Informationen vergeben wurde,
- welche Schlüssel ggf. für eine Verschlüsselung der Informationen verwendet wurde.

Im Zweifel Rückfrage beim Absender

Bei den meisten E-Mail-Systemen werden die Informationen unverschlüsselt über offene Leitungen transportiert und können auf diversen Zwischenrechnern gespeichert werden, bis sie schließlich ihren Empfänger erreichen. Auf diesem Weg können Informationen leicht manipuliert werden. Aber auch der Versender einer E-Mail hat meistens die Möglichkeit, seine Absenderadresse (From) beliebig einzutragen, so dass man sich nur nach Rückfrage oder bei Benutzung von Digitalen Signaturen der Authentizität des Absenders sicher sein kann. In Zweifelsfällen sollte daher die Echtheit des Absenders durch Rückfrage oder - besser noch - durch den Einsatz von Verschlüsselung und/oder Digitalen Signaturen überprüft werden. Grundsätzlich gilt, dass man sich nicht auf die Echtheit der Absenderangabe verlassen kann.

Regelmäßiges Lesen der E-Mail, zeitnahe Beantwortung

Beim Anschluss an E-Mail-Systeme ist mehrfach täglich zu überprüfen, ob neue E-Mails eingegangen sind. Bei längerer Abwesenheit sollte eine Vertretungsregelung getroffen werden, beispielsweise können eingehende E-Mails an einen Vertreter weitergeleitet werden (siehe auch M 2.274 *Vertretungsregelungen bei E-Mail-Nutzung*).

Da in vielen Fällen nicht vorhergesagt werden kann, welchen E-Mail-Client ein E-Mail-Empfänger benutzt und welche Software und Betriebssysteme auf dem Transportweg eingesetzt werden, sollten die Benutzer wissen, dass sowohl bei der Übertragung als auch bei der Darstellung von Nachrichten und Anhängen beim Empfänger Probleme auftreten können. Dies tritt kann insbesondere bei der Verwendung ungewöhnlicher Zeichensätze oder Dateiformate, oder auch beim Einsatz veralteter E-Mail-Software auftreten. Treten Probleme auf, kann beispielsweise versucht werden, die Anhänge vor der Übertragung in eine 7-Bit-ASCII-Darstellung umwandeln, z. B. mit *uuencode*.

Regelungen schriftlich fixieren

Alle Regelungen und Bedienungshinweise zum Einsatz von E-Mail sind schriftlich zu fixieren und sollten den Mitarbeitern jederzeit zur Verfügung stehen. Ein entsprechendes Muster ist der der IT-Grundschutz-Kataloge beiliegenden CD-ROM zu entnehmen.

Die Benutzer müssen vor dem Einsatz von Kommunikationsdiensten wie E-Mail geschult werden, um Fehlbedienungen zu vermeiden und die Einhaltung der organisationsinternen Richtlinien zu gewährleisten. Insbesondere müssen sie hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen beim Versenden bzw. Empfangen von E-Mail sensibilisiert werden.

Keine Kettenbriefe!

Zur Vermeidung von Überlastung durch E-Mail sind die Mitarbeiter über potentielles Fehlverhalten zu belehren. Sie sollten dabei ebenso vor der Teilnahme an E-Mail-Kettenbriefen wie vor der Abonnierung umfangreicher Mailinglisten gewarnt werden.

Benutzer müssen darüber informiert werden, dass Dateien, deren Inhalt Anstoß erregen könnte, weder verschickt noch auf Informationsservern eingestellt werden noch nachgefragt werden sollten. Außerdem sollten Benutzer darauf verpflichtet werden, dass bei der Nutzung von Kommunikationsdiensten

- die fahrlässige oder gar vorsätzliche Unterbrechung des laufenden Betriebes unter allen Umständen vermieden werden muss. Zu unterlassen sind insbesondere Versuche, ohne Autorisierung Zugang zu Netzdiensten - welcher Art auch immer - zu erhalten, Informationen, die über die Netze verfügbar sind, zu verändern, in die individuelle Arbeitsumgebung eines Netzbenutzers einzugreifen oder unabsichtlich erhaltene Angaben über Rechner und Personen weiterzugeben.
- die Verbreitung von für die Allgemeinheit irrelevanten Informationen unterlassen werden muss. Die Belastung der Netze durch ungezielte und übermäßige Verbreitung von Informationen sollte vermieden werden.
- die Verbreitung von redundanten Informationen vermieden werden sollte.

Ergänzende Kontrollfragen:

- Sind Regelungen für die Dateiübertragung bzw. den Nachrichtenaustausch mit Externen festgelegt worden?

M 2.120 Einrichtung einer Poststelle

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Zum reibungslosen Ablauf des E-Maildienstes muss ein Postmaster benannt werden, der folgende Aufgaben wahrnimmt:

- Bereitstellen der Maildienste auf lokaler Ebene,
- Pflege der Adresstabellen,
- Überprüfung, ob die externen Kommunikationsverbindungen funktionieren,
- Anlaufstelle bei Mailproblemen für Endbenutzer sowie für die Betreiber von Gateway- und Relaydiensten.

Alle unzustellbaren E-Mails und alle Fehlermeldungen müssen an den Postmaster weitergeleitet werden, der versuchen sollte die Fehlerquellen zu beheben. E-Mail, die unzustellbar bleibt, muss nach Ablauf einer vordefinierten Frist an den Absender mit einer entsprechenden Fehlermeldung zurückgeschickt werden.

Daneben müssen je nach Organisationsstruktur und -größe ein oder mehrere Verantwortliche für die Pflege der angebotenen Kommunikationsdienste benannt werden. Neben dem Serverbetrieb wie Mail-, News- oder FTP-Server müssen auch die von den Benutzer eingesetzten Kommunikationsclients betreut werden.

Alle Betreuer bzw. deren Vertreter sollten jederzeit von den Benutzern telefonisch erreicht werden könnten.

Ergänzende Kontrollfragen:

- Wer ist der verantwortliche Postmaster?
- Wo laufen fehlerhaft adressierte E-Mails auf?

M 2.121 Regelmäßiges Löschen von E-Mails

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

E-Mails sollten nicht unnötig lange im Posteingang gespeichert werden. Sie sollten entweder nach dem Lesen gelöscht werden oder in Benutzerverzeichnissen gespeichert werden, wenn sie erhalten bleiben sollen. Wenn im Posteingang zu viele E-Mails archiviert werden, kann es passieren, dass das IT-System, das diesen verwaltet (der Mailserver bzw. Mail-Client), aus Speicherplatzmangel neu ankommende E-Mails abweist.

Benutzer müssen andererseits darüber informiert sein, dass eine E-Mail, die sie selber über ihre Mailanwendung gelöscht haben, dadurch meistens nicht unwiederbringlich gelöscht ist. Viele Mailprogramme löschen E-Mails nicht sofort, sondern transferieren sie in spezielle Ordner. Benutzer müssen darauf hingewiesen werden, wie sie E-Mails auf ihren Clients vollständig löschen können.

Daneben können E-Mails nach dem Löschen auf den Clients trotzdem noch auf Mailservern vorhanden sein. Viele Internet-Provider und Administratoren archivieren die ein- und ausgehenden E-Mails. Viele Mailanwendungen löschen E-Mails nicht, sondern verschieben sie in einen "Papierkorb"-Bereich, der dann ebenfalls gelöscht werden muss.

Die Benutzer müssen wissen, dass die Vertraulichkeit einer E-Mail nur durch Verschlüsselung gewährleistet werden kann, und dass sie sich nicht auf "schnelles Löschen" nach dem Empfang verlassen können.

Ergänzende Kontrollfragen:

- Wissen Benutzer, wie sie ihre E-Mail löschen können?

M 2.122 Einheitliche E-Mail-Adressen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

E-Mailadressen sollten aufgrund von klaren Regelungen vergeben werden. Dabei ist es sinnvoll, Namenskonventionen für die personenbezogenen E-Mailadressen festzulegen, die an die Benutzernamen auf den verwendeten IT-Systeme angelehnt sind (z. B. E-Mail-Adresse = die ersten 8 Zeichen des Nachnamens). Die Benutzernamen auf IT-Systemen, die von außerhalb des geschützten Netzes erreicht werden können, sollten nicht aus den E-Mailadressen unmittelbar ableitbar sein, um mögliche Angriffe auf Benutzer-Accounts zu erschweren. Wichtig ist, dass die Adressen nicht häufig geändert werden und dass sie weder zu lang noch zu kompliziert aufgebaut sind. Insbesondere ist darauf zu achten, dass keine Nicht-ASCII-Zeichen wie Umlaute innerhalb von E-Mailadressen verwendet werden.

Um Angriffe zu erschweren, Werbe-E-Mail zu vermeiden bzw. um möglichst wenig Information nach außen weiterzugeben, kann es sinnvoll sein, statt benutzer- und organisationsbezogenen E-Mailadressen wie *nachname@organisation.de* schwer erratbare E-Mailadressen zu verwenden. Dies macht aber auch die Adressweitergabe unbequemer und kann die Kommunikation mit Externen erschweren.

Wenn E-Mailadressen geändert werden oder wegfallen, ist darauf zu achten, dass zumindest für eine Übergangszeit E-Mail, die noch an diese Adressen gerichtet ist, an die jetzt aktuellen Adressen weitergeleitet wird.

Neben personenbezogenen E-Mailadressen können auch organisations- bzw. funktionsbezogene E-Mailadressen eingerichtet werden, um unabhängig von Personen die Zustellung zur richtigen Organisationseinheit zu garantieren. Dies ist insbesondere bei zentralen Anlaufstellen wichtig. Siehe hierzu auch M 2.275 *Einrichtung funktionsbezogener E-Mailadressen*.

Ergänzende Kontrollfragen:

- Wie ist die Vergabe von E-Mail-Adressen geregelt?

M 2.123 Auswahl eines Mailproviders

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT

Vor der Auswahl eines Mailproviders sollten sich die Verantwortlichen über die beim Provider geltenden Regelungen informieren, beispielsweise ob er Obergrenzen für den Umfang von E-Mails beim Empfang oder Versand gesetzt hat, ob E-Mails gefiltert werden, und wenn ja, nach welchen Regeln.

Man sollte sich vom Mailprovider dokumentieren lassen, dass deren Mailserver sicher betrieben wird, also die in M 5.56 *Sicherer Betrieb eines Mailservers* beschriebenen Anforderungen erfüllt sind.

Beim Mailprovider sind Daten über die Benutzer für Abrechnungszwecke gespeichert (Name, Adresse, Benutzer-Kennung, Bankverbindung) ebenso wie Verbindungsdaten und für eine je nach Provider kürzere oder längere Zeitspanne auch die übertragenen Inhalte.

Die Anwender sollten sich bei ihrem Mailprovider erkundigen, welche Daten wie lange über sie gespeichert werden. Bei der Auswahl von Providern sollte berücksichtigt werden, dass deutsche Betreiber den einschlägigen datenschutzrechtlichen Regelungen für die Verarbeitung dieser Daten unterliegen.

Die Benutzer können durch den Einsatz von Verschlüsselung verhindern, dass der Provider die Inhalte der übertragenen Informationen mitlesen kann.

Große Provider mit großem eigenem Netz haben den Vorteil, dass E-Mail, die nur innerhalb dieses Netzes ausgetauscht wird, sicherer vor Manipulationen ist als bei Weiterleitung über das Internet.

Bei Providern, die ihren Hauptsitz im Ausland haben, wird häufig auch alle E-Mail über dieses Land geroutet. Beispielsweise werden bei AOL und Compuserve alle E-Mails über die USA weitergeleitet. Dieser Punkt sollte berücksichtigt werden, wenn man sich Gedanken darüber macht, über wie viele Gateways die E-Mail weiterverteilt wird, also wer sie beispielsweise mitlesen kann.

Ergänzende Kontrollfragen:

- Nach welchen Kriterien ist der Mailprovider ausgewählt worden?
- Welche Sicherheitsmechanismen werden beim Mailprovider umgesetzt?
- Nach welchen Kriterien werden die E-Mails beim Mailprovider gefiltert?

M 2.124 Geeignete Auswahl einer Datenbank-Software

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Bei der Beschaffung neuer Datenbank-Software besteht die Möglichkeit, diese von vornherein so auszuwählen, dass im späteren Betrieb mit nur geringem personellen und organisatorischen Zusatzaufwand ein hohes Maß an Sicherheit erreicht werden kann.

Zu Beginn muss der Einsatzbereich und Verwendungszweck des Datenbanksystems geklärt werden, um die Anforderungen bezüglich der Verfügbarkeit, der Integrität und der Vertraulichkeit formulieren zu können. Weiterhin sind die Anforderungen hinsichtlich der zu verarbeitenden Datenmengen, der Verarbeitungsgeschwindigkeit und des Durchsatzes zu quantifizieren. Daraus leiten sich die zu erfüllenden Eigenschaften für die zu beschaffende Datenbank-Software ab, wie z. B. Verfügbarkeit für bestimmte Hardware-Plattformen bzw. Betriebssysteme oder Umfang von notwendigen Sicherheitsmechanismen. In diesem Planungsstadium kann bereits erkannt werden, ob und in welchem Maße für den späteren Betrieb des Datenbanksystems Hardware nach- bzw. umgerüstet werden muss. Anhand der Verfügbarkeitsanforderungen sind auch die benötigten Überwachungsmöglichkeiten zu definieren, d. h. es muss festgelegt werden, welche Datenbankzustände in welcher Form erkennbar sein sollen (z. B. durch eine Protokollierung in einer Datei), sowie die Art der Benachrichtigung verantwortlicher Personen bzw. Personengruppen über kritische Zustände der Datenbank (z. B. durch eine Meldung an der Konsole).

Für die Beschaffung einer Datenbank-Software sollten insbesondere die folgenden Punkte berücksichtigt werden:

- Die Datenbank-Software muss über eigene geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer verfügen (siehe M 2.128 *Zugangskontrolle einer Datenbank*).
- Die Datenbank-Software muss über geeignete Mechanismen zur Ressourcenbeschränkung verfügen (siehe M 4.73 *Festlegung von Obergrenzen für selektierbare Datensätze*).
- Falls in der Datenbank vertrauliche Daten verwaltet werden sollen, so muss einem unberechtigten Zugriff vorgebeugt werden können. Die zu beschaffende Datenbank-Software muss in diesem Fall entsprechende Zugriffskontrollmechanismen zur Verfügung stellen (siehe M 2.129 *Zugriffskontrolle einer Datenbank*).

  Es sollte auch die Zusammenfassung mehrerer Benutzer mit gleichen Zugriffsrechten zu Gruppen möglich sein. Eine Unterscheidung zwischen der Gruppe der Administratoren und der Gruppe der Benutzer ist dabei obligatorisch. Weiterhin sollte eine Trennung von verschiedenen Administrator-Rollen unterstützt werden (siehe M 2.131 *Aufteilung von Administrationstätigkeiten bei Datenbanksystemen*).
- Es gibt Datenbanken mit unterschiedlich starken Zugriffsschutzmechanismen. Ähnliche Sicherheitsmechanismen können dabei auch in unterschied-

licher Granularität angeboten werden. Im Vorfeld ist zu klären, welcher Zugriffsschutz erforderlich ist und welche Datenbank-Software den definierten Sicherheitsanforderungen entspricht. Maßgeblich hierfür sind die Möglichkeiten, Zugriffsrechte auf Datenbankobjekte und die Daten selbst einzuschränken.

Beispiele:

- Den Anwendern kann das Recht entzogen werden, Datenbankobjekte (z. B. Tabellen) anzulegen oder zu modifizieren.
- Die Anwender können zwar eine lesende Zugriffsberechtigung auf eine Tabelle erhalten, gleichzeitig können aber modifizierende Zugriffsrechte ausgeschlossen werden.
- Für bestimmte Tabellen oder bestimmte Felder einer Tabelle kann der Zugriff je nach Anwender verboten werden.
- Anwender erhalten keinerlei Zugriffsberechtigungen auf Datensätze mit bestimmten Merkmalen (z. B. ein Sachbearbeiter aus Bonn hat keinen Zugriff auf die Daten eines Sachbearbeiters aus Köln).

- Einige Hersteller bieten sowohl die Möglichkeit der Definition von Gruppen als auch die von Rollen an. Dadurch kann eine differenziertere Zugriffskontrolle auf die Datenbankobjekte realisiert werden. Im Vorfeld sind die diesbezüglichen Anforderungen zu klären und mit den zur Auswahl stehenden Datenbank-Softwareprodukten abzugleichen.
- Die Datenbank-Software muss ebenfalls hinsichtlich ihrer Überwachungs- und Kontrollmechanismen überprüft werden. Die diesbezüglichen Anforderungen müssen definiert und mit den Leistungsprofilen der Produkte abgeglichen werden (Beispiele siehe M 2.133 *Kontrolle der Protokolldateien eines Datenbanksystems* bzw. M 2.126 *Erstellung eines Datenbanksicherheitskonzeptes*).
- Es muss geprüft werden, ob die Datenbank-Software eine Rollentrennung zwischen Administrator und Revisor unterstützt. Es muss möglich sein, die Rolle eines Revisors einzurichten, der als einziger in der Lage ist, die Protokolldateien auszuwerten und zu löschen. Dies verhindert potentielle Manipulationen durch den Datenbank-Administrator.
- Zum Schutz der Datenbankintegrität muss die Datenbank-Software über ein vollständiges Transaktionssystem verfügen, welches dem ACID-Prinzip genügt. Diese Anforderung wird heutzutage von allen wesentlichen relationalen Datenbankmanagementsystemen erfüllt.
- Es müssen Mechanismen zur Datensicherung der Datenbank vorhanden sein (siehe M 6.49 *Datensicherung einer Datenbank*).

  Im Vorfeld muss in diesem Zusammenhang geklärt werden, welche Möglichkeiten hinsichtlich der Datensicherung die Datenbank-Software zur Verfügung stellen muss. So wird beispielsweise eine partielle Datenbanksicherung nicht für alle am Markt erhältlichen Produkte angeboten. Im konkreten Fall gilt es also zu prüfen, ob das erstellte Datensicherungs-

konzept mit den zur Verfügung stehenden Mechanismen auch umgesetzt werden kann.

Anhand dieser Kriterien müssen die zur Auswahl stehenden Datenbanksysteme geprüft und bewertet werden. Es ist dann diejenige Software auszuwählen, die die spezifischen Anforderungen am besten erfüllt. Weitergehende Anforderungen müssen entweder durch Zusatzprodukte oder durch Eigenentwicklung abgedeckt werden. Es sollte jedoch schon vor der Beschaffung abgeklärt werden, zu welcher Datenbank-Software welche Zusatzprodukte verfügbar sind, um nicht auf teure Eigenentwicklungen zurückgreifen zu müssen.

Von den meisten Datenbankmanagementsystemen sind in der Regel mehrere unterschiedliche Versionen auf dem Markt erhältlich. Dabei unterscheiden sich auch die einzelnen Versionen desselben Datenbankmanagementsystems in ihrer Funktionalität, unter anderem auch in sicherheitsrelevanten Bereichen. Der starke Wettbewerb führt dazu, dass einige Hersteller auch noch nicht vollausgereifte Software ausliefern, bei der dann mit Fehlern und eingeschränkter Funktionalität gerechnet werden muss.

In einer Testphase sollte deshalb überprüft werden, ob die ausgewählte Datenbank-Software die erforderlichen Funktionen in der vorgegebenen Einsatzumgebung auch erfüllt. Dies gilt insbesondere für die Anforderungen an die Performance und die benötigten Mechanismen zur Notfallvorsorge.

Vor der Beschaffung sollten auch Erfahrungen aus vergleichbaren Installationen herangezogen werden.

Ergänzende Kontrollfragen:

- Wurden die Anforderungen an die Datenbank-Software formuliert und dokumentiert?
- Wurde eine Bewertung der relevanten Datenbanksysteme anhand dieser Anforderungen durchgeführt?

M 2.125 Installation und Konfiguration einer Datenbank

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Grundsätzlich muss zwischen der Erstinstallation einer Datenbank-Software und der Installation auf bestehenden Datenbanksystemen unterschieden werden.

Da bei der erstmaligen Installation einer Datenbank-Software noch keine Benutzer auf die Datenbank zugreifen wollen und auch noch keine Altdaten vorhanden sind (es sei denn in anderen Datenbanksystemen), gestaltet sich dies relativ unproblematisch und stört den normalen IT-Betrieb kaum.

Für Installationen auf bestehenden Systemen sollten dagegen die Arbeiten, wenn möglich, außerhalb der regulären Arbeitszeiten erfolgen, um Behinderungen des normalen IT-Betriebs weitestgehend zu minimieren. In jedem Fall sollten die Benutzer über bevorstehende Arbeiten informiert werden, um sie auf eventuell mögliche Störungen oder längere Antwortzeiten hinzuweisen.

Die Installation und Konfiguration einer Datenbank gliedert sich in die folgenden Aktivitäten:

1. Installation der Datenbank-Software

Vor der Installation der Datenbank-Software ist zu überprüfen, ob das IT-System entsprechend der Planung vorbereitet wurde, z. B. genügend Speicherplatz zur Verfügung steht und die notwendigen Betriebssystemeinstellungen vorgenommen wurden.

Bei der Installation der Datenbank-Software sind die Installationsanweisungen des Herstellers zu befolgen. Wenn möglich, sollten die vom Hersteller vorgeschlagenen Default-Einstellungen übernommen werden. Dies gilt vor allem für technische Parameter, die z. B. die Größe verschiedener interner Tabellen des DBMS steuern. Für Parameter, die sich auf sicherheitsrelevante Eigenschaften beziehen, muss unter Umständen von den vorgegebenen Werten abgewichen werden.

Die Installation der Datenbank-Software ist geeignet zu dokumentieren. Dies gilt insbesondere für Abweichungen von den vom Hersteller vorgeschlagenen Default-Einstellungen, die ausführlich zu begründen sind.

Sollen vom Hersteller angebotene optionale Funktionalitäten genutzt werden, so ist während der Installation darauf zu achten, dass sie auch entsprechend eingerichtet werden.

Alle Tätigkeiten in diesem Schritt werden vom fachlich übergreifenden Administrator durchgeführt.

2. Erstellen der Datenbank

Bereits bei der Erstellung der Datenbank sind Parameter anzugeben, die später während des Betriebs des Datenbanksystems nicht mehr geändert werden können. Die Bedeutung dieser Parameter und die geeignete Auswahl ihrer

Werte werden in den Installationsunterlagen und Handbüchern des Herstellers ausführlich erläutert und sind dort entsprechend nachzulesen.

Dem Installationshandbuch bzw. Administrationshandbuch sind außerdem Hinweise über eventuell erforderliche Nacharbeiten nach der Erstellung der Datenbank zu entnehmen.

Auch dieser Vorgang ist im Rahmen einer Dokumentation festzuhalten.

Alle Tätigkeiten in diesem Schritt werden vom fachlich übergreifenden Administrator durchgeführt, wobei ihm die anwendungsspezifischen Administratoren beratend zur Seite stehen müssen (z. B. um die Größe der Datenbank festlegen zu können).

3. Konfiguration der Datenbank

Im dritten Schritt ist das Benutzer- und Gruppenkonzept sowie das ggf. zum Einsatz kommende Rollenkonzept umzusetzen. Dazu erstellt der fachlich übergreifende Administrator die einzelnen Berechtigungsprofile und legt alle Gruppen sowie die administrativen Benutzer-Kennungen (für die anwendungsspezifischen Administratoren) an. Dabei sind die in M 2.132 *Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen* festgelegten Regelungen anzuwenden und zu überprüfen. Hängen die entsprechenden Zugriffsberechtigungen von einzelnen Datenbankobjekten ab, können diese natürlich erst dann definiert werden, wenn die Datenbankobjekte auch existieren (siehe Schritt 4).

Falls die Datenbank-Software eine Verteilung der Daten auf mehrere Dateien oder Festplatten unterstützt, sind zusätzliche Parametereinstellungen vorzunehmen, die das Anlegen dieser Dateien respektive der zugehörigen Speicherbereiche festlegen.

Alle vorgenommenen Einstellungen sind detailliert zu dokumentieren (siehe M 2.25 *Dokumentation der Systemkonfiguration*).

Alle Tätigkeiten in diesem Schritt werden vom fachlich übergreifenden Administrator durchgeführt.

4. Erstellen und Konfigurieren von Datenbankobjekten

Gemäß des Datenbanksicherheitskonzeptes (siehe M 2.126 *Erstellung eines Datenbanksicherheitskonzeptes*) werden im letzten Schritt die Datenbankobjekte der einzelnen Anwendungen angelegt. Dieser Vorgang sollte, wenn möglich, durch den Einsatz von Skripten automatisiert und protokolliert werden. Nach Anlage der Datenbankobjekte sind die notwendigen Zugriffsberechtigungen für Rollen, Gruppen und Benutzer zu ergänzen. Ebenso können jetzt die konkreten Benutzer anhand der existierenden Berechtigungsprofile erstellt werden.

Alle Tätigkeiten in diesem Schritt werden von den anwendungsspezifischen Administratoren durchgeführt.

Ergänzende Kontrollfragen:

- Werden die Benutzer über die bevorstehende Installation informiert?
- Sind vor Erstellen der Datenbank alle erforderlichen Parameter und deren Werte bekannt, die während der Installation benötigt werden?
- Sind alle Nacharbeiten bekannt, die nach der Erstellung der Datenbank durchgeführt werden müssen?
- Wurde der Installationsvorgang, die Erstellung und Konfiguration der Datenbank sowie der Datenbankobjekte dokumentiert?

M 2.126 Erstellung eines Datenbanksicherheitskonzeptes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Die Datenhaltung in Datenbanken über einen längeren Zeitraum hinweg ist meist ein zentraler und kritischer Aspekt des Informationsmanagements einer Behörde bzw. eines Unternehmens. Zur Organisation eines reibungslosen Datenbankbetriebs muss deshalb frühzeitig ein Datenbanksicherheitskonzept erstellt werden, in dem Sicherheitsaspekte bei der Planung, Installation, Konfiguration, Betrieb, Migration und Deinstallation beschrieben sind.

Werden Datenbanken nicht ausreichend geschützt, kann es zu einem Verlust der Vertraulichkeit, Verfügbarkeit oder Integrität der gespeicherten Daten kommen. Um diesem vorzubeugen, ist es unumgänglich, ein schlüssiges Datenbanksicherheitskonzept zu erstellen.

Im Konzept müssen insbesondere Aussagen darüber gemacht werden,

- wie die Abgrenzung der Zugriffsrechte zwischen Datenbankadministration und Anwendungsadminstration erfolgt,
- wie die Speicherung der Daten und gegebenenfalls Spiegelung der Datenbank erfolgt,
- wie die Datensicherung erfolgt,
- welche Mechanismen zur Überwachung und Kontrolle der Datenbankaktivitäten eingesetzt werden und
- wie die Datenbankkapazität überwacht werden soll.

Die Sicherheit einer Datenbank wird auf Software-Ebene durch das zugehörige Datenbankmanagementsystem (DBMS) gewährleistet. Damit ein DBMS effektiven Schutz bieten kann, müssen folgende grundlegende Bedingungen erfüllt sein.

Das DBMS muss,

- auf einer umfassenden Sicherheitspolitik aufsetzen,
- im IT-Sicherheitskonzept der Organisation eingebettet sein,
- korrekt installiert und
- korrekt administriert werden.

Direkte Zugriffe auf die Datenbank (z. B. über SQL-Interpreter wie SQL*Plus) dürfen nur für administrative Benutzer zugelassen werden, um Manipulationen an den Daten bzw. Datenbankobjekten (z. B. Tabellen und Indizes) zu verhindern (siehe M 2.134 *Richtlinien für Datenbank-Anfragen*). Datenbankobjekte dürfen ausschließlich über spezielle Benutzerkennungen kontrolliert modifiziert werden. Dementsprechend muss das DBMS über ein geeignetes Zugriffs- und Zugangskonzept verfügen (siehe M 2.129 *Zugriffskontrolle einer Datenbank* und M 2.128 *Zugangskontrolle einer Datenbank*). Benutzer-Kennungen, die nur über eine Anwendung Datenmodifikationen durchführen können, dürfen keinen direkten Zugang zur Datenbank

erhalten, während Kennungen zur Verwaltung der Datenbankobjekte der kontrollierte direkte Zugriff erlaubt sein muss.

Weiterhin müssen folgende wichtige Aspekte in einem Datenbanksicherheitskonzept geregelt werden:

- Die physische Speicherung bzw. Spiegelung der Datenbankdateien (z. B. der DBMS-Software, der Datenbank an sich oder der Protokolldateien) sowie deren Verteilung ist festzulegen, um z. B. die Verfügbarkeit und Ausfallsicherheit zu erhöhen. Aus Verfügbarkeitsgründen sollten gespiegelte Kontrolldateien auf verschiedenen Festplatten abgelegt sein. Der Ausfall einer Platte bedeutet dann nicht gleichzeitig den Verlust aller Kontrolldateien. Falls die Datenbankobjekte einer Anwendung in eigenen Datendateien abgelegt werden, so sollte man bei der Verteilung der Datendateien darauf achten, dass bei einem Ausfall einer Festplatte nicht alle Anwendungen betroffen sind.

  Beispiel:

  Eine Datenbank verwaltet die Daten zweier Anwendungen, mit jeweils einer Datendatei für die Tabellen und Indizes. Die Datendateien können beliebig auf vier Festplatten verteilt werden.

  Eine ungünstige Verteilung der Datendateien sieht folgendermaßen aus:

  Festplatte 1:

  Ablage der Datendateien für die Indizes beider Anwendungen

  Festplatte 2:

  Ablage der Datendateien für die Tabellen der ersten Anwendung

  Festplatte 3:

  Ablage der Datendateien für die Tabellen der zweiten Anwendung

  Festplatte 4: -

  Bei Ausfall der ersten Festplatte wären somit beide Anwendungen betroffen und könnten nicht mehr genutzt werden.

  Eine günstigere Verteilung der Datendateien erhält man dagegen so:

  Festplatte 1:

  Ablage der Datendateien für die Indizes der ersten Anwendung

  Festplatte 2:

  Ablage der Datendateien für die Tabellen der ersten Anwendung

  Festplatte 3:

  Ablage der Datendateien für die Indizes der zweiten Anwendung

  Festplatte 4:

  Ablage der Datendateien für die Tabellen der zweiten Anwendung

Bei Ausfall einer beliebigen Festplatte wäre immer nur eine Anwendung betroffen.

Sind Festplatte 1 und 2 auf Festplatte 3 und 4 zusätzlich gespiegelt und umgekehrt Festplatte 3 und 4 auf Festplatte 1 und 2, könnten bis zu zwei beliebige Platten ausfallen, ohne dass die Datenbank für eine der beiden Anwendungen vollständig ausfiele.

- Es muss eine regelmäßige Prüfung des tatsächlich anfallenden Datenvolumens bzw. des Zuwachses des Datenvolumens im späteren laufenden Betrieb durchgeführt werden, um den benötigten Speicherplatz auch für zukünftige Bedürfnisse geeignet dimensionieren zu können.
- Geeignete Mechanismen zur Datensicherung müssen angewendet werden (siehe M 6.49 *Datensicherung einer Datenbank*).
- Der Einsatz von Überwachungs- und Kontrollmechanismen ist festzulegen, d. h. ob und in welchem Umfang Datenbankaktivitäten protokolliert werden sollen. Hier stellt sich unter anderem die Frage, ob beispielsweise nur der Zeitpunkt einer Datenmodifikation festgehalten wird, oder ob auch die Modifikation selbst protokolliert werden soll (siehe M 2.133 *Kontrolle der Protokolldateien eines Datenbanksystems*).

Für die Konzeption und den Betrieb eines Datenbanksystems muss geeignetes Personal zur Verfügung stehen. Der zeitliche Aufwand für den Betrieb eines Datenbanksystems darf nicht unterschätzt werden. Alleine die Auswertung der angefallenen Protokolldaten nimmt erfahrungsgemäß viel Zeit in Anspruch. Ein Datenbank-Administrator muss fundierte Kenntnisse über die eingesetzte DBMS-Software besitzen und auch entsprechend geschult werden.

Ergänzende Kontrollfragen:

- Wurden die Sicherheitsziele für den Einsatz eines Datenbanksystems formuliert und dokumentiert?
- Sind die Zugriffsmöglichkeiten so eingeschränkt, dass nur Administratoren über eine interaktive Abfragesprache direkt auf die Datenbanken zugreifen können?

M 2.127 Inferenzprävention

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Zum Schutz personenbezogener und anderer vertraulicher Daten eines Datenbanksystems ist grundsätzlich jedem Benutzer nur der Zugriff auf diejenigen Daten zu gestatten, die für seine Tätigkeiten notwendig sind. Alle anderen Informationen, die sich zusätzlich in der Datenbank befinden, sind vor ihm zu verbergen.

Zu diesem Zweck müssen die Zugriffsberechtigungen auf Tabellen bis hin zu deren Feldern definiert werden können. Dies kann mittels Verwendung von Views und Grants durchgeführt werden (siehe M 2.129 *Zugriffskontrolle einer Datenbank*). Damit ist es einem Benutzer nur möglich, die für ihn bestimmten Daten einzusehen und zu verarbeiten. Stellt er Datenbankabfragen, die auf andere Informationen zugreifen wollen, werden diese vom DBMS zurückgewiesen.

Im Zusammenhang mit statistischen Datenbanken, die Daten über Personengruppen, Bevölkerungsschichten oder ähnliches enthalten, treten dagegen andere Schutzanforderungen auf. In einer statistischen Datenbank unterliegen die einzelnen, personenbezogenen Einträge dem Datenschutz, statistische Informationen sind jedoch allen Benutzern zugänglich.

Hier gilt es zu verhindern, dass aus Kenntnissen über die Daten einer Gruppe auf die Daten eines individuellen Mitglieds dieser Gruppe geschlossen werden kann. Es muss außerdem verhindert werden, dass durch das Wissen der in der Datenbank gespeicherten Informationen bzw. der Ablagestrukturen der Daten in der Datenbank die Anonymität dieser Daten durch entsprechend formulierte Datenbankabfragen umgangen werden kann (z. B. wenn die Ergebnismenge einer Datenbankabfrage nur einen Datensatz beinhaltet). Diese Problematik wird Inferenzproblem, der Schutz vor solchen Techniken Inferenzprävention genannt.

Auch wenn die Daten einer statistischen Datenbank anonymisiert sind, kann durch Inferenztechniken der Personenbezug zu bestimmten Datensätzen wiederhergestellt werden. Eine Zurückweisung bestimmter Anfragen (z. B. Anfragen mit nur einem oder wenigen Ergebnistupeln) reicht im allgemeinen nicht aus, da auch die Verweigerung einer Antwort durch das DBMS Informationen beinhalten kann.

Durch das Erstellen verschiedener Statistiken kann die Anonymität der Daten ebenfalls verloren gehen. Ein solcher indirekter Angriff zielt darauf ab, aus mehreren Statistiken Rückschlüsse auf die persönlichen Daten eines einzelnen Individuums ziehen zu können. Eine Schutzmaßnahme ist in diesem Fall, die Freigabe von so genannten sensitiven Statistiken nicht zu erlauben, was als unterdrückte Inferenzprävention bezeichnet wird. Eine weitere Möglichkeit ist die Verzerrung solcher Statistiken durch kontrolliertes Runden (gleiche Statistiken sind gleich zu runden) oder die Beschränkung auf statistisch relevante Teilmengen mit der Auflage, dass gleiche Anfragen immer Bezug auf

die gleichen Teilmengen nehmen. Dieses Verfahren wird als verzerrende Inferenzprävention bezeichnet.

Werden weitergehende Anforderungen an die Vertraulichkeit der Daten gestellt, ist deren Verschlüsselung erforderlich (vergleiche M 4.72 *Datenbank-Verschlüsselung*).

Ergänzende Kontrollfragen:

- Wurden die Vertraulichkeitsanforderungen an das Datenbanksystem erfasst und dokumentiert?
- Sind die vertraulichen Daten ausreichend vor unbefugtem Zugriff geschützt?

M 2.128 Zugangskontrolle einer Datenbank

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Datenbank-Software muss über geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer verfügen, um eine wirkungsvolle Zugangskontrolle zu gewährleisten. Die Vergabe von Zugangsberechtigungen hat nach festgelegten Regeln zu erfolgen (siehe M 2.132 *Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen*).

Generell sollte für normale Benutzer der Zugang zu einer Produktionsdatenbank über einen interaktiven SQL-Interpreter unterbunden werden. Auf solche Datenbanken sollte ausschließlich ein indirekter Zugang über die entsprechenden Anwendungen möglich sein. Die einzige Ausnahme bilden hier Datenbankkennungen zu Administrationszwecken.

Remote-Zugänge zu Datenbanken sollten äußerst restriktiv gehandhabt werden. Ist diese Art des Zugangs nicht zwingend erforderlich, so sind diese zu unterbinden. Ansonsten sollte nur denjenigen Benutzern ein Remote-Zugang ermöglicht werden, die diesen auch tatsächlich benötigen. Andere Benutzer dürfen nicht in der Lage sein, sich selbst einen Remote-Zugang zu verschaffen. Keinesfalls darf ein Remote-Zugang ohne Angabe einer gültigen Benutzer-Kennung und Eingabe eines Passwortes möglich sein.

Bei erhöhten Sicherheitsanforderungen sollte geprüft werden, ob eine starke Authentisierung, die über Benutzername und Passwort hinausgeht, erforderlich ist. Hier kommt beispielsweise der Einsatz von Chipkarten oder sogenannten Tokens in Frage.

Ergänzende Kontrollfragen:

- Gibt es Benutzer-Kennungen, die direkten Zugang zu einer Datenbank haben? Falls ja, aus welchem Grund haben sie direkten Zugang?
- Wurden die Möglichkeiten des Remote-Zugangs für die derzeit im Einsatz befindlichen Datenbanken geprüft und gegebenenfalls deaktiviert?

M 2.129 Zugriffskontrolle einer Datenbank

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um einen wirkungsvollen Schutz der Vertraulichkeit und Integrität der Daten einer Datenbank zu erreichen, müssen eine Reihe von Maßnahmen umgesetzt werden. Neben einer Zugangskontrolle der Datenbank, die in M 2.128 *Zugangskontrolle einer Datenbank* beschrieben wird, sind dies im wesentlichen die folgenden Möglichkeiten der Zugriffskontrolle:

Schutz der Datenbankobjekte

Es sollte eine logische Zuordnung der Datenbankobjekte, also der Tabellen, Indizes, Datenbankprozeduren, etc., zu den Anwendungen erfolgen, die diese Objekte benutzen. Die daraus entstehenden Gruppen von Datenbankobjekten je Anwendung werden eigens hierfür einzurichtenden Kennungen zugeordnet. Damit können die Zugriffsberechtigungen der Datenbankobjekte so eingestellt werden, dass nur über diese speziellen Kennungen eine Modifikation der Objekte stattfinden kann. Greifen mehrere Anwendungen auf dieselben Datenbankobjekte zu, sollten diese als eigene Gruppe isoliert werden.

Werden beispielsweise die Daten zweier Anwendungen A und B in der Datenbank verwaltet, so sind zwei Datenbankkennungen AnwA und AnwB anzulegen. Alle Datenbankobjekte, die eindeutig der Anwendung A zugeordnet werden können, werden mit der Datenbankkennung AnwA angelegt und verwaltet. Analog wird mit den Datenbankobjekten von Anwendung B verfahren.

Ein Beispiel für ein zentrales Datenbankobjekt, das von beiden Anwendungen benutzt wird, sei eine Tabelle, die alle ansteuerbaren Drucker beinhaltet. Datenbankobjekte dieser Kategorie sollten nicht einer Kennung der Anwendungen (AnwA oder AnwB) zugeordnet werden, statt dessen sollten solche Datenbankobjekte unter einer eigenen Kennung (z. B. Druck) zusammengefasst und mit dieser zentralen Kennung verwaltet werden.

Diese speziellen Kennungen sind nicht personenbezogen. Statt dessen erhalten eigens hierfür autorisierte Personen (z. B. der Datenbankadministrator oder der Administrator der zugehörigen Anwendung) das Passwort der benötigten Kennung, falls Modifikationen an den Datenbankobjekten vorgenommen werden müssen (siehe zu diesem Themenbereich auch M 4.68 *Sicherstellung einer konsistenten Datenbankverwaltung*).

Schutz der Daten

Durch eine Definition von *Views* und *Prozeduren* können spezielle Benutzer-Sichten auf die Daten erzeugt werden, so dass die Daten der Datenbank nach bestimmten Kriterien sichtbar gemacht bzw. unsichtbar gehalten werden. Über einen *View* oder eine *Prozedur* wird explizit festgelegt, welche Felder aus einer oder mehreren Tabellen einem Benutzer in welcher Reihenfolge angezeigt werden. Durch spezielle Bedingungen können hierbei die Daten gefiltert und durch spezifische Beschränkungen in ihrem Umfang begrenzt werden. Durch die restriktive Vergabe von Zugriffsrechten (den im folgenden beschriebenen *Grants*) auf solche *Views* und *Prozeduren* können vertrauliche Daten vor unberechtigtem Zugriff geschützt werden.

Durch Trennung von Daten und Funktionalitäten, hier die Trennung der *Views* und *Prozeduren* von den echten Daten durch Speicherung in einer eigenständigen Datenbank kann die Sicherheit zusätzlich erhöht werden. Der Benutzer oder die Anwendung greift ausschließlich auf die *Views* und *Prozeduren* in der ausgelagerten Datenbank zu. Erst diese *Views* und *Prozeduren* greifen auf die in der Datenbank abgelegten Daten zu. In der ausgelagerten Datenbank werden die Zugriffsrechte der Benutzer und Anwendungen zusammengefasst.

Hierbei können Zugriffsrechte (*Grants*) auf Tabellen, *Views*, etc. oder sogar auf einzelne Felder einer Tabelle vergeben werden. Diese Rechte sind immer an bestimmte Benutzer, Rollen oder Benutzergruppen gebunden. Vorzuziehen ist hierbei die klare Trennung zwischen Zugangsrechten von Benutzern (meist über Kennung und Passwort) einerseits und Zugriffsrechten von Benutzergruppen und Rollen auf DB-Objekte andererseits. Die Koppelung von Benutzern zu DB-Objekten geschieht dann über die Zuordnung einzelner Benutzer zu den mit den notwendigen Zugriffsrechten ausgestatteten Benutzergruppen oder Rollen. Es können Zugriffsberechtigungen lesender (*read*), ändernder (*update*), löschender (*delete*), neu einfügender (*insert*) oder neu erstellender (*create*) Art unterschieden werden, bei *Prozeduren* kommt die Ausführungsberechtigung (*execute*) hinzu. Die Schritte zur Vergabe von Zugriffsberechtigungen sollten im Datenbankkonzept präzise beschrieben sein. Grundsätzlich sollten nur die wirklich erforderlichen Zugriffsberechtigungen vergeben werden. Anderenfalls besteht die Gefahr, dass der Überblick über die aktuellen Zugriffsrechte verloren geht und zusätzliche Sicherheitslücken entstehen können. Insbesondere sollte die vom DBMS zur Verfügung gestellte Möglichkeit, Rechte an alle zu vergeben (GRANT ... TO PUBLIC), nicht genutzt werden.

Im allgemeinen ist es nur dem Besitzer eines Datenbankobjektes erlaubt, Zugriffsberechtigungen an andere Benutzer weiterzugeben. Einige Datenbanksysteme stellen jedoch die Möglichkeit zur Verfügung, dass der Besitzer eines Datenbankobjektes auch das Recht, Zugriffsrechte weiterzugeben, an andere Benutzer vergeben kann. Von dieser Möglichkeit sollte nur in begründeten Ausnahmefällen Gebrauch gemacht werden, da der Besitzer des Datenbankobjektes auf diese Weise die Kontrolle über den Zugriff auf die Daten bzw. die Datenbankobjekte verliert.

Restriktiver Datenzugriff über Anwendungen

Anwendungen sollten einen restriktiven Zugriff auf die Daten unterstützen, d. h. in Abhängigkeit der Benutzer-Kennung und der Gruppenzugehörigkeit sollten nur diejenigen Funktionalitäten und Daten zur Verfügung gestellt werden, die ein Benutzer für die Ausführung seiner Aufgaben benötigt. Eine Form der DB-seitigen Realisierung einer solchen Anwendung ist hier die Verwendung von sogenannten *Stored Procedures*.

Stored Procedures sind Abfolgen von SQL-Anweisungen, die in der Datenbank voroptimiert gespeichert werden. Beim Aufruf einer Stored Procedure müssen nur ihr Name und eventuelle Parameter angegeben werden, um die dahinterstehenden Anweisungen auszuführen. Dies hat zum einen den Vorteil, dass nicht die gesamten Anweisungen zum Datenbank-Server übertragen werden müssen, was bei komplexeren Operationen die Netzbelastung vermindert. Zum anderen kann das Datenbanksystem die Anweisungen in einer optimierten, vor-compilierten Form ablegen, so dass sie bei Aufruf schneller ausge-

führt werden. Die restriktivste Form der Rechtevergabe ist die Vergabe von Zugriffsrechten auf Stored Procedures statt auf Tabellen oder Views. Wenn Zugriffsrechte nur auf Stored Procedures vergeben werden, können die Benutzer nur die von den Datenbankverantwortlichen ausgewählten Operationen ausführen.

Beispiele:

1. In Microsoft Access können verschiedene Berechtigungen vergeben werden, die sich entweder auf die Datenbank selbst (Öffnen/Ausführen, Exklusiv, Verwalten) oder auf die Tabellen und Abfragen beziehen (Daten lesen, Daten aktualisieren, Daten löschen, Daten einfügen). Diese Berechtigungen können dann unterschiedlichen Benutzern oder Benutzergruppen zugeordnet werden. Standardmäßig sind bei Microsoft Access die Gruppen "Administratoren" und "Benutzer" eingerichtet, wobei die Gruppe "Benutzer" die Berechtigungen "Daten lesen" und "Daten aktualisieren" für Tabellen und Abfragen sowie die Berechtigung "Öffnen/Ausführen" für Datenbanken enthält. Für eine detailliertere Kontrolle der Zugriffsrechte können eigene Gruppen definiert werden, an die unterschiedliche Berechtigungen vergeben werden können.
2. In einer Oracle-Datenbank kann mit den Kommandos CREATE ROLE und GRANT die Gruppe "Abteilung_1" erstellt und die Berechtigung erteilt werden, z. B. eine Verbindung zur Datenbank herzustellen (connect), eine Session zu eröffnen (create Session) und Auswahlabfragen auf bestimmte Tabellen durchzuführen (select).

   Indem existierende Datenbank-Benutzer der Gruppe "Abteilung_1" zugeordnet werden, erhalten diese Benutzer alle Berechtigungen der zugeordneten Benutzergruppe. In diesem Beispiel könnte ein ausschließlich der Gruppe "Abteilung_1" zugeordneter Benutzer nur auf die der Gruppe zugeordneten Tabellen und hier ausschließlich lesend (select) aber nicht modifizierend (insert, delete, update, etc.) zugreifen.
3. Eine Stored Procedure unter Oracle mit PL/SQL-Anweisungen hat einen Eingabeparameter, der die Artikelnummer angibt. Die Stored Procedure durchsucht alle zur Berechnung der Ausgabeparameter benötigten Tabellen und gibt unter anderem den Artikelpreis zurück.

   Benutzer erhalten über die Zugriffsrechtevergabe ein Nutzungsrecht nur auf die Stored Procedure, jedoch keinerlei Rechte auf die entsprechenden Tabellen. Damit werden z. B. auch zeitaufwendige Suchoperationen durch eine Auswahlberechtigung direkt auf die zugehörigen Tabellen verhindert.

Ergänzende Kontrollfragen:

- Wurden die Datenbankobjekte vor unberechtigtem Zugriff geschützt?
- Wurden Zugriffsrechte auf die Daten vergeben und dokumentiert?

M 2.130 Gewährleistung der Datenbankintegrität

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Verantwortliche der einzelnen IT-Anwendungen

Die Integritätssicherung und -überwachung einer Datenbank soll die Korrektheit der zugehörigen Daten bzw. einen korrekten Zustand der Datenbank gewährleisten. Die folgenden Techniken sind zur Vermeidung inkorrekter Daten bzw. Zustände innerhalb einer Datenbank zu beachten:

- **Zugriffskontrolle**

  Damit ist der Schutz der betreffenden Datenbank vor unautorisiertem Zugriff mittels der Vergabe von Zugriffsrechten gemeint, wie in M 2.129 *Zugriffskontrolle einer Datenbank* beschrieben. Damit wird dem manipulativen Ändern von Daten bzw. Datenbankobjekten (wie z. B. Tabellen) vorgebeugt.

  Verantwortlich für die Umsetzung der Zugriffskontrolle ist der Datenbankadministrator.

  Auf eine detaillierte Ausführung wird an dieser Stelle verzichtet und statt dessen auf die Maßnahme M 2.129 *Zugriffskontrolle einer Datenbank* verwiesen

- **Synchronisationskontrolle**

  Die Synchronisationskontrolle dient der Verhinderung von Inkonsistenzen, die durch einen parallelen Zugriff auf denselben Datenbestand entstehen können. Es gibt dazu verschiedene Techniken, wie z. B. das Sperren von Datenbankobjekten (*Locking*) oder die Vergabe von Zeitstempeln (*Timestamps*).

  Verantwortlich für die Umsetzung sind die Verantwortlichen der IT-Anwendungen, insofern ein zusätzlicher Mechanismus zur Verfügung gestellt werden muss, der über die Möglichkeiten des Datenbankmanagementsystems (DBMS) hinausgeht.

  Auf eine detaillierte Ausführung wird verzichtet, da im allgemeinen jedes DBMS eine Synchronisationskontrolle durchführt. Vom Einsatz eines DBMS, welches dies nicht leisten kann, wird dringend abgeraten.

- **Integritätskontrolle**

  Hierunter fällt die Vermeidung semantischer Fehler bzw. semantisch unsinniger Zustände der Datenbank durch Einhaltung und Überwachung der geforderten Integritätsbedingungen. Diese können sich auf einzelne Relationen beziehen oder mehrere Relationen miteinander in Beziehung setzen (referentielle Integrität). Beispiele sind die Angabe eines Primärschlüssels für eine Relation, die Definition von Wertebereichen zu den einzelnen Attributen oder die Formulierung spezieller Bedingungen mittels einer *assertion*-Klausel.

  Dies kann durch das DBMS automatisch mittels eines Monitors überprüft werden, der z. B. durch die Verwendung von *Triggern* oder *Stored*

Procedures realisiert werden kann. Damit sind prinzipiell beliebige Transaktionen möglich, jedoch werden diejenigen vom DBMS zurückgewiesen, die die Datenbank-Konsistenz verletzen würden.

Verantwortlich für die Umsetzung sind die Verantwortlichen der IT-Anwendungen respektive der fachliche Administrator, falls es sich um eine Umsetzung der Integritätsbedingungen in Form von Relationen, Primärschlüsseln oder allgemeinen Datenbankobjekten handelt.

Im Rahmen der **Konzeption** einer IT-Anwendung sind zu erstellen

- ein Datenmodell, welches neben den Datenbankobjekten auch deren Beziehungen untereinander abbildet, und
- ein Fachkonzept, welches unter anderem Bedingungen beschreibt, unter denen Daten manipuliert werden dürfen.

Im Rahmen der **Realisierung** einer IT-Anwendung sind die folgenden Punkte zu beachten:

- Die konkrete Umsetzung des in der konzeptionellen Phase definierten Datenmodells muss festgelegt werden. Hierzu gehören die Definition und Anlage von Tabellen, Indizes, Wertebereichen usw.
- Die Definition von *Triggern* oder *Stored Procedures* erfolgt im Rahmen der Realisierung des Fachkonzepts. Trigger und Stored Procedures können dabei sowohl innerhalb der Anwendung (in den Programmen), als auch der Datenbank (für Tabellen) Verwendung finden. Trigger, die auf Datenbankebene eingesetzt werden, wirken unabhängig von darüberliegenden Anwendungen und sind aus diesem Grund zentral zu verwalten.

  Beispiel: *Trigger* "*Update"* für eine Tabelle:

  Immer wenn ein Datensatz der Tabelle geändert wird, dann sind die für den Trigger definierten Anweisungen auszuführen. Eine dieser Anweisungen kann der Aufruf einer *Stored Procedure* sein.

Im Rahmen von Anwendungen kann eine Integritätssicherung durch einen geeigneten Einsatz von Commit bzw. Rollback für das Betätigen bzw. Widerrufen von Transaktionen realisiert werden.

Ergänzende Kontrollfragen:

- Werden alle oben angegebenen Techniken zur Integritätssicherung eingesetzt?
- Wurden die Integritätsbedingungen mit den Verantwortlichen der einzelnen IT-Anwendungen abgestimmt?

M 2.131 Aufteilung von Administrationstätigkeiten bei Datenbanksystemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, IT-Sicherheitsmanagement

Um einen geordneten Betrieb von Datenbanksystemen zu ermöglichen, sind Administratoren zu bestimmen. Diesen obliegt neben allgemeinen Administrationsarbeiten insbesondere die Benutzerverwaltung einschließlich der Verwaltung der Zugriffsrechte. Zusätzlich sind sie für die Sicherheitsbelange der betreuten Datenbanksysteme zuständig.

Neben den in M 2.26 *Ernennung eines Administrators und eines Vertreters* und M 3.10 *Auswahl eines vertrauenswürdigen Administrators und Vertreters* genannten Maßnahmen sind speziell für Datenbanksysteme folgende Dinge zu beachten.

Es sollten grundsätzlich zwei verschiedene Administrator-Rollen unterschieden werden:

- die fachlich übergreifende Administration der Datenbank-Software und
- die Administration der anwendungsspezifischen Belange.

Diese beiden Aufgaben sollten von verschiedenen Personen durchgeführt werden, um eine Trennung der anwendungsspezifischen und fachlich übergreifenden Administration einer Datenbank zu erreichen.

Der grundsätzliche Betrieb des DBMS, die Durchführung der Datensicherungen oder die Archivierung von Datenbeständen sind beispielsweise Bestandteil der fachlich übergreifenden Datenbankadministration.

Bei der anwendungsspezifischen Administration werden dagegen die Erfordernisse der einzelnen Anwendungen an die Datenbank bearbeitet. Dies kann z. B. die Verwaltung der zugehörigen Datenbankobjekte, die Unterstützung der Benutzer bei Problemen bzw. Fragen oder die Verwaltung der entsprechenden Datenbankkennungen beinhalten. Letzteres ist allerdings nur dann möglich, wenn die Verwaltung der Datenbankkennungen je Anwendung über ein entsprechendes Berechtigungskonzept durch die Datenbank-Software unterstützt wird, also von den fachlich übergreifenden Berechtigungen getrennt werden kann.

Der fachlich übergreifende Administrator richtet die für die anwendungsspezifischen Belange zuständigen Administratorkennungen mit den zugehörigen Berechtigungen ein. Dazu gehört insbesondere das Recht, Datenbanken anzulegen. Die Rechtevergabe für die einzelnen Benutzer sollte dagegen für jede anwendungsspezifische Datenbank getrennt durchgeführt werden und zwar vom jeweils zuständigen anwendungsspezifischen Administrator.

Ergänzende Kontrollfragen:

- Sind die Administrator-Rollen getrennt worden?
- Welche Administratoren sind für die fachlich übergreifende Administration der Datenbank-Software und welche für die Administration der anwendungsspezifischen Belange benannt worden?
- Wie ist die Zusammenarbeit zwischen den Administratoren geregelt? Sind deren Aufgaben und Zuständigkeitsbereiche schriftlich fixiert?

M 2.132 Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Einrichtung von Benutzern/Benutzergruppen aus einer Datenbank bilden die Voraussetzung für eine angemessene Vergabe von Zugriffsrechten (siehe M 2.129 *Zugriffskontrolle einer Datenbank*) und für die Sicherstellung eines geordneten und überwachbaren Betriebsablaufs. Grundsätzlich erhält dazu jeder Datenbankbenutzer eine interne Datenbankkennung, über die ihn das Datenbanksystem identifiziert. Damit können nur autorisierte Personen auf die Datenbank zugreifen.

Modifizierende Operationen (Update, Insert, Delete, etc.), die nicht vom DBMS sondern von Benutzern mit Administrationsrechten ausgeführt werden, stellen ein hohes Risiko dar, das zur Zerstörung der Datenbank führen kann. Auf die Vergabe von modifizierenden Rechten auf die System-Tabellen sollte deshalb grundsätzlich verzichtet werden. Selbst ein lesender Zugriff sollte beschränkt werden, da über die System-Tabellen alle Informationen der Datenbank ermittelt werden können.

In Anlehnung an M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen* sollte ein Formblatt erstellt werden, um von jedem Benutzer bzw. für jede Benutzergruppe zunächst die erforderlichen Daten abzufragen, die für eine organisierte Benutzerverwaltung erforderlich sind:

- Name, Vorname,
- Vorschlag für die Benutzer-Kennung (wenn nicht durch Konventionen vorgegeben),
- Organisationseinheit,
- Erreichbarkeit (z. B. E-Mail, Telefon, Raum),
- Zustimmung von Vorgesetzten,
- Projekt (optional),
- Anwendungen, die benutzt werden sollen und auf das Datenbanksystem zugreifen (optional),
- Angaben über die geplante Tätigkeit im Datenbanksystem und die dazu erforderlichen Rechte sowie die Dauer der Tätigkeit (optional) und
- Restriktionen auf Zeiten, Zugriffsberechtigungen (für bestimmte Tabellen, Views etc.), eingeschränkte Benutzerumgebung (optional).

Es sollte eine begrenzte Anzahl von Rechteprofilen festgelegt werden. Ein neuer Benutzer wird dann einem oder mehreren Profilen zugeordnet und erhält damit genau die für seine Tätigkeit erforderlichen Rechte. Dabei sind die datenbankspezifischen Möglichkeiten bei der Einrichtung von Benutzern und Gruppen zu nutzen, die bereits bei der Auswahl der Datenbanksoftware zu berücksichtigen sind (siehe M 2.124 *Geeignete Auswahl einer Datenbank-Software*). Es ist sinnvoll, Namenskonventionen für die Benutzer- und

Gruppenkennungen festzulegen (z. B. Benutzer-ID = Kürzel der Organisationseinheit plus laufende Nummer).

Dabei können Benutzer-, Rollen- und Gruppenprofile benutzt werden. Soweit möglich, sollten jedoch keine benutzerspezifischen Profile verwendet werden, da dies bei einer großen Anzahl von Benutzern zu einem hohen administrativen Aufwand führt. Bei der Definition von Gruppenprofilen muss man zwischen restriktiven und großzügigen Berechtigungsprofilen abwägen. Werden die Gruppenprofile zu restriktiv gehandhabt, muss eine große Anzahl von Gruppen verwaltet werden, was zu einem hohen administrativen Aufwand führt. Werden die Gruppenprofile dagegen zu großzügig definiert, kann es zu Redundanzen zwischen verschiedenen Gruppen kommen oder zur Einräumung von unnötig umfangreichen Rechten, was wiederum zur Verletzung der Vertraulichkeit oder Integrität von Daten führen kann.

Jedem Benutzer muss eine eigene Datenbankkennung zugeordnet sein, es dürfen nicht mehrere Benutzer unter derselben Kennung arbeiten.

Grundsätzlich muss zwischen der der Datenbankkennung und der Benutzerkennung des zugrunde liegenden Betriebssystems unterschieden werden. Einige Hersteller bieten in ihrer Datenbank-Software jedoch die Möglichkeit an, die Betriebssystemkennung in das Datenbanksystem zu übernehmen. Dies erspart den Anwendern eine Authentisierung für den Zugang zur Datenbank, falls diese sich bereits mit ihrer eigenen Betriebssystemkennung angemeldet haben.

So können beispielsweise unter Oracle so genannte OPS$-Kennungen verwendet werden. Eine solche Kennung setzt sich aus dem Präfix "OPS$" und der Betriebssystemkennung des Benutzers zusammen. Nur wenn sich ein Benutzer mit seiner Betriebssystemkennung am Datenbanksystem anmeldet, wird kein Passwort vom DBMS abgefragt. Meldet sich der Benutzer dagegen unter einer anderen Kennung an, so erfolgt eine Passwortabfrage.

Diese Möglichkeit beinhaltet allerdings die Gefahr, dass bei einer unerlaubten Authentisierung auf Betriebssystemebene (z. B. bei Überwindung des entsprechenden Passwortschutzes) der Zugriff auf die Datenbank nicht mehr verhindert werden kann. Vor der Verwendung von OPS$-Kennungen sollte deshalb geprüft werden, ob die Sicherheitsmechanismen des Betriebssystems auf den Clients für den vorliegenden Anwendungsfall ausreichend sind.

Bei der Forderung nach einer einfachen Handhabung für die Benutzer (Stichwort *Single-Sign-On* - SSO) sollte alternativ der Einsatz eines Zusatzproduktes zur zentralen Benutzerverwaltung für den gesamten IT-Betrieb erwogen werden. Aber auch hier müssen die konkreten Sicherheitsanforderungen mit dem entsprechenden Zusatzprodukt abgeglichen werden.

Ergänzende Kontrollfragen:

- Werden die Zugriffsrechte über Benutzergruppen, Profile oder Rollen statt direkt an einzelne Benutzer vergeben?
- Welche organisatorischen Regelungen zur Einrichtung von Datenbank-benutzern bzw. -benutzergruppen gibt es?
- Wurden Namenskonventionen für die Benutzer- und Gruppenkennungen festgelegt?
- Wurden Rechteprofile angelegt?

M 2.133 Kontrolle der Protokolldateien eines Datenbanksystems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Revisor

Die in einem Datenbanksystem mögliche Protokollierung bzw. Auditierung ist in einem sinnvollen Umfang zu aktivieren. Werden zuviele Ereignisse protokolliert, wird die Performance der Datenbank negativ beeinflusst und die Protokolldateien wachsen stark an. Es muss also immer zwischen dem Bedürfnis, möglichst viele Informationen zur Sicherheit der Datenbank zu sammeln, und der Möglichkeit, diese Informationen zu speichern und auszuwerten, abgewogen werden.

Dabei sind insbesondere folgende Vorkommnisse von Interesse:

- Anmeldezeiten und -dauer der Benutzer,
- Anzahl der Verbindungen zur Datenbank,
- fehlgeschlagene bzw. abgewiesene Verbindungsversuche,
- Auftreten von Deadlocks innerhalb des Datenbanksystems,
- I/O-Statistik für jeden Benutzer,
- Zugriffe auf die Systemtabellen (siehe auch M 4.69 *Regelmäßiger Sicherheitscheck der Datenbank*),
- Erzeugung neuer Datenbankobjekte und
- Datenmodifikationen (eventuell mit Datum, Uhrzeit und Benutzer).

Die Protokollierung sicherheitsrelevanter Ereignisse ist als Sicherheitsmaßnahme allerdings nur dann wirksam, wenn die protokollierten Daten auch ausgewertet werden. Daher sind die Protokolldateien in regelmäßigen Abständen durch einen Revisor auszuwerten. Ist es organisatorisch oder technisch nicht möglich, einen unabhängigen Revisor mit der Auswertung der Protokolldateien zu betrauen, ist eine Kontrolle der Tätigkeiten des Administrators nur schwer möglich.

Weiterhin ist bei bei der Protokollierung sicherheitsrelevanter Ereignisse sowie bei der Prüfung (Monitoring) der Protokolldateien foldendes zu beachten:

4-Augen-Prinzip

Für die Überprüfung der Protokolldateien sind diese grundsätzlich in eine andere Umgebung zu kopieren. Geeignete Tools sollten dabei genutzt werden. Die Verantwortlichkeiten für die Protokollierung und die Verantwortlichkeiten für die zu protokollierenden Aktivitäten müssen getrennt werden.

Die Protokollierung ist zu schützen vor:

- Deaktivierung,
- Änderungen der zu protokollierenden Ereignistypen,
- Änderung der Protokolldaten (Inhalt) und
- Datenverlust bei Protokoll-Medien, z. B. durch Überschreiben, falsches Beschreiben, falsche Lagerung.

Auswertung, Löschung und Archivierung von Protokolldaten

Die Protokolldaten müssen auf dem Produktivsystem regelmäßig gelöscht werden, um ein übermäßiges Anwachsen der Protokolldateien zu verhindern. Sie dürfen allerdings nur dann gelöscht werden, wenn die Protokolldateien vorher ausgewertet und kontrolliert wurden. Unter Umständen müssen die Protokolldaten archiviert werden. Die Archivierung oder gegebenenfalls auch die Löschung der Protokolldateien kann manuell oder automatisch geschehen, falls entsprechende Werkzeuge zur Verfügung stehen.

Bei Auffälligkeiten ist das IT-Sicherheitsmanagement zu unterrichten.

Weiterhin ist der Zugriff auf die Protokolldateien strikt zu beschränken. Einerseits muss verhindert werden, dass Angreifer ihre Aktionen durch nachträgliche Änderung der Protokolldateien verbergen können, andererseits könnten über die gezielte Auswertung von Protokolldateien Leistungsprofile der Benutzer erstellt werden. Deshalb dürfen beispielsweise Änderungen überhaupt nicht vorgenommen werden können und lesender Zugriff darf nur den Revisoren gestattet werden.

Bei der Konzeption der Vorgehensweise für die Protokollierung und Auswertung der Protokolldaten müssen frühzeitig der Datenschutzbeauftragte und der Personal- bzw. Betriebsrat beteiligt werden.

Um die Auswertung der Protokolldaten zu vereinfachen, können vom Datenbank-Administrator zusätzliche Tools eingesetzt werden, die eine automatisierte Überwachung durchführen. Solche Produkte können beispielweise die Protokolldateien von Datenbanksystemen nach vorgegebenen Mustern auswerten und bei Bedarf einen Alarm erzeugen.

Weitere Maßnahmen, die in diesem Zusammenhang beachtet werden müssen, sind in M 2.64 *Kontrolle der Protokolldateien* zu finden.

Ergänzende Kontrollfragen:

- Wer wertet die Protokolldateien aus? Findet das Vier-Augen-Prinzip Anwendung?
- Können die Aktivitäten des Administrators ausreichend kontrolliert werden?
- Wird das IT-Sicherheitsmanagement bei Auffälligkeiten unterrichtet?

M 2.134 Richtlinien für Datenbank-Anfragen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Anwendungsentwickler

Die relationale Datenbanksprache SQL (Structured Query Language) ist eine international standardisierte Sprache für relationale Datenbanksysteme (DBS), die eine weite Verbreitung erfahren hat und in den meisten Datenbankmanagementsystemen (DBMS) implementiert ist. Der Sprachumfang wird in zyklisch überarbeiteten Normen (ANSI SQL-92, ANSI SQL-99, ANSI SQL-2003) festgelegt. Mittels SQL können sowohl Modifikationen der Daten (UPDATE, INSERT, DELETE), als auch der Datenbankobjekte (CREATE, ALTER, DROP) formuliert, sowie Informationen abgefragt werden (SELECT).

Es müssen Richtlinien für eine effiziente, wartbare und nachvollziehbare Programmierung von Datenbankabfragen erstellt und im Rahmen der Programmierung umgesetzt werden. Folgende Grundsätze sollten in dieser Richtlinie beschrieben sein:

- Anfragen an die Datenbank sollten möglichst nicht direkt auf Tabellen, sondern über *Views* und *Prozeduren* ausgeführt werden. Einerseits kann dadurch der Schutz der Daten besser gewährleistet werden (siehe M 2.129 *Zugriffskontrolle einer Datenbank*). Andererseits kann sichergestellt werden, dass den Benutzern die notwendigen Informationen in entsprechender Formatierung und Menge zur Verfügung gestellt werden. Zusätzlich können diese *Views* und *Prozeduren* in eine eigene DB ausgelagert werden und Benutzer sowie Anwendungen können nur auf diese ausgelagerte DB Zugriff erhalten. Die Daten in den Tabellen sind dann außer über die *Prozeduren* und *Views* der ausgelagerten DB nur einem speziellen Benutzerkreis zugänglich (Administratoren, etc.).
- SQL-Anfragen sollten exakt und explizit in Anlehnung an das DB-Modell formuliert werden. Dabei sollten alle erfragten Felder explizit angegeben und der "*"-Operator vermieden werden. Damit ist sichergestellt, dass die Daten in der erwarteten Reihenfolge zur Verfügung gestellt und nur diejenigen Daten selektiert werden, die tatsächlich benötigt werden.

  Beispiel:

  Ein DB-Modell enthält eine Tabelle mit den Feldern "Artikelnummer", "Artikelbezeichnung", "Verwendungszweck" und "Nettopreis". Im Zuge einer Erweiterung der Applikation wird hinter dem "Verwendungszweck" ein weiteres Feld mit dem Namen "Bestellnummer" eingefügt. Aus Gründen der optimalen Speicherausnutzung fügt das DBMS das neue Feld jedoch nicht dort, sondern an die zweite Stelle hinter "Artikelnummer" ein. Weil die Daten mit Hilfe einer SELECT-*-Anweisung abgefragt werden, liefert die Datenbank die Informationen in einer anderen Reihenfolge zurück, als die Applikation sie erwartet. Dies führt bei der Applikation zu Problemen, deren Ursache zunächst nicht erkennbar ist.
- Bei einschränkenden Datenbankanfragen (WHERE-Klausel) ist die Reihenfolge der angegebenen Selektionsbedingungen von großer Bedeu-

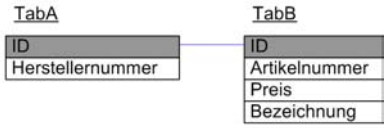
tung für die Ausführungsgeschwindigkeit. Die WHERE-Klausel sollte so formuliert werden, dass zuerst die Bedingung angegeben wird, die in kürzester Zeit die kleinstmögliche Ergebnismenge selektiert. Dabei sollte zuerst auf indizierte Felder zugegriffen werden, dann erst auf nicht-indizierte Felder, wobei hier Prüfungen auf Ziffern schneller sind als Prüfungen auf Texte. Das gleiche gilt analog für Datenbankanfragen, die über mehrere Tabellen hinweg formuliert werden (so genannte Joins).

Viele DBMS optimieren bereits Datenbankanfragen selbständig. Oft werden zusätzlich sogar mehrere Optimierungsstrategien zur Auswahl angeboten, die über verschiedene Parameter ausgewählt werden können.

Einige DBMS bieten die Möglichkeit, die Abarbeitung von Datenbankanfragen zu untersuchen (z. B. in Oracle mit EXPLAIN oder für Ingres mittels SETOEP). Des weiteren besteht die Möglichkeit, über so genannte HINTS in der Datenbankanfrage deren Abarbeitung explizit zu definieren und somit den Optimizer im Prinzip auszuschalten. Von dieser Möglichkeit sollte allerdings vorsichtig Gebrauch gemacht werden.

- Welche Optimizer das DBMS unterstützt sowie deren Vor- und Nachteile sind in den Handbüchern des DBMS normalerweise dokumentiert. Der Einsatz alternativer Optimizer innerhalb eines DBMS sollte mit dem Administrator abgesprochen werden.
- Im Falle von Joins sollte zusätzlich beachtet werden, dass die Zuordnung von Feldern zu den Tabellen eindeutig erfolgt.

Beispiel:




```
select
  TabA.ID,
  TabB.Bezeichnung,
  TabB.Preis
from
  TabA join TabB on
    TabA.ID = TabB.ID
```

Abbildung: Feldzuordnung bei Joins

Das Feld "ID" ist in beiden Tabellen vorhanden und **muss** deshalb bei der Datenbankanfrage explizit mit dem zugehörigen Tabellennamen angegeben werden. Andernfalls ist die Eindeutigkeit der Auswahl nicht mehr sichergestellt und die Datenbankanfrage wird mit einer entsprechenden Fehlermeldung abgebrochen.

Alle anderen Felder sind in diesem Fall eindeutig den jeweiligen Tabellen zuzuordnen. Eine explizite Angabe des zugehörigen Tabellennamens für jedes Feld wird von SQL nicht gefordert. Trotzdem sollte für die einzelnen Felder die eindeutige Zuordnung zur Tabelle erfolgen, wie im obigen Beispiel für die Felder "Preis" und "Bezeichnung" der Tabelle TabB. Das Hin-

zufügen eines Feldes "Bezeichnung" für TabA würde im obigen Beispiel zu keinen Problemen führen. Dies wäre jedoch nicht der Fall, wenn die SQL-Anweisung die Zuordnung der Felder zu den Tabellen nicht explizit beinhalten würde. Es wäre nicht mehr eindeutig, ob das Feld "Bezeichnung" von TabA oder TabB selektiert werden soll, da beide Tabellen nach der Änderung von TabA ein Feld mit diesem Namen haben. Die SQL-Anweisung würde mit einer Fehlermeldung abgebrochen.

- Alle Datenbanktransaktionen sollten explizit mit einem COMMIT bestätigt werden. Falls das DBMS ein automatisches COMMIT unterstützt, sollte dieses nicht aktiviert werden, da es sonst unter Umständen zu ungewollten Inkonsistenzen in der Datenbank kommen kann.

Beispiel:

Mehrere einzelne Modifikationen gehören logisch zusammen, werden aber nach der Ausführung jeder einzelnen Modifikation automatisch durch ein COMMIT bestätigt. Kommt es nun zu einem unkontrollierten Abbruch der Transaktion und infolgedessen zu einem Rollback, sind die zuerst ausgeführten Operationen bereits bestätigt und verbleiben in der Datenbank, während der Rest noch gar nicht durchgeführt werden konnte.

- Zur Vermeidung von Sperrkonflikten oder gar Deadlocks ist für jede fachliche Datenbank eine Sperrstrategie festzulegen (z. B. hierarchisches Sperren oder explizites Sperren aller Tabellen am Anfang der Transaktion).
- Anwendungsentwickler sollten nach jeder SQL-Anweisung den Fehlerstatus prüfen, so dass die Anwendung so früh wie möglich auf eingetretene Fehler reagieren kann.
- Berechtigungen auf systemspezifische Kommandos, mit denen beispielsweise die Protokollierung ausgeschaltet oder das Locking-Verfahren verändert werden kann, sollten Benutzern entzogen und auf Administratoren beschränkt werden.
- Bei der Entwicklung von Anwendungen sollten alle Datenbankzugriffe in einem Modul oder einem bestimmten Teil des Programmcodes zusammengefasst werden, da sonst zur Überprüfung der obigen Grundsätze der gesamte Programmcode des Anwendungssystems herangezogen werden müsste. Hierdurch wird die Wartung und Pflege des Anwendungssystems, z. B. bei Änderungen des Datenmodells, erleichtert.

Ergänzende Kontrollfragen:

- Sind Richtlinien für Datenbank-Anfragen erstellt worden?
- Sind den Anwendungsentwicklern die Richtlinien für Datenbank-Anfragen bekannt?
- Wie wird die Einhaltung dieser Richtlinien überprüft?

M 2.135 Gesicherte Datenübernahme in eine Datenbank

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

In vielen Datenbanksystemen besteht aus Anwendungssicht die Notwendigkeit, Daten aus anderen Systemen zu übernehmen. Dabei lassen sich prinzipiell die beiden folgenden Kategorien unterscheiden:

Erst- oder Altdatenübernahme

Bei der Übernahme von Daten aus Altsystemen, wenn beispielsweise ein neues Datenbanksystem beschafft wurde und produktiv eingesetzt werden soll, ist insbesondere sicherzustellen, dass

- die Daten in einem Format vorliegen, das in die Zieldatenbank übernommen werden kann,
- die Daten vollständig sind, d. h. für alle Felder, die in der Zieldatenbank gefüllt werden sollen, müssen Daten zur Übernahme zur Verfügung gestellt werden, und
- die Konsistenz und Datenintegrität der Datenbank gewährleistet ist.

Im Vorfeld der Datenübernahme ist ein Konzept zu erstellen, wie die zu übernehmenden Daten aufbereitet werden müssen und wie die Übernahme konkret durchgeführt werden soll. Weiterhin ist eine Komplettsicherung der Altdaten vorzunehmen. Erfolgt die Datenübernahme in mehreren Schritten, sollte vor jedem einzelnen Schritt eine unabhängige Datensicherung durchgeführt werden.

Regelmäßige Datenübernahme

Befinden sich in der Zieldatenbank bei einer Datenübernahme bereits Daten, die nicht verändert werden dürfen, oder werden in regelmäßigen Zeitabständen Daten in eine Datenbank übernommen, so

- ist vor der Datenübernahme eine Komplettsicherung der Datenbank durchzuführen,
- sollte die Datenübernahme wenn möglich außerhalb der regulären Betriebszeiten stattfinden,
- sind Vorkehrungen zu treffen, um eine mehrfache Übernahme der gleichen Daten zu verhindern,
- ist vor der ersten Datenübernahme ein Konzept zu erstellen, wie die zu übernehmenden Daten aufbereitet werden müssen bzw. wie die Übernahme konkret durchzuführen ist. Insbesondere muss in diesem Konzept berücksichtigt werden, wie Konflikte zwischen den bereits existierenden Daten in der Zieldatenbank und den zu übernehmenden Daten vermieden werden, d. h. inwieweit die Integrität und Konsistenz der Zieldatenbank gewahrt bleibt.

Von einer Datenbankaktualisierung betroffene Benutzer müssen über die bevorstehende Datenübernahme rechtzeitig informiert werden, insbesondere dann, wenn mit Einschränkungen hinsichtlich der Verfügbarkeit oder des Antwortzeitverhaltens zu rechnen ist.

Vor der Durchführung einer Datenübernahme ist festzulegen, was beim Auftreten von Fehlern zu unternehmen ist. Dies beinhaltet z. B., ob beim Auftreten eines fehlerhaften Datensatzes mit dem nächsten Satz fortgefahren werden kann, oder ob die komplette Datenübernahme abgebrochen werden muss. Weiterhin ist festzulegen, wie die Datenübernahme nach einem Abbruch wieder aufgesetzt wird.

Ergänzende Kontrollfragen:

- Wurde ein Konzept zur Datenübernahme erstellt?
- Erfolgt vor einer Datenübernahme eine Komplettsicherung der Datenbank?
- Werden die betroffenen Benutzer bei einer Datenübernahme rechtzeitig und umfassend informiert?

M 2.136 Einhaltung von Regelungen bzgl. Arbeitsplatz und Arbeitsumgebung

Verantwortlich für Initiierung: Leiter Haustechnik, Personalrat/Betriebsrat

Verantwortlich für Umsetzung: Vorgesetzte, Personalrat/Betriebsrat, Mitarbeiter

Am häuslichen Arbeitsplatz müssen dieselben Vorschriften und Richtlinien bezüglich der Gestaltung des Arbeitsplatzes (z. B. Einrichtung eines Bildschirmarbeitsplatzes) und der Arbeitsumgebung gelten wie in der Institution. Dies sollte in Absprache mit dem Telearbeiter durch den in der Institution Verantwortlichen für den Arbeits- und Gesundheitsschutz, dem IT-Sicherheitsbeauftragten, dem Datenschutzbeauftragten sowie dem Betriebs- bzw. Personalrat und dem direkten Vorgesetzten des Telearbeiters begutachtet werden können.

M 2.137 Beschaffung eines geeigneten Datensicherungssystems

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Administrator

Ein Großteil der Fehler, die beim Erstellen oder Restaurieren einer Datensicherung auftreten, sind Fehlbedienungen. Daher sollte bei der Beschaffung eines Datensicherungssystem nicht allein auf seine Leistungsfähigkeit geachtet werden, sondern auch auf seine Bedienbarkeit und insbesondere auf seine Toleranz gegenüber Benutzerfehlern.

Bei der Auswahl von Sicherungssoftware sollte darauf geachtet werden, dass sie die folgenden Anforderungen erfüllt:

- Die Datensicherungssoftware sollte ein falsches Medium ebenso wie ein beschädigtes Medium im Sicherungslaufwerk erkennen können.
- Sie sollte mit der vorhandenen Hardware problemlos zusammenarbeiten.
- Es sollte möglich sein, Sicherungen automatisch zu vorwählbaren Zeiten bzw. in einstellbaren Intervallen durchführen zu lassen, ohne dass hierzu manuelle Eingriffe (außer dem eventuell notwendigen Bereitstellen von Sicherungsdatenträgern) erforderlich wären.
- Es sollte möglich sein, einen oder mehrere ausgewählte Benutzer automatisch über das Sicherungsergebnis und eventuelle Fehlermeldungen per E-Mail oder ähnliche Mechanismen zu informieren. Die Durchführung von Datensicherungen inklusive des Sicherungsergebnisses und möglicher Fehlermeldungen sollten in einer Protokolldatei abgespeichert werden.
- Die Sicherungssoftware sollte die Sicherung des Backup-Mediums durch ein Passwort, oder noch besser durch Verschlüsselung unterstützen. Weiterhin sollte sie in der Lage sein, die gesicherten Daten in komprimierter Form abzuspeichern.
- Durch Vorgabe geeigneter Include- und Exclude-Listen bei der Datei- und Verzeichnisauswahl sollte genau spezifiziert werden können, welche Daten zu sichern sind und welche nicht. Es sollte möglich sein, diese Listen zu Sicherungsprofilen zusammenzufassen, abzuspeichern und für spätere Sicherungsläufe wieder zu benutzen.
- Es sollte möglich sein, die zu sichernden Daten in Abhängigkeit vom Datum ihrer Erstellung bzw. ihrer letzten Modifikation auszuwählen.
- Die Sicherungssoftware sollte die Erzeugung logischer und physischer Vollkopien sowie inkrementeller Kopien (Änderungssicherungen) unterstützen.
- Die zu sichernden Daten sollten auch auf Festplatten und Netzlaufwerken abgespeichert werden können.
- Die Sicherungssoftware sollte in der Lage sein, nach der Sicherung einen automatischen Vergleich der gesicherten Daten mit dem Original durchzuführen und nach der Wiederherstellung von Daten einen entsprechenden

Vergleich zwischen den rekonstruierten Daten und dem Inhalt des Sicherungsdatenträgers durchzuführen.

- Bei der Wiederherstellung von Dateien sollte es möglich sein auszuwählen, ob die Dateien am ursprünglichen Ort oder auf einer anderen Platte bzw. in einem anderen Verzeichnis wiederhergestellt werden. Ebenso sollte es möglich sein, das Verhalten der Software für den Fall zu steuern, dass am Zielort schon eine Datei gleichen Namens vorhanden ist. Dabei sollte man wählen können, ob diese Datei immer, nie oder nur in dem Fall, dass sie älter als die zu rekonstruierende Datei ist, überschrieben wird, oder dass in diesem Fall eine explizite Anfrage erfolgt.

Falls mit dem eingesetzten Programm die Datensicherung durch Passwort geschützt werden kann, sollte diese Option genutzt werden. Das Passwort ist dann gesichert zu hinterlegen (siehe M 2.22 *Hinterlegen des Passwortes*).

Bei den meisten Betriebssystemen werden Programme für Datensicherungen mitgeliefert. Nicht alle erfüllen allerdings die Ansprüche an Produkte für professionelle und komfortable Datensicherungen. Stehen aber keine solchen Produkte zur Verfügung, so sollten die systemzugehörigen Programme verwendet werden.

M 2.138 Strukturierte Datenhaltung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Eine schlecht strukturierte Datenhaltung kann zu einer Vielzahl von Problemen führen. Alle IT-Benutzer sind daher darauf hinzuweisen, wie eine gut strukturierte und übersichtliche Datenhaltung aussehen sollte. Auf allen Servern sollten entsprechende Strukturen durch die Administratoren vorgegeben werden. Dies ist ohnehin Voraussetzung, um eine differenzierte Vergabe von Zugriffsrechten realisieren zu können.

Programme und Applikationsdateien trennen

Programm- und Arbeitsdateien sollten immer in getrennten Bereichen gespeichert werden. Dies sorgt für eine bessere Übersicht und erleichtert auch die Durchführung von Datensicherungen und die Sicherstellung des korrekten Zugriffsschutzes. Bei den meisten Applikationsprogrammen ändern sich nach der Installation keine oder nur sehr wenige Konfigurationsdateien. Soweit möglich, sollten alle Dateien, die sich regelmäßig ändern, in gesonderten Verzeichnissen abgespeichert werden, damit nur diese in die regelmäßigen Datensicherungen mitaufgenommen werden müssen.

Bei einer sauberen Trennung von Programmen und Daten reicht es, die Daten in die regelmäßigen Datensicherungen aufzunehmen. Wichtig ist es, die Arbeitsdateien sorgfältig gesichert zu haben, diese können dann notfalls auch auf anderen Systemen weiterverarbeitet werden.

Bei vernetzten Systemen stellt sich außerdem die Frage, welche Programme bzw. Dateien auf den lokalen Festplatten oder auf einem Netzserver abgelegt werden sollten. Beides hat Vor- und Nachteile und muss sowohl von der organisatorischen Struktur als auch von der eingesetzten Hard- und Software abhängig gemacht werden. So sollten z. B. Dateien mit hohen Verfügbarkeitsansprüchen zusammen mit den zugehörigen Applikationsprogrammen besser auf den Arbeitsplatzrechnern gehalten werden als auf einem Netzserver. Dann muss allerdings auch die entsprechende Notfallvorsorge für diese Arbeitsplatzrechner betrieben werden.

aufgaben- oder projektbezogene Verzeichnisse

Es sollten aufgaben- oder projektbezogene Verzeichnisse eingerichtet werden, um die Zuordnung von Dateien zu erleichtern. Es sollten möglichst wenig Daten in personenbezogenen Verzeichnissen abgelegt werden.

Um zu verhindern, dass für die weitere Arbeit grundlegenden Dateien wie Briefvorlagen, Formularen, Projektplänen oder Ähnlichem unterschiedliche Versionsstände existieren, sollten diese zentral verwaltet werden. Sie sollten beispielsweise auf einem Server so vorgehalten werden, dass jeder lesend darauf zugreifen kann, aber es sollte für jede solche Datei jeweils nur eine Person geben, die sie verändern darf.

Wie auf einem Server durch Verzeichnisvorgaben Daten strukturiert werden könnten, wird in dem folgenden Beispiel gezeigt:

```
\
\bin
        \bin\program1
        \bin\program2
        \bin\program3
\user
        \user\user1
        \user\user2
\projekte
        \projekte\p1
                \projekte\p1\texte
                \projekte\p1\bilder
        \projekte\p2
                \projekte\p2\projektplan
                \projekte\p2\teilprojekt1
                \projekte\p2\teilprojekt2
                \projekte\p2\teilprojekt3
                \projekte\p2\ergebnis
        \vordrucke
```

Verzeichnisse regelmäßig aufräumen

Es sollte regelmäßig überprüft werden,

- ob Daten aus dem Produktionssystem entfernt werden können, weil sie archiviert oder gelöscht werden können,
- ob Zugriffsrechte entzogen werden können, weil Mitarbeiter die Projektgruppe verlassen haben,
- ob auf allen IT-Systemen die aktuellsten Versionen von Formularen, Vorlagen, etc. gespeichert sind.

Dies ist durch die Benutzer für deren IT-Systeme bzw. die von ihnen verwalteten Verzeichnisse und von den Administratoren der Server regelmäßig zu überprüfen. Diese Prüfungen sollten mindestens vierteljährlich durchgeführt werden, da sonst die Kenntnisse über Inhalt und Herkunft der Dateien wieder aus den Gedächtnissen der Mitarbeiter verschwunden sind.

Ergänzende Kontrollfragen:

- Werden ausschließlich aufgaben- bzw. projektbezogene Verzeichnisse für die Datenhaltung benutzt?
- Wann wurde zuletzt überprüft, ob alte Dateien gelöscht bzw. archiviert werden können?

M 2.139 Ist-Aufnahme der aktuellen Netzsituation

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Bestandsaufnahme der aktuellen Netzsituation ist Voraussetzung für eine gezielte Sicherheitsanalyse des bestehenden Netzes. Sie ist ebenso erforderlich für die Erweiterung eines bestehenden Netzes. Bei der Planung von Netzen sind die im folgenden beschriebenen Punkte bei der Konzeption zu berücksichtigen.

Hierzu ist eine Ist-Aufnahme mit einhergehender Dokumentation der folgenden Aspekte, die zum Teil aufeinander aufbauen, notwendig:

- Netztopographie,
- Netztopologie,
- verwendete Netzprotokolle,
- Kommunikationsübergänge im LAN und zum WAN sowie
- Netzperformance und Verkehrsfluss.

In den einzelnen Schritten ist im wesentlichen folgendes festzuhalten:

Ist-Aufnahme der Netztopographie

Für die Ist-Aufnahme der Netztopographie ist die physikalische Struktur des Netzes zu erfassen. Dabei ist es sinnvoll, sich an den räumlichen Verhältnissen zu orientieren, unter denen das Netz aufgebaut wird. Es ist ein Plan zu erstellen bzw. fortzuschreiben, der

- die aktuelle Kabelführung,
- die Standorte aller Netzteilnehmer, insbesondere der verwendeten aktiven Netzkomponenten,
- die verwendeten Kabeltypen sowie
- die festgelegten Anforderungen an den Schutz von Kabeln (M 1.22 *Materielle Sicherung von Leitungen und Verteilern*)

enthält. Zur Pflege dieses Plans ist es sinnvoll, ein entsprechendes Tool zur Unterstützung einzusetzen (z. B. CAD-Programme, spezielle Tools für Netzpläne, Kabelmanagementtools im Zusammenhang mit Systemmanagementtools oder Ähnlichem). Eine konsequente Aktualisierung dieser Pläne bei Umbauten oder Erweiterungen ist ebenso zu gewährleisten wie eine eindeutige und nachvollziehbare Dokumentation (vergleiche auch M 1.11 *Lagepläne der Versorgungsleitungen* und M 5.4 *Dokumentation und Kennzeichnung der Verkabelung*).

Ist-Aufnahme der Netztopologie

Für die Ist-Aufnahme der Netztopologie ist die logische Struktur des Netzes zu betrachten. Dazu ist es notwendig, die Segmentierung der einzelnen OSI-Schichten und ggf. die VLAN-Struktur zu erfassen.

Anhand der Darstellung der Netztopologie muss feststellbar sein, über welche aktiven Netzkomponenten eine Verbindung zwischen zwei beliebigen Endgeräten aufgebaut werden kann. Zusätzlich sind die Konfigurationen der aktiven Netzkomponenten zu dokumentieren, die zur Bildung der Segmente verwendet werden. Dies können bei logischer Segmentierung die Konfigurationsdateien sein, bei physikalischer Segmentierung die konkrete Konfiguration der Netzkomponenten.

Ist-Aufnahme der verwendeten Netzprotokolle

Bezogen auf die gewählte Segmentierung des Netzes, sind die in den einzelnen Segmenten verwendeten Netzprotokolle und die hierfür notwendigen Konfigurationen (z. B. die MAC-Adressen, die IP-Adressen und die Subnetzmasken für das IP-Protokoll) festzustellen und zu dokumentieren. Hier sollte auch dokumentiert werden, welche Dienste zugelassen sind (z. B. HTTP, SMTP, Telnet) und welche Dienste nach welchen Kriterien gefiltert werden.

Ist-Aufnahme von Kommunikationsübergängen im LAN und WAN

Die Kommunikationsübergänge im LAN und WAN sind, soweit sie nicht in der bereits erstellten Dokumentation enthalten sind, zu beschreiben. Für jeden Kommunikationsübergang zwischen zwei Netzen ist zu beschreiben,

- welche Übertragungsstrecken (z. B. Funkstrecke für eine LAN/LAN-Kopplung) hierfür eingesetzt werden,
- welche Kommunikationspartner und -dienste in welche Richtung hierüber zugelassen sind, und
- wer für die technische Umsetzung zuständig ist.

Hierzu gehört auch die Dokumentation der verwendeten WAN-Protokolle (z. B. ISDN, X.25). Bei einem Einsatz einer Firewall (siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)*) ist zusätzlich deren Konfiguration (z. B. Filterregeln) zu dokumentieren.

Ist-Aufnahme der Netzperformance und des Verkehrsflusses

Es ist eine Messung der Netzperformance und eine Analyse des Verkehrsflusses in und zwischen den Segmenten oder Teilnetzen durchzuführen. Für jedes eingesetzte Netzprotokoll müssen die entsprechenden Messungen erfolgen.

Bei jeder Änderung der Netzsituation sind die zuletzt durchgeführten Ist-Aufnahmen zu wiederholen. Die im Rahmen der Ist-Aufnahmen erstellte Dokumentation ist so aufzubewahren, dass sie einerseits vor unbefugtem Zugriff geschützt ist, aber andererseits für das Sicherheitsmanagement oder die Administratoren jederzeit verfügbar ist.

Ergänzende Kontrollfragen:

- Werden regelmäßig Performance-Messungen und Verkehrsfluss-Analysen durchgeführt und ausgewertet?
- Wird die erstellte Dokumentation laufend aktualisiert?
- Ist die Dokumentation auch für Dritte verständlich und nachvollziehbar?

M 2.140 Analyse der aktuellen Netzsituation

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Diese Maßnahme baut auf den Ergebnissen der Ist-Aufnahme nach M 2.139 *Ist-Aufnahme der aktuellen Netzsituation* auf und erfordert spezielle Kenntnisse im Bereich der Netztopologie, der Netztopographie und von netzspezifischen Schwachstellen. Darüber hinaus ist Erfahrung bei der Beurteilung der eingesetzten individuellen IT-Anwendungen hinsichtlich Vertraulichkeit, Integrität bzw. Verfügbarkeit notwendig. Da dies ein komplexes Gebiet ist, das neben tief gehenden Kenntnissen in allen genannten Bereichen auch viel Zeit erfordert, kann es zur Analyse der aktuellen Netzsituation hilfreich sein, externe Berater hinzuzuziehen. Im Bereich der deutschen Bundesverwaltung kann hier das BSI Hilfestellung leisten.

Eine Analyse der aktuellen Netzsituation besteht im wesentlichen aus einer Strukturanalyse, einer Schutzbedarfsfeststellung und einer Schwachstellenanalyse.

Eine **Strukturanalyse** besteht aus einer Analyse der nach M 2.139 *Ist-Aufnahme der aktuellen Netzsituation* angelegten Dokumentationen. Die Strukturanalyse muss von einem Analyseteam durchgeführt werden, das in der Lage ist, alle möglichen Kommunikationsbeziehungen nachzuvollziehen oder auch herleiten zu können. Als Ergebnis muss das Analyseteam die Funktionsweise des Netzes verstanden haben und über die prinzipiellen Kommunikationsmöglichkeiten informiert sein. Häufig lassen sich bei der Strukturanalyse bereits konzeptionelle Schwächen des Netzes identifizieren.

Eine erfolgreich durchgeführte Strukturanalyse ist unbedingte Voraussetzung für die sich anschließende detaillierte Schutzbedarfsfeststellung bzw. der Schwachstellenanalyse.

Detaillierte Schutzbedarfsfeststellung

An die Strukturanalyse schließt sich eine Schutzbedarfsfeststellung an, die über die in der IT-Grundschutz-Vorgehensweise beschriebene hinausgeht. Hier werden zusätzlich die Anforderungen an Vertraulichkeit, Verfügbarkeit und Integrität in einzelnen Netzbereichen bzw. Segmenten berücksichtigt. Hierzu ist es notwendig festzustellen, welche Anforderungen aufgrund der verschiedenen IT-Verfahren bestehen und wie diese auf die gegebene Netzsegmentierung Einfluss nehmen. Als Ergebnis muss erkenntlich sein, in welchen Netzsegmenten besondere Sicherheitsanforderungen bestehen.

Analyse von Schwachstellen im Netz

Basierend auf den bisher vorliegenden Ergebnissen erfolgt eine Analyse der Schwachpunkte des Netzes. Hierzu gehört insbesondere bei entsprechenden Verfügbarkeitsanforderungen die Identifizierung von nicht redundant ausgelegten Netzkomponenten (Single-Point-of-Failures). Weiterhin müssen die Bereiche benannt werden, in denen die Anforderungen an Verfügbarkeit, Vertraulichkeit oder Integrität nicht eingehalten werden können bzw. besonderer Aufmerksamkeit bedürfen. Zudem ist festzustellen, ob die gewählte Seg-

mentierung hinsichtlich Bandbreite und Performance geeignet ist (anhand der Ergebnisse der Verkehrsflussanalyse aus M 2.139 *Ist-Aufnahme der aktuellen Netzsituation*).

Beispielhafte Schwachstelle: Die Performance- und Verkehrsflussanalyse zeigt eine überlastete aktive Netzkomponente. Für den betreffenden Kommunikationsweg wurden im Rahmen der Schutzbedarfsfeststellung hohe Anforderungen an die Verfügbarkeit und damit auch an die Performance festgestellt. Diese Schwachstelle erfordert eine Anpassung der Segmentierung des Netzes oder den Austausch der Netzkomponente gegen ein leistungsfähigeres Modell (siehe M 5.61 *Geeignete physikalische Segmentierung,* M 5.62 *Geeignete logische Segmentierung,* M 5.60 *Auswahl einer geeigneten Backbone-Technologie* und M 5.13 *Geeigneter Einsatz von Elementen zur Netzkopplung*).

Ergänzende Kontrollfragen:

- Ist die aktuelle Netzsituation hinreichend dokumentiert?
- Steht ausreichendes "Know How" für eine Sicherheitsanalyse der Netzsituation zur Verfügung?
- Sind die Anforderungen bezüglich der Vertraulichkeit, Verfügbarkeit und Integrität des Netzes und der Daten definiert und dokumentiert?

M 2.141 Entwicklung eines Netzkonzeptes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um den Anforderungen bezüglich Verfügbarkeit (auch Bandbreite und Performance), Vertraulichkeit und Integrität zu genügen, muss der Aufbau, die Änderung bzw. die Erweiterung eines Netzes sorgfältig geplant werden. Hierzu dient die Erstellung eines Netzkonzeptes.

Die Entwicklung eines Netzkonzeptes unterteilt sich in einen analytischen und einen konzeptionellen Teil:

Analyse

Zunächst ist zu unterscheiden, ob ein bestehendes Netz zu erweitern bzw. zu verändern ist oder ob das Netz vollständig neu aufgebaut werden soll.

Im ersten Fall sind vorab die Maßnahmen M 2.139 *Ist-Aufnahme der aktuellen Netzsituation* und M 2.140 *Analyse der aktuellen Netzsituation* zu bearbeiten. Im zweiten Fall entfallen diese Maßnahmen. Stattdessen sind die Anforderungen an die Netzkommunikation zu ermitteln sowie eine Schutzbedarfsfeststellung des zukünftigen Netzes durchzuführen.

Zur Ermittlung der Kommunikationsanforderungen ist der zukünftig zu erwartende Daten- und Verkehrsfluss zwischen logischen oder organisatorischen Einheiten festzustellen, da die zu erwartende Last die Segmentierung des zukünftigen Netzes beeinflussen muss. Die notwendigen logischen bzw. physikalischen Kommunikationsbeziehungen (dienste-, anwender-, gruppenbezogen) sind ebenfalls zu eruieren und die Kommunikationsübergänge zur LAN/LAN-Kopplung oder über ein WAN zu ermitteln.

Die Schutzbedarfsanforderungen des Netzes werden aus denen der geplanten oder bereits bestehenden IT-Verfahren abgeleitet. Daraus werden physikalische und logische Segmentstrukturen gefolgert, so dass diesen Anforderungen (z. B. hinsichtlich Vertraulichkeit) durch eine Realisierung des Netzes Rechnung getragen werden kann. Zum Beispiel bestimmt der Schutzbedarf einer IT-Anwendung die zukünftige Segmentierung des Netzes.

Schließlich muss versucht werden, die abgeleiteten Kommunikationsbeziehungen mit den Schutzbedarfsanforderungen zu harmonisieren. Unter Umständen sind hierzu Kommunikationsbeziehungen einzuschränken, um dem festgestellten Schutzbedarf gerecht zu werden.

Abschließend sind die verfügbaren Ressourcen zu ermitteln. Hierzu gehören sowohl Personalressourcen, die erforderlich sind, um ein Konzept zu erstellen und umzusetzen bzw. um das Netz zu betreiben, als auch die hierfür notwendigen finanziellen Ressourcen.

Die Ergebnisse sind entsprechend zu dokumentieren.

Konzeption

Unter den oben genannten Gesichtspunkten, anhand einer Planung, die zukünftige Anforderungen (z. B. hinsichtlich Bandbreite) mit einbezieht, so-

wie unter Berücksichtigung der örtlichen Gegebenheiten, sind die Netzstruktur und die zu beachtenden Randbedingungen nach den folgenden Schritten zu entwickeln und im Konzept festzuhalten.

Die Erstellung eines Netzkonzeptes erfolgt analog M 2.139 *Ist-Aufnahme der aktuellen Netzsituation* und besteht danach prinzipiell aus den folgenden Schritten, wobei diese Schritte nicht in jedem Fall streng aufeinander folgend ausgeführt werden können. In einigen Teilen beeinflussen sich die Ergebnisse der Schritte gegenseitig, so dass eine regelmäßige Überprüfung und Konsolidierung der Teilergebnisse vorgenommen werden muss.

1. Konzeption der Netztopographie und der Netztopologie, der physikalischen und logischen Segmentierung
2. Konzeption der verwendeten Netzprotokolle
3. Konzeption von Kommunikationsübergängen im LAN und WAN

In den einzelnen Schritten sind im wesentlichen die folgenden Tätigkeiten auszuführen:

Schritt 1 - Konzeption der Netztopographie und Netztopologie

Basierend auf der Analysesituation (siehe oben) und den konkreten baulichen Gegebenheiten muss eine geeignete Netztopographie und Netztopologie ausgewählt werden (siehe hierzu M 5.60 *Auswahl einer geeigneten Backbone-Technologie,* M 5.2 *Auswahl einer geeigneten Netz-Topographie* und M 5.3 *Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht*). Aber auch zukünftige Anforderungen wie Skalierbarkeit müssen hier Berücksichtigung finden. Die so erstellte Konzeption muss dokumentiert werden (Verkabelungspläne usw.).

Ausgehend von den ermittelten Anforderungen und dem zu erwartenden bzw. ermittelten Datenfluss muss bei der Konzeption der Netztopographie und -topologie eine geeignete physikalische und logische Segmentierung durchgeführt werden (siehe M 5.61 *Geeignete physikalische Segmentierung*, M 5.62 *Geeignete logische Segmentierung* und M 5.13 *Geeigneter Einsatz von Elementen zur Netzkopplung*).

Schritt 2 - Konzeption der Netzprotokolle

In diesem Schritt sind die einzusetzenden Netzprotokolle auszuwählen und diese entsprechend zu konzipieren. Hierzu gehört beispielsweise für das IP-Protokoll die Erstellung eines Adressierungsschemas und die Teilnetzbildung. Für die Auswahl der Netzprotokolle ist zu beachten, dass diese durch die Netztopologie und die geplanten oder vorhandenen aktiven Netzkomponenten unterstützt werden können.

Schritt 3 - Konzeption der Kommunikationsübergänge im LAN und WAN

Bezogen auf den ermittelten Datenfluss über Kommunikationsübergänge hinweg und die Anforderungen bezüglich der Sicherheit und Verfügbarkeit können in diesem Schritt die Kommunikationsübergänge konzipiert werden. Hierzu gehört die Auswahl geeigneter Koppelelemente (siehe M 5.13 *Geeigneter Einsatz von Elementen zur Netzkopplung*) aber auch die sichere Konfi-

guration derselben (siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)* und M 4.82 *Sichere Konfiguration der aktiven Netzkomponenten*).

Weitere Schritte

Ausgehend von dem erstellten Netzkonzept können nun die Maßnahmen zur Erstellung eines Netzmanagement-Konzeptes durchgeführt werden (siehe M 2.143 *Entwicklung eines Netzmanagementkonzeptes*, M 2.144 *Geeignete Auswahl eines Netzmanagement-Protokolls* und M 2.145 *Anforderungen an ein Netzmanagement-Tool*) und ein Realisierungsplan nach M 2.142 *Entwicklung eines Netz-Realisierungsplans* ausgearbeitet werden.

M 2.142 Entwicklung eines Netz-Realisierungsplans

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Für die Erstellung eines Netz-Realisierungsplans ist zu unterscheiden, ob es sich um einen vollständigen Neuaufbau des Netzes, um eine Veränderung der bestehenden Konzeption und/oder eine Erweiterung handelt.

Bei einer vollständigen Neuplanung sind anhand der entwickelten Netzkonzeption (vergleiche M 2.141 *Entwicklung eines Netzkonzeptes*) die notwendigen Schritte abzuleiten. Dabei erfolgt nach abgeschlossener Planung der Aufbau des Netzes über das Verlegen der notwendigen Kommunikationskabel, das Einrichten von Räumen für die technische Infrastruktur, das Installieren der versorgenden technischen Infrastruktur, die Integration der notwendigen Koppelelemente (Bridges, Switches, Router etc.), das Einrichten der Netzmanagement-Stationen, den Einbau der entsprechenden Netzadapater in den Endgeräten, bis hin zur Konfiguration dieser Endgeräte.

Soll ein bestehendes Netz verändert oder erweitert werden, ist in einem Soll/Ist-Vergleich das nach M 2.141 *Entwicklung eines Netzkonzeptes* erarbeitete Netzkonzept mit der vorhandenen Situation nach M 2.139 *Ist-Aufnahme der aktuellen Netzsituation* zu vergleichen. Ausgehend von Differenzen kann unter Berücksichtigung der oben genannten Maßnahmen ein Realisierungsplan für die so genannte Netzmigration erstellt werden. Dabei ist zu berücksichtigen, dass der Realisierungsaufwand um so größer ist, je mehr das Netzkonzept vom Ist-Zustand abweicht.

Beispielhafte Migration eines "Shared Ethernet" zu einem "Switched Fast-Ethernet"

Eine Migration von einer Netztopologie zu einer anderen erfolgt im allgemeinen stufenweise. Im folgenden ist beispielhaft eine solche Migration von einem "Shared Ethernet" auf ein Fast-Ethernet mit Switching-Technologie skizziert. Für eine Umsetzung in der Praxis müssen allerdings die Randbedingungen genau geprüft und entsprechend ein eigenes Migrationskonzept erstellt werden.

- **Migrationsschritt 1**

  Im ersten Migrationsschritt kann das existierende Backbone durch ein Fast-Ethernet-Backbone ersetzt oder gegebenenfalls neu aufgebaut werden. Der Anschluss der verbleibenden Shared Ethernet-Segmente erfolgt über die Netzkomponenten des Backbones, die dementsprechend auch Standard-Ethernet unterstützen müssen.

- **Migrationsschritt 2**

  Aufbau einer strukturierten Verkabelung, d. h. es wird von einem Standard-Ethernet mit Stichleitung zu einem Verkabelungskonzept übergegangen, bei dem jeder Arbeitsplatz sternförmig an einen Verteilerraum angebunden wird, ohne die topologische Busstruktur aufzugeben.

- **Migrationsschritt 3**

  Die Anbindung der Server erfolgt zentral an einen Switch mit Fast-Ethernet Anschlüssen (Installation einer so genannten Serverfarm).

- **Migrationsschritt 4**

  Anwender, die eine hohe Bandbreite benötigen, werden durch Austausch der entsprechenden Schnittstellen ebenfalls mit Fast-Ethernet angeschlossen.

- **Migrationsschritt 5**

  Migration der verbleibenden Ethernet-Segmente zu einem vollständig geswitchten System. Hierzu können beispielsweise Ethernet-Switches an die Fast-Ethernet-Switches des Backbones angebunden werden.

M 2.143 Entwicklung eines Netzmanagementkonzeptes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die in einem lokalen Netz zusammengefassten vielfältigen IT-Systeme, wie z. B. Serversysteme, Endgeräte, Drucker, aktive Netzkomponenten usw., sollten auf Netzebene an einer geeigneten Stelle zentral administriert und überwacht werden können. Eine zentrale Administration der Netzkomponenten ist dabei einer dezentralen vorzuziehen, da in diesem Fall Administrationsaufwände verringert und Anforderungen an die Sicherheit zentral definiert und kontrolliert werden können. In erster Linie wird ein zentrales Netzmanagement verwendet, um die Verfügbarkeit und Integrität des Netzes sowie die Integrität und Vertraulichkeit der übermittelten Daten zu gewährleisten. Diese Aufgabe hat eine hohe Komplexität und sollte durch den Einsatz eines Netzmanagement-Tools unterstützt werden.

Vor der Beschaffung und dem Betrieb eines solchen Netzmanagement-Systems ist im ersten Schritt ein Konzept zu erstellen, in dem alle Sicherheitsanforderungen an das Netzmanagement formuliert und angemessene Maßnahmen für den Fehler- oder Alarmfall vorgeschlagen werden. Dabei sind insbesondere die folgenden Bestandteile eines Netzmanagement-Konzeptes bei der Erstellung zu berücksichtigen und in einem Gesamtzusammenhang darzustellen.

- Performance-Messungen zur Netzanalyse (siehe M 2.140 *Analyse der aktuellen Netzsituation*),
- Reaktionen auf Fehlermeldungen der überwachten Netzkomponenten,
- Fernwartung / Remote-Control, insbesondere der aktiven Netzkomponenten,
- Generierung von Trouble-Tickets und Eskalation bei Netzproblemen (Hierüber kann eine Anbindung an Systemmanagement- und User-Help-Desksysteme bzw. an externe Nachrichtenübermittler, z. B. Pager, Fax usw., erfolgen.),
- Protokollierung und Audit (Online und/oder Offline),
- Einbindung eventuell vorhandener proprietärer Systeme bzw. von Systemen mit unterschiedlichen Managementprotokollen (z. B. im Telekommunikationsbereich),
- Konfigurationsmanagement aller im Einsatz befindlichen IT-Systeme (siehe unter anderen M 4.82 *Sichere Konfiguration der aktiven Netzkomponenten*),
- Verteilter Zugriff auf die Netzmanagement-Funktionalitäten (Für die Administration oder für das Audit kann ein Remote-Zugriff auf die Netzmanagement-Funktionalitäten notwendig sein. Hier ist insbesondere eine sorgfältige Definition und Vergabe der Zugriffsrechte notwendig.).

Die konkreten Anforderungen an ein Netzmanagement-Tool sind in M 2.145 *Anforderungen an ein Netzmanagement-Tool* beschrieben. Diese müssen eine Umsetzung des Netzmanagement-Konzeptes ermöglichen.

Ergänzende Kontrollfragen:

- Wurden alle Sicherheitsanforderungen an das Netzmanagement formuliert und dokumentiert?

M 2.144 Geeignete Auswahl eines Netzmanagement-Protokolls

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Als Standardprotokolle für Netzmanagement gelten derzeit:

- SNMP (Simple Network Management Protocol), SNMP ist in RFC 1157 beschrieben, Request for Comment (RFC) ist die Bezeichnung für einen in der Internet-Society etablierten Standard.
- CMIP (Common Management Information Protocol), CMIP ist in der ITU-T-Norm X.711 bzw. in ISO/IEC 9596-1 beschrieben.

Im folgenden werden die wesentlichen Vor- und Nachteile der beiden Protokolle als Entscheidungshilfe bei der Auswahl eines Netzmanagement-Protokolls aufgezeigt.

SNMP

Für SNMP sind zwei Komponenten definiert, Manager und Agent. In einem lokalen Netz werden ein oder eventuell mehrere Manager und je ein Agent pro IT-System, das mit SNMP überwacht bzw. konfiguriert werden soll, installiert. Die Agenten sammeln über diese Systeme Informationen und legen sie in einer MIB (Management Information Base) ab. Sie tauschen mit dem Manager über ein verbindungsloses Protokoll Nachrichten aus, so dass SNMP an kein bestimmtes Transportprotokoll gebunden ist. Es wird jedoch heute üblicherweise auf UDP/IP implementiert. Andere Implementationen sind jedoch ebenfalls möglich und vorhanden (z. B. über OSI, AppleTalk, SPX/IPX). SNMP gibt es in verschiedenen Versionen. Es gibt verschiedene SNMP-Versionen, zur Zeit verbreitet sind SNMPv1, SMPv2 und SNMPv3. Sowohl die Urversion SNMPv1 als auch SNMPv2 (RFC 1901-1908) sind teilweise immer noch im Einsatz. Aus Sicherheitssicht sollte auf den Einsatz von SNMPv1 und SMPv2 verzichtet werden.

Die ersten beiden SNMP-Versionen, SNMPv1 und SMPv2, unterstützen nur einfache Authentikation, basierend auf im Klartext übertragenen Community-Namen (community strings). SNMPv3 beinhaltet verbesserte Sicherheitsmechanismen und sollte daher eingesetzt werden.

Wenn eine ältere Version von SNMP als SNMPv3 eingesetzt werden muss, muss dies begründet und dokumentiert werden, vor allem sollten die Risiken offengelegt und akzeptiert werden. Bei SNMP sind standardmäßig die Community-Namen "public" und "private" voreingestellt, typischerweise mit den Zugriffsrechten "read" oder "read and write". Community-Namen sind wie Passwörter. Die voreingestellten Community-Namen müssen daher unbedingt gegen andere, schwer zu erratende Namen ausgetauscht werden und auch regelmäßig gewechselt werden (siehe M 4.82 *Sichere Konfiguration der aktiven Netzkomponenten*). Die individuellen Netzelemente sollten unterschiedliche Community-Namen besitzen. Die mit den Community-Namen verbundenen Zugriffsberechtigungen müssen auf das absolut erforderliche Minimum gesetzt werden. Der Zugriff per SNMP auf das Netzelement sollte mit Hilfe von Access Control Listen auf die Netzwerkmanagement-Stationen

beschränkt werden (siehe M 4.80 *Sichere Zugriffsmechanismen bei Fernadministration*).

Wenn SNMPv3 technisch möglich ist, sollte es verwendet werden. Wenn SNMP nicht benötigt wird, sollte SNMP deaktiviert werden.

SNMP ist ein sehr einfaches Protokoll, das fünf Nachrichtentypen kennt. Damit tauschen Manager und Agenten die so genannten Managementinformationen aus, die hier im wesentlichen aus Werten von Statusvariablen bestehen, die im Managementagenten vorgehalten werden und den jeweiligen Zustand des zugehörigen verwalteten Objektes beschreiben. Welche Statusvariablen (Name und Typ) in den einzelnen Agenten existieren, ist in der Managementdatenbank (MIB) beschrieben. Dabei ist die Information hierarchisch organisiert, und jedem Wert ist eine eindeutige Identifikationsnummer zugeordnet, die auf den Variablen damit eine eindeutige Reihenfolge definiert. Die Nachrichtentypen sind im Einzelnen:

1. GetRequest: wird vom Manager an Agenten geschickt, um von ihnen den Wert einer oder mehrerer Statusvariablen abzufragen.
2. GetNextRequest: wird vom Manager an Agenten geschickt, um von ihnen den Wert oder die nächsten Werte gemäß der Reihenfolge der Variablen in der MIB abzufragen.
3. SetRequest: wird vom Manager an Agenten geschickt, um dort den Wert einer Variablen zu setzen.
4. GetResponse: wird vom Agenten zum Manager geschickt, um die angefragten Werte zu senden oder das Setzen eines Variablenwertes zu bestätigen.
5. Trap: wird vom Agenten verwendet, um den Manager über Ausnahmeereignisse zu informieren. Das Senden einer Trap-Nachricht erfolgt, im Gegensatz zur GetResponse-Nachricht, ohne vorherige Anfrage vom Manager.

Die wesentlichen Vor- und Nachteile sind:

+ SNMP zeichnet sich durch ein einfaches Design und damit auch durch eine einfache Implementation aus. Dies reduziert die Fehleranfälligkeit und verbessert die Stabilität des Protokolls.

+ SNMP ist sehr weit verbreitet und gilt als ein De-Facto-Standard. Dadurch wird es durch fast jedes Produkt im Netz- und Systemtechnikumfeld unterstützt.

+ Das Protokoll kann sehr einfach an zukünftige Bedürfnisse angepasst werden. Aus diesem Grund und der oben genannten weiten Verbreitung von SNMP kann es als sehr zukunftssicheres Protokoll (Investitionsschutz) bezeichnet werden.

+ Es handelt sich um ein verbindungsloses, einfaches Protokoll auf Transportebene. Damit ist die Performance der Übertragung der SNMP-Pakete im Netz besser als beim verbindungsorientierten CMIP.

- Der Einsatz von SNMP (SNMPv1 und SNMPv2) birgt Sicherheitsrisiken, die es unter Umständen einem Angreifer ermöglichen, weitgehende Informationen über die System- und Netzumgebung zu erhalten. Insbesondere existiert, abgesehen von den Community-Namen (die bei

SNMP die Möglichkeit zur Bildung von Gruppen und bei SNMPv1 und SNMPv2 einen rudimentären Passwortschutz bieten), kein echter Passwortschutz beim Zugriff auf die Netzkomponenten.

- Aufgrund der Einfachheit des Protokolls und der verfügbaren Möglichkeiten weist SNMP Schwächen im Umgang mit sehr großen oder stark expandierenden Netzen auf.
- Die Performance der Version 1 bei aufwendigeren MIB-Abfragen ist ungenügend, da immer der gesamte MIB-Baum angegeben werden muss.

Einer der großen Nachteile der Version 1 des SNMP liegt in der fehlenden Unterstützung einer Authentisierung beim Zugriff auf die überwachten Komponenten. Diese Nachteile gleicht die Version 2 von SNMP zum Teil aus, zusätzlich wurde die Performance bei der Abfrage der MIBs erhöht.

Allerdings gibt es auch in SNMPv2 bezüglich der unterstützten Sicherheit unterschiedliche Varianten. Erst die Versionen SNMPv2* und SNMPv2u bieten die Möglichkeit einer symmetrischen benutzerbasierten Authentisierung, während SNMPv2c weiterhin auf Communities aufbaut. Communities werden in SNMP zum einen genutzt, um die einzelnen Netzkomponenten zu Bereichen zusammenzufassen, und zum anderen als Passwortersatz beim Zugriff auf diese. Hinzu kommt in SNMPv2* die Möglichkeit der Datenverschlüsselung nach dem Data Encryption Standard im Cipher Block Chaining Modus (DES-CBC). Aufgrund der unterschiedlichen Varianten innerhalb von

SNMPv2 ist derzeit die Unsicherheit bei den Herstellern von Netzkomponenten und Netzmanagement-Systemen groß, so dass Implementierungen nach SNMPv2 noch nicht flächendeckend anzutreffen und nur eingeschränkt interoperabel sind.

Die unterschiedlichen Ausprägungen von SNMPv2 wurden in der nächsten SNMP-Version (SNMPv3) konsolidiert.

CMIP

CMIP setzt im Gegensatz zu SNMP auf einem implementierten OSI-Protokollstapel (die OSI-Schichten 1 bis 3 sind als Protokollstapel implementiert) auf und arbeitet damit auch verbindungsorientiert. Hierdurch wird die Verwendung des CMIP auf Komponenten eingeschränkt, die die notwendigen Hard- und Softwarevoraussetzungen für die Implementation eines vollständigen OSI-Stapels bieten. Aufgrund der hohen Anforderungen, die diese Implementation stellt, wurde auch ein "CMIP Over TCP/IP" (CMOT) definiert (RFC 1189). Hierdurch wird es möglich, CMIP auch in reinen TCP/IP-Netzen zu betreiben.

Eines der Ziele bei der Entwicklung des CMIP war es, ein objektorientiertes Management zu entwickeln. CMIP ist dementsprechend konsequent objektorientiert aufgebaut. Im CMIP übernimmt eine CMIP-Maschine (CMIPM) die Aufgaben, die unter SNMP der Manager durchführt. An diese CMIPM, die wie der SNMP-Manager als Software realisiert ist, werden von den Agenten der zu verwaltenden Objekte Service-Requests zur Einleitung verschiedener Aktionen geschickt und umgekehrt versendet die CMIPM CMIP-Nachrichten an die Agenten der zu verwaltenden Objekte. Die zu verwaltenden Objekte werden nach den Grundsätzen des objektorientierten Ansatzes in mehreren

Bäumen verwaltet, die zueinander verschiedene Relationen und Zugriffsarten aufweisen.

Das CMIP ist aufgrund der beschriebenen Objektstruktur sehr leistungsfähig und komplex. Das Protokoll selbst besteht dagegen aus relativ wenigen Operationen, mit denen das gesamte Management auf der Basis der oben genannten Objektstruktur ermöglicht wird.

Die wesentlichen Vor- und Nachteile sind:

+ CMIP bietet durch den objektorientierten Ansatz wesentlich mehr Möglichkeiten als SNMP, da z. B. auch Aktionen ausgeführt und Instanzen von Management-Objekten verwaltet werden können.
+ CMIP bietet größere Sicherheit als SNMP, insbesondere durch die Bereitstellung von Mechanismen zum Zugriffsschutz, zur Authentisierung der Benutzer und zum Auditing.
+ CMIP ist ein durch OSI genormtes Protokoll und damit ein offizieller internationaler Standard, während SNMP nur einen De-Facto-Standard auf RFC-Basis darstellt.
+ Die genannten Schwächen von SNMP werden vermieden.
- CMIP ist ein sehr komplexes Protokoll, dessen gesamte Leistungsfähigkeit jedoch nur selten benötigt und genutzt werden kann. Eine entsprechende Konfiguration des Protokolls ist aufgrund der vielen möglichen Einstellungen nur schwer möglich und erfordert ein erhebliches Know-how des Administrators.
- CMIP benötigt ungefähr zehnmal soviel Systemressourcen wie SNMP. Deshalb muss eine leistungsfähige Hardware verwendet werden, die nur in wenigen aktiven Netzkomponenten vorhanden ist. Außerdem ist im allgemeinen eine Implementation des OSI-Protokollstapels notwendig, der zusätzliche Ressourcen verbraucht. Eine Ausnahme bildet hier CMOT.
- Aufgrund der Komplexität des Protokolls und der dementsprechenden Implementationen ist CMIP potentiell fehleranfälliger als SNMP-Implementationen.
- Von CMIP existieren derzeit nur wenig verfügbare Implementationen und es wird in der Praxis, abgesehen vom Telekommunikationsbereich, kaum eingesetzt.

Im konkreten Fall muss detailliert geprüft werden, welches Netzmanagement-Protokoll das für den jeweiligen Verwendungszweck geeignete darstellt. Dazu müssen die Sicherheitsanforderungen an das Netzmanagement formuliert und abgestimmt sein. Wird der TCP/IP-Protokollstapel bereits im lokalen Netz verwendet und sind die Sicherheitsanforderungen gering, bietet sich SNMPv1 als Lösung an. Dennoch können höhere Sicherheitsanforderungen auch hier für den Einsatz von SNMPv2 oder CMIP sprechen. Beim Einsatz von CMIP muss dann erwogen werden, auf welchem Protokollstapel CMIP implementiert werden soll. Entweder auf dem OSI-Stapel (CMIP) oder auf dem TCP/IP-Stapel (CMOT).

Zu bedenken ist auch, dass CMIP bzw. CMOT derzeit nicht von allen aktiven Netzkomponenten und Netzmanagement-Systemen unterstützt wird. Vor dem Einsatz von CMIP ist also sorgfältig zu untersuchen, ob die eingesetzten Komponenten und Clients CMIP-fähig sind.

Ergänzende Kontrollfragen:

- Wurden die Sicherheitsanforderungen an das Netzmanagement formuliert und dokumentiert?
- Wurde die Kompatibilität der aktiven Netzkomponenten und der Clients bzgl. der ausgewählten SNMP-Version bzw. zu CMIP überprüft?
- Wurden die voreingestellten SNMP Communities ersetzt?

M 2.145 Anforderungen an ein Netzmanagement-Tool

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um ein effektives Netzmanagement durchführen zu können, ist der Einsatz eines Netzmanagement-Tools hilfreich. Derzeit stellt der Markt eine Vielzahl von Produkten für das Netzmanagement zur Verfügung, die alle hinsichtlich der eigenen individuellen Anforderungen geprüft werden müssen, bevor eine Entscheidung zur Beschaffung eines konkreten Tools gefällt werden kann. Dabei gilt es vor allem, die Sicherheitsanforderungen nach M 2.143 *Entwicklung eines Netzmanagementkonzeptes* zu erfüllen und die folgenden Punkte zu beachten:

- Es muss das ausgewählte Netzmanagement-Protokoll unterstützen (siehe M 2.144 *Geeignete Auswahl eines Netzmanagement-Protokolls*).
- Das Produkt muss skalierbar sein, d. h. es muss an zukünftige Anforderungen angepasst werden können.
- Es muss alle im lokalen Netz vorhandenen Netzkomponenten unterstützen.
- Es muss alle im lokalen Netz eingesetzten Netzprotokolle unterstützen.
- Es sollte modular aufgebaut sein, um auch später weitere Funktionen ohne großen Aufwand in das bestehende Netzmanagement-System integrieren zu können.
- Es sollte eine grafische Oberfläche (Graphical User Interface, GUI) besitzen, um die relevanten Informationen übersichtlich und verständlich darstellen zu können.
- Werden außerdem Produkte zum Systemmanagement eingesetzt, sollte im Sinne eines "single point of administration" eine Integration mit dem Netzmanagement unter einer Oberfläche möglich sein.

Neben diesen allgemein zu prüfenden Anforderungen sind zusätzlich die funktionalen Anforderungen an ein Netzmanagementsystem zu definieren. Die folgenden Kriterien stellen dazu eine Übersicht über die Möglichkeiten in aktuell verfügbaren Produkten dar, nicht alle Funktionen sind jedoch in allen Produkten realisiert. Vor einer Produktentscheidung muss deshalb festgelegt werden, welche Funktionen notwendig sind und welche nicht benötigt werden:

- topologische Darstellung des Netzes (z. B. auch die Möglichkeit der Einbindung von Hintergrundgrafiken wie Baupläne usw.),
- wählbare Darstellungsform der Topologie,
- topographische Darstellung des Netzes (z. B. auch die Möglichkeit der Einbindung von Hintergrundgrafiken wie Baupläne usw.),
- automatisches Erkennen und Abbilden der Netztopologie und Segmentierung (Auto-Discovery),
- Anzeige der Konfiguration der aktiven Netzkomponenten auf Portebene,

- Anzeige der Performance auf Portebene,
- graphische Visualisierung der aktiven Netzkomponenten,
- interaktives Tool für das Managementprotokoll (z. B. MIB-Browser),
- einfache Navigation im Netzmanagement-Tool, z. B. durch Zoomfunktionen oder durch Ausschnittsvergrößerungen,
- eventuell Integration eines VLAN-Managers und graphische Darstellung der VLANs,
- intuitive Bedienbarkeit der Tool-Oberfläche, insbesondere desjenigen Teils, in dem die topologischen bzw. topographischen Abbildungen editiert werden (beispielsweise durch "Drag & Drop"),
- Darstellung der Fehler- und Alarmmeldungen durch frei definierbare Farben und nach selbst zu definierenden Kriterien,
- Möglichkeit eines verteilten Managements (Client/Server und Manager-of-Manager) und
- Möglichkeit der Integration und Definition weiterer MIBs (Private-MIBs).

Ergänzende Kontrollfragen:

- Wurden alle Anforderungen an ein Netzmanagement-Tool formuliert und dokumentiert?
- Kann mit dem Netzmanagement-Tool das Netzmanagement-Konzept umgesetzt werden?

M 2.146 Sicherer Betrieb eines Netzmanagementsystems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Für den sicheren Betrieb eines Netzmanagement-Tools oder eines komplexen Netzmanagementsystems, welches beispielsweise aus mehreren verschiedenen Netzmanagement-Tools zusammengesetzt sein kann, ist die sichere Konfiguration aller beteiligten Komponenten zu überprüfen und sicherzustellen. Hierzu gehören die Betriebssysteme, auf denen das oder die Netzmanagementsystem/e betrieben werden, die zumeist notwendigen externen Datenbanken für ein Netzmanagementsystem, das verwendete Protokoll (siehe M 2.144 *Geeignete Auswahl eines Netzmanagement-Protokolls*) und die aktiven Netzkomponenten selbst. Vor dem Betrieb eines Netzmanagementsystems muss die Ermittlung der Anforderungen an den Betrieb und die Erstellung eines Netzmanagement-Konzeptes stehen (siehe M 2.143 *Entwicklung eines Netzmanagementkonzeptes*).

Insbesondere sind folgende Punkte zu beachten:

- Um ein Mitlesen oder Verändern der Netzmanagement-Informationen zu verhindern, muss der Rechner, auf dem die Netzmanagement-Konsole betrieben wird, geeignet geschützt werden. Dazu zählen beispielsweise die Aufstellung in einem besonders geschützten Raum, der Einsatz von Bildschirmsperren, Passwortschutz für die Netzmanagement-Konsole und weitere Sicherheitsmechanismen des zugrunde liegenden Betriebssystems.
- Die Maßnahme M 2.144 *Geeignete Auswahl eines Netzmanagement-Protokolls* ist vor dem Hintergrund des sicheren Betriebes zu berücksichtigen. Insbesondere ist durch eine geeignete Konfiguration der aktiven Netzkomponenten auf der Basis des verwendeten Protokolls ein Auslesen der MIBs und anderer Informationen durch unautorisierte Personen zu verhindern (siehe M 4.80 *Sichere Zugriffsmechanismen bei Fernadministration* und M 4.82 *Sichere Konfiguration der aktiven Netzkomponenten*).
- Werden Netzmanagement-Funktionen dezentral nach dem Client/Server-Modell oder durch Benutzung der X-Windows-Technologie durchgeführt, muss für diese ebenfalls der sichere Betrieb gewährleistet werden.
- Es müssen in regelmäßigen Abständen Integritätstests der eingesetzten Software durchgeführt werden, um unautorisierte Änderungen frühzeitig zu erkennen.
- Das Netzmanagement-System muss auf sein Verhalten bei einem Systemabsturz getestet werden. Insbesondere sollte ein automatischer Neustart möglich sein, um die Zeitspanne, in der das lokale Netz nicht überwacht wird, so gering wie möglich zu halten. Die Netzmanagement-Datenbank darf durch einen Systemabsturz nicht beschädigt werden und muss nach einem Neustart wieder verfügbar sein, da die darin enthaltenen Konfigurationsdaten wesentlich für den Betrieb des Netzmanagementsystems sind. Diese Daten müssen daher besonders gesichert werden, damit sie einerseits

noch verfügbar sind und andererseits keine alten oder fehlerhaften Konfigurationsdaten bei einem Neustart benutzt werden, der ggf. durch einen Angreifer aus diesem Grunde provoziert wurde. Für den Schutz der eingesetzten Datenbank ist unter Umständen auch der Baustein 9.2 Datenbanken zu beachten.

- Beim Wiedereinspielen von gesicherten Datenbeständen muss darauf geachtet werden, dass für den sicheren Betrieb des Netzmanagement-Systems relevante Dateien wie Konfigurationsdaten, Passwortdateien und auch die Metakonfigurationsdateien für die eigentlichen Netzkomponenten auf dem aktuellsten Stand sind.

  Für den sicheren Betrieb eines Netzmanagement-Systems sind folgende Daten relevant:

  - Konfigurationsdaten des Netzmanagementsystems, die sich in entsprechend geschützten Verzeichnissen befinden müssen.
  - Konfigurationsdaten der Netzkomponenten (Metakonfigurationsdateien), die sich ebenfalls in entsprechend geschützten Verzeichnissen befinden müssen.
  - Passwortdateien für das Netzmanagementsystem. Hierbei ist beispielsweise auf die Güte des Passworts und die Möglichkeit einer verschlüsselten Speicherung des Passworts zu achten (siehe M 2.11 *Regelung des Passwortgebrauchs*).

- Eine Administration der aktiven Netzkomponenten über das Netz sollte dann eingeschränkt werden und eine Administration über die lokalen Schnittstellen erfolgen, wenn die Erfüllung der Anforderungen an Vertraulichkeit und Integrität der Netzmanagement-Informationen nicht gewährleistet werden kann. In diesem Fall ist auf ein zentrales Netzmanagement zu verzichten.

Ergänzende Kontrollfragen:

- Wurde eine Regelung des Passwortgebrauchs für das Netzmanagementsystems bzw. -tool erstellt?
- Unterstützt das Netzmanagementsystem die erforderlichen Sicherheitsmaßnahmen?

M 2.147 Sichere Migration von Novell Netware 3.x Servern in Novell Netware 4.x Netze

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Unter Novell Netware 3.x verwaltet jeder Server die Informationen über seine Benutzer in der so genannten Bindery. Dies hat den Nachteil, dass in einem Netz mit mehreren Netware 3.x Servern jeder Benutzer-Account auf jedem Server, auf den der Benutzer zugreifen will, separat angelegt werden muss. Für den Administrator ist dieses mehrfache Anlegen von Benutzern-Accounts ein enormer zusätzlicher Aufwand, der prinzipiell nicht zu verhindern ist. Darüber hinaus muss sich der Benutzer auf jedem Server einzeln anmelden.

In einem Netz mit mehreren Novell Netware 4.x Servern, die in einem NDS-Baum installiert sind, meldet sich der Benutzer dagegen nur einmal am Netz an und kann sofort alle ihm zugewiesenen Ressourcen benutzen (siehe M 2.151 *Entwurf eines NDS-Konzeptes*).

Eine direkte Integration von Netware 3.x Servern in ein Netware 4.x Netz ist nicht möglich, da diese weiterhin als eigenständige Systeme arbeiten. Benutzer, die sowohl auf Netware 4.x als auch auf Netware 3.x zugreifen wollen, müssten bei dieser Konstellation weiterhin mehrfach angelegt werden.

Eine sinnvolle Alternative ist dagegen die Migration eines Netware 3.x Servers in einen NDS-Baum. Dazu kann das von Novell bei Netware 4.x mitgelieferte Produkt *NETSYNC.NLM* verwendet werden. Der Betrieb eines Netware 3.x Servers in einem Netware 4.x Netz hat den Vorteil, dass die Benutzer-Accounts zentral auf einem Netware 4.x Server administriert werden können und nicht mehr auf jedem Netware 3.x Server einzeln gepflegt werden müssen.

Hierfür muss ein Netware 4.x Server vorhanden sein, der bis zu 12 Netware 3.x Server verwalten kann. Dieser wird als Host bezeichnet und muss für die weitere Administration der Benutzer-Accounts verwendet werden, da er die Änderungen der NDS in die Bindery der Netware 3.x Server überträgt. Bei einer Migration wird ein Großteil der NLMs der Netware 3.x Server ersetzt und diese dann mit einem Host verbunden. Eine eventuell gewünschte Wiederherstellung eines eigenständigen Netware 3.x Servers ist somit mit einem erheblichen Aufwand verbunden.

Folgende Punkte müssen für eine sichere Migration beachtet werden:

- Der Bindery Kontext muss für den Behälter, in dem der Netware 3.x Server erstellt werden soll, gesetzt werden.
- Die Bindery Emulation muss auf dem Netware 4.x Host in der Datei *AUTOEXEC.NCF* mit dem Befehl *SET BINDERY CONTEXT* = ... eingetragen und damit aktiviert werden.
- Nach der Migration dürfen Änderungen nicht mehr mit dem Utility *SYS:PUBLIC\SYSCON.EXE* durchgeführt werden. Andere Utilities, wie z. B. *SYS:PUBLIC\FILER.EXE* oder *SYS:PUBLIC\PCONSOLE.EXE*, wer-

den im Rahmen der Migration durch *NETSYNC.NLM* ersetzt. Es wird jedoch empfohlen, für Administrationszwecke ausschließlich das Programm *SYS:PUBLIC\NWADMIN.EXE* zu benutzen. Das Utility *SYS:PUBLIC\SYSCON.EXE* sollte daher entfernt werden.

- Falls mehrere Netware 3.x Server in den gleichen Container migriert werden sollen oder auch mehrere Bindery Emulations aktiviert sind, müssen die entsprechenden Objekte zuvor auf Namenskonflikte überprüft werden, da sie nicht mehrfach mit dem selben Namen vorhanden sein dürfen.

M 2.148 Sichere Einrichtung von Novell Netware 4.x Netzen

Verantwortlich für Initiierung: Leiter IT, Leiter IT

Verantwortlich für Umsetzung: Administrator

Eine sichere Einrichtung eines Novell Netware 4.x Netzes beinhaltet die beiden Schritte

- Installation der zugehörigen Software und
- Einrichtung der Netzumgebung.

Installation der zugehörigen Software

Um eine sichere Installation der Novell Netware 4.x Software zu gewährleisten, muss vor der Installation das Handbuch *Installation* für Novell Netware 4.x durchgearbeitet werden. Folgende Punkte sind unbedingt zu beachten:

- Anforderungen an die Hardware: vor der Installation ist zu überprüfen, ob die vorgesehene Hardware alle Anforderungen (z. B. Massenspeicher- und Hauptspeicherbedarf) erfüllt,
- vorgezogene Funktionsüberprüfung aller Hardware-Komponenten unter MS-DOS, bevor die Hardware in einer komplexen Umgebung wie z. B. einem Multiprotokollrouter eingesetzt wird,
- Dokumentation der Hardware-Konfiguration (siehe M 2.153 *Dokumentation von Novell Netware 4.x Netzen*),
- Planung der NDS (siehe M 2.151 *Entwurf eines NDS-Konzeptes*).

Alle anderen wesentlichen Schritte zur Installation der Novell Netware 4.x Software können den entsprechenden Handbüchern *Installation* und *Handbuch zu Netware 4 Netzwerken* entnommen werden.

Anforderungen an die Verfügbarkeit

Zur Erhöhung der Verfügbarkeit von Novell Netware Servern bzw. der gespeicherten Daten stellt das Netzbetriebssystem hierarchische Fehlertolerierungsstufen zur Verfügung, die nachfolgend kurz aufgezeigt werden. Jede der hier aufgezeigten Fehlertolerierungsstufen beinhaltet dabei die Funktionalitäten der vorherigen Stufe.

- **Hot Fix I und Hot Fix II**

  Novell Netware 4.x unterstützt standardmäßig den sog. Hot Fix. Hierbei werden Datenverluste aufgrund physikalischer Festplattenfehler verhindert. Dabei wird zwischen Hot Fix I und II unterschieden. Bei Hot Fix I wird nach einem Schreibzugriff auf eine Datei ein Vergleich zwischen den veränderten Daten auf der Festplatte mit den Originaldaten veranlasst, die sich noch im Arbeitsspeicher des Novell Netware Servers befinden. Ist dieses Ergebnis fehlerhaft, so wird der entsprechende Sektor der Festplatte als defekt markiert und für zukünftige Zugriffe gesperrt.

Weiterhin werden die Daten des Arbeitsspeichers im Anschluss an den zuvor beschriebenen Fehlerfall in den so genannten "Hot Fix Bereich" der Festplatte umgeleitet.

Seit Netware 4.11 ist diese Funktionalität allerdings standardmäßig deaktiviert. Der dafür verantwortliche SET-Parameter des Netware Servers lautet *Enable Disk Read After Write Verify* und ist bei Netware 4.11 auf *OFF* gesetzt. Um die Funktion Hot Fix I zu aktivieren, muss dieser Parameter auf *ON* stehen.

Hot Fix II hingegen funktioniert auch in der Standardeinstellung von Netware 4.11. Hot Fix II stellt eine ähnliche Fehlertoleranz wie Hot Fix I zur Verfügung, dies jedoch nur bei gespiegelten und geduplexten Platten. Im Gegensatz zu Hot Fix I können hier auch Fehler erst beim Lesen korrigiert werden, da die Information redundant vorhanden ist. Werden beim Lesen Probleme erkannt, wird der Sektor der Platte als defekt markiert und ersatzweise auf einen Sektor aus dem Hot Fix Bereich zurückgegriffen. In diesem Fall werden dann die intakten Informationen der gespiegelten oder geduplexten Platte gelesen und der defekte Sektor mit der Information der Ersatzfestplatte für diesen Bereich automatisch ergänzt.

Da heutige Platten eine sehr hohe Eigenintelligenz besitzen und ähnlich Mechanismen intern zur Verfügung stehen, sind Hot Fix I und II heutzutage von geringerer Bedeutung. Sollten trotz moderner Platten Sektoren im Hot Fix Bereich belegt sein, ist ein sehr schneller Plattentausch notwendig.

Der Hot Fix Bereich kann beim Erstellen einer Netware Partition konfiguriert werden. Novell Netware schlägt eine Größe für den Hot Fix Bereich vor, die sich an der Größe der Netware Partition orientiert und bei wachsenden Partitionen prozentual abnimmt.

- **Disk Mirroring**

  Beim Disk Mirroring sollten an einen Festplattencontroller des Servers zwei identische Festplatten angeschlossen werden. Es lassen sich allerdings auch nicht identische Platten spiegeln. Einzige Voraussetzung ist, dass die Datenbereiche der beiden Netware Partitionen der zu spiegelnden Platten gleich groß sind. Die zu speichernden Daten werden gleichzeitig auf beiden Festplatten gespeichert. Fällt eine der Festplatten durch einen Fehler aus, wird ohne Ausfallzeit und Datenverlust mit der zweiten Festplatte weitergearbeitet.

- **Disk Duplexing**

  Beim Disk Duplexing werden zwei Festplatten und zwei Festplattencontroller von gleicher Art bzw. Größe im File Server installiert. Disk Duplexing gewährleistet somit eine Fortführung des Betriebes nicht nur beim Ausfall einer Festplatte, sondern auch beim Ausfall eines Festplattencontrollers. Zusätzlich sollte beim Disk Duplexing auch das Netzteil der Festplatten redundant vorhanden sein, was sich meist nur mit externen Platten-Systemen realisieren lässt.

- **Serverspiegelung (System Fault Tolerance III)**

  Eine Serverspiegelung in der sog. SFT-III-Konfiguration stellt die höchste Stufe der Toleranz gegen im Betrieb auftretende Hardware-Fehler dar. Zwei identische Novell Netware 4.x Server arbeiten hierbei gleichzeitig und "parallel" im Netz. Zu beachten ist dabei jedoch, dass der Secondary Server nur Standby zur Verfügung steht und nur beim Ausfall des Primary Servers die Arbeit im Netz übernimmt.

  Die beiden Novell Netware Server sind hierbei durch ein eigenes Hochgeschwindigkeitsnetz miteinander verbunden. Fällt hierbei der Primär-Server aus, werden dessen Aufgaben von dem Sekundär-Server im Netz übernommen.

  Die Entscheidung, ob zusätzlich zum sog. Hot Fix weitere Maßnahmen (Disk Mirroring, Disk Duplexing, SFTIII) ergriffen werden müssen, ist abhängig vom angestrebten Grad der Verfügbarkeit des Netzes.

- **Notstromversorgung**

  Durch den Einsatz einer Notstromversorgung (USV=Unterbrechungsfreie Stromversorgung bzw. im englischen UPS=Uninterruptible Power Supply) können die Folgen eines plötzlichen Stromausfalles abgefangen werden. Novell Netware unterstützt den Einsatz geeigneter Geräte durch das sogenannte UPS-Monitoring. Im Falle eines plötzlichen Stromausfalles wird der Server am Ende der Überbrückungszeit der USV geregelt heruntergefahren, d. h. die sich im Cache des Servers befindlichen Daten werden auf die Festplatten übertragen, Verbindungen zum Server ordnungsgemäß beendet sowie die Serverprozesse geregelt abgeschlossen.

Einrichtung der Netzumgebung

Novell Netware 4.x bietet ein eigenes Sicherheitssystem zum Schutz des Netzes und seiner Ressourcen. Die zugehörigen Funktionen müssen jedoch vom Administrator während der Einrichtung eines Netware 4.x Netzes manuell aktiviert werden, so dass die Sicherheit eines Netzes in nicht unerheblichem Maße in der Verantwortung des Administrators liegt.

Das wesentliche Hilfsmittel zur Verwaltung und Absicherung eines Netware 4.x Netzes ist der Novell Netware Administrator. Dieses Programm gibt es in folgenden Ausführungen:

- SYS:PUBLIC\NWADMIN.EXE für Windows 3.11,
- SYS:PUBLIC\WIN95\ NWADMN95.EXE für Windows 95,
- *SYS:PUBLIC\WINNT\NWADMNNT.EXE* für Windows NT sowie die neuere Version
- *SYS:PUBLIC\WIN32\NWADMN32.EXE* für Windows NT und Windows 95.

Das Programm Netware Administrator ermöglicht eine Vielzahl von Einstellungen, wie z. B. die Festlegung einer minimalen Passwortlänge oder der maximalen Anzahl gleichzeitiger Verbindungen eines Benutzers. Nachfolgend werden die sicherheitsrelevanten Funktionen des Netware Administrators auf-

geführt und erläutert. Dazu sind die jeweiligen Parameter und ihre Werte angegeben, die für einen sicheren Betrieb eines Netware 4.x Netzes eingestellt werden müssen.

Ein wesentlicher Punkt bei der sicheren Einrichtung von Netware 4.x Netzen ist das Anlegen von Benutzer-Accounts. Zu diesem Zweck sollten Schablonen (Templates) für Standard-Benutzer des jeweiligen Kontextes angelegt werden. Beim Einrichten konkreter Benutzer-Accounts werden dann die in der Schablone eingestellten Werte übernommen, was den entsprechenden Aufwand stark reduziert. Dazu muss die Option **SCHABLONE BENUTZEN** bzw. **USE TEMPLATE** verwendet werden. Folgende Funktionen sollten in einer Schablone eingestellt werden:

Login Restrictions

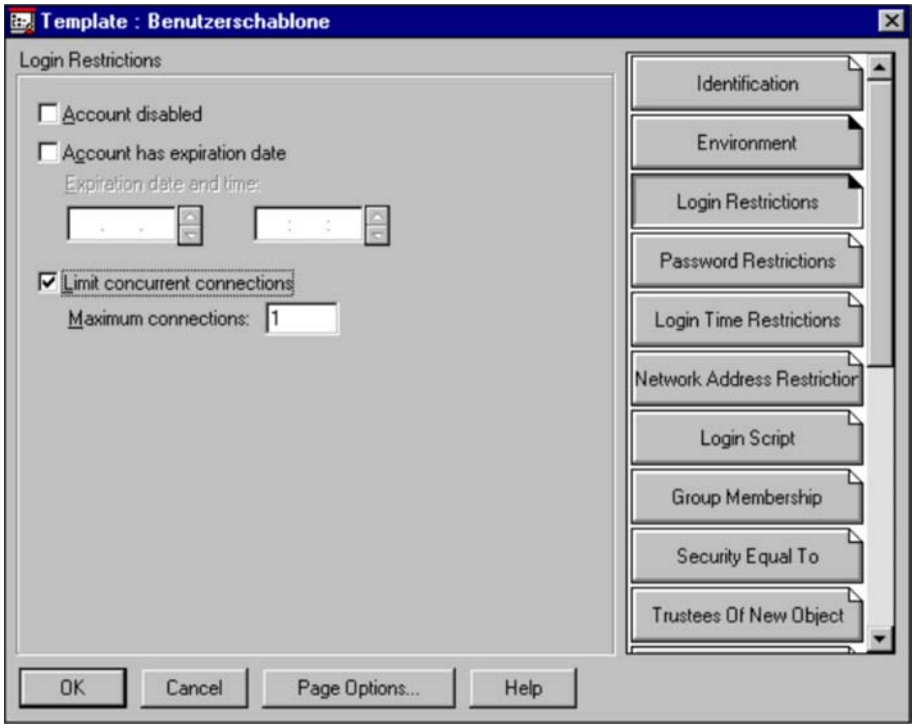


Abbildung: Netware Administrator Menü "Template: Benutzerschablone/Login Restrictions"

- **Limit Concurrent Connections**

  Hierdurch kann die Anzahl der gleichzeitigen Verbindungen eines Benutzer-Accounts zu den Netware Servern limitiert werden. Im Regelfall sollte hierbei der Wert "1" gewählt werden, um nicht unnötig Verbindungslizenzen zu verbrauchen.

Password Restrictions

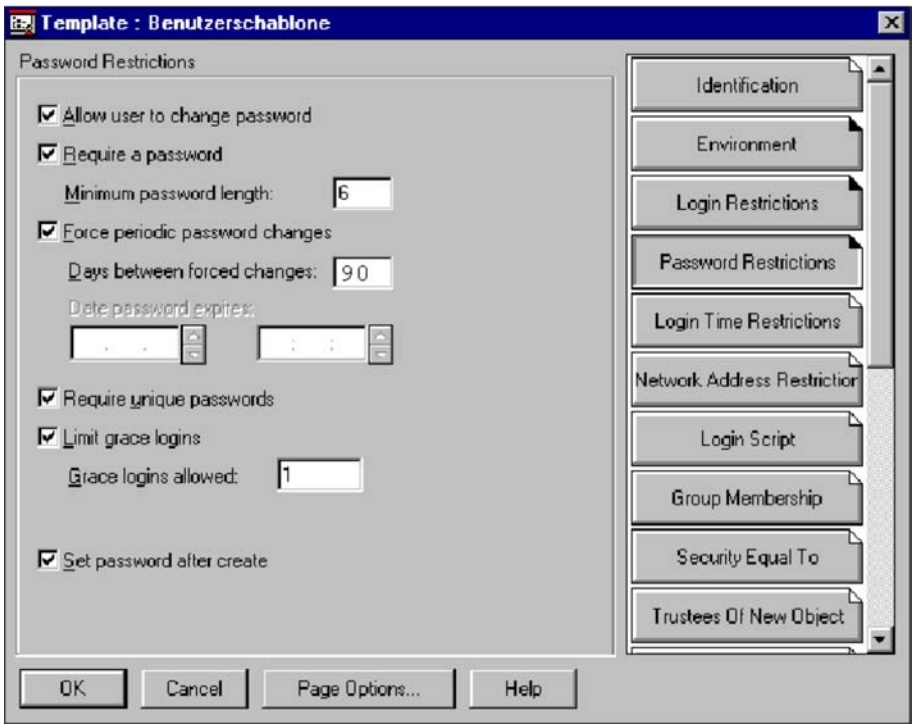


Abbildung: Netware Administrator Menü "Template: Benutzerschablone/Password Restrictions"

- **Allow user to change password**

  Diese Option muss aktiviert werden, damit ein Benutzer sein Passwort wechseln kann. Ist sie nicht aktiviert, können keine weiteren Möglichkeiten angewählt werden.

- **Require Password**

  Diese Option installiert die Passwortabfrage für jeden Benutzer und bietet die Möglichkeit, die nachfolgenden Passwortregeln zu definieren. Require Password sollte immer aktiviert werden.

- **Minimum Password Length**

  Hiermit wird die erforderliche Mindestlänge eines Passwortes eingestellt. Sie sollte mindestens sechs Zeichen betragen (vergleiche M 2.11 *Regelung des Passwortgebrauchs* M 2.11 *Regelung des Passwortgebrauchs*).

- **Force Periodic Password Changes**

  Durch die Aktivierung dieser Option wird festgelegt, dass die Benutzer ihre Passwörter regelmäßig ändern müssen. Dies sollte der Regelfall sein.

- **Days Between Password Changes**

  Unter diesem Menüpunkt wird die allgemeine Gültigkeitsdauer von Passwörtern festgelegt. Diese muss für das jeweilige System individuell festgelegt werden (vergleiche M 2.11 *Regelung des Passwortgebrauchs*).

- **Require Unique Passwords**

  Die Aktivierung der Passworthistorie (Require Unique Passwords) hat zur Folge, dass die letzten neun Passwörter eines Benutzer-Accounts mit dem neu eingegebenen Passwort verglichen werden und bei einer festgestellten Übereinstimmung das neue Passwort durch den Netware Server zurückgewiesen wird. Damit wird gewährleistet, dass nicht immer dieselben Passwörter verwendet werden können. Diese Option sollte immer aktiviert werden.

- **Limit Grace Logins**

  Grace Logins sind diejenigen Logins, die trotz Ablauf der Gültigkeitsdauer eines Passwortes noch erfolgen dürfen. Die Anzahl der Grace Logins sollte durch die Aktivierung dieser Option grundsätzlich limitiert werden.

- **Grace Logins Allowed**

  Die Anzahl der erlaubten Grace Logins sollte auf den Wert "Eins" eingestellt werden, damit ein Benutzer, dessen Passwort ungültig geworden ist, dieses sofort ändern muss.

- **Set password after create**

  Diese Option sollte immer aktiviert sein. Durch sie wird der Administrator bei der Erstellung eines neuen Benutzers-Accounts automatisch aufgefordert, ein Passwort einzugeben. Dies verhindert somit, dass temporär frei zugängliche Benutzer-Accounts angelegt werden können.

Login Time Restrictions

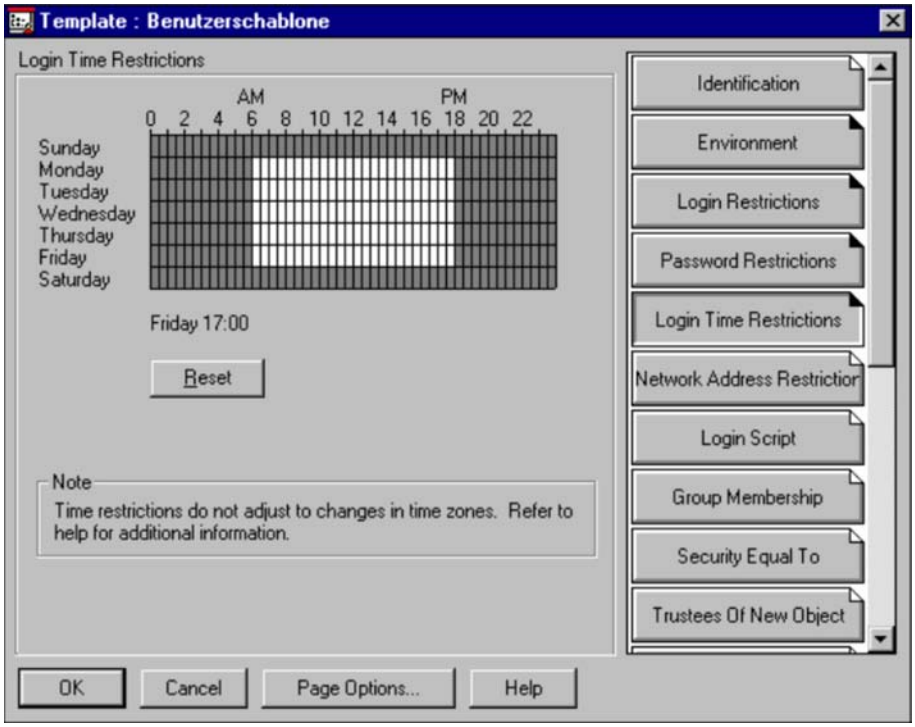


Abbildung: Netware Administrator Menü "Template: Benutzerschablone/Login Time Restrictions"

- **Default Time Restrictions**

  Mit Hilfe der Schablone Login Time Restrictions werden die erlaubten Arbeitszeiten für Benutzer-Accounts in einem Netware 4.x Netz definiert. Außerhalb der hier festgelegten Zeiten ist es keinem Benutzer möglich, sich am Netware 4.x Netz anzumelden.

  Nachträgliche Änderungen der Default Time Restrictions bei der Einrichtung bzw. Pflege von Benutzer-Accounts haben keinerlei Auswirkungen auf die erlaubten Zugangszeiten bereits existierender Benutzer. Abweichende Zugangszeiten für einzelne Benutzer können mit Hilfe von *SYS:\PUBLIC\NWADMIN.EXE* (Objects / Details on multiple Users) geändert werden.

Weiterhin können für einzelne Behälterobjekte der NDS die folgenden Sicherheitsmechanismen eingestellt werden:

Intruder Detection

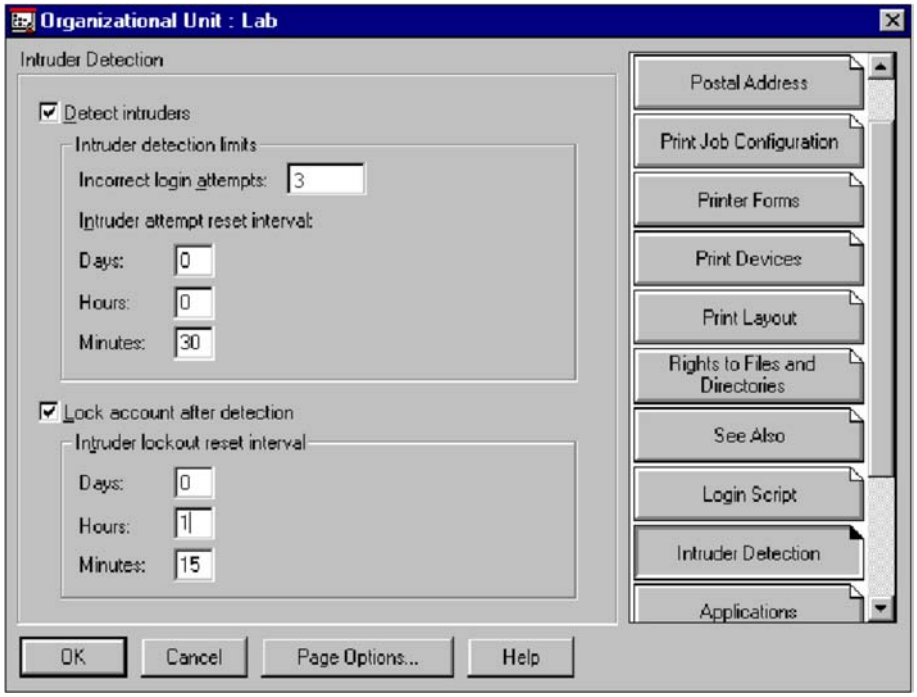


Abbildung: Netware Administrator Menü "Organizational Unit : Lab/Intruder Detection"

- **Detect Intruders**

  Durch die Aktivierung dieser Option werden unautorisierte Login-Versuche erkannt und die hiervon betroffenen Benutzer-Accounts gegebenenfalls gesperrt. Dadurch wird einer "Brute Force Attacke" unter Novell Netware 4.x vorgebeugt. Diese Einstellung muss mit dem Programm Netware Administrator für jeden Container durchgeführt werden.

- **Incorrect Login Attempts**

  Dies gibt die maximale Anzahl der zulässigen Login-Fehlversuche an; üblicherweise sollte hierbei der Wert "Drei" eingestellt werden.

- **Intruder Attempt Reset Interval**

  Damit kann die zeitliche Zurückverfolgung von fehlgeschlagenen Login-Versuchen eines Benutzer-Accounts aktiviert werden. Übersteigt die Anzahl der Login-Fehlversuche eines Benutzer-Accounts innerhalb des definierten Zeitraumes den unter Incorrect Login Attempts eingestellten Wert, so wird der Benutzer-Account gesperrt (falls die Option Lock Account After Detection aktiviert ist).

- **Lock Account After Detection**

  Dieser Menüpunkt sollte immer aktiviert werden, um einen Benutzer-Account, der die maximale Anzahl der ungültigen Login-Versuche überschritten hat, zu sperren.

- **Intruder Lockout Reset Interval**

  Dieser Zeitwert sollte keinesfalls zu gering gewählt werden (> 1 Stunde), um sicherzustellen, dass die Ursache für einen Intruder Lockout (d. h. Sperren des Benutzer-Accounts) durch die Systemadministration und den betroffenen Benutzer aufgeklärt werden kann.

Ergänzende Kontrollfragen:

- Sind die Benutzer über den korrekten Umgang mit Passwörtern unterrichtet worden?
- Wird die Passwort-Güte kontrolliert?
- Wird der Passwort-Wechsel erzwungen?
- Ist jeder Benutzer im Netz mit einem Passwort ausgestattet?
- Wurde eine Benutzerschablone erzeugt? Wurde dabei auf die Sicherheitsaspekte geachtet?

M 2.149 Sicherer Betrieb von Novell Netware 4.x Netzen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Für den sicheren Betrieb eines Novell Netware 4.x Netzes müssen die nachfolgend beschriebenen Punkte umgesetzt werden.

Vergabe von Zugriffsrechten auf Verzeichnisse, Dateien, NDS-Objekte und NDS-Objekteigenschaften

Durch die Vergabe von Zugriffsrechten (Trustee Assignments) auf NDS-Objekte, NDS-Objekteigenschaften, Verzeichnisse und Dateien im Novell Netware 4.x Netz kann die Sicherheit eines Novell Netware 4.x Netzes und seiner Daten gewährleistet werden. Wenn NDS-Objekten, z. B. Benutzern und Gruppen, verschiedene Rechte auf andere NDS-Objekte, NDS-Objekteigenschaften, Dateien oder Verzeichnisse gewährt werden, so spricht man von einem Trustee (Treuhänder oder Bevollmächtigten).

In Netware 4.11 existieren dazu drei Arten von Zugriffsrechten, die ersten beiden beziehen sich auf die NDS-Objekt- und NDS-Objekteigenschaftsrechte, das letzte auf Dateien bzw. Verzeichnisse.

- **Objektrechte**

Abbildung 1: Netware Administrator Container *zenk_gmbh* "Trustee of this Object..."

Objektrechte steuern die Zugriffsmöglichkeiten eines Trustees auf ein Objekt, also z. B. auf Benutzer, Gruppen, Drucker oder Netware Server. Folgende Objektrechte, wie dies auch in der obigen Abbildung zu entnehmen ist, stehen zur Verfügung:

- Supervisor
- Browse
- Create (nur bei Containern)
- Delete
- Rename

Ein Benutzer mit diesen Rechten auf ein anderes NDS-Objekt, z. B. einen anderen Benutzer, kann der Reihe nach Benutzer-Accounts sehen, erstellen, löschen bzw. umbenennen. Das Supervisor-Recht ist die Summe der vier anderen Rechte. Mit den Rechten *Browse*, *Create*, *Delete* und *Rename* erhält man keinerlei Objekteigenschaftsrechte bzw. Dateirechte. Ausnahme hiervon ist in diesem speziellen Fall das Supervisor-Recht auf ein Objekt. Mit diesem Recht erhält man auch Supervisor-Rechte auf die Objekteigenschaften.

- **Objekteigenschaftsrechte**

Objekteigenschaftsrechte steuern den Zugriff eines Trustees auf die über ein Objekt gespeicherten Informationen, also auf die Eigenschaften des betreffenden Objekts. Hierzu sind keinerlei Objektrechte notwendig. Mit Ausnahme des Objektrechts *Supervisor* kann man mit Objektrechten auch keinerlei Rechte auf Objekteigenschaften erlangen. Es gibt folgende Objekteigenschaftsrechte, die wieder in obiger Abbildung erkennbar sind:

- Supervisor
- Compare
- Read
- Write
- Add Self

Die Objekteigenschaftsrechte setzen sich aus den Hauptrechten *Schreiben (Write)* und *Lesen (Read)* zusammen. Im Recht *Lesen* ist das Recht *Vergleichen (Compare)* und im Recht *Schreiben* ist das Recht *Selbst Hinzufügen (Add Self)* enthalten. Das Supervisor-Recht ist hier die Summe dieser vier Rechte und hat keinerlei weitere Auswirkungen. Mit dem Recht *Lesen* können Objekteigenschaften wie z. B. die Eigenschaften des Benutzers *Nachname* oder auch *Login Script* gelesen werden. Zum Abändern benötigt man das Recht *Schreiben*. Das Recht *Vergleichen* erlaubt es, Anfragen an die NDS abzusetzen, z. B. ob der Nachname des Benutzers *XY* gleich *Mustermann* ist. Die Antwort lautet dann je nach dem "wahr" oder "falsch". Das Recht *Selbst Hinzufügen* macht nur bei Objekten Sinn, bei denen man sich selbst in eine Liste eintragen kann, wie dies z. B. bei einer Gruppe der Fall ist. Da ein Objekt häufig sehr viele Eigenschaften besitzt, gibt es zwei Möglichkeiten, Objekteigenschaften zu vergeben. Es ist prinzipiell möglich, auf alle Eigenschaften dasselbe Recht zu vergeben. Dann muss im Bereich *Property Rights* der Punkt *All Properties* markiert sein. Andererseits ist es auch möglich, auf bestimmte Objekteigenschaften explizit Rechte zu vergeben. Dazu dient die Option *Selected Properties*. Es ist dabei zu beachten, dass mit der Funktion *Selected Properties* die Rechte, die bei der Option *All Properties* vergeben wurden, überschrieben werden.

Rechte in der NDS müssen noch sorgfältiger vergeben werden als Rechte im Dateisystem. Im Dateisystem bekommt ein NDS-Objekt Rechte auf eine Datei oder ein Verzeichnis. In der NDS allerdings bekommt ein NDS-Objekt Rechte auf ein anderes NDS-Objekt. Hierbei muss genau überprüft werden, wer eigentlich auf wen Rechte bekommen soll. So kann es leicht vorkommen, dass ein Benutzer-Objekt Rechte auf ein Container-Objekt bekommen soll, doch letztendlich dem Container-Objekt Rechte auf ein Benutzer-Objekt gegeben werden.

- **Datei- und Verzeichnisrechte**

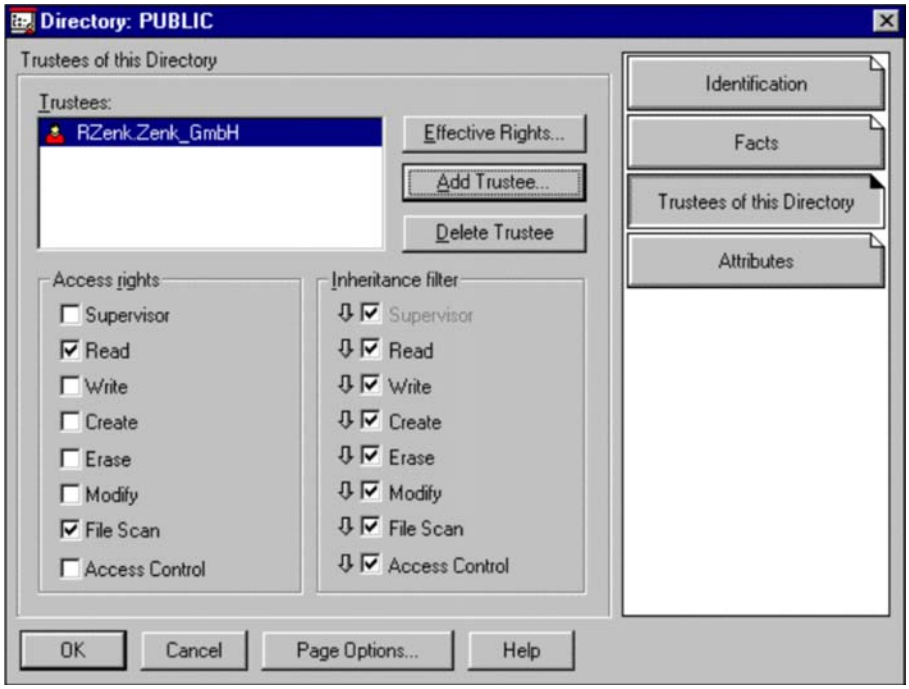


Abbildung 2: Netware Administrator Verzeichnis *PUBLIC* "Details: Trustee of this Directory"

Datei- und Verzeichnisrechte steuern die Operationen, die ein Trustee, hier der User *RZenk*, in einer Datei oder in einem Verzeichnis durchführen kann. Wie Objektrechte unabhängig von Objekteigenschaftsrechten sind, sind wiederum Datei- und Verzeichnisrechte vollkommen unabhängig von den beiden NDS-Rechten. Es gibt folgende Datei- und Verzeichnisrechte:

- Supervisor
- Read
- Write
- Create
- Erase
- Modify
- File Scan
- Access Control

Mit den Rechten *Read*, *Write*, *Create* und *Erase* kann ein Trustee Dateien bzw. Verzeichnisse lesen, verändern, erstellen und löschen. *Modify* dient nicht zum Verändern einer Datei, sondern zum Umbenennen von Dateien und

Verzeichnissen. Weiterhin können mit dem Recht Modify die Datei- und Verzeichnisattribute geändert werden. Mit *File Scan* hat man das Recht, sich Dateien und Verzeichnisse z. B. mit dem Befehl *NDIR* oder auch *DIR* anzusehen. Mit dem Recht *Access Control* können anderen NDS-Objekten Datei- und Verzeichnisrechte, mit Ausnahme des Supervisor-Rechts gewährt werden.

Im Gegensatz zu Objektrechten, wo es das Recht *Create* nur auf Containerebene gibt, kann das *Create* Recht im Dateisystem auch auf Dateien und nicht nur auf Verzeichnisse vergeben werden. Auf Dateien erlaubt dieses Recht, eine logisch gelöschte Datei durch den Mechanismus *Salvage* wieder herzustellen. In der NDS können einmal gelöschte Objekte nicht wieder hergestellt werden, was dazu führt, dass dort das Recht *Create* nur auf Containerebene Sinn macht.

Aus Gründen der Übersichtlichkeit, einer vereinfachten Administration sowie einer verbesserten Revisionsfähigkeit sollte die Vergabe von Zugriffsrechten vorrangig über die Zuweisung von Rechten an Benutzergruppen (Datei- und Verzeichnisrechte) und Container-Objekte erfolgen. Ein Container ist dabei stellvertretend für alle Objekte, insbesondere alle Benutzer-Objekte, die sich unterhalb des Container-Objekts in der NDS befinden. Dabei erhalten diese Rechte wirklich alle Benutzer, nicht nur diejenigen, die sich im Container direkt befinden.

Für NDS-Rechte auf Objekte und Objekteigenschaften gibt es das Objekt Organizational Role (OR). Die OR ist vergleichbar mit einer Gruppe. Gruppen geben das erhaltene Datei- und Verzeichnisrecht an alle ihre Benutzer, die als Mitglieder eingetragen sind, weiter. Mit einer Organizational Role werden die Rechte an die Mitglieder der Organizational Role weitergereicht. Hier heißen die Mitglieder allerdings Occupant, was soviel wie Bewohner heißt. Novell übersetzt dies allerdings als Träger. Sowohl bei Gruppen als auch bei Organizational Roles werden die Rechte auf ihre Mitglieder bzw. Träger mit Hilfe von *Security Equal To* Mechanismen übergeben. Da in der Praxis weit weniger NDS-Rechte als Dateirechte vergeben werden, wird die OR weit weniger häufig benutzt als dies bei Gruppen der Fall ist.

Rechte können auch direkt an Benutzer und über *Security Equal To* vergeben werden. Hier kann aber sehr leicht die Übersichtlichkeit verloren gehen und deshalb sollten diese Mechanismen sehr moderat eingesetzt werden. Zusammenfassend noch einmal die Möglichkeiten, wie Rechte vergeben werden können:

- Gruppen (Datei- und Verzeichnisrechte)
- Organizational Role (NDS-Objekt- und NDS-Objekteigenschaftsrechte)
- Container
- Benutzer
- Security Equal To

Um die versehentliche Freigabe von Verzeichnissen durch einen Benutzer zu verhindern, sollte die Systemadministration Benutzergruppen und Benutzern

in den ihnen zugewiesenen Verzeichnissen und Dateien die Rechte "Supervisor" (S) und "Access Control" (A) nicht erteilen.

Werden ausgewählten Verzeichnissen oder Dateien mit Hilfe von Netware-Attributen bestimmte Eigenschaften, z. B. schreibgeschützte Dateien (Ro), zugewiesen, so sollte beachtet werden, dass Benutzer, die das Zugriffsrecht "Modify" (M) auf die entsprechenden Verzeichnisse und Dateien besitzen, in der Lage sind, diese Attribute zu verändern. Daher sollte der Kreis der Benutzer mit diesem Zugriffsrecht eingeschränkt werden.

Vererbung von Zugriffsrechten in der NDS und im Dateisystem

Alle bereits behandelten Rechte unterliegen ähnlichen Mechanismen. Hierzu gehören wichtige Begriffe wie *Vererbung von Rechten*, *Vererbungsfilter (IRF)*, *Effektive Rechte (ER)* und *Access Control List (ACL)*, die im folgenden erläutert werden.

Vererbung von Rechten

Rechte werden sowohl in der NDS als auch im Dateisystem grundsätzlich vererbt. Dies bedeutet z. B., dass ein Recht, das in der Root, entweder im NDS-Baum oder auch im Dateisystem vergeben wird, sich auf alle Objekte bzw. Verzeichnisse und Dateien, die sich unterhalb der jeweiligen Root befinden, vererbt werden. Vergibt man ein Recht entsprechend tiefer in der Baumstruktur, vererben sich die Rechte ab dieser Stelle im Baum. Hiervon gibt es eine Ausnahme: Rechte, die selektiv auf Objekteigenschaften vergeben werden (*Selected Properies*), vererben sich nicht.

Beispiel 1:

SYS: RZenk [Read; File Scan]
PUBLIC
NWADMIN.EXE
NDIR.EXE

Erhält der User *RZenk* auf das Volume SYS: die Rechte *[Read; File Scan]*, vererben sich diese Rechte hier auch auf das Verzeichnis *PUBLIC* und die Dateien *NWADMIN.EXE* und *NDIR.EXE*, die sich in *PUBLIC* befinden. Vererbung kann aber auch gezielt ausgeschlossen werden. Dazu gibt es die *Inherited Rights Filter (IRF)*, die weiter unten besprochen werden. Im Grundzustand werden keinerlei Rechte gefiltert. Es gibt noch einen zweiten Mechanismus, bei dem die Vererbung ausgeschlossen wird. Erhält das gleiche NDS-Objekt tiefer im Baum noch einmal Rechte zugewiesen, werden dadurch die ursprünglichen Rechte, die dasselbe Objekt weiter oben im Baum bekommen hat, ab diesem Punkt nicht mehr weitervererbt.

Beispiel 2:

SYS: RZenk [Read; File Scan]
PUBLIC
NWADMIN.EXE RZenk [Write]
NDIR.EXE

In Beispiel 2 hat der User *RZenk* auf die Datei *NWADMIN.EXE* nur noch das Recht *[Write],* da die Rechte *[Read; File Scan]* des Benutzers *RZenk* auf die

Datei *NWADMIN.EXE* nicht weitervererbt werden. Alle anderen NDS-Objekte, die eventuell Rechte auf die Datei *NWADMIN.EXE* bekommen haben, sind dadurch nicht betroffen. Auch die Rechte, die der User *RZenk* auf die Datei *NWADMIN.EXE* über andere Mechanismen erhält, wie z. B. Gruppen, Container, etc., werden dadurch nicht eingeschränkt. Diese Rechte sind somit additiv.

Inherited Rights Filter (IRF)

Während Trustee Assignments den Zugriff auf ein Objekt, eine Objekteigenschaft oder eine Datei bzw. ein Verzeichnis gewähren, verhindert ein IRF die Vererbung der Rechte von einem Objekt, einer Objekteigenschaft oder einer Datei bzw. einem Verzeichnis auf andere NDS-Objekte bzw. Dateien und Verzeichnisse im jeweiligen Baum. Jedes Objekt, jede Objekteigenschaft und jede Datei bzw. jedes Verzeichnis in einem NDS Verzeichnis bzw. im Dateisystem kann einen anderen IRF besitzen.

Der einzige Unterschied zwischen NDS und Dateisystem betrifft das Recht Supervisor. Nur in der NDS kann dieses Recht gefiltert werden. Im Dateisystem hingegen kann dieses Recht, einmal vergeben, nicht mehr gefiltert werden.

Effektive Rechte

Die Kombination Inherited Rights Filter, Trustee Assignment und Security Equivalences werden als Effektive Rechte (ER) bezeichnet. Die effektiven Rechte, die ein NDS-Objekt auf andere NDS-Objekte bzw. deren Eigenschaften hat, aber auch die effektiven Rechte die ein NDS-Objekt auf das Dateisystem hat, können mit dem Programm Netware Administrator bestimmt werden (siehe auch vorherige Abbildungen).

Access Control List (ACL)

Die Informationen darüber, wer auf ein Objekt und die Properties zugreifen kann und mit welchen Rechten, wird im Objekt selbst gespeichert. Hierfür existiert für jedes Objekt eine spezielle Property: Access Control List (ACL).

Die ACL Property enthält die Trustee Assignments und die Inherited Rights Filter. Jedes eingetragene Objekt in der ACL kann dabei andere Trustee Assignments aufweisen. Im Dateisystem ist die ACL und die IRF in der Directory Entry Table (DET) gespeichert.

Vergabe von Netware-Attributen auf Verzeichnisse und Dateien

Neben der Benutzer- bzw. gruppenbezogenen Erteilung von Zugriffsrechten auf Verzeichnisse und Dateien kann durch die Vergabe von Netware-Attributen auf Verzeichnisse und Dateien die Datensicherheit erhöht werden. Attribute sind immer verzeichnis- bzw. dateibezogen, da NDS-Objekte keine Attribute haben, d. h. sie sind unabhängig von den zugewiesenen Zugriffsrechten und gelten für alle Benutzer einschließlich für Benutzer mit Supervisor-Rechten.

Benutzer, denen das Zugriffsrecht "Modify" (M) auf die in Frage kommenden Verzeichnisse und Dateien eingeräumt wurde, können die vergebenen

Netware-Attribute ändern und somit jede Aktion, die sich aus ihren effektiven Rechten ergibt, ausführen.

Sicherheit durch den Einsatz von Netware-Attributen stellt sich somit als ein Subsystem auf der Ebene der Verzeichnis- und Dateisicherheit dar. Das bedeutet, dass obwohl jemand das ER hat eine Datei zu löschen, dies unter Umständen nicht tun kann, da das Attribut "Delete inhibit" (Di) gesetzt ist.

Bei der Vergabe von Netware-Attributen auf Verzeichnisse und Dateien sollten die folgenden Eigenschaften von Netware-Attributen beachtet werden.

- **Verzeichnis-Attribute:**

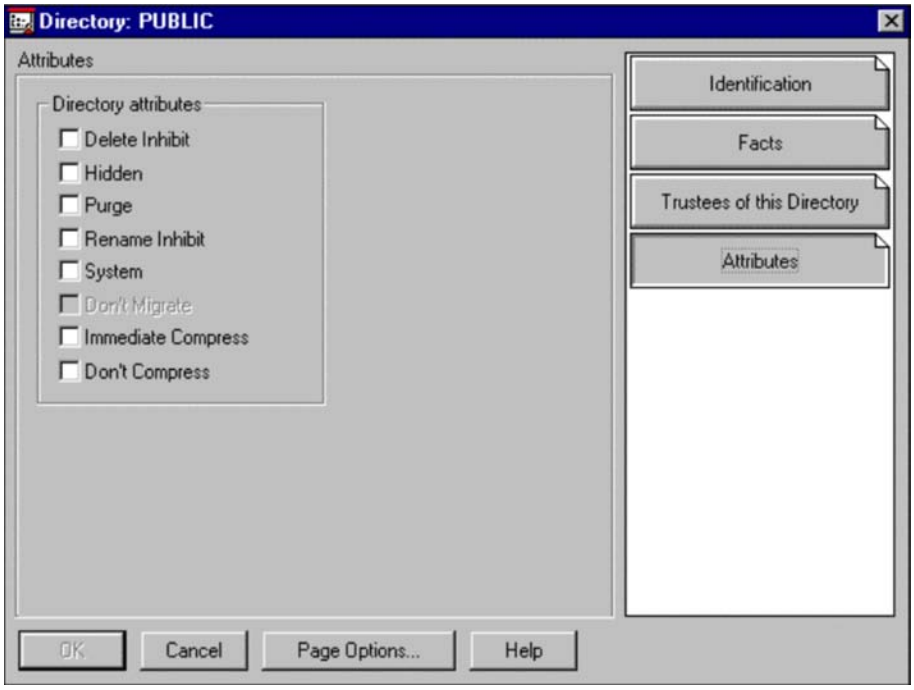


Abbildung 3: Netzwerk Attribute im Public Directory

Delete Inhibit (Di): Das Verzeichnis kann nicht gelöscht werden.

Hidden (H): Das Verzeichnis wird als versteckt gekennzeichnet; es erscheint weder in einem Inhaltsverzeichnis unter DOS, noch kann es gelöscht oder kopiert werden.

Purge (P): Das Verzeichnis sowie die in ihm befindlichen Dateien werden beim Löschen sofort, auch physikalisch, gelöscht. Eine Wiederherstellung des Verzeichnisses ist nicht möglich.

Rename Inhibit (Ri): Das Verzeichnis kann nicht umbenannt werden.

System (Sy): Das Verzeichnis wird vom System benutzt; es erscheint ebenfalls nicht in einem Inhaltsverzeichnis unter DOS und kann weder kopiert noch gelöscht werden.

Don`t Migrate (Dm): Die in dem Verzeichnis enthaltenen Dateien dürfen nicht auf einen sekundären Datenträger (z. B. ein Bandlaufwerk) ausgelagert werden.

Immediate Compress (Ic): Die in das Verzeichnis hineinkopierten Dateien werden umgehend komprimiert. Dateien, die sich schon im Verzeichnis befinden, werden durch dieses Attribute nicht beeinflusst.

Don`t Compress (Dc): Die in dem Verzeichnis enthaltenen Dateien dürfen nicht komprimiert werden.

- **Datei-Attribute:**

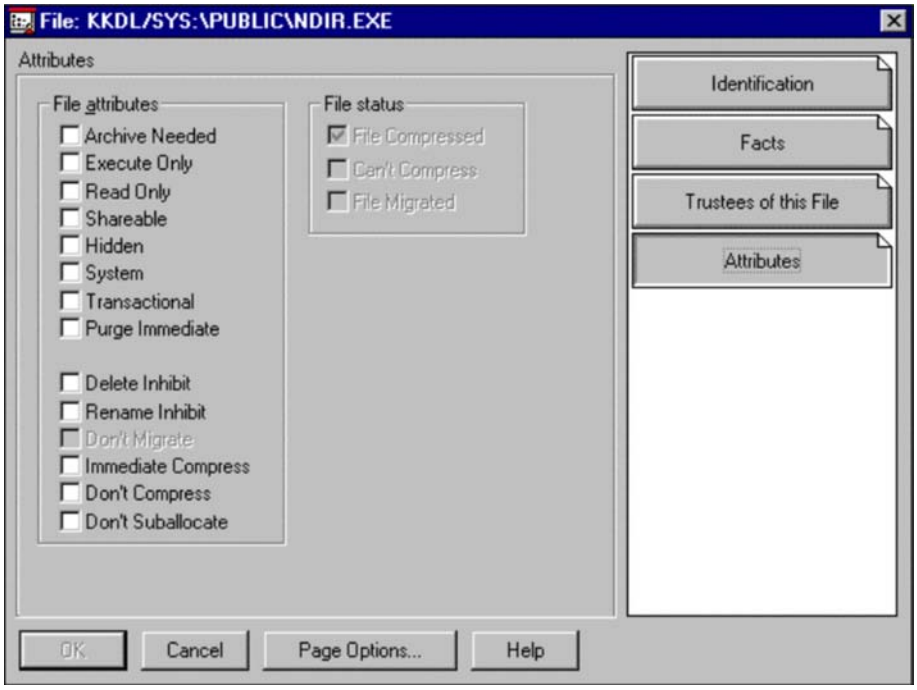


Abbildung 4: Datei Attribute: FILE: *KKDL/SYS:\PUBLIC\NDIR.EXE*

Archive needed (A): Die so durch Novell Netware gekennzeichneten Dateien sind seit der letzten Datensicherung inhaltlich verändert oder neu auf dem Novell Netware Server aufgespielt worden. Datensicherungs-software kann somit bei einer sequentiellen Datensicherung erkennen, dass die Datei erneut gesichert werden muss.

Execute Only (X): Ausführbare Programmdateien (**.exe*, **.com*), die mit diesem Attribut versehen werden, können ausschließlich ausgeführt oder gelöscht werden. Ein Kopieren der Datei ist nicht möglich. Zu beachten ist auch, dass Dateien mit diesem Attribut nicht gesichert werden (z. B. bei einem Full-Backup)

Read write (Rw): Auf die Datei ist sowohl Lese- als auch Schreibzugriff möglich.

Read only (Ro): Die Datei kann nur gelesen werden. Ein Schreibzugriff ist nicht möglich. Um Datenverluste bei einer gemeinsamen Benutzung zu vermeiden, sollten diese Dateien ebenfalls das Attribut "Shareable" (S) besitzen.

Ausführbare Programmdateien (*.exe, *.com) sollten mit dem Attribut "Read only" versehen werden, um einem möglichen Befall durch Computer-Viren vorzubeugen.

Shareable (Sh): Diese Dateien können von mehreren Benutzern gleichzeitig benutzt werden. Dateien, die mit dem Attribut "Shareable" versehen worden sind, sollten gleichzeitig das Attribut "Read Only" (Ro) besitzen. Das Attribut "Shareable" ist nur relevant für Programme, die Dateien nicht netzfähig öffnen.

Hidden (H): Die Datei wird als versteckt gekennzeichnet. Sie erscheint nicht in einem Inhaltsverzeichnis unter DOS und kann weder kopiert noch gelöscht werden.

System (Sy): Die Datei wird vom Netzbetriebssystem verwendet; sie erscheint ebenfalls nicht in einem Inhaltsverzeichnis unter DOS und kann weder kopiert noch gelöscht werden.

Transactional (T): Dateien mit diesem Attribut unterliegen der Transaktionskontrolle von Novell Netware. Als Transaktion wird hier eine zusammenhängende Folge von Veränderungen in einer oder mehreren Dateien verstanden. Das Setzen dieses Attributes bewirkt, dass nur vollständig durchgeführte Transaktionen in den Datenbestand der Datei übernommen werden. Transaktionen, die unvollständig abgebrochen wurden, werden von Novell Netware rückgängig gemacht.

Purge (P): Dateien mit dem Attribut "Purge" werden beim Löschen nicht nur logisch, sondern sofort physikalisch gelöscht. Dies hat zur Folge, dass die Datei nicht wiederhergestellt werden kann. In diesem Zusammenhang wird darauf hingewiesen, dass die physikalische Löschung von Dateien nicht nur durch das Netware-Attribut "Purge" erfolgen kann, sondern ebenso von einer Arbeitsstation mit dem Befehl *"PURGE Dateiname"* durchgeführt werden kann.

Copy Inhibit (Ci): Derartige Dateien können nicht kopiert werden. Dieses Netware-Attribut gilt allerdings nur für APPLE Macintosh Workstations.

Delete Inhibit (Di): Die Datei kann nicht gelöscht werden.

Rename Inhibit (Ri): Die Datei kann nicht umbenannt werden.

Don¿t Migrate (Dm): Eine Datei, die mit diesem Attribut versehen ist, kann nicht auf einen sekundären Datenträger (z. B. ein Bandlaufwerk) ausgelagert werden.

Immediate Compress (Ic): Die Datei wird vom Betriebssystem schnellstmöglichst komprimiert und in dieser Form auf dem Volume gespeichert.

Don¿t Compress (Dc): Die Datei wird vom Betriebssystem nicht komprimiert, auch wenn für das Volume die Kompression eingeschaltet ist.

Don¿t Suballocate (Ds): Bei der Speicherung dieser Dateien wird keine Teilblockzuordnung (Suballocation) vorgenommen, obwohl dieses Merkmal für das System aktiviert wurde.

File Compressed (Co), Can't Compress (Cc), File Migrated (M): Mit diesen Attributen werden vom Betriebssystem dementsprechende

Informationen über eine Datei gespeichert. Diese Attribute können nur vom Betriebssystem geändert werden.

Sorgfältige Vergabe von Rechten

Dateirechte, NDS-Objektrechte und NDS-Objekteigenschaftsrechte sind vollkommen unabhängige Rechte. Hiervon gibt es zwei Ausnahmen. Erhält jemand Supervisor-Rechte auf ein NDS-Objekt, hat er automatisch auch Supervisor-Rechte auf die NDS-Objekteigenschaften. Umgekehrt tritt dieses Phänomen nicht auf. Supervisor-Rechte auf NDS-Objekteigenschaften sind nicht gleichbedeutend mit Supervisor-Rechten auf das NDS-Objekt selbst. Hierbei muss allerdings beachtet werden, dass die Objekteigenschaft *Object Trustees (ACL)* eine Eigenschaft eines jeden NDS-Objekts ist. Erhält man nun Supervisor-Rechte auf die Eigenschaften eines NDS-Objekts oder nur das Recht *WRITE* auf die Eigenschaft *Object Trustees (ACL)*, ist man in der Lage, sich selbst oder anderen NDS-Objekten beliebige Rechte zu gewähren. Eine weitere wichtige Ausnahme ist das NDS-Objekt *Server*. Erhält z. B. der Benutzer *RZenk,* wie im obigen Beispiel, das Recht *WRITE* auf die Objekteigenschaft *Object Trustees (ACL)* des Servers, ist dies gleichbedeutend mit Supervisor-Rechten auf das komplette Dateisystem, das diesem Server zugeordnet ist. Die Eigenschaft *Object Trustees (ACL)* des Servers ist somit die Schnittstelle zwischen der NDS und dem Dateisystem.

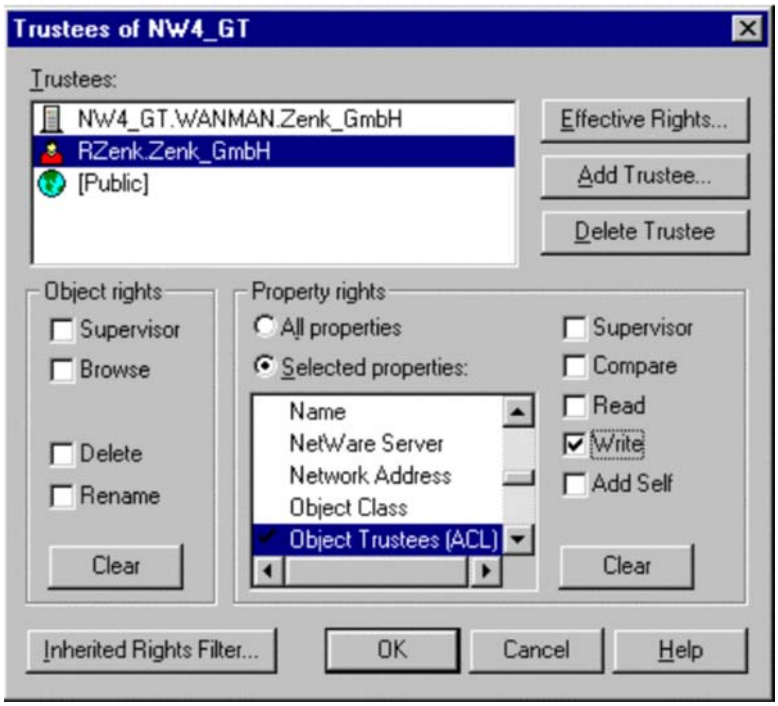


Abbildung 5: Netware Administrator Server *NW4_GT* "Trustee of this Object..."

Um zu verhindern, dass durch unsachgemäßes Vergeben von NDS-Rechten Supervisor-Rechte im Dateisystem erlangt werden können, könnten Inherited

Rights Filter (IRF) an jedem Server-Objekt aktiviert werden. Damit können die Objektrechte von den Verzeichnisrechten getrennt werden. Dabei muss das Supervisor-Recht sowohl auf NDS-Objekt- als auch auf NDS-

Objekteigenschafts-Ebene und das Recht *WRITE* der Eigenschaft *Object Trustees (ACL)* gefiltert werden. Besser ist es natürlich, wenn man sich bewusst ist, wie sich bestimmte Rechte im Detail auswirken.

Eingeschränkte Nutzung von Accounts mit Supervisor-Berechtigung auf Dateiebene

Der Account des Benutzers "Admin" sollte bei der täglichen Administrationsarbeit nicht verwendet, sondern nur in Notfällen benutzt werden. Um dennoch die Systemadministration zu gewährleisten, sollte daher für jeden Benutzer mit der Netware Sicherheitsstufe "Supervisor" ein Benutzer-Account eingerichtet werden, der über dieselben Rechte wie das Benutzer-Objekt "Admin" verfügt (ausdrückliche Trustee Zuweisung, siehe auch *Schutz vor Verlust der Administrierbarkeit*), mit dem die System-administration normalerweise erfolgt. Werden die Administrationsarbeiten nicht hauptamtlich wahrgenommen, so sollten für die nicht-administrativen Aufgaben zusätzlich aufgabenbezogene Accounts eingerichtet werden.

Der Account des Administrators bzw. seines Vertreters sollte weiterhin nur auf hierzu definierten Workstations verwendet werden, da die Integrität anderer Workstations manipuliert sein könnte.

Der Account "Admin", der standardmäßig die alleinigen administrativen Rechte besitzt, sollte als potentielles Angriffsziel keine Rechte mehr besitzen. Die notwendigen Supervisor-Rechte sollten einem anderen, weniger auffälligen Benutzer-Account übertragen werden. Man kann aber auch ganz einfach den Admin-Account umbenennen, um hierfür einen Namen zu verwenden, der den allgemeinen Regeln zur Namensvergabe innerhalb der NDS entspricht, so wie dies bei der Planung der NDS für das Unternehmen festgelegt worden ist.

Schutz vor Verlust der Administrierbarkeit

Eine neue Funktionalität ab Netware Version 4.x ist die Möglichkeit der dezentralen Administration von Novell Netware Netzen. Dies kann durch bestimmte administrative Möglichkeiten erreicht werden, wie z. B. der Definition eines eigenen Administrators für jedes Behälterobjekt. Wird dafür nur ein einziger Benutzer-Account verwendet und dieser versehentlich gelöscht, so kann der entsprechende Behälter nicht mehr administriert werden (siehe G 3.25 *Fahrlässiges Löschen von Objekten*).

Als wirksame Maßnahme **muss deswegen zusätzlich eine ausdrückliche Trustee-Zuordnung** für mindestens eines der Benutzer-Objekte des Benutzerverwalters vorgenommen werden. Das Administratorrecht darf also nicht mit dem Mechanismus *Security Equal To* erfolgen. Damit wird dem Verlust der Administrierbarkeit des Behälters vorgebeugt, falls das organisatorische Funktionsobjekt gelöscht wird. Dies gilt insbesondere auch für die Rechtezuordnung an die zentralen Administratoren eines Netware 4.x Netzes.

Information über Patches von Novell Netware

Im Verlauf der Entwicklung des Netzbetriebssystems Novell Netware haben sich diverse Schwachstellen bzw. Unzulänglichkeiten herausgestellt, die durch den Hersteller mit Hilfe von so genannten Patches bzw. Service Packs für die entsprechenden Versionen 3.x und 4.x größtenteils behoben wurden. Diese Patches werden durch den Hersteller im Internet zur Verfügung gestellt (http://support.novell.com und http://support.novell.de). Informationen über die Funktionalität sowie das ggf. erforderliche Einspielen der zur Verfügung gestellten Patches können daher Schwachstellen im laufenden Produktionsbetrieb beseitigen. Insbesondere zusätzlich installierte Softwareprodukte, wie z. B. zur Datensicherung, erfordern oftmals einen bestimmten Patchlevel des Netzbetriebssystems. Hierbei ist jedoch zu beachten, dass die angebotenen Patches keineswegs "blind" aufgespielt werden sollten, sondern nur im Bedarfsfall ("never change a running system") sowie nach gründlicher Information. Soweit vorhanden, sollten diese Patches zunächst auf einer Testkonfiguration ausgetestet werden.

Im Internet (Usenet) ist, neben den internationalen Diskussionsforen zum Thema Novell Netware (comp.os.netware.announce, comp.os.netware.misc, comp.os.netware.security, comp.os.netware.connectivity), für die deutschsprachigen Benutzer ein deutsches Novell Forum (z. Z. de.comp.sys.novell) vorhanden, in dem einige versierte Novelladminstratoren aktiv sind, die oftmals auch die schwierigsten Probleme zu lösen helfen. Außerdem werden zu den im Internet am häufigsten gestellten Fragen Dateien (so genannte FAQs - Frequently Asked Questions) zur Verfügung gestellt, die die häufigsten Probleme thematisieren und Lösungen anbieten.

Patches und Informationen über Novell Netware werden darüber hinaus auch über andere Anbieter von Netzdiensten, wie z. B. Compuserve, Fidonet und Mailboxen bereitgestellt.

Für die Richtigkeit und Vollständigkeit der jeweiligen Informationen in den Usenet Diskussionsforen sowie in den FAQs (Frequently Asked Questions) kann an dieser Stelle jedoch keine Garantie gegeben werden. Es sei darauf hingewiesen, dass eine vollständige Beschreibung des aufgetretenen Problems, sowie eine Beschreibung der jeweiligen Konfiguration des Netzes (Client, Server) besonders vorteilhaft bei der Hilfesuche im Internet (Usenet) ist.

Schwierigkeiten während des Netzbetriebes können darüber hinaus oftmals durch die Nachfrage bei dem Verkäufer des Netzbetriebssystems oder im Informationsaustausch mit Kollegen behoben werden; wobei auch hier die Problemlösung durch eine vollständige Konfigurationsbeschreibung erleichtert wird.

Prüfung auf Computer-Viren

Computer-Viren, die sich in den auf einem Novell Netware Server gespeicherten Programmen und Dateien befinden, können erhebliche Schäden im Netzverbund hervorrufen.

Aus diesem Grund sollten die Programme und Dateien eines Novell Netware Servers regelmäßig mit einem aktuellen Virensuchprogramm auf eventuell vorhandene Computer-Viren überprüft werden.

Zu diesem Zweck empfiehlt es sich, einen speziellen Benutzer-Account im Novell Netware 4.x Netz einzurichten, der über die Zugriffsrechte "Read" (R)

und "File Scan" (F) auf alle Dateien verfügt. Die Prüfung auf Computer-Viren sollte keinesfalls mit den Rechten des Supervisors bzw. Supervisor-äquivalenten Rechten durchgeführt werden, da ein Computer-Viren-Checkprogramm, welches selbst mit einem Computer-Virus infiziert ist, diesen auf alle Programme und Dateien übertragen würde.

Auch die Benutzer bzw. Benutzergruppen sollten auf die Verzeichnisse und Dateien mit ausführbarem Programmcode lediglich die effektiven Rechte "Read" (R) und "File scan" (F) erhalten, um deren Infektion mit Computer-Viren zu vermeiden, die auf lokalen Rechnern aufgetreten sind. Zudem sollten ausführbare Programme mit dem Netware-Attribut "Read only" (Ro) versehen werden.

Bei eingeschalteter Kompression ist zusätzlich zu beachten, dass durch einen kompletten Suchlauf auf den Netware Volumes alle komprimierten Dateien dekomprimiert werden müssen. Dies ist sehr zeitaufwendig und verlängert die Antwortzeiten eines Servers stark.

Regelmäßige Überprüfung der Zeitsynchronisation und der NDS-Reproduktion

Um die Zeitsynchronisation und den Abgleich mehrerer NDS-Reproduktionen zwischen verschiedenen Netware 4.x Servern zu beobachten, kann an der Konsole ein separater Netware-Screen aktiviert werden. Dies erfolgt durch die Eingabe der beiden Befehle

- SET TIMESYNC DEBUG = 7 und
- SET NDS TRACE TO SCREEN = ON.

An der Konsole werden dann die entsprechenden Pakete angezeigt, die zwischen den Servern übertragen werden. Auf diesem NDS Trace Bildschirm kann der Abgleich der einzelnen Reproduktionen des jeweiligen Servers verfolgt werden. Wenn der Abgleich erfolgreich war, wird dies in grüner Schrift angezeigt, Fehlermeldungen werden in roter Schrift dargestellt. Da dieser Bildschirm regelmäßig aktualisiert wird, können Informationen übersehen werden. Es ist daher zwingend erforderlich, regelmäßig die Konsole-Meldungen zu beobachten. Hier empfiehlt sich allerdings der Einsatz eines Netzmanagement-Tools, mit welchem man wesentlich zuverlässiger den Status des Netzes ermitteln und überwachen kann:

Im Fehlerfall ist jedoch das Utility NDS-Manager (*SYS:\PUBLIC\WIN95\ NDSMGR32.EXE - für Window 95 bzw. Windows NT*) sehr hilfreich. Hiermit kann ebenfalls der Reproduktionsstatus überwacht werden.

Regelmäßige Überprüfung der Auslastung der System-Festplatte

Damit ein störungsfreies Arbeiten gewährleistet werden kann, muss sichergestellt sein, dass das System-Volume eines jeden Netware Servers über

genügend freien Speicherplatz verfügt. Dies ist vor allem bei eingeschalteter Kompression sehr wichtig. Das System-Volume kann beispielsweise durch temporäre Dateien vollgeschrieben werden, falls deren Ausbreitung nicht kontrolliert wird und diese nicht von Zeit zu Zeit gelöscht werden. Weiterhin können große Druckerwarteschlangen zu einem Überlauf des Systemvolumes führen, wenn sehr viele Benutzer gleichzeitig große Dokumente drucken wollen.

Es sollte deshalb ein separates Volume für Druckerwarteschlangen und andere Verzeichnisse angelegt werden, in denen temporäre Dateien abgespeichert werden. Ist dies nicht möglich, so sollten zumindest Größenbeschränkungen auf die entsprechenden Verzeichnisse vergeben werden, um deren unkontrolliertes Anwachsen zu verhindern. Damit wird gewährleistet, dass das System-Volume nicht mehr vollgeschrieben werden kann und immer genügend Platz für systemspezifische Aktionen des Netware Servers vorhanden ist.

Ergänzende Kontrollfragen:

- Wurden alle Aktionen für einen sicheren Betrieb eines Netware 4.x Servers beachtet?
- Wurden zum Schutz vor Verlust der Administrierbarkeit Ersatz-Benutzer-Accounts eingerichtet und diese mit ausdrücklichen Trustee-Zuordnungen für die jeweiligen NDS-Objekte versehen?
- Werden die Plattenauslastungen und die Konsolenmeldungen regelmäßig kontrolliert?
- Werden die Supervisor-Rechte auf die Serverobjekte regelmäßig geprüft?

M 2.150 Revision von Novell Netware 4.x Netzen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Revisor

Eine wichtige Methode zur Gewährleistung der Sicherheit eines Netzes besteht darin, unabhängigen Revisoren die Überprüfung der Vorgänge im Netz zu gestatten. Netware 4.x bietet dazu die Möglichkeit, durch Aktivierung der Revision mit dem Dienstprogramm *SYS:PUBLIC\AUDITCON.EXE* eine Vielzahl von Ereignissen in der NDS und im Dateisystem zu verfolgen. Es ist bei Netware 4.x möglich, beliebigen Benutzern die Rolle eines Revisors zuzuweisen. Dieses Programm ermöglicht unter anderem die folgenden Funktionen:

- Die Revisoren können alle NDS-Dateiereignisse der Netware-Server, der Container oder eines bestimmten Volumes überwachen.
- Die Dateisystemrevision auf Volume- und Behälterebene kann aktiviert werden.
- Die Revisoren können Netzereignisse und -aktivitäten zurückverfolgen, jedoch können sie außer den Revisionsdaten- und Revisionsverlaufsdateien nur diejenigen Dateien öffnen oder ändern, zu denen ihnen vom Administrator die entsprechenden Rechte erteilt wurden.

Anmerkung: Bei der Aktivierung der Möglichkeiten zur Protokollierung ist zu beachten, dass die Protokolldatei sehr groß werden kann. Daher sollte die maximale Größe der Protokolldatei begrenzt werden, um einen Speicherplatzmangel zu verhindern. Da dies abhängig von der Anzahl der Benutzer und deren Aktivitäten ist, können hier jedoch keine konkreten Richtlinien angegeben werden.

Die dabei anfallenden Daten sind in den meisten Fällen personenbezogen und unterliegen somit dem Bundesdatenschutzgesetz (BDSG). Es ist sicherzustellen, dass diese Daten nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet werden (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*).

Um einen unabhängigen Revisor einzurichten, der keine sonstigen administrativen Rechte im Netz hat, aber die Aktivitäten eines Administrators überprüfen kann, sind folgende Maßnahmen durchzuführen:

- Für Netware 4.10 muss das Auditing für das Dateisystem bzw. für die NDS aktiviert sein und ein Passwort hierfür vergeben werden. Jeder, der dieses Passwort kennt, ist in der Lage, das Auditing auszuwerten. Deshalb sollte unter Netware 4.10 sehr sorgsam mit diesem Passwort umgegangen werden. Weitere Rechtevergaben sind unter Netware 4.10 nicht notwendig.

  Ab Netware 4.11 werden die Informationen in NDS-Audit-File-Objekte abgelegt. Somit lässt sich eine wesentlich bessere Sicherheit hierfür aufbauen. Zudem bestehen unter Netware 4.11 wesentlich bessere Überwachungsmöglichkeiten, da man die Anzahl der Auditing-Mechanismen und -Funktionen wesentlich erweitert hat.

- Erstellen eines Benutzer-Objekts für den Revisor. Die Berechtigung sollte nicht für einen herkömmlichen Benutzer-Account vergeben werden, da dies die Sicherheit aushebeln könnte.
- Ab Netware 4.11 muss der Revisor notwendige NDS-Recht auf die dementsprechenden NDS-Audit-File-Objekte erhalten.
- Aktivieren der Netzrevision. Die Person, die das NDS-Audit-File-Objekt erstellt, bekommt das Supervisor-Recht auf das NDS-Audit-File-Objekt und das Write-Recht auf das Access Control List Property. Zudem kommen noch das Read- und Write-Recht auf das Audit Policy Property und das Read-Recht für das Audit Contents Property hinzu. Somit ist der Ersteller dieses NDS-Audit-File-Objektes in der Lage, die Administration für das Auditing und Auswertungen hierzu durchzuführen.
- Vergabe eines Revisorpassworts im Utility *SYS:PUBLIC\AUDITCON.EXE*, um Unabhängigkeit vom Administrator zu erhalten (Netware 4.10 und aus Kompatibilitätsgründen auch in Netware 4.11)

  Ab Netware 4.11 sollte die Unabhängigkeit des Auditors vom Administrator über die Vergabe von NDS-Rechten erzielt werden. Hier können auch noch Abstufungen stattfinden, ob ein bestimmter Revisor Audit-Daten einsehen und/oder das Auditing administrieren darf.

Ist es aus wohl überlegten Gründen nicht gewünscht oder nicht möglich, die Rolle eines unabhängigen Revisors einzurichten, kann die Auswertung der Protokolldateien auch durch den Administrator erfolgen. Für diesen Fall bleibt zu beachten, dass damit eine Kontrolle der Tätigkeiten des Administrators nur schwer möglich ist. Das Ergebnis der Auswertung sollte daher zumindest dem IT-Sicherheitsbeauftragten, dem IT-Verantwortlichen oder einem anderen besonders zu bestimmenden Mitarbeiter vorgelegt werden.

Ergänzende Kontrollfragen:

- Wer wertet die Revisionsdateien aus?
- Können die Aktivitäten des Administrators ausreichend kontrolliert werden?
- Wird das IT-Sicherheitsmanagement bei Auffälligkeiten unterrichtet?
- Wurde die maximale Größe der Protokolldatei begrenzt, um einen Speicherplatzmangel zu verhindern?

M 2.151 Entwurf eines NDS-Konzeptes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Eine der wichtigsten Neuerungen in Novell Netware 4.x stellen die *Novell Directory Services* (NDS) dar, die im deutschen Sprachgebrauch als *Novell Verzeichnis Dienste* bezeichnet werden. Die NDS bezieht sich auf die logische Struktur des Netzes und aller darin vorhandenen Ressourcen wie z. B. Benutzer, Gruppen, Drucker oder Netware Server.

Die Technologie der NDS ersetzt die noch in Netware 2.x und Netware 3.x verwendete Bindery. In der Bindery sind alle Benutzer, Gruppen usw. in einer eindimensionalen Liste enthalten. Beim Einsatz mehrerer Netware 3.x Server steht der Administrator jedoch vor dem "Problem", dass jede Änderung (beispielsweise das Hinzufügen eines Benutzers) auf jedem Netware 3.x Server manuell ausgeführt werden musste, d. h. auf allen Servern, für die einem Benutzer Zugriffsrechte gegeben werden sollten.

Die Novell Verzeichnis Dienste hingegen sind unabhängig von einem konkreten Server und orientieren sich ausschließlich am zugrunde liegenden Netz. Dies bedeutet, dass Administrationsarbeiten wie Änderungen oder Einrichtungen eines Benutzer-Accounts von den Novell Verzeichnis Diensten auf allen betroffenen Servern vollzogen werden, ohne dass ein manuelles Eingreifen des Administrators erforderlich ist.

Die Ressourcen werden in einer Datenbank baumförmig verwaltet, deshalb spricht man auch vom NDS-Tree bzw. NDS-Baum. Im NDS-Baum werden alle Benutzer, Gruppen, Drucker, Netware Server usw. als Objekte in der so genannten NDS-Verzeichnisdatenbank verwaltet. Hierbei unterscheidet man zwei Arten von Objekten: *Containerobjects* (Behälterobjekte) und *Leafobjects* (Blattobjekte). Während sich ein Blattobjekt am Ende eines Zweiges befindet und keine weiteren Objekte mehr beinhaltet, kann ein Behälterobjekt weitere Behälter oder Blattobjekte enthalten.

Es existieren unter anderem folgende Behälterobjekte:

- **Root (Stammobjekt)**

  Die Root stellt die Wurzel des NDS-Verzeichnisbaumes dar. Jeder NDS-Verzeichnisbaum hat genau ein solches Objekt, das bei der Installation angelegt wird und weder umbenannt noch gelöscht werden kann. In jedem NDS-Verzeichnisbaum kann sich nur ein solches Objekt befinden.

- **Country (Land)**

  Das Objekt Country ermöglicht eine geographische Unterteilung der gesamten Struktur des NDS-Verzeichnisbaumes, d. h. eine Einteilung des Netzes nach verschiedenen Ländern. Dieses Objekt ist jedoch optional und wird deshalb bei der Installation der NDS auch nicht vorgegeben.

- **Organization (Organisation)**

  Das Objekt Organization dient dazu, weitere Objekte im NDS-Verzeichnisbaum hierarchisch anzuordnen. Dabei gibt es keine festen Regeln, so

dass ein Unternehmen beispielsweise sowohl den Firmennamen als auch verschiedene Niederlassungen als Bezeichnung der Organisation verwenden kann. Jeder NDS-Verzeichnisbaum muss mindestens eine Organisation beinhalten.

- **Organizational Unit (Organisatorische Einheit)**

  Die Organizational Unit kann nur unterhalb einer Organisation erstellt werden und dient zur weiteren Unterteilung der NDS. Beispielsweise lassen sich Niederlassungen, Abteilungen oder Projektgruppen in organisatorischen Einheiten anordnen. Die organisatorische Einheit ist optional und wird zur besseren Strukturierung je nach Anzahl der Blattobjekte eingesetzt.

Als Blattobjekte bezeichnet man z. B. Benutzer, Gruppen, Drucker, Server oder Datenträger. Es ist nicht möglich, unter Blattobjekten weitere Objekte anzulegen. Folgende Blattobjekte werden am häufigsten verwendet:

- **Netware Server**

  Dieses Objekt repräsentiert einen Netware Server im Netz, von dem es mindestens einen geben muss. Auf dieses Objekt wird von vielen anderen Objekten verwiesen, die die vom Server bereitgestellten Dienste verwenden. Dieses Objekt wird bereits durch das Installationsprogramm erstellt.

- **Drucker**

  Hiermit wird ein im Netz vorhandener Drucker dargestellt. Zu einem Drucker gehören immer die Objekte Druckerwarteschlange und Druckserver.

- **Benutzer**

  Dieses Objekt dient zur Verwaltung und Speicherung von Informationen über einen Benutzer des Netzes, insbesondere über seine Zugriffsrechte auf Netzressourcen.

- **Gruppen**

  Obwohl in einer Gruppe mehrere Benutzer zusammengefasst werden können, stellt eine Gruppe ein Blattobjekt und kein Behälterobjekt dar. Sie dient zur einfacheren Administration, da die Rechte einer Gruppe auf deren Mitglieder übertragen werden.

- **Volume**

  Hiermit wird ein physikalisches Volume zum Speichern von Daten dargestellt. Volumeobjekte werden in der Regel vom Installationsprogramm erstellt.

Für eine detailliertere Beschreibung der weiteren Blattobjekte wird auf die Netware Handbücher verwiesen. Auch sind der Objektvielfalt keine Grenzen gesetzt, da z. B. Objekte von Applikationen hinzugefügt, aber auch entfernt werden können.

Die Verzeichnisobjekte und deren Attribute werden, wie bereits erwähnt, in einer Datenbank verwaltet, die wesentlicher Bestandteil der NDS ist. In

Netzen mit WAN-Verbindungen empfiehlt es sich, diese Datenbank in logische Segmente aufzuteilen, welche auf verschiedene Netware-Server kopiert werden. Es ist hierbei wichtig beim Planen der Reproduktionen auf langsame WAN-Verbindungen zu achten.

Diese logische Segmentierung wird als *Partitionierung* bezeichnet. Der Kopiervorgang der logischen Segmente auf die Netware-Server wird als *Reproduktion* bezeichnet.

Jede Partition besteht aus mindestens einem Behälterobjekt und den darin enthaltenen Objekten. Zusätzlich kann es von einer Partition noch mehrere Lese- bzw. Schreib/Lese-Kopien geben, jedoch immer nur eine Haupt-Reproduktion.

Die physische Unterteilung der NDS in Partitionen ist für die Anwender transparent; d. h. die Netware-internen Mechanismen sorgen dafür, dass der Anwender nichts von der Aufteilung bemerkt.

Der Entwurf eines NDS-Verzeichnisbaumes unterliegt prinzipiell keinerlei Beschränkungen, so dass es zur Erzeugung der unterschiedlichsten Formen mit beliebiger Komplexität kommen kann. Dabei sollte jedoch eine gründliche und sorgfältige Planung durchgeführt werden, wobei folgende Grundsätze zu beachten sind:

- Eine übersichtliche NDS sollte maximal zwischen 4 und 8 Ebenen tief sein.
- Die maximale Anzahl aller Objekte in einer Organisation oder in einer organisatorischen Einheit sollte nicht mehr als 1.500 betragen.
- Mehrere kleinere Abteilungen sollten zu einer organisatorischen Einheit zusammengefasst werden, um deren Anzahl zu reduzieren und die Übersichtlichkeit zu erhöhen.
- Es sollten aussagekräftige, aber nicht zu lange Namen verwendet werden (z. B. "F&E" statt "Forschung und Entwicklung"), da die gesamte Pfadangabe innerhalb des NDS-Baumes maximal 255 Zeichen lang sein darf. Diese Begrenzung kommt allerdings nur indirekt zustande, da DOS-Zeilenkommandos keine längeren Eingaben zulassen. Diese Pfadangabe wird *Kontext* genannt.
- Von jeder Partition sollten zusätzlich zur Hauptpartition zwei weitere Schreib/Lese-Partitionen erstellt werden. Durch die somit vorhandene Redundanz ist der Verlust von NDS-Informationen gering. Eine Sicherung der NDS bleibt trotzdem obligatorisch.
- Das Netware Loadable Module (NLM) *Directory Service* (*DS.NLM*) ist auf allen Netware Servern innerhalb eines NDS-Baumes, auf dem dieselben Netware Versionen installiert sind, in derselben Version zu benutzen, da sich verschiedene Versionen unter Umständen nicht miteinander synchronisieren. In NDS-Bäumen, in denen z. B. Netware Server der Versionen 4.10, 4.11 und 5.0 installiert sind, müssen sich die Versionen der *DS.NLM* auf den einzelnen Netware Servern sehr wohl unterscheiden. Nur die *DS.NLM* auf allen Netware Servern der Versionen 4.10, 4.11 und 5.0 muss, um unnötige Probleme zu vermeiden, in derselben Version installiert

sein. Da prinzipiell Mischumgebungen erlaubt sind, zeigt die Praxis, dass eine homogene Serverlandschaft - entweder nur Netware Server der Versionen 4.10, 4.11 oder 5.0, die stabilsten und die am besten zu administrierenden NDS-Netze sind.

Bei der Planung der NDS ist nicht vorrangig die Größe des Netzes, sondern das Umfeld entscheidend, wie z. B. die Hardware, die Kommunikationsverbindungen, die LAN/WAN-Topologie und die Struktur der Organisation. Beispielsweise ist für ein kleines Netz mit mehreren WAN-Verbindungen ein größerer Aufwand für die Planung erforderlich als für ein großes Netz ohne WAN-Verbindungen, da mit den verschiedenen WAN-Architekturtypen eindeutige physische Attribute verknüpft sind. Eine Planung sollte zumindest die folgenden Punkte abdecken:

- Festlegung eines Standards für die Benennung von Objekten (insbesondere Namenskonventionen für Benutzer- und Druckerkennungen),
- Entwurf einer Verzeichnisbaumstruktur,
- Festlegung der Position von Netzressourcen (z.B. Drucker und Server) innerhalb des NDS-Baumes bzw. Container, um Benutzern und Administratoren eine transparente Sicht des Netzes zu ermöglichen,
- NDS-Baum sollte die Organisationsstruktur des abzubildenden Unternehmens widerspiegeln,
- Einheitliche sowie abgestimmte Positionierung von Netzressourcen an verschiedenen Standorten um Benutzern mit häufigen Standortwechsel ein möglichst kurze Einarbeitungszeit zu ermöglichen,
- Festlegung einer Partitions- und Reproduktionsstrategie, die unter anderem stark abhängig von WAN-Verbindungen ist.

Für weitergehende Informationen zur NDS-Planung sei an dieser Stelle auf das *Handbuch zu Netware 4 Netzwerken* von Novell verwiesen, welches die Implementierung eines Netware 4.x Netzes ausführlich beschreibt.

Ergänzende Kontrollfragen:

- Existieren regelmäßig Absprachen der einzelnen Administratoren der verschiedenen Standorte?
- Wurden alle Planungsgrundsätze eingehalten?
- Sind die NDS, Planungsgrundsätze und die Absprachen der Administratoren dokumentiert?

M 2.152 Entwurf eines Zeitsynchronisations-Konzeptes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Stabilität eines Netware 4.x Netzes hängt wesentlich von der Zeitsynchronisation ab und steht im direkten Zusammenhang mit den Novell Directory Services (NDS).

Zeitsynchronisation bedeutet in diesem Fall, dass in einem Netz mit NDS und mehreren Netware-Servern deren Uhrzeit übereinstimmen muss. Dabei beträgt die Standardtoleranz zwei Sekunden. Die Uhren sämtlicher Netware-Server der NDS dürfen also nicht mehr als zwei Sekunden voneinander abweichen. Ist dies gewährleistet, wird die Uhrzeit im Netz als *synchron* bezeichnet.

In einem Multiserver-Netz sind im allgemeinen mehrere Replikationen und/oder Partitionen der NDS auf den Netware-Servern verteilt. Wird eine Änderung an einer Partition der NDS durchgeführt, wird diese mit einem Zeitstempel versehen. Diese Änderung wird dann beim nächsten NDS-Abgleich an die Partitionen und Replikationen auf den anderen Netware-Servern im Netz weitergegeben. Geht die Uhrzeit auf einem der Netware-Server, der die Änderung empfängt, um beispielsweise eine Stunde nach und ist somit nicht *in sync*, können die Änderung für diese NDS-Replikation oder Partition erst synchronisiert werden, wenn der betroffene Server wieder *in sync* ist.

Grundsätzlich kann man die folgenden zwei Szenarien unterscheiden:

- **Einzelreferenz**

  Dieses Zeitmodell wird von Novell für Netze mit bis zu 30 Netware-Servern empfohlen. Es ist sehr einfach einzurichten, und es bedarf keiner detaillierteren Planung der Zeitsynchronisation.

  In diesem Modell dient ein einziger Netware-Server als Zeitgeber (Einzelreferenz), während die restlichen Netware-Server nur als Zeitnehmer fungieren. Der Einzelreferenz-Server gibt die Uhrzeit für das gesamte Netz vor und sollte deshalb mit einer externen Zeitquelle (z. B. einer Funkuhr) verbunden werden.

  Ein großer Nachteil dieses Zeitmodells ist, dass beim Ausfall des Einzelreferenz-Servers kein Zeitabgleich mehr stattfinden kann, mit allen daraus resultierenden Konsequenzen.

- **Zeitgebergruppen**

  Bei größeren Netzen empfiehlt es sich, Zeitgebergruppen zu verwenden. Sie sind nicht schwer zu konfigurieren, erfordern jedoch eine angemessene Planung. Hier teilen sich mehrere Netware-Server die Zeitgeber-Rolle. Einer von ihnen ist der Referenz-Server, welcher mit einer externen Zeitquelle verbunden werden sollte.

  Eine Stufe unter dem Referenz-Server stehen die primären Zeitserver, von denen mindestens zwei existieren müssen. Dieser Zeitservertyp unterscheidet sich nicht grundlegend von einem Referenz-Server. Alle Referenz- und Primär-Server bestimmen gemeinsam eine gültige Netzzeit und

geben diese Zeit an die Sekundär-Server weiter. Der Referenz-Server ist der ruhende Pol im Netz. Da er seine Zeit nicht an die Netzzeit anpaßt, muss sich zwangsläufig die Netzzeit an ihn anpassen. Daher ist er auch derjenige Server, an dem die Netzzeit, falls notwendig, korrigiert werden muss. Im Gegensatz dazu passen Primär-Server ihre Zeit an die Netzzeit an.

Ein entscheidender Vorteil dieses Modells ist, dass durch die Primär-Server Ersatz-Zeitgeber vorhanden sind und bei einem Ausfall des Referenz-Servers weiterhin eine Zeitsynchronisation stattfinden kann. Trotz der Aussage von Novell, dass dieses Modell ab 30 Netware-Servern verwendet werden soll, kann es auch mit bedeutend weniger Netware-Servern eingesetzt werden.

Zeitgeber, Einzelreferenz-, Referenz- und Primär-Server werden in der Standardkonfiguration dynamisch über SAP/RIP-Mechanismen im Netz bekannt gegeben. Dies hat den Nachteil, dass man keinen Einfluss darauf hat, welcher Zeitserver mit welchem Zeitserver kommuniziert. Dies ist unter Umständen besonders bei WAN-Verbindungen nicht wünschenswert. Darum gibt es hier die Möglichkeit, auch mit konfigurierbaren Listen zu arbeiten und den SAP/RIP-Mechanismus auszuschalten.

Beim Entwurf eines Zeitsynchronisations-Konzeptes sollten die folgenden Punkte beachtet werden:

- In jedem Netz mit mehr als einem Netware-Server sollte eine externe Zeitquelle (z. B. Funkuhr) installiert werden.
- Bei WAN-Verbindungen innerhalb eines Netzes, in dem die NDS eingesetzt wird, sollte an einem Standort mit mehreren Netware 4.x Servern mindestens ein Zeitgeber vorhanden sein, so dass die lokalen Sekundär-Server auf einen lokalen Zeitgeber zurückgreifen können.
- Sollte auf einem Netware-Server aufgrund einer Fehlkonfiguration die eingestellte Uhrzeit sehr weit in der Zukunft liegen (beispielsweise 1 Jahr), so würde der Server nach Umstellung auf die korrekte Uhrzeit für 1 Jahr die Fehlermeldung "Synthetische Zeit ..." für alle NDS-Ereignisse ausgeben. Diese Fehlermeldung könnte beseitigt werden, wenn im Programm *DSREPAIR.NLM* eine neue Zeitepoche deklariert werden würde. Dabei würde die komplette NDS auf diesem Server gelöscht und neu erstellt werden. Dies ist ein relativ kritischer Eingriff in die NDS und sollte daher wohl überlegt sein.

Ergänzende Kontrollfragen:

- Wurde die Zeitsynchronisation angemessen geplant?

M 2.153 Dokumentation von Novell Netware 4.x Netzen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Eine wichtige Maßnahme zur Gewährleistung eines sicheren Betriebs, welche aus Zeit- oder Personalmangel oft vernachlässigt wird, ist die Dokumentation der wesentlichen Informationen eines Novell Netware 4.x Netzes. Da die Verantwortlichkeit über bestimmte Bereiche des Netzes wechseln oder auch ein Personalausfall auftreten kann, ist es unerlässlich, alle relevanten Informationen zu jedem Netware Server zu erfassen und in einer übersichtlichen Dokumentation darzustellen. Dies erleichtert die Einarbeitung einer eventuell erforderlichen Vertretung und verkürzt beim Auftreten eines Fehlers die Ausfallzeit.

In einer solchen Dokumentation sollten die folgenden Informationen (mit allen erforderlichen Parametern) in einer transparenten und einfach zu aktualisierenden Form dargestellt werden:

NDS

Auf die Dokumentation der NDS ist ein besonders hohes Augenmerk zu richten, da sie unter Umständen nicht auf einem einzigen zentralen Server gehalten wird, sondern sich insbesondere in Netware Netzen mit vielen WAN-Verbindungen in verschiedenen Partitionen befinden kann und auf unterschiedlichen Netware Servern gespeichert wird. Im Einzelfall kann dies bedeuten, dass z. B. ein Server mit einer Schreib/Lese-Partition zur Haupt-Reproduktion-Partition geändert werden muss, wenn der eigentliche Haupt-Reproduktionsserver einer Partition durch einen Hardwareausfall neu installiert werden muss. Allerdings kann dieser Problemfall durch geeignete Sicherungsmechanismen umgangen werden. Man sieht schon anhand dieses Beispiels, wie komplex der Aufbau einer weitverzweigten NDS ausfallen kann, und somit die Notwendigkeit einer entsprechenden Dokumentation besteht. Hierin sollten auf jeden Fall der Aufbau der NDS und auch Informationen über die vergebenen NDS- und Datei-Rechte zu finden sein.

Zeitsynchronisation

Da NDS und Zeitsynchronisation eng verwandte Themen sind, ist es sinnvoll, sie auch in der Dokumentation miteinander zu verbinden. Dies ergibt sich aus dem Umstand, dass alle relevanten Informationen, die über das Netware 4.x Netz ausgetauscht werden, mit Zeitstempeln versehen sind.

Damit die Zeitsynchronisation in einem Novell Netware 4.x Netz ordnungsgemäß funktioniert und die entsprechenden Zeitinformationen auch auf jedem Server zum gewünschten Resultat führen, muss klar festgelegt werden, welcher Server als Zeitquelle fungiert und welches Zeitmodell verwendet wird. Aus diesem Grund ist es auch unerlässlich, die Zeitsynchronisation und die entsprechenden NDS Dienste korrekt darzustellen, um im Fehlerfall die richtigen Schritte einleiten zu können.

Die unten aufgeführte Tabelle zeigt ein Beispiel, wie eine entsprechende Dokumentation aussehen kann.

SERVER	ZEITTYP	[Root]	PARTITIONEN Public	Hamburg	Berlin
Hamburg-S1	Referenz	Haupt-Reproduktion	Haupt-Reproduktion		
Hamburg-S2	Sekundär	Lese/ Schreib-Reproduktion	Lese/ Schreib-Reproduktion		
Hamburg-S3	Sekundär			Haupt-Reproduktion	Haupt-Reproduktion
Berlin-S1	Primär	Lese/ Schreib-Reproduktion	Lese/ Schreib-Reproduktion		
Berlin-S2	Primär				Lese/ Schreib-Reproduktion

Tabelle: Beispiel Dokumentation

Hardware-Konfiguration

Hier ist anzumerken, dass bei einer Neuinstallation des Netware Servers (z. B. nach einem Systemabsturz) sämtliche Informationen zu den Einstellungen der Hardware bekannt sein müssen, um den Server sachgerecht und zügig konfigurieren zu können. Sind diese nicht bekannt, so müssen sie im Einzelfall erst über entsprechende Programme abgefragt oder am Gerät abgelesen werden, was einen nicht zu unterschätzenden Zeitaufwand darstellt. Dies gilt insbesondere für das Beheben von zeitkritischen Fehlern.

Für alle eingesetzten Hardware-Komponenten im Server, wie z. B. Netzadapterkarten, Grafikkarten, Kommunikationsschnittstellen (seriell, parallel, USB, PS/2 usw.) oder SCSI-, IDE- und RAID-Controller, müssen u. a. folgende Informationen vorgehalten werden:

- Interrupt,
- E/A-Schnittstelle,
- DMA-Kanal,
- SCSI- und LUN-Adresse,
- Speicheradresse,
- Knotenadresse,

- Steckplatznummer,
- Externe IPX-Netzwerknummer und
- Rahmentyp.

Zur Dokumentation der Server-Hardware gehören auch die externen Geräte, wie z. B.

- Drucker oder
- externe Sub-Systeme (Festplattenschränke u. Ä.).

Als Beispiel und Hilfe kann hierfür in der Original-Dokumentation zu Novell Netware 4.11 (Handbuch zu Netware 4) im *Anhang C: Beispiel zu Schablonen* unter C8 nachgeschlagen werden.

Softwarekonfiguration

Ein weiterer wichtiger Punkt ist die Konfiguration der Software. Dazu gehören u. a. die folgenden Aspekte:

- Patchlevel,
- NLMs (Netware Loadable Modules),
- Treiber und
- Konfigurationsdateien (*AUTOEXEC.NCF*, *STARTUP.NCF*, *DHCPTAB*, etc., siehe auch die Beschreibung *CONFIG.NLM* und *Config-Reader*).

Da wichtige Programme unter Umständen nur ab einem bestimmten Patchlevel arbeiten, muss dokumentiert werden, welche Systemupdates notwendig sind, um die betroffenen Programme (wie z. B. Backup-Utilities) ausführen zu können. Aus diesem Grund sollte notiert werden, welche Updates und Patches zu welchem Zweck auf dem Netware Server installiert wurden.

Es sei an dieser Stelle auch auf ein Tool hingewiesen, mit dem diese Einzelheiten der Konfiguration abgefragt und in einer ASCII-Datei gespeichert werden können. Dabei handelt es sich um das Programm *CONFIG.NLM*. Dieses Programm muss an der jeweiligen Server-Konsole gestartet werden und erzeugt eine Datei *CONFIG.TXT*. Mit Hilfe des Windows-Programms *Config-Reader* kann diese Konfigurationsdatei analysiert werden. Beide Programme sind im Internet unter *http://support.novell.com* zu finden. In der Datei *CONFIG.TXT* wird in wenigen Sekunden die komplette Konfiguration des Netware Servers abgelegt. Dies vereinfacht den Wiederanlauf eines Servers bei Hardwareausfall wesentlich.

Ergänzende Kontrollfragen:

- Wurden alle relevanten Informationen zu den Netware Servern dokumentiert?
- Wird die Dokumentation regelmäßig aktualisiert?

M 2.154 Erstellung eines Computer-Virenschutzkonzepts

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Um für eine gesamte Organisation einen effektiven Computer-Virenschutz zu erreichen, sind abgestimmte und angemessene Schutzmaßnahmen auszuwählen und umzusetzen. Dies setzt eine konzeptionelle Vorgehensweise voraus, um sämtliche betroffenen IT-Systeme mit geeigneten Maßnahmen zu versehen und durch Aktualisierung den notwendigen Schutz aufrechtzuhalten.

Nachfolgend wird das Inhaltsverzeichnis eines Computer-Virenschutzkonzeptes aufgezeigt.

Inhaltsverzeichnis Computer-Virenschutzkonzept

Teil A: Sensibilisierung
1 Abhängigkeit der Institution vom IT-Einsatz
2 Beschreibung des Gefährdungspotentials
  2.1 Computer-Viren
  2.2 Makro-Viren
  2.3 Trojanische Pferde
  2.4 Hoax
3 Schadensszenarien
4 Potentiell betroffene IT-Systeme

Teil B: Erforderliche Schutzmaßnahmen
5 Computer-Virenschutz-Strategie
  5.1 Nicht-vernetzte IT-Systeme
  5.2 Vernetzte Endgeräte
  5.3 Server
6 Aktualisierung der Computer-Viren-Suchprogramme
  6.1 Nicht-vernetzte IT-Systeme
  6.2 Vernetzte Endgeräte
  6.3 Server

Teil C: Regelungen
7 Regelungen zum Schutz vor Computer-Viren
  7.1 Nutzungsverbot nicht freigegebener Software
  7.2 Schulung der IT-Benutzer
  7.3 Umstellung der Boot-Reihenfolge
  7.4 Anlegen einer Notfalldiskette
  7.5 Verhaltensregeln bei Auftreten eines Computer-Virus
  7.6 Maßnahmen bei nicht-resident virenkontrollierten IT-Systemen
  7.6.1 Regelmäßiger Einsatz eines Computer-Viren-Suchprogramms
  7.6.2 Virenkontrolle bei Datenträgeraustausch und Datenübertragung
  7.6.3 Prüfung eingehender Dateien auf Makro-Viren
8 Regelung der Verantwortlichkeiten
  8.1 Ansprechpartner für Computer-Viren
  8.2 Verantwortlichkeit von Administratoren
  8.3 Verantwortlichkeit des einzelnen IT-Benutzers
  8.4 Verantwortlichkeit des IT-Sicherheitsmanagements

Teil D: Hilfsmittel
10 Verhaltensregeln bei Auftreten eines Computer-Virus
11 Meldewege bei Auftreten eines Computer-Virus
12 Benutzerhandbuch des Computer-Viren-Suchprogramms

Die nachfolgenden Maßnahmen erläutern, wie einige wichtige Teile dieses Konzepts erstellt werden können.

Ergänzende Kontrollfragen:

- Ist das Computer-Virenschutzkonzept vom Management in Kraft gesetzt worden?
- Ist das Computer-Virenschutzkonzept allen Betroffenen bekannt?

M 2.155 Identifikation potentiell von Computer-Viren betroffener IT-Systeme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT

Für die Erstellung eines Viren-Schutzkonzeptes müssen in einem ersten Schritt die potentiell von Computer-Viren bedrohten IT-Systeme der Behörde/Institution identifiziert werden. Aus einer Übersicht aller IT-Systeme, die im Einsatz sind oder deren Einsatz geplant ist, können dazu alle IT-Systeme herausgefiltert werden, für die Computer-Viren eine Bedrohung darstellen oder über die Computer-Viren verteilt werden können.

Durch Computer-Viren sind typischerweise alle IT-Systeme mit PC-basierten Betriebssystemen wie DOS, Windows 3.x, 95/98 oder NT betroffen oder solche mit Anwendungsprogrammen wie Microsoft Word oder Excel, die durch Makro-Viren infiziert werden können.

Server werden zwar im allgemeinen nicht direkt durch Computer-Viren bedroht, können aber eine Verteilstelle für infizierte Programme und Dateien sein.

Es kann nicht ausgeschlossen werden, dass Computer-Viren auch bei Verwendung anderer Betriebssysteme oder IT-Anwendungsprogramme auftreten können. Dies gilt zum Beispiel in wenigen Einzelfällen bei Unix-Systemen und OS/2-Systemen, die jedoch aufgrund geringer Verbreitung nur ein niedriges Bedrohungspotential darstellen (siehe G 5.23 *Computer-Viren*).

Für jedes identifizierte IT-System kann in einem nächsten Schritt ergänzend erfasst werden, welche möglichen Infektionswege für Computer-Viren bestehen. Diese Informationen können für die spätere Auswahl von Maßnahmen genutzt werden. Eine Infektion durch Computer-Viren kann beispielsweise erfolgen:

- bei Einsatz von Disketten, CD-ROMs oder anderen austauschbaren Datenträgern,
- bei der Installation neuer Software,
- durch den Zugriff auf Dateien, die nicht auf der lokalen Festplatte gespeichert sind, sondern auf einem Server im Netz bzw. in einem freigegebenen Verzeichnis innerhalb eines Peer-to-Peer-Netzes,
- durch den Zugriff auf von externer Stelle erhaltene Dateien (z. B. Attachment einer E-Mail, Dateien aus dem Internet),
- bei extern vorgenommenen Wartungsarbeiten.

Sinnvoll ist es, für jedes identifizierte IT-System oder exemplarisch für jeden identifizierten IT-System-Typ tabellarisch zu erfassen, über welche Schnittstellen eine Computer-Vireninfektion erfolgen kann. Dies können sein:

- alle lokal am Rechner vorhandenen Lesegeräte für austauschbare Datenträger (Diskettenlaufwerk, CD-ROM-Laufwerk, Streamer, Wechselplatten u. a.),
- alle mobilen, an die Rechner lokal anschließbaren Lesegeräte für austauschbare Datenträger (Diskettenlaufwerk, CD-ROM-Laufwerk, Streamer, Wechselplatten u. a.),
- die Anbindung an andere IT-Systeme im eigenen Sicherheitsbereich (LAN-Server, Peer-to-Peer-Verbindungen),
- Schnittstellen, über die ein Datentransfer von externen IT-Systemen auf das lokale IT-System erfolgen kann (Modem, Internet-Anschluss).

Der wichtigste Punkt einer solchen Übersicht ist die Benennung von Ansprechpartnern für die jeweiligen IT-Systeme, die für die Realisierung der notwendigen Maßnahmen verantwortlich sind und die Anlaufstellen für die Benutzer sind. Da die IT-Landschaft einer Organisation ständigen Änderungen unterworfen ist, müssen im Hinblick auf Veränderungen an bestehenden Systemen diese Informationen bei Bedarf aktualisiert werden.

Beispiel für die Erhebung:

Vorhandene und geplante IT-Systeme / Schnittstellen					
Bezeichnung und Art	lokal vernetzt	lokale Lesegeräte	externe Lesegeräte	Kommunikationskarten	Ansprechpartner für Virenproblematik
Server Abt. X, Novell 4	x	Disketten-, CD-ROM-Laufwerk	Streamer	Modem	Administrator Müller
Clients Abt. X Windows 95	x	Disketten-, CD-ROM-Laufwerk			PC-Betreuer Meier
Laptops, Windows NT		Disketten-Laufwerk			Laptop-Verwaltung Schulze
Server Abt. XI, Unix	x	Disketten-, CD-ROM-Laufwerk	Streamer		Administratorin Schmitz
Workstations Abt. XI Unix	x				-
PC's Sekretariat Windows 95	x				Frau Peze
...	...	...	...	...	

Tabelle: Vorhandene und geplante Schnittstellen

Ergänzende Kontrollfrage:

- Wie wird sichergestellt, dass bei Veränderungen der eingesetzten IT-Systeme oder bei Einsatz neuer IT-Systeme die erforderlichen Maßnahmen des Virenschutz-Konzeptes berücksichtigt werden?

M 2.156 Auswahl einer geeigneten Computer-Virenschutz-Strategie

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT

Für die Umsetzung eines Computer-Virenschutzes sind personelle und finanzielle Ressourcen erforderlich, die in einem angemessenen Verhältnis zu dem tatsächlichen Bedrohungspotential stehen müssen. Für die Gesamtheit der identifizierten potentiell durch Computer-Viren bedrohten IT-Systeme sind folgende Einflussfaktoren zu erheben:

- Wie häufig findet über die vorhandenen Schnittstellen ein Datentransfer statt, der zu einer Infektion bzw. Verbreitung von Computer-Viren führen kann?
- Mit welchen Folgen ist bei einer tatsächlichen Infektion zu rechnen, wenn keine Schutzmaßnahmen ergriffen werden?
- Wie zuverlässig werden von den IT-Benutzern IT-Sicherheitsmaßnahmen durchgeführt, die periodisch zu veranlassen sind?
- Wieviel Zeitaufwand kann den IT-Benutzern für Computer-Viren-Schutzmaßnahmen zugemutet werden?

Bei Kenntnis der daraus und aus Fachveröffentlichungen ableitbaren Häufigkeit von Computer-Viren-Infektionen und der daraus entstehenden möglichen Folgeschäden ist unter Einbeziehung des Managements zu entscheiden, welche finanziellen Ressourcen für notwendige Maßnahmen zur Verfügung gestellt werden müssen und welche personellen Ressourcen bereitgestellt werden.

In Kenntnis der finanziellen und personellen Ressourcen, die für den Computer-Virenschutz zur Verfügung stehen, und der identifizierten potentiell bedrohten IT-Systeme können Strategien ausgewählt werden, wie ein geeigneter Schutz erreicht werden kann.

Einige mögliche Strategien werden im folgenden vorgestellt.

Computer-Viren-Suchprogramme auf jedem Endgerät

Erfolgt auf einem IT-System der Einsatz eines aktuellen residenten Computer-Viren-Suchprogramms (also eines Programmes, das permanent im Hintergrund läuft), wird sichergestellt, dass ein infiziertes Programm nicht ausgeführt oder eine Datei mit einem Makro-Virus nicht geladen werden kann. Die Kontrolle der Schnittstellen am Endgerät übernimmt das residente Suchprogramm. Dadurch wird gewährleistet, dass eine Übertragung auf das IT-System nicht erfolgt. Der ausschließliche Einsatz nicht-residenter Computer-Viren-Suchprogamme (die nur durch explizites Starten des Programms durch den Benutzer aktiviert werden) empfiehlt sich nicht, da hierdurch heute kein wesentlicher finanzieller Vorteil erzielbar ist, jedoch die Nachteile auf Seiten des IT-Benutzers erheblich zunehmen, da er zuverlässig regelmäßig das Programm aktivieren muss.

Werden alle Endgeräte mit einem residenten Computer-Viren-Suchprogramm ausgestattet, ist sichergestellt, dass Computer-Viren sofort nach Auftreten identifiziert und dass sie nicht vom Endgerät aus weitergegeben werden. Darüber hinaus sollte der Einzelaufruf auch bei residenten Viren-Suchprogrammen auf jedem Client möglich sein, um bei Bedarf, z. B. vor dem Öffnen von E-Mail-Attachments diese gezielt überprüfen zu können.

Vorteile:

- Ein geeignetes, aktuelles und residentes Computer-Viren-Suchprogramm gewährleistet einen maximalen Schutz bei gleichzeitig minimalen Aufwand für den IT-Benutzer

Nachteile:

- Anschaffungskosten sowie Administrationsaufwand fallen für jedes Endgerät an.
- Ältere IT-Systeme haben unter Umständen nicht ausreichend Hauptspeicher. Es könnte außerdem zu Komplikationen bei der Zusammenarbeit mit anderen Programmen kommen.

Computer-Viren-Suchprogramme auf allen Endgeräten mit externen Schnittstellen

In vernetzten IT-Systemen wird ein residentes Computer-Viren-Suchprogramm nur auf den IT-Systemen installiert, die neben Schnittstellen zum eigenen internen Netz über weitere externe Schnittstellen (Diskettenlaufwerk, CD-ROM, Modem) verfügen. Vernetzte IT-Systeme ohne direkte externe Schnittstellen werden nicht mit Computer-Viren-Suchprogrammen ausgestattet.

Vorteile:

- Anschaffungskosten sowie Administrationsaufwand reduzieren sich auf die IT-Systeme mit externen Schnittstellen.

Nachteile:

- Änderungen an den IT-Systemen, die zur Einrichtung neuer externer Schnittstellen führen, müssen akribisch nachgehalten werden, da ggf. die Nachrüstung von IT-Systemen mit Computer-Virersuchprogammen notwendig wird.
- Verschlüsselte Dateien oder Programme, die Computer-Viren beinhalten und erst auf einem ungeschützten Endgerät entschlüsselt werden, führen zu Infektionen. Dies kann in gleicher Weise auch für komprimierte Dateien gelten, wenn das Suchprogramm nicht geeignet ist.

Computer-Viren-Suchprogramme auf allen Servern

In diesem Fall wird in einem vernetzten IT-System jeder Server mit einem residenten Computer-Viren-Suchprogramm ausgestattet, die angeschlossenen Endgeräte jedoch nicht. Dadurch wird sichergestellt, dass keine Übertragung von Computer-Viren von einem Endgerät auf ein anderes Endgerät erfolgen kann und so eine mögliche Infektion lokal isoliert bleibt.

Vorteile:

- Anschaffungskosten sowie Administrationsaufwand reduzieren sich auf die Server.
- Schutz der Server verhindert Re-Infektionen, z. B. nach dem Einspielen von archivierten Dateien.

Nachteile:

- Für die Endgeräte mit externen Schnittstellen muss der Benutzer das auf dem Server befindliche Computer-Viren-Suchprogramm manuell starten, um damit eingehende externe Datenträger, aber auch zu versendende Datenträger und Dateien zu überprüfen.
- Verschlüsselte Dateien oder Programme, die Computer-Viren beinhalten und erst auf einem ungeschützten Endgerät entschlüsselt werden, führen ohne Eingangskontrolle zu Infektionen. Dies kann in gleicher Weise auch für komprimierte Dateien gelten, wenn das Suchprogramm nicht geeignet ist.
- Ein Computer-Viren-Befall eines Endgerätes mit externen Schnittstellen kann nicht ausgeschlossen werden.
- Wird zusätzlich eine Peer-to-Peer-Funktionalität genutzt, können Computer-Viren ohne Kontrolle der geschützten Server zwischen Endgeräten übertragen werden.
- Schlecht für die Performance, da alle Kommunikationsinhalte überprüft werden müssen.

Computer-Viren-Suchprogramme auf allen Servern und Endgeräten

Diese Kombination obiger Strategien bietet den maximalen Schutz, da Computer-Viren sofort beim Auftreten erkannt werden und nicht über Server weiterverteilt werden. Darüber hinaus können Computer-Viren-Suchprogramme verschiedener Hersteller eingesetzt werden, um so die Erkennungsrate für Computer-Viren zu erhöhen.

Vorteile:

- Ein geeignetes, aktuelles und residentes Computer-Viren-Suchprogramm gewährleistet einen maximalen Schutz bei gleichzeitig minimalen Aufwand für den IT-Benutzer.
- Computer-Viren werden nicht über Server weiterverteilt.

Nachteile:

- Anschaffungskosten sowie Administrationsaufwand für jeden Server und jedes Endgerät.

Computer-Viren-Suchprogramme auf den Kommunikationsservern

Computer-Virenschutzprogramme können ausschließlich oder zusätzlich auf allen Kommunikationsservern installiert werden, also den IT-Systemen über die der Datenaustausch mit externen IT-Systemen läuft, z. B. Firewalls oder Mailserver. Hierdurch sind aber die Endgeräte nur dann vor Computer-Viren

geschützt, wenn diese keine weiteren Schnittstellen wie CD-ROM-Laufwerke oder Ähnliches besitzen.

Vorteile:

- Alle Dateien werden am Eingang zum LAN überprüft, nicht erst innerhalb.
- Computer-Viren werden nicht über Server weiterverteilt. Allerdings können sie sich auf den Endgeräten weiterverbreiten, wenn zwischen diesen Dateien direkt (z. B. über Disketten) ausgetauscht werden.

Nachteile:

- Diese Methode ist fehleranfällig: Attachments an E-Mail werden u. U. nicht alle erkannt. Häufig wird von solchen Programmen das Vorhandensein von Attachments nur innerhalb der ersten Zeilen einer Mail bzw. im Mail-Header überprüft. Es kann auch vorkommen, dass das Verfahren, mit dem das Attachment behandelt wurde (z. B. uuencode) vom Virensuchprogramm nicht erfasst wird. Dies ist z. B. bei MIME möglich, es kann zu Problemen kommen, wenn eine oder mehrere mit uuencode codierte Dateien einfach in den Mailbody eingefügt werden.
- Schlecht für die Performance, da alle Kommunikationsinhalte überprüft werden müssen.
- Auf allen Kommunikationsservern sollte nur ein minimales Betriebssystem installiert sein, also nur die nötigsten Dienste (siehe auch M 4.95 *Minimales Betriebssystem*).
- Um Denial-of-Service-Angriffe zu vermeiden sollte ein Computer-Viren-Suchprogramm nie auf einer Firewall installiert werden, höchstens auf einem Proxy.

Datenhygiene und zentrale Prüfung von Dateien

Hierbei werden sämtliche eingehenden und ausgehenden Dateien und Datenträger an zentraler Stelle durch ein Computer-Viren-Suchprogramm kontrolliert. Darüber hinaus wird geregelt, dass die IT-Benutzer keine Dateien, Programme und Datenträger aus zweifelhafter Herkunft verwenden.

Vorteile:

- Die Anzahl der zu beschaffenden Lizenzen für Computer-Viren-Suchprogramme reduziert sich erheblich.

Nachteile:

- Bei häufigen Einsatz externer Datenträger nimmt eine zentrale Prüfung auf Computer-Viren sehr viel Zeit in Anspruch und verzögert den Geschäftsablauf. Ein Computer-Virenbefall kann grundsätzlich nicht ausgeschlossen werden, da ggf. die Prüfung eines Datenträgers versehentlich vergessen werden kann.
- In regelmäßigen Zeitabständen müssen alle Rechner ohne Computer-Viren-Suchprogramm auf einen möglichen Computer-Viren-Befall untersucht werden.

Unabhängig davon, welche Strategie für den Computer-Virenschutz gewählt wird, verbleibt immer das Restrisiko, dass Computer-Viren-Suchprogramme nur diejenigen Computer-Viren erkennen, die zum Entwicklungszeitpunkt des Programms bekannt waren. Das heißt, dass neue Viren ggf. nicht erkannt werden und Schäden anrichten können.

Die Wahl der richtigen und unter Kostengesichtspunkten angemessenen Strategie ist von der jeweiligen IT-Landschaft abhängig. Da jedoch beim Kauf von Mehrfach-Lizenzen der gängigen, geeigneten Computer-Viren-Suchprogramme sich meist die Kosten pro Lizenz stark reduzieren, empfiehlt es sich, über eine Komplettausstattung aller Server und Endgeräte nachzudenken.

Ergänzende Kontrollfragen:

- Sind in der Vergangenheit Computer-Viren aufgetreten? Welche Schäden wurden verursacht (finanzielle Einbußen, Arbeitsausfall, ...)?
- Wird die Entscheidung über den Ressourceneinsatz für den Computer-Virenschutz vom Management getragen?
- Ist sichergestellt, dass bei Änderungen der IT-Landschaft über eine Anpassung der Computer-Virenschutz-Strategie nachgedacht wird?
- Wurden die mit der gewählten Strategie verbundenen Nachteile dem IT-Sicherheitsmanagement verdeutlicht?
- Werden die entstehenden Restrisiken getragen?

M 2.157 Auswahl eines geeigneten Computer-Viren-Suchprogramms

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT

Bundesbehörden erhalten über das BSI aktuelle Viren-Schutzprogramme. Benutzer aus anderen Bereichen müssen aus der Vielzahl der am Markt verfügbaren Computer-Viren-Schutzprogramme für sie geeignete auswählen.

Für die ITSEC, den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik, wurde eine Funktionalitätsklasse für Anti-Virus-Produkte (F-AVIR) entwickelt. Auf diese kann bei der Auswahl eines geeigneten Viren-Suchprogramms zurückgegriffen werden.

In dieser Funktionalitätsklasse werden Sicherheitsfunktionen sowie Voraussetzungen für die sichere Arbeitsumgebung von Anti-Virus-Produkten beschrieben, die als Kriterien für die Auswahl eines geeigneten Computer-Viren-Suchprogramms herangezogen werden sollten. Band 2 der BSI-Schriftenreihe zur IT-Sicherheit "Informationen zu Computer-Viren" enthält einen Abdruck dieser Funktionalitätsklasse.

Im wesentlichen sollten folgende Bedingungen vom auszuwählenden Computer-Viren-Suchprogramm erfüllt werden:

- Der Umfang der erkannten Computer-Viren sollte möglichst groß sein und dem aktuell bekannten Bestand entsprechen, insbesondere müssen alle sehr stark verbreiteten Computer-Viren erkannt werden.
- Eine ständige Aktualisierung bezüglich neuer Computer-Viren muss vom Hersteller sichergestellt sein.
- Das Programm sollte Computer-Viren auch in komprimierter Form finden, wobei gängige Komprimierungsfunktionen wie PKZIP unterstützt werden sollten.
- Gefundene Computer-Viren müssen mit einer vollständigen Pfadangabe angezeigt werden.
- Das Programm muss seine eigene Virenfreiheit feststellen, bevor die Suchfunktion ausgeführt wird.
- Nach Möglichkeit muss das Produkt als residentes Programm eine permanente Computer-Virenkontrolle ermöglichen.
- Sinnvoll ist eine Funktionalität, die es erlaubt, erkannte Computer-Viren zu entfernen, ohne weitere Schäden an Programmen oder Daten zu verursachen.
- Das Programm sollte über eine Protokollierungsfunktion verfügen, die folgende Daten festhält:
  - Versionsstand des Programms,

- Datum und Uhrzeit der Überprüfung,
- Angabe aller benutzten Parameter,
- Prüfergebnis mit Prüfumfang,
- Anzahl und Identifikation der Dateien und Objekte, die nicht geprüft werden konnten.

- Das Programm sollte eine Warnung ausgeben, wenn es feststellt, dass es offensichtlich nicht aktualisiert wurde (zwischen Aktualitätsstand des Programms und Systemdatum liegen mehr als 6 Monate).
- Das Programm sollte eine Liste der erkennbaren Computer-Viren und ihre Beschreibung beinhalten. Darüber hinaus sind jeweils Beschreibungen von Sofortmaßnahmen und Maßnahmen zum Entfernen des Computer-Virus anzugeben.

M 2.158 Meldung von Computer-Virusinfektionen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT

Bei Auftreten eines Computer-Virus muss vorrangig verhindert werden, dass weitere IT-Systeme infiziert werden. Hierzu sollte ein Ansprechpartner in der Institution benannt werden, dem unverzüglich eine Computer-Virusinfektion gemeldet wird. Dieser kann auf der Basis der gemäß M 2.155 *Identifikation potentiell von Computer-Viren betroffener IT-Systeme* erstellten Unterlagen sofort entscheiden, welche Benutzer ggf. über das Auftreten eines Computer-Virus zu informieren sind. Diese Alarmierungswege sind ebenfalls im Rahmen dieses Meldewesens zu etablieren.

Neben den eigenen Mitarbeitern müssen auch alle Externen benachrichtigt werden, die eventuell durch die Virusinfektion mitbetroffen sind. Hierzu gehören insbesondere diejenigen, die mutmaßlich den Virus weitergegeben oder erhalten haben.

Für einen Überblick über die aktuelle Bedrohungslage durch Computer-Viren führt das BSI eine Statistik über alle aufgetretenen Viren-Infektionen. Dazu wurde ein Virus-Meldebogen herausgegeben, mit dem ein Viren-Vorfall erfasst wird. Diese Virus-Meldung wird vom BSI nur zu statistischen Zwecken verwendet; sie kann auch anonym abgegeben werden (Vordruck befindet sich im Anhang).

Über die benannten Ansprechpartner sind dann schließlich auch die Maßnahmen einzuleiten, die zu der Beseitigung des festgestellten Computer-Virenbefalls führen. Diese sollten alle Infektionen mit Computer-Viren, deren Auswirkungen und deren Beseitigung dokumentieren. Diese Informationen bilden eine Grundlage für die Aktualisierung des Virenschutzkonzeptes und dokumentieren aufgetretene Schadensfälle und die Aufwände zu deren Behebung.

Für die Einrichtung des Meldewesens ist es erforderlich, dass allen Mitarbeitern in geeigneter Form der Ansprechpartner bekannt gegeben wird. Dies kann beispielsweise in Form eines Merkblattes erfolgen (siehe M 6.23 *Verhaltensregeln bei Auftreten eines Computer-Virus*). Insbesondere beim Auftreten von Hoax (siehe G 5.80 *Hoax*) ist es wichtig, dass die Benutzer diese angeblichen Sicherheitshinweise nur an den für Virenproblematik benannten Ansprechpartner weitergeben und diesen nicht weiter streuen.

In gleicher Weise muss dieser Ansprechpartner sich regelmäßig über neu aufgetretene Computer-Viren informieren, damit er im Bedarfsfall eine Aktualisierung der Computer-Viren-Suchprogramme oder eine Alarmierung der Betroffenen veranlassen kann.

Ergänzende Kontrollfragen:

- Ist sichergestellt, dass der Ansprechpartner für Computer-Virusinfektionen allen IT-Benutzern bekannt ist?
- Ist sichergestellt, dass der Ansprechpartner schnellstmöglich sämtliche potentiell von einem akuten Computer-Virus Betroffenen alarmieren kann.

M 2.159 Aktualisierung der eingesetzten Computer-Viren-Suchprogramme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT

Für die mit Computer-Viren-Suchprogrammen ausgestatteten IT-Systeme muss eine regelmäßige Aktualisierung des Programms erfolgen, damit neu aufgetretene Computer-Viren zuverlässig erkannt werden können. Hierzu ist die Festlegung einer Vorgehensweise hinsichtlich der Verantwortlichkeit, der Beschaffung und der Verteilung der Updates erforderlich.

Bereits bei der Beschaffung eines geeigneten Computer-Viren-Suchprogramms (siehe M 2.157 *Auswahl eines geeigneten Computer-Viren*-Suchprogramms) sollte darauf geachtet werden, dass es in kurzen Zeitabständen (maximal halbes Jahr) aktualisiert wird. Da Virensuchprogrammen auch zu gegebenen Anlässen, z. B. aufgrund neuer Viren, aktualisiert werden, sollte der für die Virenproblematik Verantwortliche regelmäßig (zumindest wöchentlich) die Informationen des Herstellers abfragen.

Das BSI hat für den Bereich der Bundesbehörden eine Mailingliste für die Bekämpfung von Computer-Viren aufgebaut. Über diese Adressen-Liste werden aktuelle Informationen zur Viren-Problematik verteilt. Bei akuter Virengefahr wird in Zukunft eine Virenwarnung ausgegeben. Außerdem werden über diesen Weg Extra-Treiber für neue, bisher nicht erkannte Viren verteilt. In diese Mailingliste können Mitarbeiter von Behörden über das IVBB-Intranet unter *http://www.bsi.ivbb.bund.de/antivir/mailing.htm* oder über eine formlose E-Mail an *antivir@bsi.de* aufgenommen werden.

Bei der Verteilung der Updates des Viren-Suchprogramms muss auch sichergestellt werden, dass das Update auch tatsächlich - zeitnah mit der Beschaffung des Updates - auf den IT-Systemen eingespielt wird. Sofern dies nicht automatisiert (bei vernetzten IT-Systemen) erfolgen kann, sollte das Update den entsprechenden IT-Benutzern schnell zur Verfügung gestellt werden.

Durch die häufige Aktualisierung und die dadurch geringen Testzeiten der Virensuchprogramme sind diese fehleranfällig und müssen vor der Freigabe bzw. Installation im Wirkbetrieb getestet werden (siehe auch M 2.83 *Testen von Standardsoftware*). Bei der Installation von Updates ist insbesondere darauf zu achten, dass durch voreingestellte Parameter die bestehende Konfiguration des Computer-Viren-Suchprogramms nicht verändert wird. So könnte beispielsweise durch ein Update ein zuvor residentes Computer-Viren-Suchprogramm in einen Offline-Modus geschaltet werden.

Außerdem ist sicherzustellen, dass Rechner, die keiner einzelnen Person zugeordnet sind und nicht vernetzt sind, zum Beispiel Laptops, ebenfalls mit Updates versorgt werden.

Ergänzende Kontrollfragen:

- Wurden die für die Verteilung der Updates erzeugten Duplikate auf einem nachgewiesenermaßen nicht infiziertem IT-System erzeugt?
- Wie lange dauert die Einspielung eines Updates für alle IT-Systeme?
- Wird sporadisch überprüft, ob Aktualisierungen durchgeführt werden?

M 2.160 Regelungen zum Computer-Virenschutz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT

Um einen effektiven Computer-Virenschutz zu erreichen, müssen über den Einsatz von Computer-Anti-Viren-Programmen hinaus einige zusätzliche Maßnahmen realisiert werden. In diesem Sinne sind unter anderem folgende Punkte zu regeln:

Einsatz von Computer-Viren-Suchprogrammen

Entsprechend der ausgewählten Strategie und des ausgewählten Produktes ist der Einsatz festzulegen und zu dokumentieren (vergleiche M 2.156 *Auswahl einer geeigneten Computer-Virenschutz-Strategie*, M 2.157 *Auswahl eines geeigneten Computer-Viren-Suchprogramms*). Darüber hinaus ist zu regeln, wie, in welchen Abständen und durch wen die Computer-Anti-Viren-Programme aktualisiert werden (vergleiche M 2.159 *Aktualisierung der eingesetzten Computer-Viren-Suchprogramme*).

Schulung der IT-Benutzer

Die betroffenen IT-Benutzer sind bezüglich der Gefahren durch Computer-Viren, Makro-Viren, Trojanische Pferde und Hoax (vergleiche G 5.23 *Computer-Viren*, G 5.43 *Makro-Viren*, G 5.21 *Trojanische Pferde*, G 5.80 *Hoax*), der notwendigen IT-Sicherheitsmaßnahmen, der Verhaltensweise beim Auftreten von Computer-Viren und im Umgang mit dem Anti-Viren-Programm zu informieren bzw. zu schulen (vergleiche M 3.5 *Schulung zu IT-Sicherheitsmaßnahmen,* M 3.4 *Schulung vor Programmnutzung*, M 6.23 *Verhaltensregeln bei Auftreten eines Computer-Virus*).

Verbot der Nutzung nicht freigegebener Software

Die Installation und Nutzung nicht freigegebener, insbesondere nicht virenkontrollierter Software ist zu verbieten (vergleiche M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*). Darüber hinaus ist gegebenfalls zu regeln, dass regelmäßig Prüfungen auf Einhaltung des Verbots durchgeführt werden (vergleiche M 2.10 *Überprüfung des Hard- und Software-Bestandes*).

Schutzmaßnahmen am IT-System

Die Boot-Reihenfolge beim Betriebssystemstart ist so umzustellen, dass generell zuerst von der Festplatte (oder vom Netz) und dann erst von einem externen Medium (Diskette, CD-ROM) gestartet wird (vergleiche M 4.84 *Nutzung der BIOS-Sicherheitsmechanismen*). Zusätzlich ist für jeden vorhandenen Rechnertyp ein Notfallmedium anzulegen, um im Falle einer Computer-Vireninfektion eine erfolgreiche Säuberung zu ermöglichen (vergleiche M 6.24 *Erstellen eines Notfall-Bootmediums*). Für den Fall, dass ein neuer Computer-Virus dennoch Schäden verursacht, muss auf eine Datensicherung zurückgegriffen werden. Es sind daher regelmäßig Datensicherungen anzulegen (vergleiche M 6.32 *Regelmäßige Datensicherung*). Beim Wiedereinspielen von Datensicherungen muss darauf geachtet werden, dass damit keine vom Computer-Virus befallenen Dateien wiederaufgespielt werden.

Maßnahmen bei nicht-resident virenkontrollierter IT-Systeme

Generell sollte auf allen IT-Systemen ein residentes Computer-Anti-Viren-Programm installiert werden. Auf IT-Systemen, auf denen kein residentes Anti-Viren-Programm installiert worden ist, sind ersatzweise ein regelmäßiger Einsatz eines Computer-Viren-Suchprogramms (siehe M 4.3 *Regelmäßiger Einsatz eines Anti-Viren-Programms*) sowie eine Virenkontrolle bei Datenträgeraustausch und Datenübertragung (vergleiche M 4.33 *Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung*) festzulegen, um eine rasche Erkennung und Verhinderung der Weiterverbreitung von Computer-Viren sicherzustellen.

Meldung von Computer-Viren

Es ist zu regeln, an wen ein entdeckter Computer-Virus unverzüglich zu melden ist. Die Form der Meldung (Formblatt) und der Übermittlungsweg (telefonisch, persönlich, schriftlich, E-Mail) ist ebenfalls zu reglementieren (siehe M 2.158 *Meldung von Computer-Virusinfektionen*).

Regelung der Verantwortlichkeiten

Die Aufgaben, Kompetenzen und Verantwortlichkeiten für den Computer-Virenschutz sind zu regeln für

- den Ansprechpartner für Computer-Viren,
- den Administrator von Netzservern,
- den IT-Benutzer von Endgeräten und
- das IT-Sicherheitsmanagement.

Aktualisierung des Computer-Virenschutzkonzeptes

Bei Änderungen an IT-Systemen, bei Installation neuer IT-Systeme und bei Änderungen der Vernetzung ist das Computer-Virenschutzkonzept zu aktualisieren und anzupassen (vergleiche M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*).

Diese Regelungen sind den Betroffenen zur Kenntnis zu geben. Die Überprüfung der Einhaltung dieser Regelungen sollte sporadisch erfolgen, um ein durchgängig umgesetztes Computer-Virenschutzkonzept sicherzustellen.

Ergänzende Kontrollfragen:

- Wann wurde die letzte Überprüfung vorgenommen? Wurde das Ergebnis dokumentiert?
- Wie werden Betroffene über die relevanten Regelungen unterrichtet?

M 2.161 Entwicklung eines Kryptokonzepts

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Unternehmen und Behörden sind mittlerweile zunehmend von ihrer informationstechnischen Infrastruktur abhängig. Aus diesem Grund sind Sicherheitsdienste erforderlich und in ein Gesamtsystem zu integrieren, die über die bloße Verschlüsselung hinausgehen.

Aufgrund der Vielfalt kryptographischer Problemstellungen und unterschiedlicher Einflussfaktoren gibt es auch vielfältige Lösungsansätze und Realisierungsmöglichkeiten. Man kann nicht davon ausgehen, dass es eine Lösung gibt, die alle Sicherheitsprobleme in Rechnernetzen und/oder Kommunikationssystemen beseitigen kann. Vielmehr kommt es auf ein abgestimmtes Zusammenspiel passend ausgewählter Komponenten an, um den benötigten Grad an Sicherheit zu erreichen. Daher ist es erforderlich, ein Kryptokonzept zu entwickeln, das in das IT-Sicherheitskonzept der Behörde bzw. des Unternehmens integriert wird.

Die Auswahl geeigneter kryptographischer Komponenten muss dabei auf diesem Konzept basieren. Dabei ist das Schlüsselmanagement ein kritisches Element im gesamten Kryptokonzept. Konzepte und Lösungsansätze können nur dann erfolgreich erarbeitet und gezielt umgesetzt werden, wenn deutlich wird, welche speziellen Sicherheitsfunktionalitäten bzw. Sicherheitsdienste benötigt werden. Darüber hinaus gibt es eine Reihe systemrelevanter Fragestellungen und Aspekte, die nicht speziell in den Bereich der Sicherheitstechnik fallen. Dies umfasst z. B. Performanceanforderungen, Systemanbindungs- oder Interoperabilitäts- und Standardkonformitätsanforderungen.

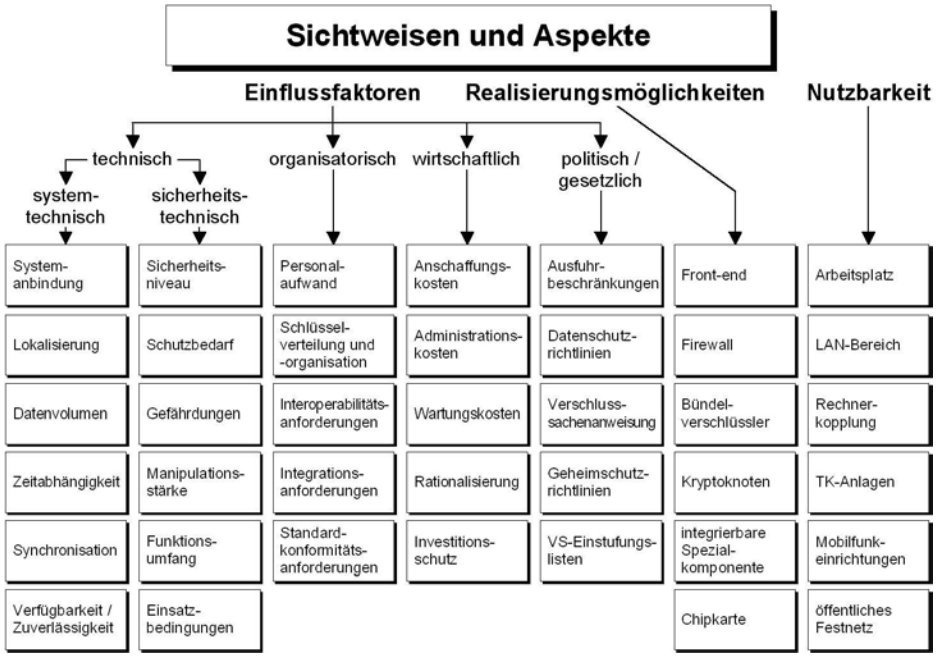


Abbildung: Sichtweisen und Aspekte

In vernetzten IT-Infrastrukturen ist es nicht mehr ausreichend, die Sicherheit einer einzelnen Domäne zu gewährleisten. Vielmehr muss die Sicherheit aller beteiligten Endeinrichtungen und Übertragungssysteme aufeinander abgestimmt werden. Diese Abstimmung gestaltet sich insbesondere in solchen Fällen als besonders schwierig, in denen es sich nicht nur um vernetzte Einrichtungen innerhalb einer organisatorischen Einheit (z. B. LAN-Umgebung), sondern um einen Verbund von IT-Installationen unterschiedlicher Zuständigkeits- und Anwendungsbereiche handelt.

Der Einsatz - aber auch die Funktionalität und technologische Ausgestaltung - eines IT-Sicherheitssystems wird von zahlreichen Einflussfaktoren bestimmt, wie z. B. Lokalisierung, Sicherheitsniveau, Häufigkeit und Umfang der Anwendung, die für das IT-Sicherheitsmanagement wichtige Rahmen- und Entscheidungsbedingungen darstellen. Des weiteren sind die technischen Möglichkeiten für die Realisierung und Gestaltung eines IT-Sicherheitssystems vielfältig, z. B. integriert in einer Applikation auf dem Arbeitsplatzrechner, in einer Firewall oder als Spezialkomponente für Netzkomponenten wie Switch oder Router. Ein erschwingliches Preisniveau für ein Kryptoprodukt ist nur durch eine querschnittliche Nutzbarkeit zu erzielen. Hier spielen z. B. eine standardisierte Systemanbindung, einheitliche Einsatzbedingungen etc. eine wichtige Rolle. Ein letzter Punkt betrifft das Zusammenwirken der Sicherheitsdienste auf unterschiedlichen Protokollschichten. Die Sicherheitsdienste der höheren Protokollschichten (nach OSI-Referenzmodell) schützen in aller Regel nur dann ausreichend, wenn die unteren Schichten ebenso einen Schutz bieten (siehe M 4.90 *Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI*-Referenzmodells).

Des weiteren ist die Definition einer organisationseigenen Kryptopolitik wichtig. Dabei muss aus Sicht des Managements geklärt werden,

- welcher Schutzbedarf besteht bzw. welches Sicherheitsniveau es zu erreichen gilt,
- welches Budget und wieviel Personal zur Verfügung stehen, um die geplanten Sicherheitsmechanismen einzurichten und - ganz wichtig - auch den Betrieb zu gewährleisten,
- welche Systemanbindung angestrebt wird bzw. welche Einsatzbedingungen für Sicherheitskomponenten vorherrschen,
- welcher Funktions- und Leistungsumfang anzupeilen ist und
- wer letztendlich die Verantwortung übernimmt.

Im Kryptokonzept ist außerdem der technische bzw. organisatorische Einsatz der kryptographischen Produkte zu beschreiben, also z. B.

- wer welche Zugriffsrechte erhält,
- welche Dienste remote angeboten werden,
- wie die Verwaltung von Passwörtern und Schlüsseln bezüglich Gültigkeitsdauer, Verwendung von Zeichen, Länge, Vergabe gehandhabt werden soll,

- ob, wann und wie die Daten verschlüsselt oder signiert werden müssen,
- wer mit wem kryptographisch gesichert bzw. ungesichert kommunizieren darf,
- wer bestimmte Rechte vergeben darf, usw.

In Abhängigkeit von den systemtechnischen Rahmenbedingungen bezüglich

- des zu betrachtenden Datenvolumens und der Zeitabhängigkeit,
- der Verfügbarkeitsanforderungen und Gefährdungslage,
- Art und Häufigkeit der zu schützenden Anwendungen etc.

können darauf basierend geeignete Realisierungsmöglichkeiten analysiert und für konkrete Einsatzbereiche wie z. B. einen PC-Arbeitsplatz, im LAN-Bereich oder in Verbindung mit einer TK-Anlage konzipiert und technisch ausgestaltet werden. Nur aufgrund einer solch ganzheitlichen Betrachtungsweise gelingt es, Entscheidungsgrundlagen und -bedingungen für kryptographische Produkte zusammenzutragen, deren Einsatz bzw. Verwendung sowohl sicherheitstechnisch angemessen als auch wirtschaftlich vertretbar ist. Es sollte jedoch darauf hingewiesen werden, dass die vorgenommene Einteilung keinesfalls zwingend oder von grundsätzlicher Bedeutung, sondern bestenfalls hilfreich ist. Wesentlich ist nur, dass der Fragenumfang die Vorstellung nach einer möglichst umfassenden Klärung der Ausgangslage konsequent widerspiegelt. Natürlich ergeben sich in der Praxis zwischen einigen Fragestellungen bzw. Antworten Wechselwirkungen und Abhängigkeiten, die im allgemeinen allerdings zur Vervollständigung des Gesamtbildes beitragen.

Die diversen Einflussgrößen für den Einsatz kryptographischer Verfahren sind zu bestimmen und nachvollziehbar zu dokumentieren (siehe M 2.163 *Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte*). Anschließend muss eine geeignete Verfahrensweise für ihren Einsatz entwickelt und dokumentiert werden. Zum Abschluss muss durch die Behörden- bzw. Unternehmensleitung die Durchführung angeordnet werden.

Die Ergebnisse sollten aktualisierbar und erweiterbar im Kryptokonzept niedergelegt werden. Ein möglicher Aufbau eines Kryptokonzepts ist im nachfolgenden Inhaltsverzeichnis beispielhaft aufgezeigt:

Inhaltsverzeichnis Kryptokonzept

1. Definitionen
- Kryptographische Verfahren
- ...

2. Gefährdungslage zur Motivation
- Abhängigkeit der Institution vom Datenbestand
- Typische Gefährdungen wie ...
- Institutionsrelevante Schadensursachen
- Schadensfälle im eigenen Haus

3. Festlegung einer organisationsinternen Sicherheitspolitik
- Festlegung von Verantwortlichkeiten
- Zielsetzung, Sicherheitsniveau

4. Einflussfaktoren

- Identifikation der zu schützenden Daten
- Vertraulichkeitsbedarf der Daten
- Integritätsbedarf der Daten
- Verfügbarkeitsanforderungen an die Daten
- Anforderungen an die Performance
- Schlüsselverteilung
- Datenvolumen
- Art der Daten (lokal / verteilt (LAN/WAN))
- Art der Anwendungen, bei denen kryptographische Verfahren zum Einsatz kommen sollen
- Häufigkeit des Einsatzes des kryptographischen Verfahrens
- Anforderungen an die Widerstandsfähigkeit der Algorithmen bzw. Verfahren (Manipulationsresistenz)
- Wiederherstellbarkeit der gesicherten Daten
- Personalaufwand
- Erforderliche Funktionalität
- Kosten einschließlich Folgekosten (Wartung, Administration, Updates, ...)
- Kenntnisse/datenverarbeitungsspezifische Qualifikationen der IT-Benutzer

5. Festlegung des Einsatzes

- Art der kryptographischen Verfahren
- Einsatzbedingungen an die kryptographischen Produkte
- Häufigkeit und Zeitpunkt des Einsatzes
- Benennung der Verantwortlichen
- Festlegung der organisatorischen Regelungen
- Durchführung der personellen Maßnahmen (Schulung, Vertretungsregelungen, Verpflichtungen, Rollenzuteilung)
- Dokumentation der Einsatzbedingungen / Konfiguration
- Interoperabilität, Standardkonformität, Investitionsschutz

6. Schlüsselmanagement

Einzelne Punkte dieses Konzepts werden in den Maßnahmen M 2.162 *Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte*, M 2.163 *Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte*, M 2.166 *Regelung des Einsatzes von Kryptomodulen* etc. näher ausgeführt.

Bei der Erstellung eines Kryptokonzepts handelt es sich nicht um eine einmalige Aufgabe, sondern um einen dynamischen Prozess. Ein Kryptokonzept muss daher regelmäßig den aktuellen Gegebenheiten angepasst werden.

Ergänzende Kontrollfragen:

- Ist das vorliegende Konzept aktuell?
- Sind sämtliche betroffenen IT-Systeme in diesem Konzept aufgeführt?
- Wie werden Mitarbeiter über den sie betreffenden Teil des Konzepts unterrichtet?
- Wird die Einhaltung dieses Konzepts kontrolliert?
- Wie werden Änderungen der Einflussfaktoren berücksichtigt?

M 2.162 Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Verantwortliche der einzelnen IT-Anwendungen

Um bei der Verarbeitung und Übertragung sensitiver Informationen zu realistischen, verlässlichen und anwendungsgerechten Bedarfsanforderungen und Rahmenbedingungen für den Einsatz kryptographischer Verfahren und Produkte zu kommen, müssen zunächst die schützenswerten Daten identifiziert und bewertet werden.

Identifikation der zu schützenden Daten

Zunächst muss festgestellt werden, für welche Aufgaben kryptographische Verfahren eingesetzt werden sollen und welche Daten damit gesichert werden sollen. Der Einsatz kryptographischer Verfahren kann aus verschiedenen Gründen erforderlich sein (siehe auch M 3.23 *Einführung in kryptographische Grundbegriffe*):

- zum Schutz der Vertraulichkeit bzw. der Integrität von Daten,
- zur Authentisierung,
- für Sende- oder Empfangsnachweise.

Je nach Einsatzzweck können verschiedene kryptographische Methoden wie z. B. Verschlüsselung oder Hashverfahren sinnvoll sein. Die typischen Einsatzfelder für kryptographische Verfahren sind:

1. lokale Verschlüsselung,
2. Kommunikationssicherung, auf Anwendungsebene bzw. auf Übertragungsebene,
3. Authentikation,
4. Nichtabstreitbarkeit,
5. Integrität.

Im folgenden werden einige Beispiele aus den verschiedenen typischen Einsatzfeldern für kryptographische Verfahren gegeben:

- Auf einer PC-Festplatte befinden sich Daten, die vor unbefugtem Zugriff durch Verschlüsselung geschützt werden sollen.
- Es sollen Informationen über Telefon, Fax oder Datennetze weitergegeben werden, z. B. sollen sie per E-Mail oder per Datenträgeraustausch versandt werden.
- Die zu schützenden Informationen sind nicht unter alleiniger Kontrolle der verantwortlichen Organisationseinheit (LAN führt durch Gebäudeteile, die von Fremdfirmen benutzt werden; ein Server mit Personaldaten wird durch Mitarbeiter betreut, die nicht zum Personalreferat gehören).
- Remote-Zugriffe sollen durch eine starke Authentisierung abgesichert werden.

- Bei E-Mails soll zweifelsfrei feststellbar sein, wer die Absender waren und ob die Inhalte unverändert übertragen wurden.

Um festzustellen, welche kryptographischen Verfahren bzw. Produkte benötigt werden und welche Daten damit zu schützen sind, sollte zunächst die aktuelle IT-Struktur ermittelt werden. Ermittelt werden sollte,

- welche IT-Systeme es gibt, auf denen Daten verarbeitet bzw. gespeichert (PCs, Laptops, Server, ...) oder mit denen Daten übermittelt werden (Bridge, Router, Gateway, Firewall, ...) und
- welche Übertragungswege es gibt. Dazu sollte die logische und physikalische Vernetzungsstruktur erfasst werden (siehe auch M 2.139 *Ist-Aufnahme der aktuellen Netzsituation*).

Schutzbedarf der Daten (Vertraulichkeit, Integrität, Authentizität, Nichtabstreitbarkeit)

Es sollten alle Anwendungen bzw. Daten ermittelt werden, bei denen ein besonderer Anspruch an Vertraulichkeit, Integrität, Authentizität bzw. Nichtabstreitbarkeit besteht. Allerdings werden nicht nur für IT-Systeme, Anwendungen oder Informationen mit höherem Schutzbedarf kryptographische Produkte benötigt, sondern auch für solche mit mittlerem Schutzbedarf.

Beispiele für Daten mit besonderem Vertraulichkeitssanspruch sind

- personenbezogene Daten,
- Passwörter und kryptographische Schlüssel,
- vertrauliche Informationen, deren Veröffentlichung Regressforderungen nach sich ziehen könnte,
- Daten, aus denen ein Konkurrenzunternehmen finanzielle Gewinne ziehen könnte,
- Daten, ohne deren Vertraulichkeit die Aufgabenerfüllung gefährdet ist (z. B. Ermittlungsergebnisse, Standortregister über gefährdete Pflanzen),
- Daten, deren Veröffentlichung eine Rufschädigung verursachen könnte.

Hinweis: Durch die Kumulation von Daten erhöht sich der Schutzbedarf einer Datensammlung, so dass eine Verschlüsselung erforderlich sein kann, auch wenn deren einzelne Datensätze nicht so sensitiv sind.

Beispiele für Daten mit besonderem Integritätsanspruch sind

- finanzwirksame Daten, durch deren Manipulation finanzielle Schäden entstehen können,
- Informationen, deren verfälschte Veröffentlichung Regressforderungen nach sich ziehen könnte,
- Daten, deren Verfälschung zu falschen Geschäftsentscheidungen führen kann,

- Daten, deren Verfälschung zu einer verminderten Produktqualität führen kann.

Ein Beispiel für Anwendungen mit besonderem Anspruch an Authentizität sind Remote-Zugriffe. Ein Beispiel für Daten mit besonderem Anspruch an Nichtabstreitbarkeit sind Bestellungen oder Reservierungen, bei denen der Besteller identifizierbar sein sollte.

Als Ergebnis der Schutzbedarfsfeststellung sollte festgelegt werden, welche Anwendungen oder Daten kryptographisch gesichert werden sollen. Diese Festlegung kann später noch verfeinert werden und sollte regelmäßig überarbeitet werden.

Als Resultat ergibt sich somit ein Überblick über alle Speicherorte und Übertragungsstrecken, die kryptographisch gesichert werden müssen. Damit erhält man praktisch eine IT-Landschaftskarte mit markierten Kryptobereichen.

Bedarfs- und Anforderungsabfrage

Als Hilfsmittel für eine derartige Bedarfserhebung bietet sich ein Fragenkatalog mit den in der Abbildung dargestellten Gliederungspunkten an. Dabei können die technischen, organisatorischen und wirtschaftlichen Aspekte jeweils in 4 weitere Unterkategorien aufgeteilt werden.

Technische Aspekte	**Organisatorische Aspekte**	**Wirtschaftliche Aspekte**
Benutzerdienste und Anwendungen	Einsatzbereich	Rationalisierungsaspekte / Kosteneinsparungen
Nutzungsprofil	Migrationskonzept	Stückzahlen
Netzinfrastruktur	Zeitvorstellungen	Beschaffungskosten
IT-Endgerät	Betriebliche Rahmenbedingungen	Administrations- und Wartungsaufwendungen

Abb: Gliederungsgesichtspunkte zur Erstellung eines Fragenkataloges

Bei den technischen Aspekten ist es unter "Benutzerdienste und Anwendungen" beispielsweise wichtig zu erfahren, ob vornehmlich Echtzeit- oder Nicht-Echtzeit-Daten betrachtet werden. In der Kategorie Nutzungsprofil ist zu erfragen, für welche Anwendungen und Daten kryptographische Verfahren eingesetzt werden sollen, z. B. für die externe Kommunikation oder für die kurzzeitige oder längerfristige Bearbeitung von VS-Daten. Weiterhin sind die Netzinfrastruktur und das Endgerät betreffende Informationen zu ermitteln, wie z. B. Anschlusskonfiguration.

Als organisatorische Aspekte sind der Einsatzbereich, d. h. Teilnehmer- oder Netzbereich; die Frage nach einem existierenden Migrationskonzept sowie die Zeitvorstellungen und betrieblichen Rahmenbedingungen des Endbenutzers zu betrachten.

Aus wirtschaftlicher Sicht sind die wesentlichen Punkte:

- Rationalisierungsaspekte, z. B. durch Einsatz eines Produktes mit transparenter Verschlüsselung statt manueller Ansteuerung,
- eine Abschätzung im Hinblick auf Stückzahlen und Beschaffungskosten sowie
- die zu erwartenden Administrations- und Wartungskosten.

Auf Basis dieser Abfrage kann ein möglichst praxisnahes Einsatz- und Anforderungskonzept erstellt werden, was dann als Ausgangspunkt für konkrete Realisierungsentscheidungen bzw. die Auswahl geeigneter Kryptokomponenten/-produkte (siehe M 2.165 *Auswahl eines geeigneten kryptographischen Produktes*) dient.

Die hier vorgestellte Vorgehensweise soll dem Sicherheitsverantwortlichen helfen, den Einsatz und den Umfang einzusetzender Sicherheitstechnik in unterschiedlichen Systemlokalitäten, Netzübergängen und Endeinrichtungen festzustellen, zu bewerten und zu koordinieren. Ferner soll im Verlauf der Planungsphase durch die Ermittlung des notwendigen Schutzes (Schutzbedarf) die Frage nach Angemessenheit der IT-Sicherheit beantwortet werden. Die skizzierte Vorgehensweise stellt einen pragmatischen Ansatz dar und berücksichtigt Sicherheitsaspekte in offenen, verteilten IT-Infrastrukturen, so wie sie sich vielerorts darstellen.

Die so betrachteten Sicherheitsinvestitionen müssen für den betroffenen Einsatzbereich wirtschaftlich vertretbar sein. Die Funktions- und Betriebsweise von realisierten Sicherheitsstrategien müssen den Erwartungen der Endbenutzer hinsichtlich der Flexibilität, Transparenz und Performance Rechnung tragen. Die geplanten und integrierten Sicherheitsdienste dürfen den Endbenutzer nicht über das notwendige Maß hinaus einschränken.

M 2.163 Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Verantwortliche der einzelnen IT-Anwendungen

Bevor eine Entscheidung getroffen werden kann, welche kryptographischen Verfahren und Produkte eingesetzt werden sollen, müssen eine Reihe von Einflussfaktoren ermittelt werden. Dazu können die Systemadministratoren und die Verantwortlichen der einzelnen IT-Systeme bzw. IT-Anwendungen befragt werden. Die Ergebnisse sind nachvollziehbar zu dokumentieren.

Für sämtliche in M 2.162 *Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte* festgelegten Speicherorte und Übertragungsstrecken sind folgende Einflussfaktoren zu ermitteln:

Sicherheitsaspekte

- Welcher Schutzbedarf besteht bzw. welches Sicherheitsniveau gilt es zu erreichen?
- Welche kryptographischen Funktionen sind dafür notwendig (Verschlüsselung, Integritätsschutz, Authentizität und/oder Nichtabstreitbarkeit)?
- Angreiferpotential: Mit welchen Angreifern wird gerechnet (zeitliche und finanzielle Ressourcen, technische Fähigkeiten)?

Die Antworten auf diese Fragen ergeben sich aus M 2.162 *Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte*.

Technische Aspekte

Der Betrieb von weitverzweigten IT-Infrastrukturen mit ihrer Vielzahl von Einzelkomponenten und Spezialeinrichtungen (Netzknoten, Server, Datenbanken, etc.) macht ein ebenfalls weit verzweigtes Sicherheitssystem mit mehreren Funktionseinheiten (Sicherheitsmanagement, Sicherheitsserver, Sicherheitsanwenderkomponente, etc.) erforderlich. In der Regel müssen dabei Systembetrachtungen angestellt werden, die nicht nur auf die eigentlichen Funktionalitäten abzielen, sondern auch bauliche und organisatorische Aspekte einbeziehen. Auch in bezug auf die konkrete technische Platzierung von Sicherheitskomponenten sowie deren Integration in Nicht-Sicherheitskomponenten gilt es zu differenzieren, da dies einen unmittelbaren Einfluss auf die Implementierung der Sicherheitsfunktionen, auf die notwendige Unterstützung durch die Betriebssysteme, die Aufwände und den Kostenfaktor und nicht zuletzt auf die erreichbare Sicherheit hat. Ganz entscheidend für die Sicherheitsbewertung ist der Umstand, an welchen geographischen Lokalitäten und in welchen Ebenen des Protokollstacks die jeweiligen Sicherheitsdienste realisiert sind und wie diese in die Prozesse des zu schützenden IT-Systems eingebunden sind. Somit ergeben sich als Fragen:

- Umfeldschutz: Welchen Schutz bietet das Umfeld (infrastrukturell (Zutritt), organisatorisch, personell, technisch (Schutz durch Betriebssystem, ...))?
- IT-Systemumfeld: Welche Technik wird eingesetzt, welche Betriebssysteme, etc.?
- Datenvolumen: Welches Datenvolumen ist zu schützen?
- Häufigkeit: Wie häufig besteht Kryptierbedarf?
- Performance: Wie schnell müssen kryptographische Funktionen arbeiten (Offline, Online-Rate)?

Personelle und organisatorische Aspekte

- Benutzerfreundlichkeit: Benötigen die Benutzer für die Bedienung kryptographische Grundkenntnisse? Behindert der Einsatz eines Kryptoprodukts die Arbeit?
- Zumutbarkeit: Wie viel Belastung durch zusätzliche Arbeit ist dem Anwender zumutbar (Arbeitszeit, Wartezeit)?
- Zuverlässigkeit: Wie zuverlässig werden die Benutzer mit der Kryptotechnik umgehen?
- Schulungsbedarf: Inwieweit müssen die Benutzer geschult werden?
- Personalbedarf: Ist zusätzliches Personal erforderlich, z. B. für Installation, Betrieb, Schlüsselmanagement?
- Verfügbarkeit: Kann durch den Einsatz eines Kryptoprodukts die Verfügbarkeit reduziert werden?

Wirtschaftliche Aspekte

- Finanzielle Randbedingungen: Wie viel darf der kryptographische Schutz kosten? Wie hoch sind die
  - einmaligen Investitionen,
  - laufenden Kosten, inklusive der Personalkosten,
  - Lizenzgebühren?
- Investitionsschutz: Sind die geplanten kryptographischen Verfahren bzw. Produkte konform zu bestehenden Standards? Sind sie interoperabel mit anderen Produkten?

Key Recovery

Falls die zur Verschlüsselung benutzten Schlüssel verloren gehen, sind im allgemeinen auch die damit geschützten Daten verloren. Viele Kryptoprodukte bieten daher Funktionen zur Datenwiedergewinnung für solche Fälle an. Bevor solche Funktionen eingesetzt werden, sollte man sich auch deren Risiken klar machen: Wenn dadurch vertrauliche Schlüssel wiederhergestellt werden können, muss sichergestellt sein, dass dies nur Berechtigte können. Wenn es möglich ist, ohne Wissen des Original-Schlüsselbenutzers auf dessen Daten zuzugreifen, hat dieser keine Möglichkeit, böswillige Manipulationen zu beweisen. Der Einsatz von Key Recovery Mechanismen führt auch häufig

aufgrund des entgegengebrachten Misstrauens zu Vorbehalten innerhalb des eigenen Unternehmens bzw. Behörde, aber auch bei den Kommunikationspartnern. Bei der Datenübertragung sollte daher generell auf Key Recovery verzichtet werden. Hierfür gibt es auch keine Notwendigkeit, da beim Schlüssel- oder Datenverlust diese einfach noch einmal ausgetauscht werden können. Bei der lokalen Speicherung von Daten sollte der Einsatz sorgfältig überlegt werden (siehe auch M 6.56 *Datensicherung bei Einsatz kryptographischer Verfahren*). Unter den Hilfsmitteln zum IT-Grundschutz befindet sich ein Artikel zu Möglichkeiten und Risiken des Key-Recovery.

Lebensdauer von kryptographischen Verfahren

Kryptographische Verfahren und Produkte müssen regelmäßig daraufhin überprüft werden, ob sie noch dem Stand der Technik entsprechen. Die verwendeten Algorithmen können durch neue technische Entwicklungen, z. B. schnellere, billigere IT-Systeme, oder durch neue mathematische Erkenntnisse zu schwach werden. Die eingesetzten kryptographischen Produkte können Implementierungsfehler aufweisen. Bereits bei der Auswahl kryptographischer Verfahren sollte daher eine zeitliche Grenze für deren Einsatz festgelegt werden. Zu diesem Zeitpunkt sollte noch einmal gründlich überdacht werden, ob die eingesetzten Kryptomodule noch den erwarteten Schutz bieten.

Gesetzliche Rahmenbedingungen

Beim Einsatz kryptographischer Produkte sind diverse gesetzliche Rahmenbedingungen zu beachten. In einigen Ländern dürfen beispielsweise kryptographische Verfahren nicht ohne Genehmigung eingesetzt werden. Daher muss untersucht werden (siehe M 2.165 *Auswahl eines geeigneten kryptographischen Produktes*),

- ob innerhalb der zum Einsatzgebiet gehörenden Länder Einschränkungen beim Einsatz kryptographischer Produkte zu beachten sind (innerhalb Deutschland gibt es keinerlei Einschränkungen) und
- ob für in Frage kommende Produkte Exportbeschränkungen beachtet werden müssen.

Es gibt allerdings nicht nur Maximalanforderungen, sondern auch Minimalanforderungen an die verwendeten kryptographischen Algorithmen oder Verfahren. So müssen z. B. bei der Übermittlung von personenbezogenen Daten Verschlüsselungsverfahren mit ausreichender Schlüssellänge eingesetzt werden.

Technische Lösungsbeispiele:

Im folgenden finden sich einige Anwendungsbeispiele zu den verschiedenen Einsatzfeldern für kryptographische Verfahren. Dabei ist zu sehen, dass die meisten Produkte gleich mehrere Einsatzfelder abdecken.

Beispiel 1: Festplattenverschlüsselung

Die auf der Festplatte eines Stand-Alone-PC gespeicherten sensitiven Daten sollen so geschützt werden, dass

- der PC nur von autorisierten Nutzern gebootet werden kann,
- nur autorisierte Nutzer Zugriff auf die gespeicherten Daten erhalten,
- die gespeicherten Daten bei abgeschaltetem PC - auch im Falle des Diebstahls - hinreichend vor Kenntnisnahme durch Unberechtigte geschützt sind.

Im Vordergrund soll hier der Schutz der Vertraulichkeit stehen. Dabei soll der PC gegen die folgenden Bedrohungen geschützt werden:

- Unbefugte Kenntnisnahme der auf der Festplatte gespeicherten Daten
- Manipulation der auf der Festplatte gespeicherten Daten
- Manipulation des Kryptosystems

Bei Diebstahl bzw. Verlust des PC oder der Festplatte steht dem Angreifer sehr viel Zeit für die unbefugte Kenntnisnahme zur Verfügung. Eine Schutzmaßnahme muss auch bei solchen Langzeitangriffen die Vertraulichkeit der gespeicherten Daten gewährleisten.

Als Schutzmaßnahme soll daher ein Produkt mit Boot-Schutz und Festplattenverschlüsselung eingesetzt werden. Auf dem Markt sind verschiedene Lösungen verfügbar. Zum Einsatz kann entweder eine Verschlüsselungs-Software (Lösung A), eine Verschlüsselungs-Hardware-Komponente (Lösung B) oder eine Kombination aus Hardware- und Software-Komponente (Lösung C) kommen. Lösung C wird typischerweise aus einer Verschlüsselungs-Software in Kombination mit einem Chipkartenleser zur Zugangskontrolle bestehen. Welche Lösung gewählt werden sollte, hängt von verschiedenen Entscheidungskriterien ab:

- Sicherheit (Kryptoalgorithmus und Schlüssellänge, Betriebsart der Verschlüsselung, Zugriffsschutz, Schlüsselerzeugung/ -verteilung/ -speicherung/ -eingabe, Einbindung in das Betriebssystem, etc.)

  Je nachdem, auf welcher Betriebssystem-Plattform Verschlüsselung betrieben wird, stößt man mit Software-Lösungen (Lösungen A oder C) unweigerlich an Grenzen. Kann man kein sicheres Betriebssystem mit strikter Task- und Speicherbereichs-Trennung voraussetzen (bisher ist das bei keinem Betriebssystem sicher nachgewiesen!), muss der während der Ver- bzw. Entschlüsselung verwendete Schlüssel zumindest kurzzeitig ungeschützt im Speicher des PC gehalten werden. Die Vertraulichkeit des Schlüssels ist somit nicht mehr sichergestellt. Hardware-Verschlüsselungs-Komponenten (Lösung B) können (müssen aber nicht!) mehr bieten. Der Schlüssel kann in die Hardware-Komponente geladen und dort - gegen Auslesen gesichert - gespeichert werden. Der Schlüssel wird die Hardware-Komponente nicht mehr verlassen und ist vor Ausspähversuchen geschützt. Er kann nur durch berechtigte Benutzer mittels Besitz und Wissen (z. B. Chipkarte und Passwort) aktiviert werden. Wichtig sind weitere Aspekte wie die zur Verschlüsselung verwendeten Algorithmen (meist ein Blockchiffrier-Algorithmus), deren Betriebsarten (z. B. CBC) sowie die Art und Weise der Einbindung in das PC-System. Die Verschlüsselungs-Hardware sollte idealerweise so eingebunden werden, dass sie die gesamte Festplatte zwangsweise kryptiert und durch Angriffe nicht unbemerkt abgeschaltet bzw. umgangen werden kann. Werden im Gegensatz dazu le-

diglich einzelne Dateien verschlüsselt besteht die Gefahr, dass die Inhalte dieser Dateien unkontrollierbar zumindest teilweise zusätzlich im Klartext auf die Festplatte geschrieben werden (z. B. in den Auslagerungsdateien verschiedener Betriebssysteme oder in Backup-Dateien).

- Performance (Geschwindigkeit der ausführbaren Programme)

  Software-Verschlüsselung nutzt die Systemressourcen des PC, belastet also die CPU und benötigt Arbeitsspeicher. Spätestens bei der Verschlüsselung der gesamten Festplatte wird die Performance des PC sinken. Hardware-Komponenten mit eigenem Prozessor können die Verschlüsselung ohne Belastung der PC-CPU und somit ohne nennenswerten Performanceverlust durchführen. Hier ist je nach Bauart die Durchsatzrate der verwendeten Kryptier-Hardware mitentscheidend.

- Organisatorischer/Personeller Aufwand (Administration, Keymanagement, Schulung, etc.)

  Der organisatorische bzw. personelle Aufwand ist von der Umsetzung der Sicherheitspolitik und dem "Komfort" der Verschlüsselungs-Komponenten abhängig. Generelle Entscheidungskriterien für oder gegen eine der drei Lösungen können nicht allgemein gültig formuliert werden.

- Wirtschaftlichkeit (Anschaffung, Schulungs-/Administrationskosten, ...)

  Eine allgemeine Aussage zur Wirtschaftlichkeit ist schwierig. Betrachtet man nur die Anschaffungskosten, so werden Software-Lösungen oft preiswerter sein als Hardware-Lösungen. Kalkuliert man dagegen auch die Schäden ein, die durch unzureichenden Schutz auf längere Sicht entstehen können, kann sich im Vergleich die Investition in sicherere und vielleicht teurere Lösungen lohnen. Wirtschaftliche Nachteile können u. U. durch Performanceverlust des PC-Systems entstehen.

- Restrisiken (Betriebssystem, Kompromittierung des Festplattenschlüssels, etc.)

  Bei der Auswahl der geeigneten Verschlüsselungs-Komponente spielt die Restrisikobetrachtung eine wesentliche Rolle. Es stellen sich u. a. die Fragen

  - Welche Restrisiken kann man in Kauf nehmen? und
  - Welche Restrisiken werden bzw. können durch andere Maßnahmen (z. B. materielle oder organisatorische Maßnahmen) minimiert werden?

  Es können sich durchaus mehrere tragbare Lösungsmöglichkeiten durch die Kombination verschiedener Maßnahmen ergeben.

Beispiel 2: E-Mail-Verschlüsselung

Der Austausch von elektronischer Post (E-Mail) über bzw. in Computer-Netzen gewinnt zunehmend an Bedeutung. Werden dabei sensible Informationen (z. B. Firmengeheimnisse) über ungesicherte Netze ausgetauscht, so sind dabei Mechanismen zum Schutz der Vertraulichkeit bzw. für die Gewähr der Authentizität von Nachrichten erforderlich. Zu diesen Zwecken dienen

E-Mail-Verschlüsselungsprogramme. Am weitesten verbreitet sind dabei zwei Programmpakete bzw. Standards amerikanischer Herkunft:

- PGP ("Pretty Good Privacy") und
- S/MIME (Secure Multipurpose Internet Mail Extensions).

Dabei ist PGP ein Programmpaket, das ursprünglich als Freeware im Internet erhältlich war und sich daher weit verbreitet hat. Der S/MIME Standard wird u. a. von den Secure-E-Mail Anwendungen der Firmen Microsoft, Netscape und RSA Data Security Inc. verwendet.

Was muss ein solches E-Mail-Verschlüsselungsprogamm leisten?

Die Antwort hängt zu einem gewissen Grad natürlich von den umgebenden Sicherungsmaßnahmen ab. Die Anforderungen sind sicherlich dann am größten, wenn die Nachrichten über ein großes, offenes, ungesichertes Netz wie z. B. das Internet verschickt werden sollen. Hier wollen eventuell sogar einander persönlich Unbekannte vertraulich und authentisch miteinander kommunizieren. Welche kryptographischen Dienste sind dazu erforderlich?

Vertraulichkeit

Da die Nachrichten verschlüsselt werden sollen, müssen (einer oder mehrere) Verschlüsselungsalgorithmen implementiert sein. Dazu bieten sich wegen der höheren Performance symmetrische Verfahren an.

Schlüsselmanagement

- Erzeugung: die Schlüssel für das symmetrische Verfahren müssen durch einen geeigneten (Zufalls-) Prozess so erzeugt werden, dass Erraten bzw. Vorhersage weiterer Schlüssel auch bei Kenntnis einiger vorhergehender Schlüssel praktisch unmöglich ist.
- Schlüsseleinigung/Austausch: da eine zentrale Schlüsselversorgung mittels symmetrischer Verfahren im Internet schon wegen der schieren Masse der möglichen Kommunikationspartner ausscheidet, ist die Verwendung asymmetrischer Verfahren für Schlüsseleinigung bzw. Schlüsselaustausch geboten.

Authentizität

Da aufgrund der Anforderungen aus dem Schlüsselmanagement ohnehin ein asymmetrisches Verfahren implementiert ist (und evtl. Verbindlichkeit verlangt wird), wird man zu diesem Zweck eine digitale Signatur einsetzen. Signaturschlüssel sollten dabei ausschließlich zu Signaturzwecken verwendet werden. Dabei muss - wie immer bei der Verwendung von Public-Key-Verfahren - das Problem der Authentizität der öffentlichen Schlüssel gelöst werden.

Verbindlichkeit

Verbindlichkeit setzt eine Public-Key-Infrastruktur voraus (PKI, Registrierung von Teilnehmern und Zertifizierung von öffentlichen Schlüsseln durch eine vertrauenswürdige dritte Instanz, inkl. Einsatzregeln). Bisher existiert allerdings keine globale PKI, daher ist es schwierig, für E-Mails von vorher unbekannten Teilnehmern einen verbindlichen Herkunftsnachweis zu bekom-

men. In einem lokalen Netz wäre zu diesem Zweck eine geeignete PKI zu schaffen.

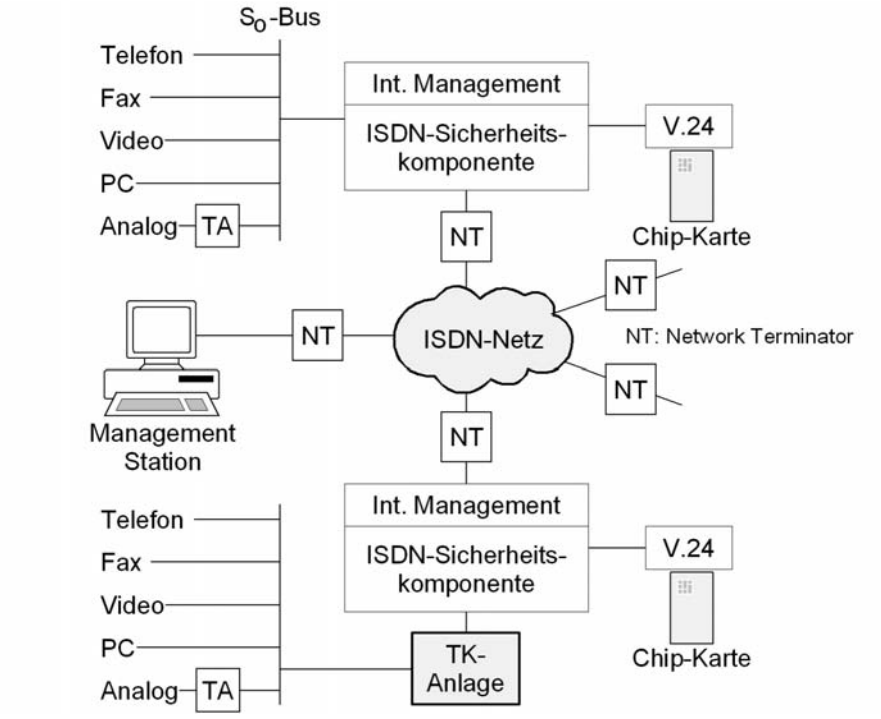
Standardkonformität

Aus Interoperabilitätsgründen und zum Investitionsschutz ist es sinnvoll, möglichst weit verbreitete und akzeptierte Internet-Standards zu verwenden. Sowohl S/MIME als auch PGP befinden sich im Stadium der Standardisierung.

Beispiel 3: Sichere Sprach- und Datenkommunikation bei ISDN-Netzanbindungen

Beim folgenden Anwendungsbeispiel wird die Kommunikation per ISDN betrachtet. Geschützt werden sollen die Anwendungen "Telefonverkehr" und "Videokonferenzen" sowie der Datenverkehr zwischen Rechnernetzen. Als Ziel soll ein wirkungsvoller Schutz übermittelter vertraulicher Informationen und verbindlicher personenbezogener Daten gewährleistet werden. Es wird davon ausgegangen, dass alle zu übertragenen Informationen in digitaler Form (PCM-Code) vorliegen und dass die in firmeneigenen Netzen und TK-Anlagen übliche Sprachkomprimierung für verschlüsselte Anwendungen abgeschaltet werden kann, damit die Nutzkanäle (B-Kanäle) verschlüsselt werden können.

Dafür soll eine ISDN-Sicherheitskomponente eingesetzt werden, mit der ein S0-Anschluss mit zwei 64 kbit/s-Kanälen abgesichert werden kann. Dabei ist es unerheblich, ob am S0-Bus einzelne ISDN-Endgeräte (Telefon, Fax, PC mit ISDN-Einsteckkarte etc.) angeschlossen sind oder eine kleine TK-Anlage nachgeschaltet ist. Alle Verbindungen sollen wahlweise verschlüsselt oder unverschlüsselt aufgebaut und betrieben werden. Folgende Abbildung zeigt die entsprechende Systemkonfiguration.



Es wurde ein ISDN-Kryptogerät ausgewählt, das mittels einer Chipkarte gegen unbefugte Benutzung abgesichert werden kann. Alternativ steht auch eine serielle V.24-Schnittstelle zur Verfügung, um die Sicherheitskomponente mit Hilfe eines PC konfigurieren zu können. Der Benutzer oder die Endanwendung kann die Verschlüsselung direkt mit der Chipkarte bzw. durch die Vorwahl einer speziellen Kennziffer steuern. Auch ist es möglich, die ISDN-Sicherheitskomponente so zu konfigurieren, dass bestimmte Verbindungen (Nummern) verschlüsselt oder unverschlüsselt voreingestellt sind. Für das Schlüsselmanagement, d. h. die Generierung und Verteilung von Schlüsselzertifikaten wird an einer zentralen Stelle des ISDN-Netzes eine Managementstation angeschlossen. Somit ist sichergestellt, dass die einzelnen ISDN-Sicherheitskomponenten netzweit registriert und mit aktuellem Schlüsselmaterial versorgt werden können.

Die Möglichkeit des sicheren Transports von Informationen und schützenswerten Daten in einem ISDN-Netz sind vielfältig und komplex. Dabei muss jeder relevanten Grundbedrohung mit einer konkreten Sicherheitsmaßnahme begegnet werden. Zur Gewährleistung der Vertraulichkeit erfolgt eine Online-Verschlüsselung des übertragenen Datenstroms am wirkungsvollsten auf der Sicherungsschicht. Hierzu werden die Daten vor ihrer Übertragung von einer Kryptohardware automatisch verschlüsselt und auf der Empfängerseite wieder entschlüsselt. Die Verschlüsselung ist dabei vollständig transparent für den Endteilnehmer und für Anwenderprogramme. Das verwendete Kryptomodul ermöglicht nicht nur eine Echtzeitverarbeitung, sondern bietet - im Vergleich zu einer Dateiverschlüsselung (Softwarelösung) - einen höheren Schutz gegen Angriffsversuche. Zur Sicherung der Übersendung von verbindlichen oder beweispflichtigen Daten können diese zusätzlich mit einer digitalen Signatur des Absenders versehen werden. Damit kann die Herkunft und Echtheit der übertragenen Nachricht vom Empfänger verifiziert und eventuelle Manipulationen innerhalb des öffentlichen Netzes zuverlässig erkannt werden. Für die sichere Erzeugung und Speicherung des Signaturschlüssels wird wiederum auf die Chipkarte zurückgegriffen, die ein wesentlicher Bestandteil des Sicherheitskonzeptes ist. Außerordentlich wichtig für die Verbindung von Rechnern ist es, dass der Möglichkeit einer ungewollten Fehlvermittlung, die - anders als bei Telefongesprächen - meist nicht vor oder während der Übertragung erkannt werden, angemessen begegnet wird. Dies kann durch eine eingebaute Firewall-Funktionalität in der ISDN-Sicherheitskomponente erreicht werden. Durch eine Überwachung des Signalisierungskanals (D-Kanal) kann dann die Sicherheitskomponente so eingestellt werden, dass ausschließlich explizit vorkonfigurierte Kryptoverbindungen zustande kommen. In Verbindung mit TK-Anlagen ist ferner vorgesehen, dass bestimmte Rufnummern und Funktionen

Um sowohl ein sicheres Schlüsselmanagement als auch eine schnelle Echtzeitverschlüsselung der Nutzdaten zu erreichen, sollten Hybridverfahren eingesetzt werden. Unter Beibehaltung der symmetrischen Informationsverschlüsselung wird der so genannte Sitzungsschlüssel mit Hilfe eines asymmetrischen Verfahrens ausgetauscht. Dies läuft im Praxisbetrieb völlig

automatisch ab. Ohne nennenswerte Beeinträchtigung des Bedienungskomforts können auf diese Weise für jede neue ISDN-Verbindung neue Sitzungsschlüssel vereinbart werden.

Aus sicherheitstechnischer Sicht sollte der Endteilnehmer folgende Einsatzkriterien und -auflagen bei der Auswahl bzw. beim Einsatz einer ISDN-Sicherheitskomponente heranziehen:

(Bewertung: + = wichtig bis +++ = sehr wichtig):

- Die individuellen Teilnehmerschlüssel und Authentisierungsinformationen sind auf einem sicheren Medium (z. B. einer Chipkarte) zu speichern und mit Hilfe einer vertrauenswürdigen Signatur zu sichern (+++).
- Für die Verschlüsselung einer Kommunikationsbeziehung (Sprache, Daten, Bild, etc.) ist pro Übertragung ein geheimer Schlüssel, der sogenannte Sitzungsschlüssel, neu zu vereinbaren (++).
- Die ausgeführten Sicherheitsdienste erfolgen automatisch und für das Endsystem bzw. den Endteilnehmer völlig transparent (+).
- Für ausgewählte Verbindungen ist die Sicherheitskomponente immer im Kryptobetrieb eingerichtet (+++).
- Die bestehende Infrastruktur sollte bei Verwendung der Sicherheitskomponenten voll erhalten bleiben (+).
- Die Sicherheitsadministration der Sicherheitskomponenten sollte netzweit und möglichst von zentraler Stelle aus möglich sein (+).
- Wünschenswert ist eine Online-Betriebsüberwachung und Registrierung aller Sicherheitskomponenten im Dialog mit der Managementstation (+).

Es sollten ISDN-Sicherheitskomponenten ausgewählt werden, die normierte Schnittstellen haben, keine Änderungen in den zu schützenden Endgeräten erfordern und die leicht in eine bestehende Kommunikationslandschaft zu integrieren sind.

M 2.164 Auswahl eines geeigneten kryptographischen Verfahrens

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Die Auswahl eines kryptographischen Verfahrens zerfällt in die beiden Teilaufgaben

- Auswahl des kryptographischen Algorithmus und
- Auswahl einer technischen Realisierung.

Bevor der Anwender sich auf bestimmte Verfahren festlegt, sollte er genaue Vorstellungen davon haben, welche Anforderungen er an Vertraulichkeit und Authentizität der bearbeiteten Daten in jedem "Punkt" seines informationsverarbeitenden Systems stellt.

Auswahl von kryptographischen Algorithmen

Bei der Auswahl von kryptographischen Algorithmen ist zunächst zu klären, welche Art kryptographischer Verfahren benötigt werden, also symmetrische, asymmetrische oder hybride Verfahren, und dann sind geeignete Algorithmen, also solche mit entsprechender Mechanismenstärke auszuwählen.

Verschlüsselungsverfahren

- symmetrische Verschlüsselung: Die Vor- bzw. Nachteile symmetrischer Verfahren sind in M 3.23 *Einführung in kryptographische Grundbegriffe* beschrieben. Geeignete Algorithmen sind z. B. Triple-DES, IDEA, AES, RC 5, wobei die Schlüssellänge mindestens 100 Bit sein sollte.
- asymmetrische Verschlüsselung: Die Vor- bzw. Nachteile asymmetrischer Verfahren sind ebenfalls in M 3.23 *Einführung in kryptographische Grundbegriffe* beschrieben. Geeignete Algorithmen sind z. B. RSA oder auf Elliptischen Kurven basierende Verschlüsselungsverfahren (zur Schlüssellänge siehe unten).

Authentisierungsverfahren

- Nachrichtenauthentisierung

  Zur Nachrichtenauthentisierung können verschiedene Verfahren eingesetzt werden, etwa ein Message Authentication Code (MAC) oder ein digitales Signaturverfahren. Der Einsatz eines MACs ist von Vorteil, wenn extrem hohe Durchsatzraten gefordert sind (oder nur eine geringe Rechenkapazität zur Verfügung steht) und das Risiko der Schlüsseloffenlegung auf beiden Seiten sehr gering ist. Der Einsatz eines digitalen Signaturverfahrens ist von Vorteil, wenn das Risiko der (Signatur-) Schlüsseloffenlegung auf einer Seite wesentlich höher ist als auf der anderen Seite; und in aller Regel geboten, wenn Verbindlichkeitsdienste verlangt werden. Es sei noch einmal bemerkt, dass für den Dienst Verbindlichkeit eine Infrastruktur vertrauenswürdiger Dritter vorhanden sein muss.

  Der bekannteste MAC-Algorithmus ist die Verschlüsselung einer Nachricht mit DES oder einem anderen Block-Chiffrierverfahren im CBC- oder CFB-Mode. Dabei wird als MAC der letzte verschlüsselte Block an

die Nachricht angehängt. Solche Varianten sind z. B. in den Normen ANSI X9.9, ANSI X9.19, ISO 8731-1 oder ISO 9797 spezifiziert.

In neuerer Zeit gab es weitere Vorschläge für Blockchiffren-basierte MAC-Konstruktionen, hier hat sich von der amerikanischen NIST standardisierte Verfahren C-MAC (ehedem OMAC1) als allgemein akzeptiertes MAC-Verfahren durchgesetzt. Daneben gibt es dedizierte MAC-Konstruktionen auf Basis von Hashfunktionen, hier ist an erster Stelle der weithin akzeptierte und verwendete HMAC aus dem RFC 2104 zu nennen.

Geeignete Algorithmen für Digitale Signaturen sind z. B. RSA, DSA (Digital Signature Algorithm) oder auf elliptischen Kurven basierende DSA-Varianten, z. B. ISO/IEC 15946-2, IEEE-Standard P1363, Abschnitt 5.3.3 ("Nyberg-Rueppel Version"), IEEE-Standard P1363, Abschnitt 5.3.4 ("DSA Version").

- Authentisierung von Benutzern oder Komponenten

  Ein einfaches Verfahren zur Authentisierung ist eine Passwortabfrage. Werden die Passwörter dabei aber unverschlüsselt über ein Netz übertragen, können diese verhältnismäßig einfach mitgelesen werden. Daher sollten hier bessere Verfahren verwendet werden. Geeignete Verfahren sind beispielsweise

  - Einmalpasswörter (siehe auch M 5.34 *Einsatz von Einmalpasswörtern*), die software- oder hardwaregestützt erzeugt werden können. Hierbei sind die hardwarebasierten Authentisierungsmethoden vorzuziehen, da sie einen geringeren organisatorischen Aufwand und höhere Sicherheit bieten.
  - Die Authentisierung mittels PAP oder besser CHAP, die bei der Nutzung des Point-to-Point-Protocol eingesetzt werden (siehe auch M 5.50 *Authentisierung mittels PAP/CHAP*).
  - Die Authentisierung mittels CLIP/COLP, die bei der Kommunikation über ISDN eingesetzt wird (siehe auch M 5.48 *Authentisierung mittels CLIP/COLP*).
  - Ein weiteres bekanntes Verfahren ist das Authentikationsprotokoll Kerberos, das am MIT (Massachusetts Institute of Technology) entwickelt wurde. Es wird in Netzen zur gegenseitigen Authentisierung von Benutzer/Client und Servern eingesetzt. Die zentrale Autorität bei Kerberos ist der Ticket-Granting-Server, der Tickets ausstellt, mit denen sich Clients und Server gegenseitig authentisieren können. Mit Hilfe dieser Tickets können Benutzer sich nach einmaliger Authentikation Sitzungsschlüssel für die verschiedensten Dienste anfordern.

Hashverfahren

Bei der Kryptoanalyse von Hash-Funktionen hat es in neuerer Zeit große Fortschritte gegeben. Aufgrund dieser Ergebnisse kann SHA-1 nicht mehr uneingeschränkt für alle Einsatzzwecke empfohlen werden, die Verwendung im HMAC ist aber nach wie vor unkritisch.

Geeignete Algorithmen sind neben RIPEMD-160 (bei niedrigeren Anforderungen an die Kollisisionsresistenz, d. h. circa 80 Bit Aufwand) vor allem die neueren SHA-2 Versionen (SHA-224, SHA-256, SHA-384, SHA-512), die für Anwendungen mit höheren Anforderungen an die Kollisionresistenz ausgelegt sind.

Auswahlkriterien

- Mechanismenstärke / Schlüssellänge

  Ein wesentliches Kriterium für die Auswahl von kryptographischen Verfahren ist ihre Mechanismenstärke. Bei symmetrischen Verfahren sollte insbesondere die Schlüssellänge ausreichend groß sein. Je größer die verwendete Schlüssellänge bei einem kryptographischen Verfahren ist, desto länger dauert es, ihn z. B. durch eine Brute-Force-Attacke zu berechnen. Andererseits werden die Verfahren bei der Verwendung längerer Schlüssel langsamer, so dass immer zu überlegen ist, welche Schlüssellänge unter Nutzen-/Leistungsgesichtspunkten angemessen ist. Als Faustregel für gute Verfahren (Triple-DES, IDEA, RC5, AES,...) und mittleren Schutzbedarf gilt derzeit, dass die eingesetzten Schlüssel mindestens 100 Bit lang sein sollten. Bei Verwendung von Blockchiffren sollten größere, strukturierte Datenmengen nicht im ECB-Modus verschlüsselt werden. Stattdessen sollten dazu der CBC-Modus oder der CFB-Modus verwendet werden. Mindestens eine dieser Betriebsarten sollte daher implementiert sein.

  Bei asymmetrischen Verfahren sollte die Mechanismenstärke so gewählt werden, dass die Lösung der zu Grunde liegenden mathematischen Probleme einen unvertretbar großen bzw. praktisch unmöglichen Rechenaufwand erfordert (die zu wählende Mechanismenstärke hängt daher vom gegenwärtigen Stand der Algorithmik und der Rechentechnik ab). Gegenwärtig kann man davon ausgehen, dass man mit

  - Modullängen von 1024 Bit bei RSA bzw.
  - Untergruppenordnungen in der Größe von 160 Bit bei ElGamal-Verfahren auf einer geeigneten elliptischen Kurve

  derzeit noch "auf der sicheren Seite" ist. Allerdings wird von maßgeblichen Experten vorhergesagt, dass 1024 Bit RSA-Moduli mit einem Aufwand von circa 2 hoch 80 Operationen faktorisierbar sind, und auch der Aufwand der besten generischen Algorithmen für das diskrete Logarithmusproblem in einer Gruppe der Ordnung 160 Bit liegt in dieser Größenordnung. Für langfristige Sicherheitsanwendungen sollten deswegen zu 2048 Bit RSA-Moduli bzw. Untergruppenordnungen von mindestens 224 Bit gewechselt werden. Beispiele für geeignete Kurven findet man im Internet unter www.ecc-brainpool.org.

  Es sollten keine "unbekannten" Algorithmen verwendet werden, d. h. es sollten Algorithmen eingesetzt werden, die veröffentlicht sind, die von einem breiten Fachpublikum intensiv untersucht worden sind und von denen keine Sicherheitslücken bekannt sind. Häufig bieten Hersteller Sicherheitsprodukte an mit neuen Algorithmen, die "noch viel sicherer und noch viel schneller" sein sollen als andere Algorithmen. Aber vor der Verwendung von unbekannten Algorithmen aus Quellen, deren

kryptographische Kompetenz nicht ausreichend nachgewiesen ist, kann nur gewarnt werden.

- Symmetrische oder hybride Verfahren?

  Aus Performancegründen werden für Verschlüsselungszwecke keine reinen Public-Key-Implementierungen eingesetzt. Alle gängigen Implementierungen von Public-Key-Kryptographie nutzen hybride Verfahren (siehe auch M 3.23 *Einführung in kryptographische Grundbegriffe*).

  In Anwendungen mit großen oder offenen Nutzergruppen empfiehlt sich meist die Verwendung eines hybriden Verfahrens (wegen der Vorzüge für das Schlüsselmanagement). Bei kleinen, geschlossenen Nutzergruppen (insbesondere natürlich bei einem einzelnen Benutzer) kann man sich auf symmetrische Verfahren beschränken. Bei Einsatz hybrider Verfahren ist es sinnvoll, die Stärken des symmetrischen und des asymmetrischen Anteils aufeinander abzustimmen. Da mit dem asymmetrischen Verfahren vor einem Schlüsselwechsel in der Regel viele Schlüssel für das symmetrische Verfahren überschlüsselt werden, sollte der asymmetrische Algorithmus eher etwas stärker ausgelegt werden.

- Realisierbarkeit von technischen Anforderungen

  Die Chiffrieralgorithmen müssen so beschaffen sein, dass die technischen Anforderungen, insbesondere die geforderte Performance, durch eine geeignete Implementation erfüllt werden können. Hierunter fallen Anforderungen an die Fehlerfortpflanzung (z. B. falls über stark rauschende Kanäle gesendet wird), aber auch Anforderungen an Synchronisationsoverhead und Zeitverzögerung (z. B. falls "Echtzeit"-Verschlüsselung von großen Datenmengen erfordert wird).

  Beispiel: Sprachverschlüsselung bei ISDN

  Für die Planung eines Kommunikationsnetzes sind eine Reihe von Parametern zu berücksichtigen, die einen Einfluss auf die zu erwartende Sprachqualität haben und sich in Form von Rauschen, Knacken, Nebensprechen oder Pfeifen bemerkbar machen. Zu solchen Einflussfaktoren zählen beispielsweise die eingesetzten Verschlüsselungsverfahren. Um eine zufrieden stellende Sprachqualität erzielen zu können, müssen alle Einrichtungen längs eines Übertragungsweges betrachtet und bewertet werden. Eine isolierte Betrachtungsweise einer Einzelkomponente ist zwar aufgrund der Verkopplung aller relevanten Einzeleffekte als nicht gerechtfertigt anzusehen, dennoch ist die Kenntnis der Einflussfaktoren jeder Einzelkomponente (z. B. der Kryptokomponente) wichtig. Hieraus können sowohl die Rahmenbedingungen für die Realisierung als auch für die Auswahl abgeleitet werden. Das Verhalten einer Verschlüsselungskomponente wird dabei hauptsächlich durch folgende Faktoren charakterisiert:

  - die verstreichende Zeitdauer bei der Verschlüsselung eines Datenblocks (führt im Allgemeinen zu Verzögerungen),
  - die für Synchronisationszwecke zusätzlich in den Datenstrom eingeführten Steuerinformationen (führen unter Umständen zu Schwankungen),

- der von der Kryptokomponente maximal zu leistende Datendurchsatz (führt - wenn Zwischenspeicherung notwendig - ebenfalls zu Schwankungen),
- die durch die Verschlüsselung resultierende Fehlerfortpflanzung (führt im Allgemeinen zu einem Anstieg der Fehlerrate).

Gerade bei einer Sprachverschlüsselung (Echtzeitdienst) machen sich die vorgenannten Einflussfaktoren in einer Erhöhung der Ende-zu-Ende-Laufzeit, in Laufzeitschwankungen sowie in einer höheren Fehlerrate negativ bemerkbar, d. h. in einer Qualitätsminderung, die messtechnisch ermittelt und der Kryptokomponente zugeordnet werden kann.

- Andere Einflussfaktoren

  Manche kryptographische Algorithmen (z. B. IDEA) sind patentiert, für ihren Einsatz in kommerziellen Anwendungen (wozu auch der behördliche Bereich zählt) sind eventuell Lizenzgebühren zu entrichten.

Veröffentlichungen der Bundesnetzagentur

Die Bundesnetzagentur veröffentlicht regelmäßig im Bundesanzeiger eine Übersicht über die Algorithmen, die zur Erzeugung von Signaturschlüsseln, zum Hashen zu signierender Daten oder zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen als geeignet angesehen werden können. Diese Veröffentlichungen können auch vom Webserver der Bundesnetzagentur (www.bundesnetzagentur.de) herunter geladen werden. Sie können zusätzliche Hinweise zur Auswahl liefern.

M 2.165 Auswahl eines geeigneten kryptographischen Produktes

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Das Spektrum kryptographischer Anwendungen ist sehr breit, es reicht von einem einfachen Programm zur Dateiverschlüsselung auf einem Single-User PC über Firewall-Rechner mit Kryptofunktionen zur Absicherung eines lokalen Netzes bis hin zur "Echtzeit"-Hardwareverschlüsselung von Videokonferenzen. Es ist klar, dass bei dieser Breite Empfehlungen zur Auswahl von kryptographischen Produkten allgemein gültig gehalten sind.

Vor einer Auswahl sollte der Nutzer **sämtliche** Anforderungen an das Produkt festlegen. Das ausgewählte Produkt sollte die Benutzeranforderungen in einem möglichst hohen Grad abdecken.

Funktionalität

Das ausgewählte Produkt muss die vom Anwender spezifizierte Funktionalität aufweisen, insbesondere muss es

- die geforderten kryptographischen Grunddienste leisten,
- evtl. besonderen Anforderungen durch die Einsatzumgebung genügen (z. B. Single-User/Multi-User-PC, LAN-Umgebung, WAN-Anbindung),
- die geforderten technischen Leistungsmerkmale aufweisen (z. B. Durchsatzraten),
- die geforderten Sicherheitsfunktionalitäten aufweisen, insbesondere müssen die eingesetzten kryptographischen Mechanismen die erforderliche Stärke aufweisen.

Interoperabilität

Das ausgewählte Produkt wird in der Regel in eine bestehende IT-Umgebung eingefügt. Es muss dort möglichst interoperabel sein. Die Einhaltung interner Standards ist nötig, um die Interoperabilität mit dem bereits vorhandenen IT-System bzw. Systemkomponenten zu gewährleisten. Die Anwendung internationaler Standards für kryptographische Techniken sollte selbstverständlich sein, sie erleichtert auch eine Sicherheitsevaluierung der kryptographischen Komponente.

Wirtschaftlichkeit

Das ausgewählte Produkt sollte möglichst wirtschaftlich sein. Dabei müssen Anschaffungskosten, Stückzahlen, Kosten für Wartung und Produktpflege, aber auch Einsparungen durch etwaige Rationalisierungseffekte berücksichtigt werden.

Zertifizierte Produkte

In den letzten Jahrzehnten hat sich eine international anerkannte Methodologie zur Bewertung von IT-Sicherheitsprodukten durchgesetzt: die europäischen ITSEC (Information Technology Security Evaluation Criteria) bzw. deren

Weiterentwicklung CC (The Common Criteria for Information Technology Security Evaluation). Die ITSEC bzw. CC bieten einen Rahmen, innerhalb dessen die Sicherheitsfunktionalitäten eines IT-Produktes durch Anlegen von etablierten Kriterien in eine genau spezifizierte Hierarchie von Sicherheitsstufen eingeordnet werden können. Die Informationssicherheitsbehörden mehrerer Staaten haben jeweils ein nationales Zertifizierungsschema nach diesen Kriterien aufgebaut.

Der Einsatz eines zertifizierten Produktes bietet die Gewähr, dass die Sicherheitsfunktionalität dieses Produktes unabhängig geprüft wurde und den im Evaluationslevel spezifizierten Standard nicht unterschreitet (siehe auch M 2.66 *Beachtung des Beitrags der Zertifizierung für die Beschaffung*).

Importprodukte

In mehreren Staaten, insbesondere den USA, unterliegt der Export von starker Kryptographie gegenwärtig (noch) starken Beschränkungen. Insbesondere wird die Stärke von an sich starken Verschlüsselungsprodukten künstlich (durch Reduzierung der Schlüsselmannigfaltigkeit) herabgesetzt. Solche künstlich geschwächten Verfahren erreichen in der Regel nicht die für normalen Schutzbedarf erforderliche Mechanismenstärke.

In Deutschland und den meisten anderen Ländern unterliegen kryptographische Produkte beim Einsatz innerhalb der Landesgrenzen keinerlei Einschränkungen. Beim Einsatz von Importprodukten sollte immer darauf geachtet werden, ob sie den vollen Leistungsumfang bieten.

Grenzüberschreitender Einsatz

Viele Unternehmen und Behörden haben zunehmend das Problem, das sie auch ihre internationale Kommunikation, z. B. mit ausländischen Tochterunternehmen, kryptographisch absichern wollen. Hierfür muss zunächst untersucht werden,

- ob innerhalb der jeweiligen Länder Einschränkungen beim Einsatz kryptographischer Produkte zu beachten sind und
- ob für in Frage kommende Produkte Export- oder Importbeschränkungen beachtet werden müssen.

Fehlbedienungs- und Fehlfunktionssicherheit

Das Gefährliche an kryptographischen Produkten ist, dass sie den Anwender in einer - mitunter trügerischen - Sicherheit wiegen: Es ist ja "alles verschlüsselt"! Insofern kommt Maßnahmen gegen Kompromittierungen durch Bedienungsfehler oder technisches Versagen besondere Bedeutung zu, da deren Folgen eben nicht nur auf einen schlichten Defekt beschränkt werden können, sondern sogleich einen Sicherheitseinbruch nach sich ziehen. Allerdings ist die Bandbreite bezüglich redundanter Systemauslegung und zusätzlicher Überwachungsfunktionen - und damit an Gerätekosten - groß, so dass hier die Maßnahmen im Einzelfall in Abhängigkeit von den Anforderungen festzulegen sind.

Implementierung in Software, Firmware oder Hardware

Kryptographische Algorithmen können sowohl in Software, in Firmware als auch in Hardware implementiert werden. Softwarerealisierungen werden in der Regel vom Betriebssystem des jeweiligen IT-Systems gesteuert. Unter Firmware versteht man Programme und Daten, die permanent so in Hardware gespeichert sind, dass die Speicherinhalte nicht dynamisch verändert werden können, und die während ihres Ablaufs nicht modifiziert werden können. Bei Hardware-Lösungen wird das kryptographische Verfahren direkt in Hardware realisiert, z. B. als separates Sicherheitsmodul oder als Einsteckkarte.

Dazu, welche Art der Implementierung gewählt werden sollte, kann keine generelle Empfehlung abgegeben werden, da die Entscheidung eine Abwägung von verschiedenen Faktoren erfordert:

- den Schutzbedarf der durch das kryptographische Verfahren zu schützenden Daten bzw. das angestrebte Sicherheitsniveau,
- den angestrebten Datendurchsatz,
- wirtschaftliche Überlegungen und Zwänge,
- die Einsatzumgebung sowie umgebende Sicherungsmaßnahmen,
- eine evtl. vorliegende nationale Einstufung der bearbeiteten Daten.

Softwarelösungen bieten den Vorteil, leicht anpassbar und kostengünstig zu sein. Hardware-Realisierungen bieten im allgemeinen sowohl höhere Manipulationsresistenz (und damit Sicherheit) als auch höheren Datendurchsatz als Softwarerealisierungen, sie sind aber normalerweise auch teurer.

Firmwarelösungen kann man als Kompromiss der beiden vorangegangenen Möglichkeiten verstehen. Die Vor- und Nachteile der jeweiligen Realisierung beziehen sich jedoch immer nur auf lokale Aspekte (dazu gehört vor allem das Schlüsselmanagement). Sind die Daten einmal verschlüsselt und befinden sie sich auf dem Kommunikationsweg, ist im Prinzip das Zustandekommen der Verschlüsselung nicht mehr relevant.

Ein Beispiel für (relativ) preiswerte, transportable und benutzerfreundliche Kryptomodule sind Chipkarten, die im Bereich der lokalen Verschlüsselung als sicheres Speichermedium für die kryptographischen Schlüssel oder im Bereich der Authentikation zur Passwort-Generierung und Verschlüsselung eingesetzt werden können.

Wenn alle Anforderungen an das kryptographische Produkt festgelegt worden sind, erhält man damit einen Anforderungskatalog, der dann auch direkt für eine Ausschreibung verwendet werden kann, sofern eine solche notwendig ist.

M 2.166 Regelung des Einsatzes von Kryptomodulen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Auch im laufenden Betrieb müssen eine Reihe von Sicherheitsanforderungen an den Einsatz von Kryptomodulen gestellt werden. Diese müssen adäquat in das technische und organisatorische Umfeld eingebunden sein, in dem sie eingesetzt werden.

Dafür müssen einige organisatorische Regelungen getroffen werden:

- Es müssen Verantwortliche benannt werden, und zwar für die Erstellung des Kryptokonzepts, für die Auswahl sowie für den sicheren Betrieb der kryptographischen Produkte.
- Es sind geeignete personelle Maßnahmen festzulegen bzw. durchzuführen (Schulung, Benutzer-Support, Vertretungsregelungen, Verpflichtungen, Rollenzuteilungen).
- Die Benutzer sollten nicht nur im Umgang mit den von ihnen zu bedienenden Kryptomodulen geschult werden, sie sollten darüber hinaus für den Nutzen und die Notwendigkeit der kryptographischen Verfahren sensibilisiert werden und einen Überblick über kryptographische Grundbegriffe erhalten (siehe auch M 3.23 *Einführung in kryptographische* Grundbegriffe).
- Falls Probleme oder gar der Verdacht auf Sicherheitsvorfälle beim Einsatz von Kryptomodulen auftritt, muss klar definiert sein, was in solchen Fällen zu unternehmen ist. Alle Benutzer müssen über die entsprechenden Verhaltensregeln und Meldewege informiert sein.
- Im Rahmen des Kryptokonzepts ist festzulegen, wer wann welche Kryptoprodukte benutzen muss bzw. darf und welche Randbedingungen dabei zu beachten sind (z. B. Schlüsselhinterlegung).
- Der korrekte Einsatz der Kryptomodule sollte regelmäßig überprüft werden. Ebenso ist regelmäßig zu hinterfragen, ob die eingesetzten kryptographischen Verfahren noch dem Stand der Technik entsprechen (siehe dazu auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*).
- Je nach den definierten Verfügbarkeitsanforderungen sollten Ersatz-Kryptomodule vorrätig gehalten werden, um einen reibungslosen Betrieb zu gewährleisten. Dies ist insbesondere dort wichtig, wo der Zugriff auf verschlüsselte Daten von der Funktionsfähigkeit eines einzelnen Kryptomoduls abhängt, z. B. bei der Datenarchivierung oder der ISDN-Verschlüsselung.

Es ist ein sicherer Betrieb der Kryptomodule zu gewährleisten, dazu gehören:

- Vor der Inbetriebnahme muss die optimale Konfiguration der Kryptomodule festgelegt werden, z. B. hinsichtlich Schlüssellänge, Betriebsmodi oder Kryptoalgorithmen.

- Die festgelegte Konfiguration muss dokumentiert sein, damit sie nach einem Systemversagen oder einer Neuinstallation schnell wieder eingerichtet werden kann.
- Für die Benutzer müssen die Kryptoprodukte durch den Administrator so vorkonfiguriert sein, dass ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht werden kann.
- Bei komplexeren Kryptoprodukten müssen geeignete Handbücher verfügbar sein.
- Die Kryptomodule müssen sicher installiert werden und anschließend getestet werden (z. B. ob sie korrekt verschlüsseln und ob sie von Benutzer bedient werden können).
- Die Anforderungen an die Einsatzumgebung müssen festgelegt sein, eventuell sind dafür ergänzende Maßnahmen im IT-Umfeld zu treffen. Die sicherheitstechnischen Anforderungen an die IT-Systeme, auf denen die kryptographischen Verfahren eingesetzt werden, sind den jeweiligen systemspezifischen Bausteinen zu entnehmen, z. B. für Clients (inklusive Laptops) und für Server aus Schicht 3.
- Es muss festgelegt werden, wer wie häufig die Kryptomodule zu warten hat.

Auch im Rahmen des Schlüsselmanagements (siehe M 2.46 *Geeignetes Schlüsselmanagement*) müssen diverse Vorgaben gemacht werden:

- Vorgaben zur Schlüsselerzeugung und -auswahl,
- Vorgaben zur gesicherten Speicherung kryptographischer Schlüssel,
- Festlegung der Schlüsselwechsel-Strategie und -Intervalle.

Ergänzende Kontrollfragen:

- Sind Regelungen für den Einsatz kryptographischer Verfahren festgelegt worden?
- Ist das Kryptokonzept aktuell?
- An wen können sich die Benutzer bei Fragen zum Einsatz von Kryptomodulen wenden?

M 2.167 Sicheres Löschen von Datenträgern

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: IT-Verfahrensverantwortlicher,

Eine geregelte Vorgehensweise für die **Löschung** oder **Vernichtung** von Datenträgern verhindert einen Missbrauch der gespeicherten Daten. Bevor Datenträger wieder verwendet werden, müssen die gespeicherten Daten vollständig gelöscht werden, z. B. durch vollständiges Überschreiben oder Formatieren. Dies ist insbesondere wichtig, wenn Datenträger an Dritte weitergegeben werden sollen. Auch der Empfänger des Datenträgers muss nach dem Empfang prüfen, ob der Schutzwert der Daten ein sofortiges Löschen des Datenträgers erfordert, nachdem die Daten auf ein anderes IT-System übertragen wurden.

Es gibt verschiedene Methoden um Informationen auf Datenträgern zu löschen, z. B. über Löschkommandos, durch Formatieren, durch Überschreiben oder durch Zerstörung des Datenträgers. Welche Methode gewählt werden sollte, hängt hierbei auch vom Schutzbedarf der zu löschenden Daten ab, der Schutz gegen die Restaurierung von Restdaten steigt in der genannten Reihenfolge.

Löschkommandos

Bei der Benutzung von Löschkommandos ist insbesondere bei DOS-/ Windows-basierten Betriebssystemen zu beachten, dass dabei nicht tatsächlich die Dateiinformationen gelöscht werden, sondern nur der Verweis auf diese Informationen im "Inhaltsverzeichnis" des Datenträgers. Die Datei ist weiterhin vorhanden. Es gibt eine Vielzahl von Programmen, mit denen die gelöscht geglaubten Informationen wiederhergestellt werden können (z. B. UNDELETE unter DOS).

Um Dateien unwiederbringlich zu löschen, müssen alle Einträge auf dem Datenträger überschrieben werden. Dafür können Programme wie PC-Tools (Option "Überschreiben" um Datenträger oder Programm WIPE um einzelne Dateien zu überschreiben) oder Norton Utilities (Programm WIPEINFO) eingesetzt werden.

Formatieren

Um Datenträger wieder in den "Urzustand" zu versetzen und damit auch vorhandene Informationen zu löschen, können diese formatiert werden. Wie zuverlässig dabei allerdings die alten Daten gelöscht werden, ist stark abhängig vom zu Grunde liegenden Betriebssystem. Ein Überschreiben der alten Daten ist auf jeden Fall zuverlässiger.

Beim Formatieren von DOS-Datenträgern ist beispielsweise darauf zu achten, dass der Parameter */U* (z. B. bei DOS 6.2 *format a: /U*) benutzt wird, damit das Formatieren nicht über den Befehl *unformat* wieder rückgängig gemacht werden kann. Unter Windows 95 und Windows NT ist aus gleichem Grunde eine Formatierung mit dem Parameter *Vollständig* und nicht mit *Quick-Format* durchzuführen.

Überschreiben

Eine für den mittleren Schutzbedarf ausreichende physikalische Löschung kann erreicht werden, indem der komplette Datenträger oder zumindest die genutzten Bereiche mit einem bestimmten Muster überschrieben werden. Es werden einige handelsübliche Produkte angeboten, die sogar die physikalische Löschung einzelner Dateien gewährleisten.

Zum Überschreiben sollten keine gleichförmigen Muster wie "0000" benutzt werden, sondern es sollten Muster wie "C1" (hexadezimal, entspricht der Bitfolge 11000001) benutzt werden. Dazu sollte bei einem zweitem Durchlauf ein dazu komplementäres Muster (also z. B. 3E, entspricht der Bitfolge 00111110) benutzt werden, damit möglichst jedes Bit einmal geändert wird.

Die Überschreibprozedur sollte daher mindestens zweimal, besser aber dreimal wiederholt werden, da hierdurch eine verbesserte Schutzwirkung erzielt wird.

Schreibgeschützte oder nicht mehrfach beschreibbare Datenträger wie CD-ROMs oder CD-Rs können selbstverständlich auch nicht gelöscht werden und sollten vernichtet werden.

Löschgeräte

Flexible magnetische Datenträger (Disketten, Bänder) können mit einem Löschgerät gelöscht werden. Dabei werden die Datenträger einem externen magnetischen Gleich- oder Wechselfeld ausgesetzt (Durchflutungslöschen). Geeignete Löschgeräte, die die Norm DIN 33858 erfüllen, sind in der BSI-Publikation 7500 aufgeführt.

Grundsätzlich sind die Datenträger nach dem Löschen wiederverwendbar. Es ist aber zu beachten, dass Datenträger mit einer magnetisch geschriebenen Servospur (z. B: Bandkassetten IBM 3590, Travan 4, MLR und ZIP-Disketten) nach einem solchen Löschen unbrauchbar werden.

Löschen von Festplatten

Auch Festplatten, die weitergegeben werden, müssen gelöscht werden. Dies gilt insbesondere dann, wenn auf der Festplatte sensitive Daten gespeichert waren, oder wenn die Festplatte ausgesondert oder zur Reparatur gegeben werden soll.

Für Festplatten, die lediglich innerhalb einer Organisation weitergegeben werden, ist es normalerweise ausreichend, die Dateien mit den normalen Löschfunktionen des Betriebssystems zu löschen oder die Platte zu formatieren.

Festplatten, die an Externe weitergegeben werden, sollten zumindest auf die folgende Weise gelöscht werden: Zunächst sollten alle vorhandenen Partitionen gelöscht werden (z. B. unter DOS mit dem Befehl *fdisk*) und eine große Partition angelegt werden. Danach sollte die gesamte Festplatte formatiert werden (z. B. unter DOS mit dem Befehl *format /U*). Dabei muss jedoch beachtet werden, dass die Daten auf der Festplatte selbst dann noch mit geeigneten Tools zumindest teilweise ausgelesen werden können.

Als zusätzliche Sicherheitsmaßnahme sollte daher auch für Fesplatten ein Lösch-Tool verwendet werden, das die ganze Platte mehrmals mit verschiedenen Mustern überschreibt.

Defekte Festplatten

Bei defekten Festplatten ist ein Löschen durch Überschreiben nicht mehr möglich. Daher bleibt nur das Löschen mit einem Löschgerät, obwohl diese Geräte nicht für das Löschen von Festplatten vorgesehen sind. Wegen des unterschiedlichen Aufbaus von Festplattenlaufwerken, insbesondere der Anzahl von Platten, kann keine generelle Aussage über die erzielbare Löschwirkung gemacht werden. Die Anwendung eines Löschgerätes auf eine Festplatte macht diese im allgemeinen unbrauchbar.

Vernichtung der Datenträger

Eine einfache Möglichkeit, Datenträger zu vernichten, besteht darin, dass Disketten und Magnetbänder zerschnitten und Festplatten mechanisch zerstört werden. Dies ist allerdings zu umständlich bei größeren Mengen zu vernichtender Datenträger und auch nicht ausreichend bei höherem Schutzbedarf.

Geeignete Vernichtungsgeräte für Magnetbänder, Disketten und CD-ROMs, die der Norm DIN 32757 entsprechen, sind in der BSI-Publikation 7500 aufgeführt. Bei diesen Vernichtungsgeräten werden die Datenträger entweder zerkleinert oder eingeschmolzen. Vernichtungsgeräte für Festplatten sind nicht bekannt.

Ergänzende Kontrollfragen:

- Gibt es ein geregeltes Vorgehen zum Löschen von Datenträgern?

M 2.168 IT-System-Analyse vor Einführung eines Systemmanagementsystems

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Administrator

Vor der Einführung eines Systemmanagementsystems müssen die IT-Systeme, die zukünftig verwaltet werden sollen, untersucht und analysiert werden. Die daraus resultierende Systemdokumentation kann dann als Planungs- und Entscheidungsgrundlage für die festzulegende Systemmanagementstrategie (siehe M 2.169 *Entwickeln einer Systemmanagementstrategie*) dienen. Wichtig ist, dass schon zum Zeitpunkt der Planung alle relevanten Informationen über die zu verwaltenden Systeme möglichst vollständig vorliegen, um Fehlentscheidungen aufgrund mangelnder Information auszuschließen. Aus den lokalen Gegebenheiten lassen sich außerdem konkrete Anforderungen formulieren, die von dem zu beschaffenden Managementsystem erfüllt werden müssen (K.O.-Kriterien).

Es sind folgende Maßnahmen (mit den dort beschriebenen Untermaßnahmen) durchzuführen, die idealerweise bei der Planung und im laufenden Betrieb des Systems gemäß IT-Grundschutz schon durchgeführt wurden bzw. werden:

- Ist-Aufnahme der aktuellen Netzsituation (siehe M 2.139 *Ist-Aufnahme der aktuellen Netzsituation*)
- Dokumentation der Systemkonfiguration (siehe M 2.25 *Dokumentation der Systemkonfiguration*)

  Es sollten alle IT-Systeme erfasst und dokumentiert werden. Insbesondere in heterogenen Systemen müssen z. B. alle vorhandenen Betriebssysteme erfasst werden, um die entsprechenden Anforderungen an das Managementsystem formulieren zu können.
- Feststellung und Überprüfung des Softwarebestandes (siehe M 2.10 *Überprüfung des Hard- und Software-Bestandes*)

  Soll im Rahmen des Systemmanagements auch Software verwaltet werden (Applikationsmanagement), so sollte hier eine Bestandsaufnahme erfolgen. Alternativ kann als Anforderung an das Managementsystem das automatische Feststellen des Softwarebestandes ("Autodiscovery", "Software-Discovery") formuliert werden. Welche der beiden Varianten im Einzelfall notwendig ist, hängt von der Aufgabe ab, die im Bereich Softwaremanagement erbracht werden soll. Wird das Managementsystem z. B. dazu angeschafft, um einen existierenden Softwarebestand, dessen Zusammensetzung nicht in Gänze bekannt ist, automatisch zu verwalten (Softwareupdate, Einspielen neuer Software), so muss dass Managementsystem nach seiner Installation in der Lage sein, den Softwarebestand automatisch zu erfassen. Sollen im Rahmen des Applikationsmanagements einzelne Softwarepakete zusätzlich auf Anwendungsebene verwaltet werden, so muss geprüft werden, ob die Software dies aktiv unterstützt (z. B. durch ein entsprechendes Protokoll), was eine vorherige Bestandsaufnahme der vorhandenen Software nötig macht. Daraus ergeben sich dann Anforderungen an den Funktionsumfang des zu beschaffenden Managementsystems (z. B. Unterstützung des Applikationsverwaltungsprotokolls).

Soll z. B. ein Webserver über ein HTTP-basiertes Managementinterface verwaltet werden, so muss das Managementsystem HTTP-basierte Managementfunktionen besitzen oder aber ein Erweiterungsinterface anbieten, das es erlaubt, Eigenentwicklungen zu integrieren.

Neben der Dokumentation des Ist-Zustandes sollte auch die zukünftige Planung für das IT-System berücksichtigt werden, da ein Managementsystem auch auf zukünftige Änderungen im IT-System ausgelegt sein sollte (z. B. Skalierbarkeit).

M 2.169 Entwickeln einer Systemmanagementstrategie

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Die in einem Netz angesiedelten Komponenten müssen von einem Administrator regelmäßig verwaltet werden. Die zu erledigenden Aufgaben reichen von der Einrichtung neuer Benutzer bis hin zur Installation neuer Software, deren verteilte Natur die Installation von Teilsoftware auf jedem einzelnen Rechner verlangt (Workflowsystem, Dokumentenverwaltungssystem, o. Ä.). In großen Organisationen bedeutet alleine die Einrichtung eines neuen Benutzers, der sich auf allen für ihn freigegebenen Rechnern anmelden können soll, einen hohen administrativen Aufwand, da beim Stand-alone-Betrieb jeder einzelne dieser Rechner dementsprechend konfiguriert werden muss. Moderne netzfähige Betriebssysteme (z. B. Unix, Windows NT, Novell) sind daher mit Mechanismen ausgestattet, die den administrativen Aufwand verringern sollen (z. B. zentrale Benutzerverwaltung). Soll allerdings die Verwaltung aller Hard- und Software-Komponenten eines lokalen Netzes auf allen Ebenen (technisch und organisatorisch) in einheitlicher Weise erfolgen, so müssen einerseits technische Hilfsmittel in Form von Managementsystemen eingesetzt werden, deren erfolgreicher Einsatz andererseits aber auch von einer zu erstellenden Managementstrategie abhängt. Die Vorgaben und Regeln der Managementstrategie werden dann durch die Systemadministration mit Hilfe der Managementsoftware umgesetzt. Eine Managementstrategie muss individuell auf die Bedürfnisse der jeweiligen Unternehmen bzw. Behörden angepasst sein. Hierzu müssen folgende Schritte durchgeführt werden:

Festlegung der vom Managementsystem zu verwaltenden Objekte

Nach der Durchführung der Bestandsaufnahme (siehe M 2.168 *IT-System-Analyse vor Einführung eines Systemmanagementsystems*) muss festgelegt werden, welche Bereiche des IT-Systems durch ein zu beschaffendes Managementsystem verwaltet werden sollen:

- Welche Rechner bzw. Hardware sollen in das Managementsystem einbezogen werden?
- Welche Software soll einbezogen werden?
- Welche Benutzer bzw. Benutzergruppen werden einbezogen?

Festlegung der im Managementsystem anzuwendenden Sicherheitsrichtlinien

Neben diesen Entscheidungen müssen aber auch schon existierende Vorschriften und Methoden einbezogen werden. So muss z. B. die festgelegte Sicherheitspolitik der Behörde bzw. des Unternehmens, die Datenschutzrichtlinien und die Richtlinien zur Einführung neuer Software in das Managementkonzept einfließen, da die geltenden Vorschriften auch beim Einsatz eines Managementsystems beachtet und umgesetzt werden müssen. Auch für den Gebrauch des Managementsystems selbst sind Regelungen zu treffen bzw. existierende Regelungen auf Validität zu prüfen und gegebenenfalls anzupas-

sen, und dann auch anzuwenden. Dies gilt insbesondere in den Bereichen:

- Zugriffsrechte auf Managementinformationen
- Dokumentation des Managementsystems
- Erstellung oder Abgleich von Notfallplänen für den Ausfall des Managementsystems oder einzelner Komponenten

Im Vorfeld sollten auch bereits die Reaktionen auf Verletzung der Sicherheitspolitik im Bereich Systemmanagement festgelegt werden. Ähnlich wie in anderen IT-Bereichen, muss auch für den Bereich des Systemmanagements eine Sicherheitspolitik festgelegt bzw. die vorhandene Sicherheitspolitik des Unternehmens bzw. der Behörde auch auf den Bereich Systemmanagement angewandt werden. Da ein Managementsystem mit wichtigen Netz- und Systemkomponenten interagiert und deren Funktion verwaltet und überwacht, sind Verletzungen der Sicherheitspolitik in diesem Bereich als besonders schwer anzusehen. Insbesondere sind hier Regelungen und Vorgehensweisen zu definieren, die nach einer solchen Sicherheitsverletzung zum Einsatz kommen. Diese sind einerseits technischer Natur (z. B. Vergabe neuer Passwörter für alle Benutzer nach Kompromittierung der Managementkonsole), aber auch organisatorischer Natur.

Revision, Datenschutzbeauftragte und IT-Sicherheitsmanagement sollten schon in der Planungsphase einbezogen werden. Nach Einführung des Managementsystems müssen die ihnen hier obliegenden Aufgaben in Bezug auf das Managementsystem klar sein. Beispiel: Der Datenschutzbeauftragte kann schon in der Planungsphase auf die Einhaltung der Datenschutzrichtlinien achten, z. B. welche Benutzerinformationen im Rahmen des Systemmanagements erfasst werden sollen bzw. dürfen. Nach Einführung des Systems muss er zudem in der Lage sein, die Einhaltung der Richtlinien zu überprüfen. Ähnliches gilt für die Zuständigkeitsbereiche des Revisors und des IT-Sicherheitsbeauftragten.

Festlegung der Randbedingungen für die Produktauswahl des Managementsystems

Die Einführung eines Systemmanagementsystems erfordert eine umfangreiche und sorgfältige Planung. Teile der Systemmanagementstrategie hängen zudem davon ab, ob sie mit einem konkreten Produkt realisiert werden können oder nicht. Dies führt dazu, dass die Erstellung der Managementstrategie und die (Vor-)Auswahl eines Produktes iteriert werden müssen.

Folgende Punkte sollten bei der Erstellung der Systemmanagementstrategie Berücksichtigung finden:

- Ist mehr als eine Managementdomäne nötig? Wenn ja: Wie sind diese zu bilden? Managementdomänen erlauben die Einteilung der Komponenten des zu verwaltenden Systems in Gruppen. Die einzelnen Gruppen können voneinander getrennt verwaltet werden. Die Aufteilung in verschiedene Managementdomänen ist für kleinere und mittlere zu verwaltende Systeme nicht zwingend, unterstützt jedoch ein strukturierteres Systemmanagement. Für große zu verwaltende Systeme ist die Aufteilung in verschiedene Ma-

nagementdomänen in der Regel zwingend. Die Planung der Managementregionen hängt dabei von mehreren Faktoren ab:

- Netztopologie

  Insbesondere für mittlere Systemgrößen bietet sich die Aufteilung des Systems in Managementdomänen entsprechend der konkreten Netztopologie an (gerade auch, wenn es z. B. keine unterschiedlichen Verantwortlichkeiten gibt).

- Organisatorische Verantwortlichkeiten innerhalb des Unternehmens oder der Behörde

  So kann die Organisationsstruktur mit dem Managementsystem nachgebildet werden, so dass z. B. Domänen wie "Rechnungswesen", "Programmierung" oder auch "Bereich Produktion", "Bereich Softwareentwicklung" entstehen.

  Auch sicherheitstechnische Gründe, die sich in der Managementpolitik niederschlagen, können zu mehreren Managementregionen führen. Dies ist insbesondere dann der Fall, wenn Managementaufgaben für bestimmte Organisationseinheiten delegiert werden sollen, ohne dass der lokale Administrator Zugriffsrechte auf die Managementfunktionen für die Komponenten außerhalb seines Zuständigkeitsbereiches haben soll.

- vorhandene Infrastruktur

  Hier ist z. B. die geographische Verteilung von Filialen oder die räumliche Verteilung von Arbeitsgruppen über die Stockwerke eines Gebäudes zu betrachten.

- Sicherheitsbetrachtungen

  - Mehrere Managementregionen können dann nötig werden, wenn das Managementprodukt zwar verschiedene Verschlüsselungsmechanismen pro Region unterstützt, von denen jedoch pro Region in der Regel nur eine zum Einsatz kommen kann. Sollen zwischen einzelnen Managementkomponenten tatsächlich verschiedene Mechanismen zum Einsatz kommen, so sind mehrere Managementregionen nötig. Beispiel: Ein System aus mehreren Datenbank-Servern mit sensitiven Daten und den zugehörigen Clients, die selbst keine Daten speichern, wird verwaltet. Die Managementkonsole soll mit den Servern nur stark verschlüsselt kommunizieren, da auch die Datenbanken über das Managementsystem verwaltet werden. Die Kommunikation mit den Clients soll hingegen aus Performancegründen nur schwach verschlüsselt geschehen. In diesem Fall müssen in der Regel zwei Managementregionen gebildet werden: eine Region, in der die Server enthalten sind, und eine zweite Region, die die Clients umfasst.

  - Mehrere Managementregionen erhöhen die Ausfallsicherheit, da z. B. beim Ausfall einer Managementregion die restlichen

Regionen unabhängig davon weiterhin verwaltet werden können.

- Einfluss hat auch die Anzahl der zu verwaltenden Rechner pro Managementregion. Die meisten Produkte geben Empfehlungen über die Anzahl der Rechner, die durch den Managementserver einer Region verwaltet werden können. Eine Zahl von 200 Rechnern pro Server ist aber keine Seltenheit.

- Welche Maschinen sollen als Managementserver dienen? In der Regel ist mit steigender Anzahl von Clients an einem Managementserver mit Performanceeinbußen zu rechnen. Dies muss bei der Planung berücksichtigt werden.
- Welche physikalische Anordnung müssen die Managementserver haben und wo werden sie aufgestellt? Die Lokation eines Servers hat z. B. Einfluss darauf, wie Rechner, die von diesem Server verwaltet werden sollen, über das Netz an diesen angebunden sind. Bei einigen Plattformen gibt es z. B. Mindestanforderungen an die Kommunikationsbandbreite zwischen Server und Client (so unterstützt z. B. TME 10 keine Anbindung von Clients über Leitungen mit weniger als 14.4 Kbps). Dies hat direkte Auswirkungen auf die mögliche Managementsystemkonfiguration und macht z. B. die Neuanschaffung von Rechnern oder den Ausbau von Netzverbindungen nötig.
- Sind so genannte Gateways oder Proxies nötig, die ein hierarchisch aufgebautes Management und/oder den Anschluss an Produkte von Drittanbietern ermöglichen?
- Einige Systeme unterscheiden zwischen so genannten "Managed Nodes" und "Endpoints". Bei beiden handelt es sich um Arbeitsplatzrechner, sie unterscheiden sich aber in der Art und Weise, wie diese in das Managementsystem eingebunden sind: So halten "Endpoints" z. B. im Unterschied zu "Managed Nodes" keine eigene lokale Datenbank mit Managementinformationen vor und können auch nicht zur Weiterleitung von Managementinformationen an weitere Rechner benutzt werden. Hier muss entschieden werden, welche Maschinen als "Managed Nodes" in das Managementsystem eingebunden sein sollen und welche lediglich als "Endpoints" verwaltet werden. In der Regel sollte das Gros der Arbeitsplatzrechner als "Endpoint" eingebunden werden.

Die so erstellte Managementstrategie induziert eine Reihe von Anforderungen an das zu beschaffende Managementprodukt. Durch die Gewichtung der Anforderungen ergibt sich eine konkrete Produktauswahl. Die Managementstrategie muss nun dahingehend überprüft werden, ob sie mit dem zur Verfügung stehenden Funktionsumfang vollständig umgesetzt werden kann. Eine Reformulierung der Strategie kann dadurch in einzelnen Bereichen notwendig sein. Beispiel: Die Produktauswahl ergibt, dass das System, das starke Verschlüsselung unterstützt, leider nicht die Delegation von Verwaltungsaufgaben an "Subadministratoren" erlaubt. Daraufhin muss die Managementstrategie angepasst werden (korrekte Gewichtung der Anforderungen vorausgesetzt).

M 2.170 Anforderungen an ein Systemmanagementsystem

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Ein Systemmanagementsystem dient zur Unterstützung eines Administrators eines lokalen Netzes (oder Virtuellen Lokalen Netzes). Ein Systemmanagementsystem muss daher gewisse Voraussetzungen erfüllen, um den Administrator geeignet unterstützen zu können. Die Anforderungen an ein solches System hängen jedoch wesentlich vom geplanten Einsatz (siehe M 2.169 *Entwickeln einer Systemmanagementstrategie*) und von der gewählten Architektur des Systemmanagementsystems ab (siehe M 2.171 *Geeignete Auswahl eines Systemmanagement-Produktes*).

Ein Systemmanagementsystem sollte folgende Funktionen bereitstellen:

- Benutzermanagement

  Hierzu gehören das Hinzufügen, Verändern und Löschen von Benutzer- und Gruppenkonten.

- Policymanagement

  Zugriffsrechte sollten sowohl für Zugriffe aus dem und in das lokale Netz als auch für Zugriffe auf das bzw. vom Internet verwaltet werden können.

- Softwaremanagement

  Das Hinzufügen, Löschen und Aktualisieren von Softwarekomponenten sollte mit dem Systemmanagementsystem möglich sein.

  Daneben ist insbesondere für die Einführungsphase das automatische Feststellen der installierten Software unter Umständen wichtig. Eine Verwaltung von Softwarelizenzen ist zwar wünschenswert, wird von heutigen Systemen jedoch kaum unterstützt (siehe auch Applikationsmanagement unten. Ausnahme: Lizenzen liegen z. B. als Dateien vor, so dass die Lizenzdateien im Rahmen der Dateiverteilungsmechanismen eines Managementsystems verwaltet werden können).

- Feststellen, Verändern und Verwalten von Systemkonfigurationsdaten.

- Verwalten von Applikationsdaten

  Es muss möglich sein, Dateien eines Datenbanksystems oder Konfigurationsdateien einer Applikation zu verwalten, so dass z. B. das Verteilen einer neuen Version einer Datenbank oder die Verteilung neuer Konfigurationsdateien möglich ist.

- Überwachen von Systemkomponenten

  Dies kann auch für externe Komponenten sinnvoll sein, die nicht der eigenen Administration unterliegen, zum Beispiel für den Router des Internet Service Providers (ISP), über den der Internet-Anschluss realisiert ist.

- Applikationsmanagement

  Das Verwalten von Software auf Anwendungsebene sollte möglich sein, z. B. die Verwaltung von HTTP-Zugriffsrechten auf die Daten eines WWW-Servers ("Realms"). Diese Art von Management wird in der Regel kaum unterstützt, da hierzu die Kooperation der Applikation selbst erforderlich ist.

Idealerweise lässt ein solches System die Delegation von administrativen Aufgaben zu, so dass z. B. ein Systemverwalter einem Arbeitsgruppensystemadministrator das Recht zum Installieren von Software auf den Rechnern der Arbeitsgruppe einräumen kann. Dieser Mechanismus ist insbesondere in mittleren und großen Netzen notwendig.

Die Netz- und Systemadministration werden in der Regel durch die gleichen administrativen Einheiten in einem Unternehmen bzw. einer Behörde durchgeführt. Da in einigen Bereichen die Aufgabentrennung zwischen Netzadministration und Systemadministration nicht klar ist, empfiehlt es sich darauf zu achten, inwieweit ein vorhandenes Netzmanagementsystem in ein zu beschaffendes Systemmanagementsystem integriert werden kann.

Neben diesen vorwiegend funktionalen Anforderungen ergeben sich auch technische Anforderungen im Rahmen der Kriterien, die für die Auswahl einer Systemmanagementsoftware relevant sind (siehe M 2.171 *Geeignete Auswahl eines Systemmanagement-Produktes*). Besonders sind hier folgende hervorzuheben:

- Das Managementsystem muss in der Lage sein, die Betriebssysteme aller für das Management genutzten und aller verwalteten Rechner zu unterstützen (betriebssystemspezifische Komponenten des Managementsystems, graphische Benutzungsoberfläche).
- Existiert bereits ein lokales Datenbanksystem, so sollte das Managementsystem die Möglichkeit besitzen, seine Managementinformationen im vorhandenen Datenbanksystem zu speichern.
- Das Managementsystem sollte erweiterbar sein. Dies betrifft einerseits die Komponenten des Managementsystems (z. B. Modulkonzept mit der Möglichkeit, Module jederzeit nachkaufen und integrieren zu können), aber auch die Funktion des Managementsystems (z. B. Programmier-API, um eigene Komponenten anschließen zu können).

Generell können die in M 2.171 *Geeignete Auswahl eines Systemmanagement-Produktes* vorgestellten Kriterien zur Kategorisierung von Anforderungen im Rahmen der vorliegenden Maßnahme herangezogen werden. Für ausgesuchte Kategorien ergeben sich die Anforderungen durch die Festlegung einer Vorgabe im Rahmen des jeweiligen "Wertebereiches".

M 2.171 Geeignete Auswahl eines Systemmanagement-Produktes

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Administrator

Nach Aufnahme der aktuellen Systemsituation (siehe M 2.168 *IT-System-Analyse vor Einführung eines Systemmanagementsystems*) und Festlegung der Managementstrategie (siehe M 2.169 *Entwickeln einer Systemmanagementstrategie*) muss ein geeignetes Systemmanagementsystem ausgewählt werden. Je nach Größe des zu verwaltenden Systems können hier unterschiedliche Realisierungen zweckmäßig sein:

- Für kleine Systeme kann das Systemmanagement von der Systemadministration "von Hand" erledigt werden.
- Für kleine und mittlere Systeme kann das Systemmanagement auch durch eine Sammlung von einzelnen Tools durchgeführt werden.
- Für große Systeme sollte ein Systemmanagementsystem benutzt werden.

Moderne netzfähige Betriebssysteme sind in der Regel schon mit Funktionen ausgestattet, die eine zentrale Verwaltung z. B. von Benutzern und Benutzergruppen erlauben. Für den Unix-Bereich kann hier z. B. NIS oder NIS+ genannt werden, im Windows-Bereich erlaubt das Windows NT-Domänen-Konzept eine zentrale Benutzerverwaltung über den Domain Controller. Ähnliche Möglichkeiten bietet auch Novell mit Intranetware an. In der Regel existieren zudem auch Möglichkeiten, ein netzweites Policymanagement zu betreiben.

In kleineren und mittleren Netzen stellen daneben das Softwaremanagement, das Management der Rechnerkonfigurationen sowie das Überwachen von Systemkomponenten die drängensten Problembereiche dar. Hier können dann zusätzliche Softwaretools eingesetzt werden, die die Aufgaben einzeln übernehmen können. Insbesondere in den Bereichen, die auch durch die Disziplinen des Netzmanagements abgedeckt sind (Konfigurationsmanagement, Überwachung), kann der Einsatz eines Netzmanagement-Tools in Betracht gezogen werden.

Für den Windows-Bereich lassen sich z. B. Tools wie das "Novell Zero Administration Kit", das den Administrator bei der Installation neuer Rechner unterstützt, die "Microsoft Management Console", die eine einheitliche zentrale Sicht auf alle Administrationstools anbietet, sowie den "Microsoft Systems Management Server (SMS)" nennen. So bietet z. B. das Produkt SMS dem Administrator folgende Möglichkeiten:

- Inventarisieren von Hard- und Software-Komponenten
- Installieren und Verteilen von Daten und Applikationen auf Netzrechnern
- Kontrolle bei der Ausführung von Netzanwendungen
- Unterstützung bei der Administration von Rechnern über das Netz
- Überwachung des Netzverkehrs

SMS ist dabei allerdings nicht für eine heterogene Umgebung ausgelegt. Zudem erfolgt die Fernwartung nur halbautomatisch und erfordert einen Administrator vor Ort, so dass der Einsatz nur für kleinere und räumlich zusammenliegende Netze angezeigt ist.

Für den Unix-Bereich kann z. B. zur Verwaltung und Verteilung von Software das Programm "rdist" eingesetzt werden, mit dem auf entfernten Rechnern Software installiert oder aktualisiert werden kann. Dabei ist es möglich, aus einem zentralen Softwarepool genau die Produkte auf den jeweiligen Rechnern zu installieren, die von den Mitarbeitern für die Erledigung ihrer Aufgaben benötigt werden. Weitere, auch kostenfrei, erhältliche Zusatzprogramme (meist aus dem universitären Umfeld) erlauben z. B. die Überwachung des Netzes über SNMP.

Die so zusammengestellten Lösungen bieten für kleinere und mittlere Netze eine kostengünstige Alternative. Allerdings setzen sie in der Regel einen versierten Administrator voraus, der auch unter Umständen durch Eigenprogrammierung Anpassungen an lokale Gegebenheiten vornimmt oder Zusatzfunktionalität integriert.

Für größere und große Netze sind solche Lösungen jedoch ungeeignet, da die Funktionalitäten in verschiedenen, nicht integrierten Tools angesiedelt ist. Für große Unternehmens- oder Behördennetze kommen nur Systemmanagementsysteme in Frage. Vor der Einführung eines solchen Systems sollte beachtet werden, dass dies in der Regel einen beträchtlichen Eingriff in das laufende System darstellt und gut geplant werden muss. Nicht selten dauert die Einführung mehr als 12 Monate, bei einer mindestens sechsstelligen Investitionssumme für größere Netze. Die Wahl des richtigen Managementsystems ist deshalb wichtig. Folgende Kriterien sollten bei der Wahl des zu beschaffenden Systems beachtet werden:

- Welchen Funktionsumfang bietet das Produkt an?
- Kosten
  - für die Anschaffung der Software
  - für die Anschaffung zusätzlicher Hardware (Bei einigen Systemen müssen ein oder mehrere zentrale Managementserver angeschafft werden.)
  - für Installations- und Betriebsaufwand (U. U. müssen sogar Externe engagiert werden.)
  - für die Schulung der Mitarbeiter
  - andere (z. B. Migrationskosten bei einer existierenden Plattform, Anpassung/Neuentwicklung lokaler Software, bauliche Maßnahmen z. B. gesicherter Serverraum)
- Investitionssicherung
  - Inwieweit ist das Systemmanagement-Produkt skalierbar (z. B. Anzahl der Rechner erweiterbar)?

  - Kann die Plattform mit dem Unternehmen wachsen (z. B. Anzahl der möglichen Managementdomänen, Delegation von Aufgaben)?
  - Wie sind die Migrationspfade zur Plattform?
  - Wie sind die Migrationspfade von dieser Plattform zu einer anderen Plattform?
- Integrationsmöglichkeit mit anderen Produkten
  - Welche Server- bzw. Client-Systemplattformen werden unterstützt?
  - Kann ein bestehendes Netzmanagementsystem integriert werden?
  - Kann ein bestehendes Datensicherungssystem integriert werden?
  - Welche Applikationen von Drittanbietern gibt es für dieses Produkt?
- Zuverlässigkeit und Ausfallsicherheit
  - Gibt es Aussagen oder sogar Garantien über maximale Ausfallzeiten?
  - Ist ein Hotswap für zentrale Komponenten möglich?
  - Existiert ein systemeigener Backup- und Recovery-Mechanismus? Bei einem Ausfall des Managementsystems müssen innerhalb des Managementsystems Mechanismen zum geregelten Wiederanlaufen existieren. Dies umfasst u. U. das Einspielen von Daten aus einer Datensicherung und die automatische Konsistenzprüfung - idealerweise mit Konfliktauflösung bei der Feststellung von Inkonsistenzen.
  - Werden regelmäßig Updates zur Verfügung gestellt? Sind sie einfach einspielbar?
- Sicherheit: Zugriffsbeschränkungen auf die Managementfunktionen
  - Kann der Zugriff auf Benutzer-ID-Ebene (Welcher Benutzer darf was?) eingeschränkt werden?
  - Kann der Zugriff auf Komponentenebene (Welcher Rechner darf was?) eingeschränkt werden?
  - Kann der Zugriff auf die ausführbaren Kommandos Benutzer- oder Systemabhängig eingeschränkt werden?
  - Kann eine Aufteilung der Administrationstätigkeiten vorgenommen werden? Kann also z. B. die Verwaltung von Komponenten auf bestimmte Bereiche eingeschränkt werden (z. B. nur die Abteilungsrechner)?
- Sicherheit: Administration von Rechnern über das Netz
  - Wie sind Fernzugriffe abgesichert?
  - Können Fernzugriffe verschlüsselt erfolgen?
  - Ist sichergestellt, dass eine (starke) Authentisierung vor einer Fernadministration erforderlich ist?

  - Ist es möglich, die Berechtigung für Fernadministration auf bestimmte Personen oder Rollen einzuschränken?
  - Wird der Benutzer automatisch über Fernzugriffe informiert?
- Sicherheit: Datensicherheit, Datenschutz
  - Werden die gesammelten Daten sicher abgelegt (Zugriffsbeschränkungen, Verschlüsselung)?
  - Findet die Datenübertragung zwischen den Managementkomponenten gesichert statt (Authentisierung, Verschlüsselung, Integritätssicherung)?
  - Kann die Art der gesammelten Informationen reguliert werden (Anonymisierung, Rückverfolgung, Beweisbarkeit)?
  - Ist die Integration von Virensuchprogrammen möglich?
  - Welche Protokollierungsmöglichkeiten werden angeboten?
  - Kann die lokale Softwareeinspielung überwacht oder verhindert werden?
- Benutzerfreundlichkeit
  - Gibt es ein graphisches Benutzungsinterface (z. B. X-Windows, Motif, Windows-Oberfläche, Web-Browser)?
  - Wie einfach ist die Navigation?
  - Wird die lokale Sprache oder auch mehrere Sprachen (bei globalem Einsatz) unterstützt?
  - Lassen sich Programme einfach ausführen (auch auf entfernten Rechnern)?
  - Wie einfach lässt sich das Interface vom Benutzer umgestalten?
  - Werden Ausnahmen und Alarmierungen geeignet angezeigt?
  - Ist das Monitoring, auch im Detailgrad, einstellbar?
  - Wird die Komplexität von Netzkomponenten geeignet "versteckt" (So dass der Benutzer nicht ein Experte für die jeweilige Komponente, die verwaltet werden soll, sein muss)?
  - Können alle Funktionen über das gleiche Benutzungsinterface erreicht werden?
  - Sind Onlinehilfen und Anleitungen vorhanden?
- Ergonomie beim Management komplexer Systeme
  - Werden verschiedene Netzprotokolle, Netzkomponenten und Betriebssysteme unterstützt?
  - Wie geht die Plattform mit geographisch verteilten Systemen um und wie ist deren Repräsentation?
  - Wie einfach ist es, neue Komponenten zu integrieren oder aus dem System zu entfernen (Autodiscovery, manuell)?

- Konformität zu Standards (je nach Umgebung kann die Konformität zu mindestens einem Standard erforderlich sein)
  - Plattformen
    - Distributed Management Environment (DME) von der Open Software Foundation (OSF)
    - Spezifikation der Desktop Management Task Force (DMTF)
    - OMNIpoint Spezifikation des Network Management Forum (NMF)
  - Datenbank
    - Welche DBMSe (Data Base Management Systeme) werden unterstützt?
    - Wird SQL als Anfragesprache unterstützt, für den Fall, dass die Managementsoftware eine eigene Datenbank enthält?
  - CORBA (Common Object Request Broker Architecture) der Object Management Group (OMG)
  - Application Program Interface (API), für den Fall, dass eigene Erweiterungen des Managementsystems notwendig sind (z. B. APIs für SNMP, XMP, DMI).

Die hier angeführten Aspekte sind als Anhaltspunkte bei der Bewertung von Managementsystemen zu verstehen. Je nach lokalen Gegebenheiten sollten aufgrund der aktuellen Systemsituation (siehe M 2.168 *IT-System-Analyse vor Einführung eines Systemmanagementsystems*) und aufgrund der Managementstrategie (siehe M 2.169 *Entwickeln einer Systemmanagementstrategie*) Anforderungen an das Managementsystem formuliert werden, die als "K.O.-Kriterien" bei der Entscheidung herangezogen werden können. Die obigen Kriterien sollten immer eine Gewichtung erfahren, die die lokalen Präferenzen wiedergeben.

Die Anforderungen an das Managementsystem und die Leistungen des ausgewählten Managementsystems sind in der Regel nicht vollständig in Einklang zu bringen. Dies macht es notwendig, die erstellte Managementstrategie nach Auswahl des konkreten Produktes an dessen Funktionsumfang anzupassen.

M 2.172 Entwicklung eines Konzeptes für die WWW-Nutzung

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Bevor ein Webangebot eingerichtet wird, muss zunächst in einem Konzept dargestellt werden, welche Informationen und Dienste angeboten werden sollen. Das Konzept sollte mindestens einen allgemeinen und einen organisatorischen Teil enthalten:

Ziele und Inhalte festlegen

Im allgemeinen Teil sollte beschrieben werden,

- welche Ziele die Organisation mit dem Webangebot verfolgt,
- welches die Zielgruppen des Webangebots sind und
- welche Informationen oder Dienstleistungen in dem Webangebot zur Verfügung gestellt werden sollen.

Erscheinungsbild und Redaktion

Im organisatorischen Teil sollte eine grobe Übersicht darüber gegeben werden, wer in der Organisation verantwortlich ist für

- die Bereitstellung und Aktualisierung der Informationen und
- die Ausarbeitung und Pflege des optischen Erscheinungsbildes des Webangebots (*Webdesign*).

Technik

Im organisatorischen Teil des WWW-Konzepts sollte auch festgelegt werden, wer für die technischen Aspekte des Betriebs des Webservers verantwortlich ist.

Das Konzept für das Webangebot sollte regelmäßig auf Aktualität überprüft werden. Bei Änderungen in den Zielen oder Strategien der Organisation muss geprüft werden, welche Auswirkungen diese auf das WWW-Konzept haben.

Bei der Entwicklung des Konzeptes sollten folgende Aspekte berücksichtigt werden:

Verwendungszweck beeinflusst Sicherheitsanforderungen

Ein Webangebot kann als rein interner Informationsdienst eingesetzt werden, als Mittelpunkt eines Intranets, oder als öffentliches Angebot im Internet, das verschiedene Dienste anbietet. Je nach Art der geplanten Ausgestaltung unterscheiden sich auch die Sicherheitsanforderungen, die an den Webserver gestellt werden müssen. In einer kleinen Organisation, in der ein Webserver als Intranet-Server ohne kritische Anwendungen betrieben wird, sehen die Anforderungen ganz anders aus als für einen Webserver, der ans Internet angeschlossen werden soll und vielleicht sogar Daten enthält, die nicht jeder abrufen können soll.

Firewall

Wenn sowohl im Intranet als auch im Internet WWW-Dienste angeboten werden sollen, empfiehlt es sich, hierfür zwei getrennte Systeme einzusetzen: einen Intranet-Webserver und einen Internet-Webserver. Wenn der Internet-Webserver auch mit dem internen Netz verbunden werden soll, muss der Übergang zum internen Netz durch eine Firewall geschützt werden, siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)*. Wenn vorgesehen ist, dass Teile der Inhalte des Webservers

aus einer Datenbank kommen sollen, muss auch die Verbindung zur Datenbank in das Firewall-Konzept für den Webserver einbezogen werden. Was bei der Anordnung von Informationsservern zu beachten ist, ist in M 2.77 *Integration von Servern in das Sicherheitsgateway* beschrieben. Bei der Erarbeitung des Konzepts für das Webangebot sollte zumindest grob festgelegt werden, wie die Anbindung ans Internet geregelt ist und welche Arten von Verbindungen zum internen Netz benötigt werden.

Der Anschluss ans Internet darf erst dann erfolgen, wenn überprüft worden ist, dass mit dem gewählten WWW-Konzept sowie den personellen und organisatorischen Randbedingungen alle Risiken beherrscht werden können.

Outsourcing in Betracht ziehen

Ein Webserver für die Präsenz einer Organisation im Internet muss nicht zwangsläufig von dieser selbst betrieben werden. Wenn die Betriebskosten oder der Administrationsaufwand zu hoch oder die Restrisiken zu unkalkulierbar erscheinen, können auch die entsprechenden Angebote von Internet Service Providern oder anderen Dienstleistern in Anspruch genommen werden, einen Webserver durch diese betreiben zu lassen. In diesem Fall muss der Baustein B 1.11 *Outsourcing* berücksichtigt werden.

Ergänzende Kontrollfragen:

- Existiert ein Konzept für das Webangebot?
- Wird das Konzept regelmäßig überprüft und nötigenfalls angepasst?

M 2.173 Festlegung einer WWW-Sicherheitsstrategie

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Webserver sind für Angreifer sehr attraktive Ziele, da einem erfolgreichen Angriff oft sehr große Publizität zuteil wird. Daher muss der Absicherung eines Webservers ein hoher Stellenwert eingeräumt werden. Vor dem Einrichten eines Webservers sollte in einer WWW-Sicherheitsstrategie beschrieben werden, welche Sicherheitsmaßnahmen in welchem Umfang umzusetzen sind. Anhand der in der WWW-Sicherheitsstrategie festgelegten Anforderungen kann dann regelmäßig überprüft werden, ob die getroffenen Maßnahmen ausreichend sind.

In der Sicherheitsstrategie für den Betrieb eines Webservers sollten die folgenden Fragen beantwortet werden:

- Wer darf welche Informationen einstellen?
- Wer ist für die Aktualität und Korrektheit der Informationen verantwortlich? Falls in einem Bereich mehrere Organisationseinheiten oder Personen Informationen einstellen dürfen, so muss außerdem ein Gesamtverantwortlicher benannt sein, der bei Konflikten entscheidet.
- Welche anderen Systeme und welche Netzverbindungen sind für den sicheren Betrieb des Webservers wichtig? Können zeitweise Störungen oder Ausfälle dieser Systeme gegebenenfalls überbrückt werden?
- Wie werden die Verantwortlichen geschult, insbesondere hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen?
- Welche Informationen dürfen nicht auf dem Webserver eingestellt werden (z. B. weil die Inhalte vertraulich sind, nicht zur Veröffentlichung geeignet sind oder nicht der Firmen- bzw. Behördenpolitik entsprechen)?
- Welche Zugriffsbeschränkungen auf den Webserver sollen realisiert werden (siehe auch M 2.175 *Aufbau eines WWW-Servers*)?

Vorgehen bei Sicherheitsvorfällen

Insbesondere wenn der Webserver ein öffentliches Webangebot beherbergt, müssen in der Sicherheitsstrategie auch Reaktionen auf bestimmte webserverspezifische Sicherheitsvorfälle festgelegt werden (siehe auch Baustein B 1.8 *Behandlung von Sicherheitsvorfällen*).

Informationsleck

- Es sollte festgelegt werden, wie verfahren wird, wenn falsche Informationen auf dem Webserver veröffentlicht wurden. Eventuell reicht das bloße Löschen der entsprechenden Dokumente nicht aus, da diese schon von Besuchern gelesen wurden. Ein solcher Vorfall muss zumindest dokumentiert werden. In Abhängigkeit von der Brisanz der Informationen müssen eventuell die Pressestelle oder die Behörden- oder Unternehmensleitung informiert werden.

Hackerangriff

- Es sollte beschrieben werden, was beim Verdacht auf einen Hackerangriff auf dem Webserver zu tun ist. Wichtig ist vor allem die Frage, wann der

Server notfalls vom Netz genommen werden muss und wer die Entscheidung dazu trifft.

- Es sollte eine Reaktion auf ein *Defacement* des Webservers festgelegt werden, also für den Fall, dass nach einem erfolgreichen Einbruch auf dem Webserver Daten oder besonders die Homepage von den Angreifern verändert wurden. In einem solchen Fall müssen grundsätzlich auch die Behörden- oder Unternehmensleitung sowie die Pressestelle bzw. die für Öffentlichkeitsarbeit zuständige Organisationseinheit informiert werden.

Defacement

Diese Punkte sollten selbst dann berücksichtigt werden, wenn der Schutzbedarf des Webangebots ansonsten nur als niedrig eingeschätzt wird. Insbesondere ein Hackerangriff oder ein Defacement können unabhängig vom konkreten Schutzbedarf bei allen öffentlichen Webangeboten passieren.

Teil einer Sicherheitsstrategie muss auch die regelmäßige Informationsbeschaffung über potentielle Sicherheitslücken sein, um rechtzeitig Vorsorge dagegen treffen zu können. Neben den in M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems* angesprochenen Informationsquellen ist für Sicherheitshinweise zur WWW-Nutzung besonderes die "World Wide Web Security FAQ" eine wertvolle Quelle. Die Master-Kopie dieses Dokumentes ist unter *http://www.w3.org/Security/Faq/* zu finden.

Ergänzende Kontrollfragen:

- Existiert eine Sicherheitsstrategie für den Betrieb eines WWW-Servers?
- Werden die getroffenen Regelungen regelmäßig überprüft und gegebenenfalls angepasst?

M 2.174 Sicherer Betrieb eines WWW-Servers

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

WWW-Server sind attraktive Ziele für Angreifer und müssen daher sehr sorgfältig konfiguriert werden, damit sie sicher betrieben werden können. Das Betriebssystem und die Software müssen so konfiguriert sein, dass der Rechner so gut wie möglich gegen Angriffe geschützt wird. Solange der Rechner nicht entsprechend konfiguriert ist, darf er nicht ans Netz genommen werden.

Daher sollte ein WWW-Server, der Informationen im Internet anbietet, entsprechend den folgenden Vorgaben installiert werden:

Minimales Betriebssystem

- Auf einem WWW-Server sollte nur ein Minimum an Programmen vorhanden sein, d. h. das Betriebssystem sollte auf die unbedingt erforderlichen Funktionalitäten reduziert werden und auch sonst sollten sich nur unbedingt benötigte Programme auf dem WWW-Server befinden (siehe M 4.95 *Minimales Betriebssystem*).
- Ein WWW-Server sollte insbesondere keine unnötigen Netzdienste enthalten, verschiedene Dienste gehören auf verschiedene Rechner (siehe M 4.97 *Ein Dienst pro Server*).

Zugriffsschutz

- Der Zugriff auf Dateien oder Verzeichnisse muss geschützt werden (siehe M 4.94 *Schutz der WWW-Dateien*).
- Die Kommunikation mit dem WWW-Server sollte durch einen Paketfilter auf ein Minimum beschränkt werden (siehe M 4.98 *Kommunikation durch Paketfilter auf Minimum beschränken*).
- Die Administration des WWW-Servers darf nur über eine sichere Verbindung erfolgen, d. h. die Administration sollte an der Konsole direkt, nach starker Authentisierung (bei Zugriff aus dem LAN) oder über eine verschlüsselte Verbindung (bei Zugriff aus dem Internet) erfolgen.
- Weiterhin sollte der WWW-Server vor dem Internet durch einen Firewall-Proxy oder aber zumindest durch einen Paketfilter (siehe M 4.98 *Kommunikation durch Paketfilter auf Minimum beschränken* beschränken) abgesichert werden. Er darf sich nicht zwischen Firewall und internem Netz befinden, da ein Fehler auf dem WWW-Server sonst Zugriffe auf interne Daten ermöglichen könnte.

Minimale Rechte

Je nach Art des WWW-Servers bieten sich unterschiedliche Möglichkeiten zum Schutz an. Allen diesen Möglichkeiten gemeinsam ist allerdings, dass der eigentliche Serverprozeß des WWW-Servers, der sogenannte *http-Daemon* oder *http-Dienst*, nur mit eingeschränkten Rechten ausgestattet sein sollte. Nicht alle Webserver-Produkte ermöglichen es, den Prozess direkt mit sehr eingeschränkten Rechten zu starten. Je nach eingesetztem Produkt muss daher individuell geprüft werden, wie ein minimales Rechteprofil realisiert werden kann.

Der Webserver-Prozess sollte, wenn möglich, nur auf einen Teil des Dateibaumes zugreifen können. Unter Unix kann dies z. B. mit dem *chroot*-Programm realisiert werden. Kann ein Angreifer nun eine Schwachstelle über den Webserver-Prozess ausnutzen, so hat er trotzdem keinen Zugriff zum eigentlichen Betriebssystem.

Beispielskripte entfernen

Außerdem sollten vom Hersteller mitgelieferte cgi-Skripte, asp-Dateien oder sonstige serverseitige Programme, die meist nur Beispielcharakter haben, vollständig entfernt werden, da sie oft Schwachstellen enthalten.

Das Verzeichnis, in dem die abrufbaren Dateien gespeichert sind, sollte auf einer eigenen Partition einer Festplatte liegen, um eine leichtere Wiederherstellung nach einem Festplattenschaden zu ermöglichen. Außerdem sollten die Unterverzeichnisse und Dateien einem speziellen Benutzer gehören (zum Beispiel *wwwadmin*) und durch minimale Zugriffsrechte vor unbefugtem Zugriff geschützt werden.

Bei der Konfiguration der Webserver-Anwendung sollten, unabhängig von der eingesetzten Webserveranwendung, einige grundlegende Aspekte berücksichtigt werden. Wie diese im einzelnen konfiguriert werden, hängt von der Webserver-Anwendung ab.

Indexdateien und Verzeichnisinhalte

Meist existieren Optionen, mit denen festgelegt werden kann, ob bei einer HTTP-Anfrage nach einem Verzeichnis (also ohne Angabe eines konkreten Dateinamens), der Inhalt des betreffenden Verzeichnisses aufgelistet werden soll, oder ob stattdessen bestimmte Dateien (beispielsweise *index.html*) zurückgegeben werden sollen. Dies sollte folgendermaßen konfiguriert werden:

- Falls eine Index-Datei existiert, wird diese zurückgeliefert.
- Falls nicht, wird eine entsprechende Fehlermeldung zurückgegeben.

Ausführung von Programmen und Skripten

Falls festgelegt werden kann, dass Programme oder cgi-Skripte nur in bestimmten Verzeichnissen ausgeführt werden dürfen, so sollte diese Option auf jeden Fall sehr eng eingestellt werden. Keinesfalls sollte die Ausführung von Programmen für den gesamten WWW-Bereich freigegeben werden. Es ist empfehlenswert, wenn möglich für Programme und Skripte ein eigenes Verzeichnis anzulegen und die Ausführung nur in diesem Verzeichnis zu gestatten.

Symbolische Links oder Verknüpfungen

Oft kann festgelegt werden, ob Dateien oder Verzeichnisse, die mittels eines symbolischen Links (Unix) oder einer Verknüpfung (Windows) in den WWW-Dateibaum "eingeblendet" wurden, angezeigt werden sollen. Dies sollte möglichst unterbunden werden, da auf diese Weise leicht Dateien zugreifbar werden können, die eigentlich nicht veröffentlicht werden sollen.

Folgende Checkliste wird empfohlen:

1. Sind nur die benötigten Komponenten installiert?
2. Ist die Webserver-Anwendung so restriktiv wie möglich konfiguriert? Beispielsweise sollten cgi-Programme entweder ganz gesperrt werden oder aber die cgi-Programme auf ein eigenes Verzeichnis beschränkt sein. Der Dateizugriff des Webserver-Prozesses sollte auf einen Teil des Verzeichnisbaums eingeschränkt sein. Für Administration und Betrieb des Servers sollten eigene unprivilegierte Benutzerkennungen verwendet werden.

3. Sind alle überflüssigen cgi-Programme, asp-Seiten, sonstige Demo-Anwendungen und WWW-Seiten gelöscht?
4. Sind nur die unbedingt nötigen Ports zugänglich (siehe auch M 4.97 *Ein Dienst pro Server*)? Auf einem Webserver wird der HTTP-Dienst üblicherweise über Port 80 angesprochen. Falls die Administration des Servers oder die Pflege der WWW-Dateien über das Netz erfolgt, können noch weitere Dienste erforderlich sein. In diesem Fall sollte aber der Zugriff auf diese Dienste so restriktiv wie möglich geregelt werden (siehe auch M 4.98 *Kommunikation durch Paketfilter auf Minimum beschränken*).
5. Ist eine angemessene regelmäßige Sicherung des Datenbestandes gewährleistet (siehe Baustein B 1.4 *Datensicherungskonzept*)?
6. Falls cgi-Programme genutzt werden, sind diese ausreichend sicher programmiert? Es dürfen keine Eingabewerte ungeprüft übernommen werden. Es muss sichergestellt sein, dass Buffer-Overflows und Race-Conditions ausgeschlossen sind. In allen Perl-Skripten sollte der Taint-Check aktiviert sein.
7. Gibt es eine funktionierende Routine für einen regelmäßigen Integritätscheck (z. B. Tripwire, siehe M 4.93 *Regelmäßige Integritätsprüfung*)?
8. Wird die Konfiguration regelmäßig überprüft? Werden Konfigurationsänderungen dokumentiert?

Beispiel: Aufbau eines einfachen WWW-Servers

Als einfacher WWW-Server wird ein Server betrachtet, bei dem sich die Inhalte einzelner Seiten nur selten ändern, keine cgi-Programme verwendet werden und es keinen besonderen Zugriffsschutz gibt. Die einzelnen WWW-Dokumente werden über einen Datenträger auf den WWW-Server eingespielt. Bei einem solchen Server können alle Systemdateien und auch alle HTML-Seiten mit einem Schreibschutz versehen werden. Ein Angreifer kann bei einem solchen Aufbau zwar noch temporäre Dateien und Protokolleinträge abändern, das System selber aber nicht mehr. Ein solcher Zugriffsschutz sollte durch ein physikalisch schreibgeschütztes Medium realisiert werden, z. B. eine oder mehrere CD-ROMs oder eine schreibgeschützte Wechselplatte. Zumindest aber sollten regelmäßige Integritätsprüfungen (siehe M 4.93 *Regelmäßige Integritätsprüfung*.

In dem http-Daemon sollten die nicht benötigten Funktionalitäten abgeschaltet werden, wie z. B. die Möglichkeit zum Ausführen von cgi-Skripten. Auf jeden Fall sollten mitgelieferte cgi-Programme entfernt werden.

Bei einer häufig vorkommenden Variante eines einfachen Webservers können die Dokumente mit entsprechenden Berechtigungen auf dem WWW-Server interaktiv abgeändert werden. In diesem Fall ist der Schutz vor unbefugten Veränderungen und eine regelmäßige Integritätsprüfung in kurzen Intervallen besonders wichtig.

M 2.175 Aufbau eines WWW-Servers

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Leiter IT, Administrator

Inbetriebnahme eines Webservers

Um einen Webserver aufbauen zu können, muss neben adäquater Hardware auch entsprechende Software beschafft werden. Dafür stehen eine Vielzahl von Produkten zur Verfügung. Bei der Auswahl ist neben der Stabilität insbesondere Wert auf die Sicherheitsmechanismen zu legen (zur Beschaffung und Installation siehe auch Baustein B 1.10 *Standardsoftware*).

Organisationsstruktur anpassen

Es muss überlegt werden, welche Informationen im Internet bzw. in einem Intranet zur Verfügung gestellt werden sollen. Weiterhin ist zu klären, wie und wo Dokumente erstellt werden, wer welche Dokumente erzeugt, welche Dokumente wo zum Einsatz kommen und wer diese Dokumente benötigt. Auf Basis dieser Erkenntnisse sollten dann Richtlinien für ein einheitliches Erscheinungsbild von Dokumenten, Dateinamen und Verzeichnisnamen aufgestellt und nach Möglichkeit standardisierte Entwicklungswerkzeuge bestimmt werden. Eventuell sollte ein eigenes WWW-Redaktionsteam eingerichtet werden (siehe M 2.272 *Einrichtung eines WWW-Redaktionsteams*).

Verantwortliche benennen

Beim Betrieb eines Webservers, egal ob intern oder extern, sollte nicht jeder Benutzer beliebig Dateien einstellen können. Es sollte daher ein Verantwortlicher für das Einstellen von Informationen benannt werden, der neue Dateien auch auf die Einhaltung der Richtlinien überprüft. Je nach Größe der Organisation können auch weitere Teil-Verantwortliche für einzelne Organisationseinheiten oder Teilbereiche des Webservers benannt werden. Entsprechend der hier gewählten Organisationsstruktur ist auch die Rechtevergabe und die Verzeichnisstruktur auf dem Webserver festzulegen. Vor allem sollte jeder Teil-Verantwortliche nur Zugriff auf die von ihm betreuten Unterverzeichnisse haben.

Automatische Kontrolle der Richtlinien

Um sicherzustellen, dass die angelegten Dateien und Verzeichnisse immer den jeweiligen Richtlinien genügen, sollte deren Einhaltung automatisiert überprüft werden, z. B. über geeignete Skripten oder Makros. Ein entsprechend vorbereitetes Programm sollte für alle zur Verfügung gestellt werden und nach jeder Änderung aufgerufen werden. Dabei sollte insbesondere überprüft werden, ob die Zugriffsrechte aller

- Verzeichnisse,
- Dateien und
- CGI-Skripte (falls eingerichtet)

korrekt gesetzt wurden.

Ein Protokoll über die durchgeführten Änderungen sollte ebenfalls direkt erzeugt werden.

Rechte- und Rollenkonzept

Ein allgemeines Problem bei der Einrichtung und beim Betrieb eines Webservers ist die notwendige Zusammenarbeit vieler verschiedener Personen mit unterschiedlichen Kompetenzen. So werden Aufgaben wie

- Erstellen neuer Inhalte,
- Administration des Webservers,
- Durchführung des Designs des Webauftritts,
- Entwurf einzelner Grafiken,
- Programmierung von Zusatzfunktionalität für den Webserver (z.B. eine Datenbankanbindung) und
- Programmieren von Zusatzfunktionalität, die auf dem WWW-Client genutzt wird (Javascript, etc.),

in der Regel von unterschiedlichen Personen wahrgenommen. Aus technischen Gründen ist in der Regel eine vollständige Trennung der Zugriffsrechte nicht oder zumindest nicht vollständig möglich. Die oben geforderten Zugriffsbeschränkungen lassen sich auf einem Entwicklungssystem daher in der Regel nicht durchsetzen. In diesem Fall muss darauf geachtet werden, dass das Entwicklungssystem keine sensitiven Daten enthält. Die Zugriffsrechte auf einem produktiven Webserver lassen sich jedoch auch in einer solchen Umgebung restriktiv handhaben. Neben der Zuständigkeit müssen auch die für den Transfer notwendigen Tätigkeiten geplant werden. Dies umfasst neben der oben erwähnten Kontrolle der vergebenen Zugriffsrechte auch eine Überprüfung der zu veröffentlichenden Inhalte.

Zugriffsbeschränkungen auf den Webserver

Vor der Inbetriebnahme bzw. jeder Aktualisierung eines Webservers muss festgelegt werden, wer Informationen vom Webserver abfragen darf. Es ist zu klären, ob nur Personen innerhalb der eigenen Organisation, eventuell zusätzlich Telearbeiter, oder auch jeder Externe oder nur ein eingeschränkter Kreis auf bereitgestellte Informationen zugreifen dürfen. Diese Einschränkungen können auch abhängig von den jeweiligen Informationen variieren

Wenn der Zugriff auf den Webserver nur einem begrenzten Personenkreis möglich sein soll, sind entsprechende Maßnahmen zu implementieren, wie z. B. in M 4.94 *Schutz der WWW-Dateien*.

Es muss außerdem geklärt werden, ob grundsätzlich nur Informationen abgerufen werden dürfen oder ob es auch für Benutzer möglich sein soll, selber neue Informationen einzustellen. Auch hier ist wieder festzulegen werden, welcher Personenkreis welche Rechte hat.

Übersichtliche Strukturierung

Da HTML-Dateien nicht hierarchisch angeordnet werden müssen, ist die Verzeichnisstruktur innerhalb eines Webservers für die Funktionsweise irrelevant. Um die Wartung zu erleichtern, sollte allerdings auf eine übersichtliche Struktur geachtet werden.

Sprechende Pfadnahmen

Es ist empfehlenswert, die Verzeichnisstruktur so zu wählen, dass der URL, unter dem eine Datei erreichbar ist, bereits gewisse Informationen über die Datei gibt. Dies führt zwar unter Umständen zu relativ langen Pfadnamen,

aber es macht es Besuchern leichter, sich bestimmte Stellen zu merken und wieder zu finden. Da viele Internet-Suchmaschinen bei einer Suche den vollständigen WWW-Pfad eines Treffers ausgeben, verbessert diese Art der Strukturierung auch die Auffindbarkeit der Informationen.

Da unter Umständen in anderen Webservern Links auf ihre Dokumente angelegt werden, sind Änderungen an Dokument- und Verzeichnisnamen zu vermeiden. Die Verzeichnisstruktur muss deshalb erweiterungsfähig geplant werden.

Dokumente bereitstellen

Ein öffentliches Webangebot im Internet ist eine Form der Außendarstellung einer Organisation. Entsprechend sorgfältig sollte daher die Internet-Präsenz vorbereitet werden.

Es empfiehlt sich, mit einem Webangebot im Intranet erste Erfahrungen zu sammeln, bevor ein Webserver an das Internet angebunden wird. Hier sollte mit wenigen, einfachen Anwendungen begonnen werden.

Informationen in einem Webangebot werden normalerweise in HTML-Dateien bereitgestellt, die direkt im Webbrowser dargestellt werden können. Es können aber auch Dateien in beliebigen anderen Formaten zum Download bereitgestellt werden. In diesem Fall muss die Anwendung zum Anzeigen des Dokuments beim Benutzer vorhanden sein und die Dateien müssen im Allgemeinen zunächst auf dem IT-System des Benutzers gespeichert werden, bevor sie weiterverarbeitet werden können.

Sofern es nicht erforderlich ist, dass Benutzer in den bereitgestellten Dokumenten Änderungen vornehmen (beispielsweise Ausfüllen von Formularen), sollten Dokumente in Formaten bereitgestellt werden, bei denen Veränderungen nicht einfach möglich sind. Proprietäre Dokumentenformate sollten so weit wie möglich vermieden werden.

Qualitätssicherung

Alle für die Veröffentlichung im Internet vorgesehenen HTML-Dokumente und WWW-Dateien sollten vor der Veröffentlichung genauso qualitätsgesichert und inhaltlich genehmigt werden wie jede andere Veröffentlichung.

HTML-Dokumente werden meist mit speziellen HTML-Editoren erstellt. In anderen Formaten erstellte Dokumente können mit HTML-Konvertern in HTML umgewandelt werden.

Sollen viele, sich oft ändernde Dokumente zur Verfügung gestellt werden, empfiehlt es sich, den Webserver mit einer Dokumentendatenbank zu verbinden. Diese Lösung bietet dem Benutzer schnelle Such-, Ansichts- und Dokumentenverwaltungsmöglichkeit. Nützlich ist es auch, wenn mit Hilfe einer Datenbankanbindung der Zugriff auf bereits vorhandene Firmendaten ermöglicht wird. In diesem Fall muss jedoch der Datenbankserver bzw. die Dokumentendatenbank in das WWW-Sicherheitskonzept mit einbezogen werden.

Vor dem Einstellen neuer Dateien auf einem Webserver sind diese auf eventuell noch enthaltene Restinformationen zu überprüfen (siehe M 4.64 *Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen*).

Konfigurationsmanagement

Da sich die Inhalte von WWW-Seiten erfahrungsgemäß häufig ändern, ist es wichtig, ein funktionierendes Konfigurationsmanagement aufgebaut zu haben. Die Aktualität von Links und Verweisen ist zu überprüfen, ebenso wie vor Veröffentlichung eine Virenkontrolle mit einem aktuellen Computer-Virensuchprogramm durchzuführen ist.

Kontrolle und Freigabeverfahren

Freigabeverfahren

Es ist ebenso wichtig, dass alle Veröffentlichungen ein festgelegtes und nachvollziehbares Kontrollverfahren durchlaufen. Dies sollte eine inhaltliche Qualitätskontrolle ebenso umfassen wie eine formale Freigabe. Hier muss auch überprüft werden, ob die Informationen überhaupt für eine Veröffentlichung geeignet sind oder ob sie z. B. vertraulich sind, dem Datenschutz unterliegen, Copyright-geschützt sind oder ähnliches.

Bei größeren Webangeboten kann es sinnvoll sein, ein Web-Content-Management-System einzusetzen. Solche Systeme vereinfachen viele Arbeitsabläufe, die im Zusammenhang mit der Pflege eines Webangebots anfallen. Informationen, die zur Veröffentlichung über elektronische Medien freigegeben worden sind, sollten digital signiert werden, um allen Lesern die Möglichkeit zu geben, die Authentizität der Informationen zu überprüfen.

Veröffentlichungen, die nicht die Meinung der Organisation widerspiegeln, müssen als solche gekennzeichnet sein.

Beachtung rechtlicher Rahmenbedingungen

Beim Betrieb eines Webservers müssen verschiedene rechtliche Rahmenbedingungen (in Deutschland sind dies unter anderem das Teledienstegesetz, der Mediendienste-Staatsvertrag, Vorschriften zum Datenschutz) berücksichtigt werden.

Beispielsweise wird für ein gewerbliches WWW-Angebot das Vorhandensein eines Impressums gefordert, in dem der Name der verantwortlichen Person und eine Kontaktadresse genannt werden müssen. Je nach dem Inhalt des WWW-Angebots oder der Branche des Anbieters sind unter Umständen weitere Angaben erforderlich. Bevor ein WWW-Angebot freigeschaltet wird, sollte geklärt sein, welche Informationen dies sind und wo und in welcher Form diese veröffentlicht werden müssen.

Ergänzende Kontrollfragen:

- Existieren Richtlinien für Inhalt und Form von Dokumenten, die auf dem Webserver veröffentlicht werden? Gibt es Richtlinien für ein einheitliches Erscheinungsbild?
- Wie werden Dokumente vor ihrer Veröffentlichung qualitätsgesichert?
- Existiert ein Rechte- und Rollenkonzept?
- Gibt es ein Freigabeverfahren bei der Veröffentlichung von Dokumenten auf dem Webserver?
- Werden Links regelmäßig überprüft?
- Sind alle vorgeschriebenen Angaben wie Impressum vorhanden?

M 2.176 Geeignete Auswahl eines Internet Service Providers

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT

Bei einem Provider, über den ein Benutzer an das Internet angeschlossen ist, fallen nicht nur Informationen über ein- und ausgehende E-Mail an, sondern auch über alle WWW-Seiten, die die Benutzer aufrufen. Außerdem laufen alle Daten, die zwischen dem Rechner des Benutzers und einem Server im Internet ausgetauscht werden, über die IT-Systeme des Providers.

Bei der Auswahl eines Internet Service Providers sollte hinterfragt werden,

- ob Ansprechpartner zu technischen Problemen rund um die Uhr zur Verfügung stehen und wie kompetent diese sind,
- wie er auf den Ausfall einer oder mehrerer seiner IT-Systeme vorbereitet ist (Notfallplanung, Datensicherungskonzept),
- welche Verfügbarkeit (maximale Ausfallzeit) er garantieren kann,
- ob er regelmäßig überprüft, ob die Verbindungen zum Kunden noch stabil sind und im negativen Fall entsprechende Schritte unternimmt,
- was er zur Absicherung seiner IT-Systeme und der seiner Kunden unternimmt.

Sicherheitsrichtlinien des Providers vorlegen lassen

Man sollte sich vom Provider dokumentieren lassen, dass dessen IT-Systeme sicher betrieben werden, also z. B. die in M 2.174 *Sicherer Betrieb eines WWW-Servers* beschriebenen Anforderungen erfüllt sind. Alle relevanten Maßnahmen zu vernetzten Systemen und zu Datenübertragungseinrichtungen sollten umgesetzt sein. Bei jedem Provider sollte ein IT-Sicherheitskonzept und Sicherheitsrichtlinien selbstverständlich sein. Die Sicherheitsrichtlinien sollten für Externe einsehbar sein. Die Mitarbeiter des Providers sollten für IT-Sicherheitsaspekte sensibilisiert sein, auf die Einhaltung der Sicherheitsrichtlinie verpflichtet worden sein und regelmäßig geschult werden (nicht nur in Sicherheitsfragen).

Datenschutz

Beim Provider sind Daten über die Benutzer für Abrechnungszwecke gespeichert (Name, Adresse, Benutzer-Kennung, Bankverbindung) ebenso wie Verbindungsdaten und für eine je nach Provider kürzere oder längere Zeitspanne auch die übertragenen Inhalte.

Die Anwender sollten sich bei ihrem Provider erkundigen, welche Daten wie lange über sie gespeichert werden. Bei der Auswahl von Providern sollte berücksichtigt werden, dass deutsche Betreiber den einschlägigen datenschutzrechtlichen Regelungen für die Verarbeitung dieser Daten unterliegen.

Ergänzende Kontrollfragen:

- Nach welchen Kriterien ist der Provider ausgewählt worden?
- Welche Sicherheitsmechanismen werden beim Provider umgesetzt?

M 2.177 Sicherheit bei Umzügen

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter Organisation, Leiter Haustechnik, Leiter IT, IT-Sicherheitsmanagement

Bei einem Umzug müssen neben Möbeln auch die verschiedensten Datenträger (z. B. Papier, Disketten, Magnetbänder, CD-ROMs) und IT-Systeme hin und her transportiert werden. Dabei verlassen Informationen, IT-Systeme und sonstiges Material den gesicherten Bereich der Büroumgebung und werden durch Personal transportiert, das normalerweise keine Zugriffsrechte hat. Bei einem Umzug, insbesondere wenn größere Teile der Organisation davon betroffen sind, ist ein gewisses Durcheinander nie auszuschließen und es kann auch nicht jede Umzugskiste permanent persönlich beaufsichtigt werden. Trotzdem ist dafür Sorge zu tragen, dass bei einem Umzug sensitive Daten weder verloren, beschädigt, noch Unbefugten zugänglich werden.

In die Umzugsplanung sollte möglichst frühzeitig das IT-Sicherheitsmanagement und der Datenschutzbeauftragte einbezogen werden, um die aus Sicht der IT-Sicherheit festzulegenden Rahmenbedingungen festzulegen:

- Bei der Planung eines Umzuges muss im Vorfeld detailliert festgelegt werden, wer mit welchem Transportgut wann wohin umzieht (Erstellung eines Umzugskonzepts). Dies sollte ohnehin eine Selbstverständlichkeit sein, damit die Arbeit nach dem Umzug möglichst reibungslos wieder aufgenommen werden kann.
- In Abhängigkeit vom Schutzbedarf der Daten muss festgelegt werden, welche Randbedingungen für den Transport einzuhalten sind. Beispielsweise sollten für sensiblere Daten verschließbare Transportbehälter (siehe M 2.44 *Sichere Verpackung der Datenträger*) benutzt werden oder die Datenträger vor dem Transport verschlüsselt werden.
- Vor jedem Transport von IT-Systemen sollten Datensicherungen angefertigt werden. Hierbei ist neben den in M 6.35 *Festlegung der Verfahrensweise für die Datensicherung* beschriebenen Modalitäten insbesondere zu beachten, dass die Datensicherungen auf keinen Fall zusammen mit den gesicherten IT-Systemen transportiert werden dürfen. Hierdurch wird sichergestellt, dass nicht alle Speichermedien gleichzeitig beschädigt werden oder abhanden kommen.
- Es sollte ein Merkblatt (Umzugsmerkblatt)für alle betroffenen Mitarbeiter ausgearbeitet werden, in dem alle durchzuführenden IT-Sicherheitsmaßnahmen genau beschrieben sind.

Bei einem Umzug ist nicht nur der Transport eine kritische Phase, sondern auch der Zeitraum kurz vor bzw. danach. In dieser Phase kommen erfahrungsgemäß viele Sachen abhanden, da zu diesem Zeitpunkt die Standardsicherheitsverfahren wie z. B. die Zutrittskontrolle noch nicht greifen. Auch während des Umzugs sollten daher gewisse organisatorische Mindestanforderungen erfüllt sein:

- Für alle zu transportierenden Materialen sollten Transportpapiere ausgestellt werden, aus denen hervorgeht,

  - ob eine bestimmte Transportart zu beachten ist (z. B. zerbrechlich, Computerspezialtransport, etc.),
  - wohin sie gebracht werden sollen (genaue Gebäude-, Etagen- und Raumbeschreibung),
  - wer berechtigte Empfänger der transportierten Gegenstände sind,
  - wer sie abgeholt bzw. angeliefert hat (inklusive Name, Datum und Uhrzeit).
- Das Transportgut muss so gekennzeichnet sein, dass es eindeutig identifiziert werden kann, so dass auch der Transportweg nachvollzogen werden kann. Die Kennzeichnung sollte jedoch keine Rückschlüsse auf die Sensitivität des Inhalts erlauben. Die Art der Kennzeichnung sollte so gewählt sein, dass sie nicht problemlos nachgemacht und werden kann. Hierfür könnten die Umzugsvorbereiter spezielle Etiketten zur Verfügung stellen. Hierbei ist darauf zu achten, dass sich die Etiketten von den Gegenständen auch rückstandsfrei wieder ablösen lassen, ohne das Umzugsgut zu beschädigen bzw. zu verunreinigen.
- Auch während eines Umzuges sollte kein ungeordnetes Kommen und Gehen herrschen. Die beauftragten Umzugsfirmen sollten die Personalien der vorgesehenen Mitarbeiter vorher bekannt geben. Bei plötzlichen Personalwechsel (Urlaub, Krankheit, etc.) sollten die Namen des Ersatzpersonals kurzfristig mitgeteilt werden. Mit einer Namensliste der am Umzug Beteiligten können dann die Pförtner oder andere interne Mitarbeiter je nach Liegenschaft und Gegebenheit sporadisch oder kontinuierlich kontrollieren. Die am Umzug beteiligten externen Kräfte sollten mit gut sichtbaren Ausweisen (ggf. mit Namen) versehen werden, damit klar erkennbar ist, wer zutrittsberechtigt ist.
- Das Transportgut, insbesondere die Datenträger sind vor und nach dem Umzug sicher aufzubewahren. Die Räume, in denen keine Umzugstätigkeiten stattfinden, in denen sich aber keine Mitarbeiter aufhalten, also z. B. die, die noch nicht ausgeräumt bzw. bereits eingeräumt wurden, sollten abgeschlossen werden.

Nach erfolgtem Umzug sollte möglichst rasch ein geordneter Betrieb aufgenommen werden. Als Erstes ist die infrastrukturelle und organisatorische Sicherheit in den neuen Büros wiederherzustellen, also z. B.

- sollte die Zutrittskontrolle wieder in vollem Umfang aufgenommen werden,
- sollten die Brandlasten aus den Fluren entfernt werden, d. h. die Umzugskartons in die neuen Arbeitsräume geschafft werden,
- ist das angelieferte Umzugsgut darauf zu überprüfen, ob es vollständig und voll funktionsfähig ist und nicht manipuliert wurde,
- sollte die Vollständigkeit des Umzugsgutes von jedem Mitarbeiter sofort überprüft werden und gegebenenfalls eine Verlust-Liste angefertigt werden. Hierzu könnte den Betroffenen ebenfalls ein bereits im Vorfeld vorbereitetes Formular ausgehändigt werden, in dem bereits das abtransportierte Umzugsgut aufgelistet werden kann. So kann auch der

Vertreter bei Abwesenheit wegen Urlaub, Krankheit oder dringender Dienstgeschäfte der betroffenen Kollegen sofort das Fehlen von Teilen des Umzugsgutes feststellen und melden. Der zu vertretende Mitarbeiter sollte hiervon eine Kopie erhalten, um im nachhinein noch etwaige Unstimmigkeiten melden zu können.

Besondere Sorgfalt sollte auf die Umzugsplanung für alle Server und Netzkoppelelemente verwendet werden, da auch bei Ausfall nur einer Komponente unter Umständen das ganze Netz nicht betriebsfähig ist.

Vor einem Umzug sollten daher auf Seiten der zentralen IT-Administration verschiedene Vorkehrungen getroffen werden, um den reibungslosen Arbeitsablauf sicherzustellen:

- Vor Beginn der Umzugsphase sollte frühzeitig ein Plan für die erforderlichen Änderungen der Benutzeranbindung erstellt werden. Hierbei sollte besonders analysiert werden, ob neue Beschaffungen für den reibungslosen Wechsel der Rechneranbindung von Mitarbeitern erforderlich sind. Auch aus Sicherheitsgründen ist es wichtig zu wissen, welche Änderungen sich durch den Umzug im Kommunikationsverhalten der IT-Systeme ergeben. Je nach dem Schutzbedarf der Arbeit von Mitarbeitern kann es beispielsweise erforderlich werden, eine Netzverbindung zu verschlüsseln oder den Zugriff auf bestimmte Datenbestände zu unterbinden.
- Bevor ein Mitarbeiter umzieht, sollte sichergestellt sein, dass er in seinem neuen Büro über das lokale Netz erreichbar ist und seine Applikationen und Dienste betriebsbereit sind. Dies erfordert gegebenenfalls neben Änderungen am Endgerät (Routing, Softwarekonfiguration etc.) auch baldige Änderungen auf Serverseite im LAN oder gar auf Routern im WAN. Hier kann es erforderlich sein, neue Adressen oder Routen einzurichten und alte zu löschen. Möglicherweise müssen vorher neue Netzkomponenten beschafft und eingerichtet werden.
- Bei einem Umzug ist es oft auch erforderlich, für die betroffenen Mitarbeiter Benutzer-Accounts auf einem neuen Server einzurichten. Es ist darauf zu achten, dass die erforderlichen Rechte und Zugriffe auf Applikationen und Protokolle eingerichtet werden. Auch die Sicherheitseinstellungen der Benutzerumgebung müssen seinem Sicherheitsprofil entsprechend gewahrt bleiben. Alte Benutzereinträge und Endgerät-Zugangseinträge müssen auf dem alten System angepasst oder gelöscht werden. Der Zugriff auf benutzereigene Datenbereiche sollte ihm dennoch für eine Übergangszeit, jedoch mit verbindlichem Hinweis auf Löschung nach einer Karenzzeit, gewährt bleiben. Nach dieser Karenzzeit muss die Löschung durch den Administrator vollzogen werden.

Besondere Vorkehrungen sind beim Umzug der Komponenten des Rechenzentrums, wie Daten- oder Kommunikationsservern, zu treffen. Im Folgenden werden Maßnahmen beschrieben, die möglichst kurze Ausfallzeiten der Komponenten gewährleisten sollen.

- Wenn möglich, sollte ein neuer Server vorab installiert und in der neuen Räumlichkeit getestet werden. Ist dies nicht möglich, so sollte der alte Server so gut wie möglich vorkonfiguriert werden und erst zu einer Zeit, zu

der wenig Zugriffe zu erwarten sind, nach ausreichender Vorankündigung umgestellt werden. Hierbei sollte die alte Konfiguration immer vorab gesichert sein.

- Der Server sollte vor dem Umzug komplett gesichert werden. Wenn nicht bereits vorhanden, ist auch ein bootfähiges Sicherungsmedium zu erzeugen. Sensible Serverteile wie Festplatten sollten für den Ausfall des Originals als Image redundant vorgehalten sein und getrennt vom Server transportiert werden. Es ist darauf zu achten, dass die Datensicherung und das Image ebenso wie der Server beim Transport gesichert ist (z. B. Verschlüsselung, verschlossene Box, Bewachung).
- Vor dem Umzug ist sicherzustellen, dass die Infrastruktur in den neuen Räumlichkeiten für den einwandfreien Serverbetrieb vorhanden und getestet sind. Hier ist neben dem Vorhandensein des Netzes (Strom, LAN, WAN) auch auf die richtige Reihenfolge des Umzuges der Komponenten zu achten. Es ist beispielsweise wenig sinnvoll, zuerst den Internet-Webserver umziehen zu lassen, wenn der Firewall mit seinem Kommunikationsrouter erst wesentlich später aufgebaut wird.
- Vor dem Umzug sollte überprüft werden, ob unter den zu transportierenden IT-Komponenten solche sind, die besondere Umgebungsbedingungen während des Umzuges benötigen. Beispielsweise gibt es Controller für größere (und teurere!) IT-Systeme, die nicht nur in klimatisierten Räumen betrieben, sondern auch klimatisiert transportiert werden müssen.

Weiterhin sollte sichergestellt sein, dass die neuen Telefonnummern bereits erreichbar sind, sobald die Mitarbeiter ihre neuen Büros bezogen haben. Bei einem Umzug innerhalb eines Ortes sollte versucht werden, die alten Telefonnummern zumindest übergangsweise zu behalten. Während des Umzugs sollte sowohl in der alten als auch in der neuen Liegenschaft die telefonische Erreichbarkeit gewährleistet sein, damit bei auftretenden Problemen Rückfragen jederzeit möglich sind.

Ergänzende Kontrollfragen:

- Sind rechtzeitig vor einem geplanten Umzug Sicherheitsrichtlinien erarbeitet worden?
- Sind alle Mitarbeiter über die vor, während und nach dem Umzug zu beachtenden IT-Sicherheitsmaßnahmen informiert worden?
- Liegt eine Liste des zu transportierenden Umzugsgutes vor?

M 2.178 Erstellung einer Sicherheitsleitlinie für die Faxnutzung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Vor der Installation, Konfiguration und Freigabe von Faxservern sollte zunächst eine Sicherheitsleitlinie für die Faxnutzung festgelegt werden. Folgende Punkte werden üblicherweise mit solch einer Sicherheitsleitlinie geregelt:

1. Einsatzkonzept

Bevor ein Faxserver für die Nutzung freigegeben wird, muss zunächst festgelegt werden, in welcher Einsatzart das System betrieben werden soll. So ist z. B. denkbar, dass ein Faxserver nur dazu dient, Faxe über das LAN entgegenzunehmen und dann nach außen zu versenden. Ein Faxserver kann aber auch von außen eingehende Faxsendungen entgegennehmen. In diesem Fall muss festgelegt werden, wie die Eingangs-Faxsendungen an die Empfänger weitergeleitet werden. Die erste Möglichkeit besteht dabei in der Weiterleitung durch den Faxserver selbst, ggf. mit Anbindung an bereits bestehende E-Mail oder Workflow-Systeme. Eine andere Möglichkeit ist die manuelle Weiterleitung der Eingangs-Faxsendungen durch die Poststelle. Hier besteht einmal die Möglichkeit der Weiterleitung per E-Mail. Denkbar ist aber auch, dass die Poststelle eingehende Faxe ausdruckt und diese Ausdrucke an den Empfänger weiterleitet (siehe M 2.181 *Auswahl eines geeigneten Faxservers*).

2. Integration in den Geschäftsablauf

Von der Betriebsart hängt auch ab, wie bei Benutzung eines Faxservers versandte oder empfangene Faxe in den Geschäftsablauf integriert werden. Sofern die Poststelle alle Faxeingänge ausdruckt und die Ausdrucke an den jeweiligen Empfänger weiterleitet, entspricht dies dem Ablauf, wie er auch bei herkömmlichen Faxgeräten üblich ist. Werden aber Faxe direkt aus einer Applikation vom Arbeitsplatzrechner des Benutzers versandt oder werden Faxeingänge direkt vom Faxserver an den Empfänger übermittelt, unterscheiden sich diese Verfahren erheblich von denen bei der Benutzung herkömmlicher Faxgeräte. Daher sollte in diesem Fall in der Richtlinie für die Faxnutzung festgelegt werden, von welchen Faxeingängen und Faxausgängen Ausdrucke für die Akten gefertigt werden müssen.

3. Regelungen zum Faxserver-Einsatz

Um den sicheren Betrieb und Einsatz eines Faxservers sicherstellen zu können, müssen eine Reihe von Regelungen getroffen werden (siehe M 2.179 *Regelungen für den Faxserver-Einsatz*).

4. Inhaltliche Restriktionen

Weiterhin sollte in der Fax-Sicherheitsleitlinie festgelegt werden, welche Informationen überhaupt per Fax weitergegeben werden dürfen. Es kann in der Fax-Sicherheitsleitlinie zudem festgelegt werden, welche Kommunikationspartner welche Informationen erhalten dürfen. Damit wird erreicht, dass der Empfänger auch die notwendigen Berechtigungen zum Weiterverar-

beiten der Information besitzt. Beispielsweise kann festgelegt werden, dass Preislisten nur an Einkäufer oder Projektunterlagen nur an Projektbeteiligte per Fax versendet werden dürfen.

5. Notfallvorsorge und Ausfallsicherheit

Außerdem sollten in der Faxsicherheitsleitlinie Aussagen zur Notfallvorsorge und zur Ausfallsicherheit des Faxbetriebes enthalten sein. Abhängig von den Anforderungen an den Wert Verfügbarkeit ist ggf. der Einsatz redundanter Faxserver sinnvoll. In diesen Bereich fallen auch Überlegungen, ob für den Notfall noch herkömmliche Faxgeräte verfügbar gehalten werden (siehe auch M 6.69 *Notfallvorsorge und Ausfallsicherheit bei Faxservern*).

6. Datensicherung

Der Faxserver sollte in das Datensicherungskonzept der Organisation aufgenommen werden (siehe Baustein B 1.4 *Datensicherungskonzept*). Insbesondere ist dabei festzulegen, wer für die Durchführung der Datensicherungen zuständig ist und was zu sichern ist. Gegenstand der Datensicherung können dabei die Software, Konfigurationsdaten, gespeicherte bzw. archivierte Faxdaten oder auch Protokolldateien sein. Außerdem sind Festlegungen hinsichtlich des Sicherungsintervalls und der Anzahl der aufzubewahrenden Generationen notwendig. Es muss festgelegt werden, wer für die Überprüfung der bei der Datensicherung anfallenden Protokolle zuständig ist. Schließlich sollten sowohl die Durchführung der Datensicherung als auch die Auswertung der Protokolle dokumentiert werden.

7. Schulung

Die Faxsicherheitsleitlinie sollte zudem um ein organisationsweites Schulungskonzept ergänzt werden. Zunächst ist das Personal, dass das IT-System und die Faxserver-Applikation administriert, entsprechend zu schulen. Dann sollten die Benutzer für die Gefährdungen sensibilisiert werden, die durch einen Faxserver im Vergleich zu einem herkömmlichen Faxsystem entstehen.

Ergänzende Kontrollfragen:

- Existiert eine Sicherheitsleitlinie für die Faxnutzung?
- Wird die Sicherheitsleitlinie für die Faxnutzung regelmäßig an das Einsatzumfeld angepasst?

M 2.179 Regelungen für den Faxserver-Einsatz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Fax-Poststelle

Um den reibungslosen Betrieb des oder der Faxserver zu gewährleisten, müssen folgende Punkte geregelt werden:

1. Festlegung von Zuständigkeiten

Ein Faxserver besteht aus einem IT-System, dem darauf installierten Betriebssystem sowie der Faxserver-Applikation. Dazu kommen dann noch die Faxclients der Benutzer. Dementsprechend muss auch die Betreuung geregelt werden. Je nach der vorhandenen Organisationsstruktur müssen Verantwortliche für diese Bereiche benannt werden. Im Extremfall kann dies heißen, dass jeder dieser Bereiche von anderen Administratoren betreut wird. Die Administration des Betriebssystems kann z. B. durch die Organisationseinheit erfolgen, die auch für die Administration der sonstigen IT-Systeme zuständig ist. Die Administration der Faxapplikation sollte hingegegen durch die Fax-Poststelle erfolgen. Je nach Einsatzart ist diese Stelle auch dafür verantwortlich, dass eingehende Faxsendungen an den zuständigen Bearbeiter weitergeleitet werden. Diese Stelle sollte dann auch für die Vergabe von Berechtigungen auf dem Faxserver verantwortlich sein. Weitere Aufgaben sind z. B. die Rücksetzung von Passwörtern und die Einrichtung von neuen Benutzern. Von besonderer Bedeutung ist daher die Festlegung der Aufgaben und Zuständigkeiten der Fax-Poststelle (siehe M 2.180 *Einrichten einer Fax-Poststelle*).

2. Festlegung des Benutzerkreises

Außerdem sollte der Personenkreis festgelegt werden, der berechtigt ist, den Faxserver zu benutzen. Dabei sind u. a. folgende Berechtigungen für eingehende Faxsendungen denkbar:

- lesen,
- weiterleiten,
- löschen.

Für ausgehende Faxsendungen sind folgende Berechtigungen denkbar:

- senden,
- anhalten,
- löschen,
- Sendeoptionen verändern.

Diese Berechtigungen sollten, wie in der Administration allgemein üblich, möglichst nur an Benutzergruppen und nur im Ausnahmefall an einzelne Benutzer vergeben werden (siehe auch M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*).

3. Festlegung von Nutzungsprofilen

Es sollte auch geregelt werden, in welchem Umfang berechtigte Benutzer den Faxserver in Anspruch nehmen dürfen. Dies ist insbesondere wichtig, um Überlastungen durch Serienfaxe zu verhindern.

4. Nutzungszeiten

Außerdem sollte überlegt werden, ob die Nutzung von Faxservern nur zu bestimmten Zeiten zugelassen wird. So kann z. B. verhindert werden, dass außerhalb der Arbeitszeiten Faxe versendet werden können.

5. Einrichtung von Gruppen

Sofern Faxeingänge automatisch an die Empfänger durch den Faxserver weitergeleitet werden, sollten für bestimmte Funktionen und Aufgaben eigene Faxnummern eingerichtet werden. Allen Mitgliedern einer Gruppe kann dann der Zugriff auf die für die entsprechende Rufnummer eingehenden Faxsendungen gewährt werden. Dies erleichtert auch etwaige Vertretungsregelungen.

Beispiel: In einem Unternehmen wird ein Faxserver betrieben, der eingehende Faxsendungen automatisch an die Empfänger weiterleitet. Eine -Rufnummer wird die Bestellannahme vergeben. Der Faxserver leitet alle Faxsendungen mit Bestellungen, die über diese Rufnummer an das Unternehmen übermittelt werden, nicht an einen einzelnen Mitarbeiter, sondern an alle Mitglieder der Bestellannahme weiter. Dabei muss durch das Unternehmen festgelegt werden, in welcher Reihenfolge die Mitarbeiter Eingangsfaxsendungen bearbeiten, um Bestellungen nicht doppelt auszuführen.

6. Vertretungsregelung

Gerade beim Einsatz von Faxservern, die Faxeingänge an einzelne Benutzer zustellen, ist eine Vertretungsregelung im Falle der Abwesenheit unumgänglich und daher eine entsprechende Verpflichtung in die Sicherheitspolitik aufzunehmen. Ansonsten kann nicht ausgeschlossen werden, dass wichtige Faxeingänge über einen längeren Zeitraum nicht zur Kenntnis genommen werden. Insoweit unterscheidet sich das Verfahren beim Einsatz von Faxservern erheblich von dem beim Einsatz herkömmlicher Faxgeräte. Bei letzteren werden Eingänge durch die Vertreter eher wahrgenommen, da die Faxe in Papierform vorliegen.

7. Protokollierung

Es sollten Regelungen für den Umgang mit anfallenden Protokolldaten erarbeitet werden. So sollte festgelegt werden, wer welche Protokolldaten in welchen Abständen auswerten muss (siehe *M 2.64* Kontrolle der Protokolldateien).

8. Adressbücher

Auch sollte festgelegt werden, welche Adressbücher zum Einsatz kommen und wer die Pflege übernimmt. Viele Faxserver-Applikationen bieten die Möglichkeit, sowohl individuelle als auch unternehmensweit gültige Adressbücher anzulegen. Zudem ist es häufig auch möglich, die Adressbücher von Faxservern mit den Verteilerlisten/Adressbüchern bereits vorhandener E-Mail-

systeme zu synchronisieren. Während organisationsweit gültige Adressbücher zentral durch die Fax-Poststelle gepflegt werden sollten, muss dies bei den individuellen Adressbüchern durch die Benutzer selbst erfolgen. Die Benutzer sollten außerdem verpflichtet werden, bei wichtigen Faxsendungen (z. B. individuelle Angebote) die Empfängerrufnummer zu überprüfen.

9. Nutzung des Faxservers

Außerdem müssen auch Regelungen für die Nutzung des Faxservers durch die Mitarbeiter erarbeitet werden (siehe M 3.15 *Informationen für alle Mitarbeiter über die Faxnutzung*). Schließlich ist festzulegen, welche Rechte die Mitarbeiter auf dem Faxserver ausüben dürfen.

10. Schutz der Faxclients

Es muss durch geeignete organisatorische und technische Maßnahmen sichergestellt werden, dass keine Faxe unbefugt gelesen oder unbefugt bzw. unbeabsichtigt gesendet werden. Die Benutzer sind daher für die Benutzung der Fax-Programme zu schulen und hinsichtlich der auftretenden Risiken zu sensibilisieren.

Von besonderer Bedeutung ist die Authentisierung der Mitarbeiter am Faxserver. Diese kann explizit über einen Faxclient oder aber auch mit der Anmeldung an einem Verzeichnisdienst, einem Domänen-Controller (bei Verwendung von Microsoft Windows NT) oder an einem E-Mail-System erfolgen. Sofern die Authentisierung zwischen Mitarbeiter und Faxserver über einen Client erfolgt, sollte möglichst darauf verzichtet werden, das Anmelde-Passwort auf der Festplatte abzulegen, da dadurch dieser Sicherheitsmechanismus seinen Wert verliert. Jeder, der auf den entsprechenden Faxclient Zugriff hat, kann unter fremdem Namen Faxe versenden und unbefugt eingehende Faxsendungen lesen. Weiterhin sind die Mitarbeiter dazu anzuhalten, sich nach der Abholung eingegangener Faxsendungen und nach der Versendung von Ausgangsfaxen wieder am Faxserver abzumelden. Es ist darauf hinzuwirken, dass Mitarbeiter beim Verlassen des Arbeitsplatzes den Rechner schützen, z. B. durch die Benutzung eines Bildschirmschoners mit Passwort oder über Mechanismen des eingesetzten Betriebssystems (siehe M 4.1 *Passwortschutz für IT-Systeme* und M 4.2 *Bildschirmsperre)*.

11. Reparatur und Wartung

Es sollten auch Regelungen zur Durchführung von Reparatur- und Wartungsarbeiten des Faxservers festgelegt werden. Für die Administratoren des Systems muss klar sein, wer im Wartungs- und Reparaturfall zu benachrichtigen ist. Auch sollte geregelt werden, wie mit defekten Datenträgern, insbesondere defekten Festplatten umgegangen werden muss.

Ergänzende Kontrollfragen:

- Werden die Regelungen für den Faxserver-Einsatz regelmäßig an das Einsatzumfeld angepasst?
- Sind Regelungen für die Weiterleitung von eingehenden Faxsendungen bei Abwesenheit des Empfängers in Kraft?
- Sind Regelungen für die Schulung der Mitarbeiter über die Nutzung der Faxprogramme vorhanden?

M 2.180 Einrichten einer Fax-Poststelle

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um den reibungslosen Betrieb des oder der Faxserver zu gewährleisten, muss eine Fax-Poststelle eingerichtet und damit ein Fax-Verantwortlicher benannt werden. Die Fax-Poststelle hat dabei diverse organisatorische und technische Aufgaben wahrzunehmen, die auch von der Betriebsart des Faxservers abhängen.

sorgfältige Auswahl der Mitarbeiter

Da die Mitarbeiter der Fax-Poststelle im Regelfall Zugriff auf alle eingehenden und ausgehenden Faxsendungen haben, muss an die Auswahl des Personals ebenso hohe Anforderungen gestellt werden, wie dies bei Administratoren notwendig ist.

Die Fax-Poststelle muss außerdem mit den Verantwortlichen für die sonstigen Kommunikationsdienste (insbesondere E-Mail und Telekommunikationsanlage) eng zusammenarbeiten.

ständige Erreichbarkeit

Die Fax-Poststelle sollte für alle Benutzer jederzeit erreichbar sein. Im Rahmen von Vertretungsregelungen ist sicherzustellen, dass die Fax-Poststelle ständig besetzt ist.

Typische Aufgaben einer Faxserver-Poststelle sind:

- Administration der Faxserver-Applikation. Dazu gehört:
  - Einrichtung neuer Benutzer,
  - Vergabe von Berechtigungen an Benutzer und Benutzergruppen,
  - Rücksetzen von Passwörtern,
  - Überprüfung der Kommunikationsverbindungen,
  - Auswertung der anfallenden Protokolle,
  - Anlaufstelle der Benutzer bei Problemen,
  - Pflege der zentralen Adressbücher und Verteilerlisten,
  - Durchführung von Datensicherungen, sofern dies nicht Aufgabe der Administration des Betriebssystems ist,
- Faxzustellung und Archivierung,
- Fehlerbehebung bei der Faxzustellung
- Koordination der Zusammenarbeit mit TK-Anlagen- und E-Mail-Verantwortlichen.

Betreuung der Faxclients

Schließlich sollte auch die Faxclient-Software auf den Arbeitsplatzrechnern betreut werden. Diese Aufgabe kann sowohl durch die Fax-Poststelle als auch durch die Organisationseinheit erfolgen, die die Arbeitsplatzrechner betreut.

Einer besonderen Betrachtung bedürfen noch die Aufgaben im Zusammenhang mit den Faxeingängen, da diese von der Betriebsart des Faxservers abhängig sind.

Manuelle Weiterleitung von Eingangs-Faxsendungen

Sofern Eingangs-Faxsendungen nicht automatisch an den Empfänger zugestellt werden, müssen diese durch die Fax-Poststelle manuell weitergeleitet werden. Dies kann z. B. in der Form erfolgen, dass durch die Fax-Poststelle von den Faxeingängen ein Ausdruck gefertigt wird, der dann an den Empfän-

ger auf dem üblichen Weg weitergeleitet wird. Dieses Verfahren unterscheidet sich nicht wesentlich von dem beim Einsatz eines herkömmlichen Faxgerätes. Denkbar ist allerdings, dass eingegangene Faxsendungen digital auf externen Datenträgern archiviert werden.

Automatische Weiterleitung von Eingangs-Faxsendungen

Bei der automatischen Weiterleitung von Eingangs-Faxsendungen an den Empfänger (automatisches Fax-Routing) ist ebenfalls möglich, dass durch die Fax-Poststelle Ausdrucke zum Zwecke der Archivierung gefertigt werden. Auch hier besteht die Möglichkeit, eingehende Faxsendungen digital auf externen Datenträgern zu archivieren.

Behandlung nicht zustellbarer Faxeingänge

Sofern Faxsendungen nicht zugestellt werden können, muss die Fax-Poststelle hiervon Kenntnis erlangen und versuchen, die Fehlerquelle zu beheben. Sofern die Zustellung endgültig scheitert, ist der Absender entsprechend zu informieren. Gründe dafür, dass Faxeingänge unzustellbar sind, können sein:

- Der Absender hat eine falsche Durchwahl benutzt.
- Der Empfänger ist nicht mehr Mitglied der Organisation.
- Die automatische Weiterleitung von Eingangs-Faxsendungen erfolgt aufgrund der Absenderkennung (CSID) und der Absender ist in der Organisation noch nicht bekannt oder es existiert keine entsprechende Zuordnungsregel.

In all diesen Fällen muss von der Fax-Poststelle die Weiterleitung von Faxeingängen manuell erfolgen. Sofern Faxeingänge endgültig nicht zugestellt werden können, muss der Absender benachrichtigt werden.

Ergänzende Kontrollfragen:

- Wer ist Fax-Verantwortlicher?
- Wo laufen nicht zustellbare Faxsendungen auf?

M 2.181 Auswahl eines geeigneten Faxservers

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT

Ein Faxserver besteht im Regelfall aus folgenden Komponenten: Dem IT-System selbst, dem Betriebssystem, der Kommunikationskomponente (z. B. Faxmodem, aktive oder passive ISDN-Karte bzw. dedizierte Faxkarte) und der eigentlichen Faxserver-Applikation. Zusätzlich wird unter Umständen für die Arbeitsplatzrechner ein entsprechender Faxclient benötigt.

Bevor Faxserver beschafft werden, sind zunächst die wesentlichen Einflussfaktoren für deren Einsatz zu erheben. Dies sind:

- Das voraussichtlich abzuwickelnde Faxvolumen,
- die Anzahl der Mitarbeiter, die den Faxserver benutzen sollen,
- die Anforderungen an die Verfügbarkeit des Faxservers,
- die Anforderungen an die Einbindung in bereits bestehende E-Mail- und Workflow-Systeme,
- die Anforderungen an die Protokollierung auf dem Faxserver,
- Anforderungen an die Art der Weiterleitung eingehender Faxsendungen an den Empfänger.

IT-System

Die Wahl des IT-Systems wird in der Regel durch die Anforderungen der Software und des Betriebssystems an die Leistungsfähigkeit bestimmt. Das IT-System muss zudem kompatibel zum ausgewählten Betriebssystem sein. Je nach Anforderungen an die Verfügbarkeit des Faxservers kann über den Einsatz zusätzlicher Schutzmechanismen nachgedacht werden. Möglichkeiten, die Verfügbarkeit sicherzustellen bzw. zu erhöhen, sind:

- RAID
- Replikation
- Lastverteilung

Betriebssystem

Faxserver-Applikationen gibt es für alle gängigen Netzbetriebssysteme wie Unix, Microsoft Windows NT und Novell Netware. Bei der Wahl des Betriebssystems sollte die Integrationsmöglichkeit in das bestehende Netz und die Anforderungen durch die Faxserver-Applikation den Ausschlag geben. Sofern bisher in einer Organisation ausschließlich ein Netzbetriebssystem zum Einsatz kommt, also z. B. nur Server unter dem Betriebssystem Unix im Einsatz sind, so sollte auch möglichst dieses Netzbetriebssystem ausgewählt und eine geeignete Faxserver-Applikation beschafft werden. Hiervon wird man abweichen müssen, wenn eine bestimmte Applikationssoftware als Einzige ein dringend benötigtes Leistungsmerkmal anbietet, aber nur auf einer anderen als der bisher eingesetzten Betriebssystemplattform einsetzbar ist. Ein neues Netzbetriebssystem bedeutet einen erheblichen Mehraufwand bei der Administration. Sofern im Netz bereits verschiedene Netzbetriebssysteme im Einsatz sind, ist das zu wählen, das sich am einfachsten integrieren lässt, sofern die gewünschte Faxserver-Applikation dies zulässt.

Kommunikationskomponente

Die Kommunikationskomponenten stellen die Verbindung zwischen dem Server und dem öffentlichen Telefonnetz her. Die Kommunikation wird auf der Grundlage des T.30 Protokolls abgewickelt. Durch dieses Protokoll wird u. a. der Verbindungsaufbau, der Austausch der Absender-Faxnummer und die Übertragung und die Quittierung des Dokuments geregelt. Die Übertragung im Gruppe-3-Standard erfolgt hauptsächlich bei 9.600 bps und 14.400 bps. Außerdem sind die Kompressionsverfahren Modified Huffmann, Modified Read und Modified Modified im Einsatz. Der Gruppe-3-Standard ist am weitesten verbreitet. Daneben gibt es noch den Gruppe-4-Standard, der allerdings ISDN voraussetzt. Hier werden Übertragungsgeschwindigkeiten von 64 kBit pro Sekunde erreicht. Der Standard Gruppe 4 hat sich gleichwohl in den vergangenen Jahren nicht durchsetzen können, da entsprechende Stand-alone-Geräte relativ teuer sind. Es besteht außerdem keine Kompatibilität zwischen dem Gruppe-3- und dem Gruppe-4-Standard.

Bei Beginn der Kommunikation wird zwischen den Geräten sowohl die Übertragungsgeschwindigkeit als auch das Kompressionsverfahren ausgehandelt. Es wird die höchste Geschwindigkeit und das bestmögliche Kompressionsverfahren gewählt, das von beiden Geräten unterstützt wird.

Folgende Kommunikationskomponenten sind beim Einsatz eines Faxservers denkbar:

a) Faxmodem

Faxmodems sind recht preisgünstig verfügbar. Sie sind aber u. U. nicht ausreichend manipulationsresistent und werden zudem nicht von allen Faxserver-Applikationen im Dauereinsatz unterstützt. Daher sollte ihr Einsatz auf den privaten Gebrauch und auf einzelne Arbeitsplätze beschränkt bleiben.

b) passive ISDN-Karten

Passive ISDN-Karten sind einfach aufgebaut und damit preiswert. Die Hauptlast der Kommunikation trägt der Rechner. Dies ist bei starker Inanspruchnahme des Faxservers (z. B. Serien-Faxsendungen) problematisch. Bei passiven ISDN-Karten ist - ein entsprechendes Gerät auf Empfängerseite vorausgesetzt - generell auch die Übertragung nach dem Gruppe-4-Standard möglich. Müssen Faxdaten nach dem Gruppe-3-Standard übertragen werden, so sind die Daten entsprechend zu konvertieren. Wie beim Faxmodem gilt auch hier, dass das Hauptanwendungsgebiet auf einen einzelnen Arbeitsplatz oder auf den privaten Bereich beschränkt bleiben sollte.

c) aktive ISDN-Karten

Aktive ISDN-Karten, auch ISDN-Controller genannt, verfügen über einen eigenen Prozessor. Sie können daher das ISDN-Protokoll weitestgehend eigenständig abwickeln. Gemäß der Spezifikation des Common-ISDN-API (CAPI) müssen die Faxdaten im Structured Fax File (SFF)-Format an die ISDN-Karte übergeben werden. Die Konvertierung muss auf dem Faxserver erfolgen. Genau wie Modems unterstützen aktive ISDN-Karten im Gruppe-3-Standard nur die Übertragungsgeschwindigkeiten 9.600 und 14.400 bps unter Benutzung des Kompressionsverfahrens Modified Huffmann. Ein wesentlicher Nachteil sowohl von Faxmodems als auch von aktiven und passiven

ISDN-Karten ist, dass diese auch zu anderen Zwecken als der Faxübertragung benutzt werden können, z. B. im Modembetrieb oder als Remote-Access-Komponente. Dies ist aber bei einem Faxserver aus Gründen der Netzsicherheit gerade nicht erwünscht. Aktive ISDN-Karten können bis zu 30 ISDN-Kanäle zur Verfügung stellen. Beim Einsatz von aktiven ISDN-Karten sind auch die ISDN-Signalisierungsmöglichkeiten für das automatische Fax-Routing verfügbar. Trotz der Verwendbarkeit für nicht-Fax-Betrieb sind aktive ISDN-Karten für den Einsatz in Faxservern durchaus empfehlenswert.

d) Faxkarten (ggf. mit ISDN-Schnittstelle)

Spezielle Faxkarten sind auf die Abwicklung des T.30-Protokolls optimiert. Sie übernehmen den Verbindungsaufbau und das "Aushandeln" der Kommunikationsparameter. Die Konvertierung der Daten und die Kompression können auf der Karte erfolgen. Der Faxserver wird damit deutlich entlastet. Es gibt Faxkarten, die die Übertragung von Faxdaten mit 9.600 und 14.400 bps und Anwendung aller drei Kompressionsverfahren bieten. Vorteil dieser Karten ist auch, dass sie im Regelfall nur das T.30-Protokoll beherrschen und daher nicht für den Modembetrieb oder als Remote-Access-Komponente einsetzbar sind. Teilweise werden Faxkarten um eine ISDN-Schnittstelle erweitert. Der Vorteil davon ist, dass die Signalisierungsmöglichkeiten von ISDN für das Fax-Routing nutzbar werden.

aktive ISDN-Karten oder Faxkarten verwenden

Zusammenfassend folgt, dass in Faxservern im Regelfall nur aktive ISDN-Karten und Faxkarten zum Einsatz kommen sollten. Die Karte muss kompatibel zur Applikationssoftware sein, da nicht jede Karte durch alle Faxserver-Applikationen unterstützt wird. Die Anzahl der notwendigen Karten hängt von der Auslastung des Faxservers ab. Je Stunde und Leitung bzw. je Kanal ist die Übertragung von ca. 40-50 Seiten Faxdaten möglich.

Faxserver-Applikation

Bei der Auswahl der Applikationssoftware ist sowohl das Faxvolumen, das über den Faxserver abgewickelt werden soll, als auch die Anzahl der Benutzer zu berücksichtigen.

Integration in ein E-Mail- bzw. Workflow-System

Ist in der Organisation bereits ein E-Mail- bzw. Workflow-System vorhanden, so sollte eine Integration der Applikationssoftware mit diesen Systemen möglich sein. Es ist dann z. B. denkbar, dass Faxeingänge und Fax-Ausgänge zwischen dem Arbeitsplatzrechner des Benutzers und dem Faxserver über das bereits bestehende Workflow- bzw. E-Mail-System ausgetauscht werden. Interessant ist in diesem Zusammenhang auch, ob und wie ggf. bestehende Adressbücher bzw. Verteilerlisten mit den Adressbüchern des Faxservers synchronisiert werden können. Außerdem sollte die Archivierung von ein- und ausgehenden Faxsendungen in bestehenden Workflow-Systemen möglich sein.

Übertragung vom Arbeitsplatz zum Faxserver

Auch ist in die Überlegungen mit einzubeziehen, wie Faxsendungen vom Arbeitsplatz des Benutzers zum Faxserver gelangen und wo eine Umwandlung der Daten in ein für den Faxserver kompatibles Datenformat erfolgt. Die Konvertierung der Faxdaten am Arbeitsplatz erfolgt beim Senden im Regelfall mittels eines Druckertreibers oder einer besonderen Faxclient-Applikation. Die konvertierten Daten können dann entweder über E-Mail oder auch mittels der Faxclient-Applikation an den Faxserver übermittelt werden. Denkbar ist

auch, dass der Benutzer die konvertierten Daten in ein spezielles Verzeichnis auf dem Faxserver kopiert. Schließlich gibt es Faxserver, bei denen eine Druckerwarteschlange im Netz eingerichtet wird, in die die Faxdaten von der Anwendungssoftware, z. B. einem Textverarbeitungsprogramm, geschrieben werden. Außerdem ist es möglich, dass die Daten auf dem Faxserver komplett konvertiert werden. In diesem Fall erstellt der Benutzer mit einer entsprechenden Anwendungssoftware, z. B. einem Textverarbeitungsprogramm, die als Fax zu versendende Datei, die dann dem Faxserver übergeben werden muss. Dies kann mittels E-Mail, einer entsprechenden Faxclient-Applikation oder durch Kopieren in ein auf dem Faxserver freigegebenes Verzeichnis erfolgen. Zu bedenken ist, dass die Konvertierung der Faxdaten am Arbeitsplatz dort Ressourcen verbraucht. Dies kann in der Regel vernachlässigt werden, wenn nur wenige Faxe am Tag versendet werden. Gerade bei Serien-Faxsendungen kann es aber passieren, dass der Arbeitsplatzrechner für längere Zeit blockiert wird. Andererseits verlangt eine Konvertierung auf dem Faxserver bei hoher Inanspruchnahme entsprechend leistungsfähige Hard- und Software.

Protokollierung am Faxserver

Schließlich sollten bei der Auswahl geeigneter Applikationssoftware auch die Protokollierungmöglichkeiten am Faxserver mit berücksichtigt werden. Neben den Fehlerprotokollen sind auch die Sendeprotokolle von Interesse. Zunächst sollten den Benutzern durch den Faxserver die Sendeprotokolle zu den jeweiligen Faxsendungen zur Verfügung gestellt werden. Nur so können die Benutzer kurzfristig z. B. auf Verbindungsfehler reagieren. Weiterhin sollte die Möglichkeit bestehen, die anfallenden Gebühren mittels der Sendeprotokolle zu ermitteln und auf die entsprechenden Kostenstellen zu verteilen.

Übertragung vom Faxserver zum Arbeitsplatz

Ein weiterer Einflussfaktor für die Auswahl der Applikationssoftware ist die Frage, wie Faxeingänge den Empfänger erreichen. Die digitale Weiterleitung von Faxeingängen über das Netz wird auch als Fax-Routing bezeichnet.

Ausdruck auf Papier

Die technisch am einfachsten zu realisierende Möglichkeit ist natürlich der Ansatz, Faxeingänge an zentraler Stelle (Fax-Poststelle) auszudrucken und den Ausdruck an den Empfänger weiterzuleiten. Der Vorteil dieser Lösung ist, dass die Faxeingänge für die Akten zentral ausgedruckt werden. Zudem können die eingehenden Faxsendungen sowohl digital als auch manuell archiviert werden. Außerdem sind bestehende Vertretungsregelungen problemlos zu übernehmen. Nachteilig an diesem Verfahren ist die u. U. daraus entstehende Arbeitsbelastung der Fax-Poststelle. Außerdem stehen die Faxdaten dann nicht in elektronischer Form an den Arbeitsplätzen zur Verfügung.

manuelle Weiterleitung mittels E-Mail

Eine weitere Möglichkeit besteht darin, dass von der Fax-Poststelle Faxeingänge per E-Mail an den Empfänger gesandt werden. Der Nachteil dieses Verfahrens besteht ebenfalls in der Arbeitsbelastung der Fax-Poststelle. Dabei wird nicht automatisch von jedem Eingangs-Fax ein Ausdruck gefertigt. Wenn ein solcher Ausdruck aus organisatorischen oder sonstigen Gründen gewünscht wird, müssen entsprechende Regelungen getroffen werden.

automatische Weiterleitung

Für die automatische Weiterleitung von Eingangs-Faxsendungen an den Empfänger über das Netz gibt es folgende Möglichkeiten:

a) Linerouting

Hier wird jeder Leitung ein fester Empfänger zugeordnet. Die Anzahl der direkt erreichbaren Empfänger ist auf die Anzahl der zur Verfügung stehenden Leitungen begrenzt.

b) Auswertung der Absenderkennung

Ein weiteres Verfahren stellt auf die übermittelte Absenderkennung eines Faxeingangs (CSID - Call Subscriber ID) ab. Hierbei wird auf dem Faxserver festgelegt, dass Faxeingänge bestimmter Absender jeweils an einen bestimmten Empfänger weitergeleitet werden. Der Nachteil dieses Verfahrens besteht darin, dass nur Faxeingänge bereits bekannter Absender automatisch weitergeleitet werden. Alle anderen Faxeingänge müssen manuell an die Empfänger weitergeleitet werden. Problematisch ist zudem, dass Absenderkennungen vom Absender frei gewählt werden können und daher unter Umständen nicht zuverlässig sind.

c) Signalisierung mittels ISDN

Sofern ISDN zum Einsatz kommt, gibt es weitere Möglichkeiten des automatischen Fax-Routings. Hierbei muss allerdings zwischen dem so genannten Mehrgeräteanschluss und dem Anlagenanschluss unterschieden werden.

Bei einem Mehrgeräteanschluss stehen 2 Leitungen und bis zu maximal 10 Rufnummern je Anschluss zur Verfügung. Die Rufnummern werden durch die jeweilige Telefongesellschaft vergeben. Sofern im Faxserver eine ISDN-Karte oder eine Faxkarte mit ISDN-Schnittstelle vorhanden ist, kann anhand der durch den Sender benutzten Rufnummer der Empfänger bestimmt werden. Aufgrund der Begrenzung auf 10 Rufnummern ist es somit auch nur möglich, an maximal 10 Empfänger Faxeingänge automatisch zu verteilen.

Beim ISDN-Anlagenanschluss ist zwischen dem öffentlichen Telefonnetz und dem organisationsinternen Telefonnetz eine Telekommunikationsanlage geschaltet. Auch bei dieser Anschlussart kann der Faxserver die durch den Sender benutzte Rufnummer erkennen und einen Faxeingang anhand dieser Nummer automatisch zum entsprechenden Empfänger routen. Die maximal mögliche Anzahl der Empfänger ist dabei deutlich höher. Die Realisierung erfolgt dadurch, dass jeder Mitarbeiter, der vom Faxserver Faxeingänge erhalten soll, eine zweite Durchwahlnummer erhält. Die Telefonanlage leitet Eingänge, die auf dieser zweiten Nummer erfolgen, direkt an den Faxserver weiter. Einziger Nachteil dieses Verfahrens ist, dass der Rufnummernpool einer Organisation stärker belastet wird. Die Telekommunikationsanlage muss also entsprechend leistungsfähig sein.

d) Auswertung des Empfängers mittels optischer Zeichenerkennung

Ein weiteres, aber wenig verbreitetes Verfahren zum automatischen Routing von Faxeingängen ist die optische Zeichenerkennung (OCR). Dabei wird versucht, im Faxeingang z. B. im Anschriftenfeld, Namen oder Nummern zu erkennen. Dieses Verfahren setzt leistungsfähige OCR-Software und entsprechende Rechenleistung sowie möglichst genormte Adressfelder bei Faxeingängen voraus.

e) weitere Verfahren

Es gibt zwei weitere Verfahren zur automatischen Weiterleitung von Faxeingängen, das Dual Tone Multi Frequency Verfahren und das Direct Inward Dialing Verfahren. Da beide Verfahren in Deutschland nicht anwendbar sind, werden sie hier nur aus Gründen der Vollständigkeit erwähnt.

automatische Weiterleitung bei hohem Faxvolumen

Die automatische Weiterleitung von eingehenden Faxsendungen hat den Vorteil, dass das Personal der Fax-Poststelle entlastet wird. Zudem erreichen eingehende Faxsendungen den Empfänger schneller. Nachteilig ist insbesondere bei der Signalisierung mittels ISDN, dass der Rufnummernpool entsprechend belastet wird. Dafür ist die automatische Weiterleitung von Eingangs-Faxsendungen hiermit am besten zu realisieren. Bei einem hohen Aufkommen an eingehenden Faxsendungen sollte dieser Lösung der Vorzug gegeben werden. Sofern eingehende Faxsendungen nur für wenige Arbeitsplätze bzw. Gruppen bestimmt sind und überwiegend immer von den gleichen Absendern kommen, ist die Auswertung der Absenderkennung auch eine praktikable Lösung. Bei nur geringem Aufkommen an Eingangs-Faxsendungen kann die manuelle Verteilung eine sinnvolle Alternative darstellen.

Ergänzende Kontrollfragen:

- Werden bei der Auswahl des Faxservers Kompatibilitätsgesichtspunkte berücksichtigt?
- Ist sichergestellt, dass das zu erwartende Faxvolumen durch die ausgewählten Kommunikationskarten bewältigt werden kann?
- Unterstützt die ausgewählte Faxserver-Applikation alle benötigten Leistungsmerkmale?

M 2.182 Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

unangekündigte Kontrollen

In den IT-Grundschutz-Katalogen werden eine Vielzahl von Regelungen, Sicherheitsmaßnahmen und Konfigurationshinweisen vorgestellt, die für die Erreichung der angestrebten IT-Sicherheit notwendig sind. Es ist aber nicht ausreichend, diese Regelungen bekannt zu geben, es muss auch regelmäßig deren Einhaltung kontrolliert werden. Regelmäßig heißt hierbei aber nicht, dass die Kontrollen an vorhersagbaren Terminen stattfinden, da angekündigte Kontrollen meist ein verzerrtes Bild des Untersuchungsgegenstands ergeben.

Kontrollen sollten vor allen Dingen darauf ausgerichtet sein, Mängel abzustellen. Für die Akzeptanz von Kontrollen ist es wichtig, dass dies allen Beteiligten als Ziel der Kontrollen erkennbar ist und dass die Kontrollen nicht den Charakter von Schulmeisterei haben. Es ist daher sinnvoll, während einer Kontrolle mit den Beteiligten über mögliche Problemlösungen zu sprechen und entsprechende Abhilfen vorzubereiten.

Regelungen auf Arbeitsabläufe abstimmen

Wenn Mitarbeiter eine Regelung ignorieren oder umgehen, ist das meist ein Zeichen dafür, dass diese nicht mit den Arbeitsabläufen vereinbar ist oder durch die Mitarbeiter nicht umgesetzt werden kann. Beispielsweise ist eine Anweisung, vertrauliche Schreiben nicht unbeaufsichtigt am Drucker liegen zu lassen, unsinnig, wenn zum Drucken nur ein weit entfernter Netzdrucker zur Verfügung steht.

Ursachen der Sicherheitsdefizite beseitigen

Wenn bei Kontrollen Mängel festgestellt werden, kommt es nicht darauf an, nur die Symptome zu beseitigen. Vielmehr ist es wichtig, die Ursachen für diese Probleme festzustellen und Lösungen aufzuzeigen. Diese können beispielsweise in der Änderung bestehender Regelungen oder in der Hinzunahme technischer Maßnahmen bestehen.

Schuldzuweisungen vermeiden

Kontrollen sollen helfen, Fehlerquellen abzustellen. Es ist für die Akzeptanz von Kontrollen extrem wichtig, dass dabei keine Personen bloßgestellt werden oder als "Schuldige" identifiziert werden. Wenn die Mitarbeiter dies befürchten müssen, besteht die Gefahr, dass sie nicht offen über ihnen bekannte Schwachstellen und Sicherheitslücken berichten, sondern versuchen, bestehende Probleme zu vertuschen.

Ergänzende Kontrollfragen:

- Werden alle Regelungen und IT-Sicherheitsmaßnahmen auf ihre Umsetzbarkeit untersucht?
- Wie häufig werden die bestehenden Regelungen und IT-Sicherheitsmaßnahmen auf ihre Einhaltung kontrolliert?

M 2.183 Durchführung einer RAS-Anforderungsanalyse

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Bevor ein System für den entfernten Zugang eingesetzt wird, sollte eine Anforderungsanalyse durchgeführt werden. Ziel der Anforderungsanalyse ist es einerseits, alle im konkreten Fall in Frage kommenden Einsatzszenarien zu bestimmen und andererseits daraus Anforderungen an die benötigten Hard- und Softwarekomponenten abzuleiten. Durch das Aufstellen und "Durchspielen" von Nutzungsszenarien können insbesondere spezielle Anforderungen aufgedeckt werden, so dass sich entsprechende Anforderungen (K.-o.-Kriterien) an die RAS-Systemarchitektur oder die RAS-Software stellen lassen.

Im Rahmen der Anforderungsanalyse sind u. a. folgende Fragen zu klären:

- Welche Benutzer werden den RAS-Zugang nutzen (Telearbeiter, Außendienstmitarbeiter, Mitarbeiter auf Dienstreise)?
- Soll der RAS-Zugang von mobilen Benutzern genutzt werden?
- Zu welchem Zweck wird der RAS-Zugang jeweils genutzt (Abfragen von Informationen, Einstellen von Informationen, Programmnutzung)?
- Müssen die entfernten Benutzer auf das komplette LAN, d. h. alle dort verfügbaren Daten und Dienste) Zugriff haben?
- Müssen spezielle Softwareprodukte über den RAS-Zugang genutzt werden?
- Müssen spezielle Protokolle über den RAS-Zugang genutzt werden?
- Von welchen (entfernten) Orten wird der RAS-Zugang genutzt (national, international)?
- Welche Telekommunikations-Zugangstechnologien kommen zum Einsatz (Festnetz, Mobiltelefon, Internet)?

Die Anforderungen für die geplanten Szenarien sollten dokumentiert und mit den Netzadministratoren und dem technischen Personal abgestimmt werden. Sie bilden u. a. die Grundlage für das weitere Vorgehen (Architektur, Beschaffung, Einsatz).

Ergänzende Kontrollfragen:

- Wurde eine RAS-Anforderungsanalyse durchgeführt?
- Sind alle speziellen Anforderungen erfasst, die aus den lokalen Gegebenheiten resultieren?
- Wurde die Anforderungsliste mit den Netzadministratoren und dem technischen Personal abgestimmt?

M 2.184 Entwicklung eines RAS-Konzeptes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Der Aufbau eines RAS-Systems erfordert, dass nach der Durchführung der Anforderungsanalyse (siehe Maßnahme M 2.183 *Durchführung einer RAS-Anforderungsanalyse*) und vor der technischen Realisierung des Systems ein RAS-Konzept entworfen wird. Das Konzept legt im Wesentlichen fest, welche RAS-Systemarchitektur gewählt werden soll und welche Regeln für den Umgang mit dem RAS-System für alle Betroffenen gelten. Das Konzept kann grob in drei Teilbereiche unterteilt werden:

1. Das organisatorische Konzept, durch das alle organisatorischen Belange für das RAS-System erfasst werden. Es ist darauf zu achten, dass das RAS-System in existierende organisatorische Abläufe integriert wird, so dass deren Homogenität und Konsistenz gewahrt bleibt.

Organisation

2. Das technische Konzept, das eine technische Realisierung des RAS-Systems beschreibt. Dieses sollte den Bedarf abdecken, der durch die Anforderungsanalyse festgestellt wurde, und - so weit realisierbar - alle erforderlichen Zugangsszenarien ermöglichen. Bei der technischen Planung sind alle existierenden Rahmenbedingungen aus der aktuellen technischen Situation zu berücksichtigen, um technische Inkompatibilitäten zu vermeiden.

Technik

3. Das Sicherheitskonzept, das die sicherheitsrelevanten Belange des RAS-Systems umfasst. Da die Sicherheit in der Regel nur durch organisatorische und technische Maßnahmen gemeinsam zu gewährleisten ist, sollte die Konzeption der Sicherheit eine separate Einheit bilden und nicht innerhalb des organisatorischen und des technischen Konzeptes lediglich als Unterabschnitt enthalten sein.

IT-Sicherheit

Im Folgenden werden jeweils die wesentlichen Fragestellungen aufgezeigt, die im Rahmen der Teilkonzepte beantwortet werden müssen. Je nach konkreter Situation ergibt sich naturgemäß ein speziell auf die jeweiligen organisatorischen und technischen Gegebenheiten zugeschnittener zusätzlicher Abstimmungsbedarf.

Das **organisatorische Konzept** sollte folgende Punkte beinhalten bzw. regeln:

- Es sollten die Verantwortlichkeiten für das RAS-System festgelegt werden (Installation, Verwaltung, Überprüfung, Überwachung). Je nach organisatorischer Struktur müssen die Verantwortlichkeiten existierender Rollen erweitert werden oder es ist die Schaffung neuer Rollen notwendig (siehe auch Maßnahme M 2.1 *Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz*).

Verantwortlichkeiten festlegen

- Es sollten verbindliche Regelungen darüber festgelegt werden, welchen Benutzern der entfernte Zugang über das RAS-System erlaubt werden soll. Es empfiehlt sich, auch für den RAS-Zugang unterschiedliche Gruppen mit verschiedenen Berechtigungen zu definieren. Die Gruppenzugehörigkeit von einzelnen Benutzern sollte durch ein entsprechendes Anforderungsprofil geregelt werden, das festlegt, welche Voraussetzungen

Berechtigungskonzept

für die Mitgliedschaft in einer Gruppe erfüllt werden müssen. Mögliche Voraussetzungen sind die Notwendigkeit (Telearbeiter, Außendienstler), die Länge der Betriebszugehörigkeit und eine Befürwortung durch Vorgesetzte. Ob und wie die Erlaubnis zum entfernten Zugriff reglementiert werden soll, muss jeweils innerhalb der Organisation entschieden werden. Oft existieren schon entsprechende Regelungen, z. B. für die Erlaubnis zur Nutzung von Internetzugängen, die dann adaptiert werden können.

Die erteilten Zugangs- und Zugriffsberechtigungen sind im Rahmen der RAS-System-Dokumentation zu erfassen und müssen bei Änderungen fortgeschrieben werden.

Anforderungen an Betriebsorte

- Für feste entfernte Standorte (wie Telearbeitsplätze) müssen Anforderungen festgelegt werden, die beschreiben, welchen Ansprüchen (z. B. in Bezug auf Sicherheit und technischer Ausstattung) der entfernte Arbeitsplatz genügen muss, damit von dort RAS-Verbindungen in das lokale Netz erlaubt werden können. Das Konzept kann weiterhin eine anfängliche sowie eine periodisch wiederkehrende Überprüfung der Räumlichkeiten vorsehen und regeln, wie und durch wen diese erfolgt.
- Die Betriebsorte von RAS-Clients unterliegen in der Regel nicht der Kontrolle des LAN-Betreibers und besitzen daher auch ein besonderes Gefährdungspotential. Kann das Gefährdungspotential für stationäre Clients (beispielsweise bei Telearbeit) durch entsprechende Vorgaben noch eingeschränkt werden, so muss für mobile RAS-Clients in der Regel ein sehr hohes Gefährdungsmaß angenommen werden. Nicht jeder Ort, der die technischen Voraussetzungen zum RAS-Verbindungsaufbau bereitstellt, ist auch dafür geeignet. Daher müssen Regelungen dafür getroffen werden, von welchen entfernten Standorten aus RAS-Verbindungen zum Ziel-LAN aufgebaut werden dürfen. Je nach geplantem Einsatzszenario kann es aber zweckmäßiger sein, eine Negativliste von besonders ungeeigneten Standorten zu führen. Dazu können z. B. Hotel-Foyers, Hotel-Business-Center oder Zug-Abteile gehören.

Änderungsmanagement

- Für die RAS-Administration sollten Prozeduren festgelegt werden, wie Änderungen an der RAS-Konfiguration durchzuführen sind. Da Verletzungen der Sicherheit von RAS-Zugängen u. U. die Kompromittierung des gesamten LANs nach sich ziehen können, sollten Änderungen an der RAS-Konfiguration nur durch eine festgelegte Vorgehensweise erfolgen (Beispiel: Beantragung, Überprüfung der geplanten Konfiguration, Durchführung, Überprüfung der durchgeführten Veränderung).

Das **technische Konzept** sollte folgende Punkte beinhalten bzw. regeln:

technische Ausstattung

- Es sollte beschrieben sein, wie das RAS-System durch Hard- und Software-Komponenten technisch realisiert ist. Die Komponenten werden lediglich durch ihre Funktion definiert. Durch eine nachgeschaltete Analyse vorhandener Systemkomponenten und am Markt beschaffbarer neuer Komponenten können dann die Elemente des Konzeptes tatsächlichen Geräten und Software-Komponenten zugeordnet werden (siehe M 2.186 *Geeignete Auswahl eines RAS-Produktes*).

- Alle möglichen Zugangspunkte und die darüber verwendeten Zugangsprotokolle sind zu beschreiben.
- Alle Dienste und Protokolle, die über den RAS-Zugang zugelassen werden, sowie die darüber zugreifbaren Ressourcen sind aufzuführen.
- Es ist zu planen, welche Teilnetze über den RAS-Zugang erreichbar sein sollen bzw. müssen (vergleiche auch RAS-Sicherheitskonzept).

Das **RAS-Sicherheitskonzept** sollte folgende Punkte beinhalten bzw. regeln:

RAS-Sicherheitsrichtlinie

- Für die RAS-Nutzung sollte eine Sicherheitsrichtlinie formuliert werden. Diese RAS-Sicherheitsrichtlinie muss sich an den existierenden übergreifenden Sicherheitsrichtlinien orientieren. In der Regel gilt der Grundsatz, dass beim Zugriff über das RAS-System geringere Berechtigungen gelten und stärkere Überprüfungen stattfinden sollten, als beim lokalen Zugriff.

Authentisierung

- Die Art und Weise der Benutzer-Authentisierung sowie die dafür zu verwendenden Mechanismen sollten festlegt werden.
- Alle an der Authentisierung beteiligten Komponenten sollten erfasst und deren Aufgaben und Interaktionen beschrieben werden.

Zugriffskontrolle

- Alle an der Zugriffskontrolle beteiligten Komponenten sollten erfasst und deren Aufgaben und Interaktionen beschrieben werden. Auf diese Weise kann festgestellt werden, ob z. B. existierende Zugriffskontrollmechanismen so konfiguriert werden können, dass beim entfernten Zugriff automatisch restriktivere Einstellungen gelten.

Erfassung aller RAS-Zugangspunkte

- Im Rahmen der Sicherheitskonzeption sind alle RAS-Zugangspunkte zum lokalen Netz zu erfassen und es ist zu beschreiben, wie diese Zugangspunkte an das LAN angeschlossen werden (siehe auch Baustein B 3.301 *Sicherheitsgateway (Firewall)*).

Eingrenzen der externen Zugriffe

- Das Sicherheitskonzept muss analysieren, aufbauend auf der aktuellen Netzstruktur, welche Teilnetze bei Nutzung eines RAS-Zugangs erreichbar sind. Für Bus-basierte Netze (beispielsweise Ethernet) sind typischerweise alle Rechner des Teilnetzes zugreifbar, in dem der RAS-Zugang angesiedelt ist. Hier sollte überlegt werden, dedizierte Zugangsnetze (Access Network) zu bilden, aus denen nur kontrolliert (über Router, Paketfilter bzw. interne Firewall) in das produktive Netz zugegriffen werden kann. Die Bildung von Zugangsnetzen erfordert dabei die Anschaffung und Wartung zusätzlicher Hard- und Software (siehe auch M 5.77 *Bildung von Teilnetzen*).

Meldewesen für Sicherheitsprobleme

- Für den Fall von Sicherheitsvorfällen sind organisatorische Meldewege zu planen, über die gezielt und schnell auf Sicherheitsvorfälle reagiert werden kann. Im technischen Konzept sollten entsprechend Mechanismen geplant werden, die das Erkennen von Sicherheitsvorfällen erlauben und diese Vorfälle zu dem zuständigen Administrator leiten, der den Anfang des organisatorischen Meldewegs bildet.

Schulung und Sensibilisierung

- Da beim entfernten Zugriff auf ein LAN besondere Sicherheitsrisiken durch die meist ungesicherte Umgebung eines RAS-Clients bestehen, sollte jeder Benutzer, für den der RAS-Zugang erlaubt werden soll, eine besonde-

re Schulung erhalten. Im Rahmen dieser Schulung sollen die Benutzer einerseits für die Gefahren sensibilisiert und andererseits im Umgang mit den technischen Geräten und der Software unterrichtet werden.

- Falls Authentisierungs-Token zum Einsatz kommen sollen, müssen die Benutzer über deren ordnungsgemäße Handhabung informiert werden.
- Ebenso müssen auch die Administratoren sowohl für die eingesetzten Produkte gründlich ausgebildet als auch für Sicherheitsrisiken sensibilisiert werden.
- Den Administratoren muss nicht nur für den Betrieb der RAS-Systeme ausreichend Zeit zur Verfügung stehen, sondern auch für die Informationssuche über aktuelle Sicherheitslücken und die Einarbeitung in neue Komponenten.
- Bestehende Regelungen zur Rollentrennung (z. B. Administrator und Revisor) sollten auf die Verwaltung des RAS-Systems übertragen werden.
- Schließlich müssen die Anforderungen an die Verfügbarkeit der RAS-Systeme festgelegt werden. Falls erforderlich sind außerdem Ausweichlösungen vorzusehen, die beim Ausfall eines RAS-Systems ersatzweise verwendet werden können.

Anforderungen an die Verfügbarkeit

Aus der RAS-Anforderungsanalyse und -Konzeption ergeben sich naturgemäß konkrete Anforderungen an die Hard- und Software-Komponenten, die eingesetzt werden sollen. Diese sollten für eine Beschaffung verfeinert und konkretisiert werden, wie in Maßnahme M 2.186 *Geeignete Auswahl eines RAS-Produktes* beschrieben.

Ergänzende Kontrollfragen:

- Existiert ein Sicherheitskonzept für die RAS-Nutzung?
- Existieren Sicherheitsrichtlinien für die RAS-Nutzung, an denen sich die Benutzer orientieren können?
- Ist ein Berechtigungskonzept für entfernte Zugriffe vorhanden?
- Werden die Maßnahmen des RAS-Sicherheitskonzepts regelmäßig auf deren korrekte Umsetzung geprüft?

M 2.185 Auswahl einer geeigneten RAS-Systemarchitektur

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Je nach den geplanten Einsatzszenarien können unterschiedliche RAS-Systemarchitekturen genutzt werden, um den entfernten Zugang zu einem LAN zu realisieren. Die verschiedenen Systemarchitekturen haben naturgemäß unterschiedliche Eigenschaften und sind daher für die einzelnen Einsatzzwecke unterschiedlich gut geeignet. Prinzipiell ist zwar jede Kombination möglich, erfordert jedoch bei einer ungünstigen Wahl zusätzlichen Aufwand (z. B. zusätzliche Hardware, administrativer Mehraufwand).

Die folgenden RAS-Szenarien, denen jeweils eine typische Systemarchitektur zugeordnet werden kann, kommen in der Praxis häufig zum Einsatz.

1. Anbindung einzelner Rechner an ein LAN

In diesem Fall kommt oft eine Architektur in Frage, die mit "Direct Dial-In" (Direkte Einwahl) bezeichnet wird. Die RAS-Software wird auf dem Rechner des entfernten Benutzers installiert. Der Rechner besitzt eine Verbindung zu einem Telekommunikationsnetz. Der Anschluss kann hier beispielsweise über ein analoges Modem, eine ISDN-Karte oder auch über ein Mobiltelefon erfolgen. Zur Verbindungsaufnahme wählt die RAS-Client-Software die Telefonnummer, unter der die RAS-Server-Software zu erreichen ist. Auch der RAS-Server ist über ein Modem oder eine ISDN-Karte mit dem Telekommunikationsnetz verbunden. Je nach RAS-Server-Produkt (auch Access-Server genannt) kann ein Server mehrere Kommunikationsverbindungen aufbauen (z. B. über so genannte "Modem-Pools"), so dass sich gleichzeitig mehrere RAS-Clients einwählen können.

Vorteilhaft ist hier, dass durch dieses Verfahren ein einzelner Rechner von einem beliebigen Ort aus an das LAN angeschlossen werden kann. Dies ist insbesondere für mobile Benutzer günstig. Durch die direkte Einwahl auf dem RAS-Server des Ziel-LANs wird die Verbindung zwar nur über die Telekommunikationsnetze der benutzten Telekommunikationsanbieter geschaltet, der Einsatz von Mechanismen zur Kommunikationsabsicherung ist jedoch auch hier zu empfehlen, also z. B. Verschlüsselung, digitale Signaturen, Authentisierung.

Nachteilig ist hier, dass je nach Entfernung zum Ziel-LAN unterschiedlich hohe Telefonkosten entstehen können, die (ohne besondere Vorkehrungen) in der Regel beim entfernten Benutzer anfallen. Für die Anbindung mehrerer Benutzer, die sich gemeinsam an einem entfernten Ort befinden, ist diese Variante nicht geeignet, da jeweils eine dedizierte Verbindung zwischen Client und Server aufgebaut wird. Jeder Client muss daher mit einem entsprechenden Modem ausgestattet sein; die gleichzeitige Nutzung genau einer gemeinsamen Verbindung durch mehrere Client-Rechner ist auf diese Weise nicht möglich.

2. Anbindung mehrerer Rechner an ein LAN

In diesem Fall kommt oft eine Architektur in Frage, die mit "Direct LAN-to-LAN-Dial-In" bezeichnet wird. Die Rechner der entfernten Benutzer bilden hier ein eigenes LAN. Die RAS-Client-Software ist dabei in der Regel nicht auf einem der Benutzerrechner installiert, stattdessen wird die RAS-Funktionalität durch eine dedizierte Hardware in Form eines Routers zur Verfügung gestellt. Müssen Datenpakete von einem LAN in das andere übertragen werden, so stellt der im Router enthaltene RAS-Client automatisch eine Verbindung mit dem Ziel-LAN her, indem er den dortigen RAS-Server anwählt. In dieser Konfiguration wird meist eine symmetrische Architektur für beide LANs gewählt, so dass der anzuwählende RAS-Server auch in einem Router enthalten ist und eine Punkt-zu-Punkt Verbindung entsteht. Alternativ können mehrere entfernte LANs über einen Access-Server (RAS-Server, der mehrere gleichzeitige Verbindungen erlaubt) angebunden werden.

Vorteilhaft ist hier, dass durch die Funktionstrennung von RAS-Client und Rechner des entfernten Benutzers über *eine* Verbindung zum Ziel-LAN *mehrere* entfernte IT-Systeme angebunden werden können. Der Router, der den RAS-Client enthält, stellt dabei die aufgebaute Verbindung für alle am entfernten LAN angeschlossenen Rechner zur gleichzeitigen Nutzung bereit. Dies ist jedoch zugleich auch nachteilig, da die Verbindungskapazität unter den zugreifenden entfernten IT-Systemen aufgeteilt wird und nicht exklusiv genutzt werden kann.

Selbstverständlicher Nachteil ist hier, dass die Clients nicht mehr mobil sind.

3. Anbindung eines Rechners oder eines LANs über einen Service Provider

Als Erweiterung der beiden vorangegangenen Szenarien kann die Anbindung eines Rechners oder eines LANs auch über eine spezielle Zugangsrufnummer eines Service Providers erfolgen. In diesem Fall kontaktiert der RAS-Client eine besondere Telefonnummer, die häufig eine Ortsgespräch-Rufnummer oder eine kostenfreie Rufnummer ist. Anrufe für diese spezielle Nummer werden vom anbietenden Service Provider innerhalb des Kommunikationsnetzes an den RAS-Server des Ziel-LANs weitergeleitet. Diese Variante erlaubt insbesondere Mitarbeitern auf Dienstreise eine für sie kostengünstige Verbindungsaufnahme.

4. Anbindung eines Rechners oder eines LANs über Internet

Dieser Fall unterscheidet sich von den obigen Szenarien dadurch, dass vom Client zunächst eine Verbindung zu einem Internet-Dienstanbieter (Internet Service Provider - ISP) aufgebaut wird. Erst im zweiten Schritt verbindet sich der Client über die bestehende Internet-Anbindung mit dem Ziel-LAN. Dazu muss der entfernte Benutzer eine Zugangsberechtigung für den Internet-Zugang des jeweiligen ISP besitzen und das Ziel-LAN über einen Internet-Anschluss verfügen. Die Kommunikation mit dem Ziel-LAN erfolgt in diesem Fall über Internetprotokolle. Ein eigener RAS-Server (für direkte Verbindungen über ein Telekommunikationsnetz) ist im Ziel-LAN nicht erforderlich.

Diese Variante wird in der Regel genutzt, um die Telefonkosten für den entfernten Benutzer gering zu halten (z. B. Ortsgesprächsgebühren), kann sich jedoch in der Konfiguration als relativ komplex erweisen. Da der Internet-Zugang eines LANs in der Regel durch eine Firewall geschützt wird, muss bei der Planung der Firewall-Architektur die Möglichkeit des Internet-basierten Zugangs entfernter Benutzer berücksichtigt werden (siehe auch Baustein B 3.301 *Sicherheitsgateway (Firewall)*).

5. Aufbau eines Virtuellen Privaten Netzes (VPN)

Neben der Möglichkeit, mit Hilfe von Internet-basierten Protokollen und Programmen (z. B. telnet, ftp, POP3) auf Daten des internen Netzes zuzugreifen, können auch so genannte Tunnel-Protokolle benutzt werden. Diese erlauben es, über das Internet als Transportmedium eine Direktverbindung zwischen dem RAS-Client und dem RAS-Server des Ziel-LANs zu *simulieren*. Über diese scheinbare Direktverbindung erfolgt die eigentliche RAS-Kommunikation (siehe auch M 5.76 *Einsatz geeigneter Tunnel-Protokolle für die RAS-Kommunikation*). Der RAS-Server des Ziel-LANs muss hierzu über das Internet erreichbar sein. Oft bieten Firewall-Produkte RAS-Unterstützung an, so dass die Konfiguration des RAS-Zugangs mit Hilfe des Werkzeugs zur Firewall-Administration erfolgen kann.

Der Vorteil einer solchen Lösung liegt darin, dass Internetzugänge mittlerweile weit verbreitet sind, so dass hier in einfacher Weise auf einem existierenden Verbindungsnetz aufgebaut werden kann. Nachteilig ist jedoch, dass das Internet aufgrund seiner offenen Struktur nicht als sicheres Netz konzipiert wurde. Aus diesem Grund ist hier die Absicherung der Kommunikation besonders wichtig. Beim Tunneling geschieht dies durch den Einsatz kryptographischer Verfahren. Hierdurch wird ein so genanntes Virtuelles Privates Netz (VPN) realisiert.

Nach erfolgreichem Verbindungsaufbau besteht eine Verbindung über das Internet zwischen dem entfernten Rechner und dem LAN, meist über die Firewall hinweg. Unter dem Gesichtspunkt der IT-Sicherheit ist dies jedoch problematisch, da ein Angreifer unter Umständen weitreichende Zugriffsmöglichkeiten auf das Ziel-LAN hat, wenn es ihm gelingt, in einen Client-Rechner einzudringen. Der ausreichende Schutz aller Clients ist also entscheidend für die Sicherheit des Gesamtsystems. Aufgrund der fehlenden Durchsatzgarantien bei der Internet-Kommunikation muss zusätzlich davon ausgegangen werden, dass die Dienstqualität in der Regel geringer ausfällt als bei direkten und dedizierten Verbindungen zum LAN über das Telefonnetz. Bei dieser Architektur sollten daher die Auswirkungen auf die IT-Sicherheit und die Performance sorgfältig geprüft werden.

Die vorgestellten Szenarien und Systemarchitekturen sind gängige Varianten für die Realisierung von RAS-Zugängen, können jedoch trotzdem nur als Beispiele verstanden werden. Welche konkrete Systemarchitektur zu wählen ist, hängt sehr von den geplanten Einsatzszenarien ab. Oft besteht auch die Anforderung, mehrere Szenarien gleichzeitig zu realisieren (z. B. Telearbeit und mobile Benutzer). Insbesondere mobilen Benutzern soll eine größtmögliche Freiheit bei der Wahl der Zugangstechnologie angeboten werden, damit

sie von möglichst vielen Orten und Arbeitsumgebungen aus auf das lokale Netz zugreifen können.

Unter dem Gesichtspunkt der IT-Sicherheit ist jedoch zu berücksichtigen, dass die Verwendung von unterschiedlichen Zugangstechnologien in der Regel auch unterschiedliche Zugangspunkte im Ziel-LAN erfordert. Generell ist ein LAN, das über mehrere externe Zugänge verfügt, einer größeren Zahl von Gefährdungen ausgesetzt als ein LAN, das nur über genau einen externen Zugang erreichbar ist. Andererseits kann jedoch durch unterschiedliche Zugangspunkte die Verfügbarkeit des RAS-Systems erhöht werden.

M 2.186 Geeignete Auswahl eines RAS-Produktes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

RAS-Produkte unterscheiden sich in ihrem Leistungsumfang, den angebotenen Sicherheitsmechanismen, Bedienkomfort und Wirtschaftlichkeit. Zudem stellen sie unterschiedliche Voraussetzungen an Hard- und Software-Komponenten im Einsatzumfeld.

Bevor ein "RAS-Produkt" beschafft wird, sollte daher eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Aufgrund der Bewertung kann dann eine fundierte Kaufentscheidung erfolgen, die sicherstellt, dass das zu beschaffende Produkt im praktischen Betrieb den Anforderungen genügt.

Ein RAS-System besteht in der Regel aus mehreren Hard- und Software-Komponenten, so dass genau genommen, nicht von "einem RAS-Produkt" gesprochen werden kann: Zunächst kann grob zwischen LAN-seitigen und Client-seitigen Komponenten unterschieden werden. Die konkret zu beschaffenden Komponenten hängen von der gewählten RAS-Systemarchitektur ab. So können im einfachsten Fall z. B. ein Windows-basierter PC und ein Laptop, die jeweils mit einer ISDN-Karte ausgestattet sind (siehe auch M 2.106 *Auswahl geeigneter ISDN-Karten in der Beschaffung*), als RAS-Server und -Client fungieren und den RAS-Dienst von Windows NT nutzen. Hingegen betreiben große Institutionen oft gleichzeitig viele RAS-Verbindungen für unterschiedliche Einsatzzwecke. Hierfür geeignete Lösungen erfordern in der Regel besondere IT-Systeme (Hardware mit Software), die speziell für den Einsatz als RAS-Server konzipiert sind.

Die folgende Liste gibt einen groben Überblick über mögliche allgemeine Bewertungskriterien, erhebt jedoch keinen Anspruch auf Vollständigkeit und kann um weitere allgemeine Anforderungen erweitert werden. Neben den hier aufgeführten Kriterien müssen im Rahmen der RAS-Anforderungsanalyse (siehe Maßnahme M 2.183 *Durchführung einer RAS-Anforderungsanalyse*) weitere spezifische Anforderungen erarbeitet werden, die aus den geplanten konkreten Einsatzszenarien resultieren.

1 Allgemeine Kriterien

1.1 Performance und Skalierbarkeit

- Kann das System den Ansprüchen an die Performance gerecht werden?
- Kann für das System ein transparentes Load-balancing oder Datenkompression konfiguriert werden?
- Kann das System so konzipiert werden, dass es einem zukünftigen Wachstumsbedarf gerecht werden kann (z. B. durch modularen Systemaufbau, einfaches Einbinden neuer RAS-Server, keine getrennte Benutzerverwaltung für neue RAS-Zugänge)?

1.2 Wartbarkeit

- Ist das Produkt einfach wartbar?
- Bietet der Hersteller regelmäßige Software-Updates an?
- Wird für das Produkt die Möglichkeit des Abschlusses von Wartungsverträgen angeboten?
- Können im Rahmen der Wartungsverträge maximale Reaktionszeiten für die Problembehebung festgelegt werden?
- Bietet der Hersteller einen kompetenten technischen Kundendienst (Call-Center, Hotline) an, der in der Lage ist, sofort bei Problemen zu helfen?

1.3 Zuverlässigkeit/Ausfallsicherheit

- Wie zuverlässig und ausfallsicher ist das Produkt?
- Bietet der Hersteller Hochverfügbarkeitslösungen an?
- Ist das Produkt im Dauerbetrieb einsetzbar?

1.4 Benutzerfreundlichkeit

- Lässt sich das Produkt einfach installieren, konfigurieren und nutzen? Genügt das Produkt den geltenden Ergonomievorschriften?
- Ist insbesondere für den RAS-Client die Benutzerführung so gestaltet, dass auch ungeübte Benutzer damit arbeiten können, ohne Abstriche in der Sicherheit in Kauf nehmen zu müssen (kontextsensitive Hilfen, Online-Dokumentation, schrittweise Anleitung mit verständlichen Erklärungen - "Wizards", detaillierte Fehlermeldungen)?
- Ist die Nutzung des RAS-Clients so konfigurierbar, dass die Benutzer möglichst wenig mit technischen Details belastet werden? Ist die Sicherheit dabei trotzdem immer gewährleistet?

1.5 Kosten

- Wie hoch sind die Anschaffungskosten der Hard- und Software?
- Wie hoch sind die voraussichtlichen laufenden Kosten der Hard- und Software (Wartung, Betrieb, Support)?
- Wie hoch sind die voraussichtlichen laufenden Kosten für das Personal (RAS-Administrator/Revisor)?
- Müssen zusätzliche Soft- oder Hardware-Komponenten angeschafft werden (z. B. Einwahl-Server, Server für zusätzliche Authentisierungsdienste)?
- Wie hoch sind die Kosten für die Schulung von Mitarbeitern und Administratoren, die mit dem RAS-Produkt umgehen werden?

2. Funktion

2.1 Installation und Inbetriebnahme

- Garantieren die Default-Einstellungen des RAS-Systems nach der Installation eine sichere RAS-Konfiguration?
- Kann die Installation der RAS-Client-Software automatisiert mit vorgegebenen Konfigurationsparametern erfolgen?
- Ist die Installation der RAS-Client-Software auch für weniger versierte Mitarbeiter durchführbar?
- Können wichtige Konfigurationsparameter vor Veränderungen durch Benutzer geschützt werden?
- Arbeitet das Produkt mit gängiger Hard- und Software zusammen (Betriebssysteme, Einschubkarten, Treiber)?
- Ist das RAS-System mit gängigen Systemmanagementsystemen kompatibel?

2.2 Verhalten im Fehlerfall

- Bleibt die Sicherheit des RAS-Zugangs auch nach einem kritischen Fehler gewährleistet (indem z. B. jegliche Verbindungen nach einem Programmabbruch verhindert werden)?
- Kann das Systemverhalten nach einem kritischen Fehler konfiguriert werden? Kann z. B. eingestellt werden, dass nach einem kritischen Fehler automatisch ein Neustart durchgeführt oder der Administrator benachrichtigt wird?

2.3 Administration

- Enthält die mitgelieferte Produktdokumentation eine genaue Darstellung aller technischen und administrativen Details?
- Kann die Administration über eine graphische Benutzerschnittstelle erfolgen, die sich intuitiv bedienen lässt? Ist die administrative Schnittstelle so gestaltet, dass auf fehlerhafte, unsichere oder inkonsistente Konfigurationen hingewiesen wird oder diese verhindert werden?
- Wird neben der graphischen administrativen Schnittstelle auch ein kommandozeilenbasiertes Interface angeboten?
- Ist der Zugriff auf die administrative Schnittstelle durch eine adäquate Zugriffskontrolle geschützt, beispielsweise durch Passworteingabe, Umsetzung eines Rollenkonzeptes (Administrator, Revisor), Vier-Augen-Prinzip?

2.4 Protokollierung

- Bietet das Produkt Protokollierung an?
- Ist der Detailgrad der Protokollierung konfigurierbar? Werden durch die Protokollierung alle relevanten Daten erfasst?
- Ist die Protokollierung so möglich, dass die Daten nach unterschiedlichen Kategorien erfasst werden können (z. B. verbindungsorientiert, benutzerorientiert, protokollorientiert, dienstorientiert)?

- Ist der Zugriff auf die Protokolldaten mit einem Zugriffsschutz versehen?
- Bietet das Produkt die Möglichkeit an, die Protokolldaten nicht nur lokal zu speichern, sondern auch auf entfernten Rechnern (zentrales Protokoll)? Werden für die entfernte Speicherung unterschiedliche Datenübertragungstechniken angeboten, so dass auch Fremdsysteme zur Protokollierung benutzt werden können (z. B. syslog)? Kann die Übertragung der Protokolldaten abgesichert erfolgen?
- Bietet das Produkt eine Komponente zur Auswertung der Protokolldaten an?
- Kann der Protokollmechanismus mit dem eingesetzten Systemmanagementsystem zusammenarbeiten (Übertragungsformat, Übertragungsprotokoll)?
- Bietet das Produkt die Möglichkeit an, beim Auftreten bestimmter Ereignisse (z. B. Zugriffsverweigerung, mehrere fehlgeschlagene Authentisierungsversuche in Folge) den Administrator zu informieren oder auch geeignete Schutzmaßnahmen (Abweisen des RAS-Clients, Sperren von Benutzerkonten) automatisch durchzuführen?
- Kann die Protokollierung so erfolgen, dass die Bestimmungen des Datenschutzes erfüllt werden können?

2.5 Kommunikation und Datenübertragung

- Unterstützt die Server-Software LAN-seitig alle lokal existierenden Netzwerktechnologien (z. B. Ethernet, Token Ring, ATM)?
- Unterstützt die Client- und Server-Software WAN-seitig alle geplanten Zugangstechnologien (z. B. ISDN, Mobiltelefon, analoge Telefonleitung, X.25)?
- Erlaubt der RAS-Server die gleichzeitige Einwahl mehrerer RAS-Clients?
- Unterstützt das RAS-Produkt verschiedene Protokolle für den entfernten Zugang über Telekommunikationsnetze (z. B. PPP, SLIP)?
- Unterstützt das RAS-Produkt verschiedene Dienstprotokolle für den entfernten Zugriff (z. B. TCP/IP, NetBEUI, XPC, DECnet)?
- Werden für den Internet-basierten Zugriff Tunnel-Protokolle (z. B. PPTP, L2F, IPSec) unterstützt?
- Erlaubt das RAS-Produkt je nach verwendeter Zugangstechnologie die Nutzung von zusätzlichen, technologieabhängigen Mechanismen (z. B. Kanalbündelung für ISDN, Rückruf des RAS-Clients durch den RAS-Server)?

2.6 Sicherheit: Kommunikation, Authentisierung und Zugriff

- Gestattet das Produkt eine gesicherte Datenübertragung?
- Erlaubt das Produkt die alternative Nutzung von Sicherungsmechanismen (IPv4-Mechanismen, IPSec)?
- Erfolgt die Absicherung der Kommunikation durch standardisierte Mechanismen? Insbesondere sollten alle verwendeten kryptographischen Algorithmen etabliert sein und dem Stand der Technik entsprechen. Das Produkt sollte konform zu aktuellen Standards sein.
- Erlaubt die Produktarchitektur die nachträgliche Installation neuer Sicherheitsmechanismen?
- Wird dem entfernten Benutzer nur nach erfolgreicher Authentisierung der Zugang zum lokalen Netz erlaubt?
- Bietet das System die Möglichkeit an, die Authentisierung entfernter Benutzer durch mehrere Authentisierungsmechanismen durchzuführen (z. B. Benutzername und Passwort, Challenge-Response, Calling Line Identification - CLI)?
- Ist die Systemarchitektur so aufgebaut, dass neue Authentisierungsmechanismen nachträglich integriert werden können?
- Erlaubt das RAS-System die Nutzung einer oder mehrerer gängiger externer Authentisierungsdienste (z. B. SecureID, Radius, TACACS+)?
- Ist es möglich, zusätzliche externe Authentisierungsdienste einzubinden?
- Überträgt das RAS-System die zur Zugriffskontrolle für den Zugriff auf Daten im lokalen Netz notwendigen Informationen (Benutzer-Kennung, Sicherheits-ID) an die lokalen Mechanismen zur Zugriffskontrolle?

Sind alle Anforderungen an das zu beschaffende Produkt dokumentiert, so müssen die am Markt erhältlichen Produkte dahin gehend untersucht werden, inwieweit sie diese Anforderungen erfüllen. Es ist zu erwarten, dass nicht jedes Produkt alle Anforderungen gleichzeitig oder gleich gut erfüllt. Daher sollten die einzelnen Anforderungen mit Gewichten versehen werden, die reflektieren, wie wichtig die Erfüllung der jeweiligen Anforderung ist. Analog kann auch der Erfüllungsgrad einer Anforderung durch das einzelne Produkt in mehrere Stufen eingeteilt werden. Aufgrund der durchgeführten Produktbewertung (gemäß dem erstellten Anforderungskatalog) kann dann eine fundierte Kaufentscheidung getroffen werden.

M 2.187 Festlegen einer RAS-Sicherheitsrichtlinie

Verantwortlich für Initiierung: IT-Sicherheitsmanagement-Team

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement-Team, Administrator

Regelungen dokumentieren und fortschreiben

Im Rahmen der Planung eines RAS-Zugangs zu einem LAN muss auch für den entfernten Zugang eine Sicherheitsrichtlinie festgelegt werden. Die durch die organisationsweiten IT-Sicherheitsrichtlinien geltenden Vorschriften sind dazu entsprechend anzupassen und zu erweitern. Die Regelungen sind zu dokumentieren und bei Änderungen fortzuschreiben.

alle Benutzer informieren

Die für den entfernten Zugriff auf das lokale Netz geltenden Sicherheitsvorschriften sind allen Benutzern, denen der entfernte Zugriff erlaubt wird, mitzuteilen (siehe auch M 2.184 *Entwicklung eines RAS-Konzeptes*). Im Rahmen der Sicherheitsrichtlinie sollten Regelungen für folgende Bereiche festgelegt werden:

- Welcher Benutzer darf auf welche Daten zugreifen?
- Welcher Benutzer darf welche Applikationen nutzen?
- Welcher Benutzer darf auf welche Dienste bzw. Rechner zugreifen?
- Welcher Benutzer darf sich zu welchen Zeiten mit welchem RAS-Zugang verbinden?
- Welche Administratoren haben welche Aufgaben?
- Welche Authentisierungsmechanismen sind für den Zugriff zu benutzen?
- Welche Zugriffsrechte werden beim RAS-Zugriff jeweils vergeben?
- Ist der schreibende Zugriff auf Daten erlaubt?
- Ist für den schreibenden Zugriff nur ein spezieller Datenbereich zu nutzen (z. B. Incoming-Verzeichnis)?
- Wie werden mehrfache Authentisierungsfehler behandelt (z. B. Time-out verlängern, Benutzer sperren, RAS-Zugang sperren)?
- Unter welchen Umständen kann ein gesperrter RAS-Zugang wieder freigeschaltet werden? Wie ist der organisatorische Ablauf dafür?
- Unter welchen Umständen kann die Freischaltung auch aus der Entfernung veranlasst werden? Wie ist der organisatorische Ablauf dafür?
- Welche Daten werden protokolliert?

existierende Richtlinien berücksichtigen

Dieser Fragenkatalog muss entsprechend den lokalen Gegebenheiten erweitert, angepasst und konkretisiert werden. Dabei sind die existierenden Sicherheitsrichtlinien zu berücksichtigen. Die übergreifenden Sicherheitsvorgaben dürfen durch die RAS-Sicherheitsrichtlinien nicht ausgehöhlt werden.

Im Rahmen des IT-Sicherheitskonzepts sollten für die durch die RAS-Sicherheitsrichtlinie vorgegebenen Regeln auch mögliche Reaktionen bei Verstößen festgelegt werden. Diese müssen jedem RAS-Benutzer bekannt sein.

Ergänzende Kontrollfragen:

- Werden alle relevanten RAS-Komponenten (Client, Server, Netzkoppelelemente) durch die RAS-Sicherheitsrichtlinie erfasst?
- Wie wird die Einhaltung der RAS-Sicherheitsrichtlinie überprüft?
- Unterliegt die RAS-Sicherheitsrichtlinie einer Fortschreibung, so dass veränderte Rahmenbedingungen erfasst werden?

M 2.188 Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Bei der Nutzung von Mobiltelefonen gibt es eine Vielzahl von Möglichkeiten, diese vor Missbrauch zu schützen. Damit diese Möglichkeiten auch genutzt werden, sollte eine Sicherheitsrichtlinie erstellt werden, in der alle umzusetzenden Sicherheitsmechanismen beschrieben werden. Zusätzlich sollte für die Benutzer ein kurzes und übersichtliches Merkblatt für die sichere Nutzung von Mobiltelefonen erstellt werden.

Anfallende Datenarten

Sobald ein Mobiltelefon eingeschaltet wird, meldet es sich über die nächstgelegene Basisstation beim Netzbetreiber an. Bei diesem werden Daten zur Identität des Nutzers, die Seriennummer des Mobiltelefons und die Kennung der Basisstation, über die die Anmeldung erfolgt ist, protokolliert und gespeichert. Dies erfolgt auch dann, wenn kein Gespräch geführt wird. Weiterhin wird jeder Verbindungsversuch, unabhängig vom Zustandekommen der Verbindung, gespeichert.

Die bei der Telekommunikation anfallenden Datenarten lassen sich grob in drei Gruppen untergliedern:

- Bestandsdaten (oder auch Stammdaten) sind diejenigen Daten, die in einem Dienst oder Netz dauerhaft gespeichert und bereit gehalten werden. Hierzu gehören die Rufnummer und gegebenenfalls der Name und die Anschrift des Teilnehmers, Informationen über die Art des Endgerätes, gegebenenfalls für den Anschluss jeweils verfügbare Leistungsmerkmale und Berechtigungen sowie Daten über die Zuordnung zu Teilnehmergruppen.
- Inhaltsdaten sind die eigentlichen "Nutzdaten", d. h. die übertragenen Informationen und Nachrichten.
- Verbindungsdaten geben Auskunft über die näheren Umstände von Kommunikationsvorgängen. Hierzu gehören Angaben über Kommunikationspartner (z. B. Rufnummern des rufenden und des angerufenen Anschlusses), Zeitpunkt und Dauer der Verbindung, in Anspruch genommene Systemleistungen, benutzte Anschlüsse, Leitungen und sonstige technische Einrichtungen, Dienste und - bei mobilen Diensten - die Standortkennungen der mobilen Endgeräte.

Im Folgenden werden Empfehlungen gegeben, wie diese Daten vor Missbrauch geschützt werden können.

Schutz vor Kartenmissbrauch

Das Mobiltelefon und die SIM-Karte müssen stets sicher aufbewahrt werden. Bei Dienstreisen sollten sie nicht unbeaufsichtigt gelassen werden. Insbesondere sollten sie nicht in Fahrzeugen zurückgelassen werden.

Mobiltelefone und dazu angebotene Dienstleistungen können an verschiedenen Stellen durch PINs oder Passwörter abgesichert werden. Dazu gehören:

- der Zugriff auf die SIM-Karte,
- der Zugriff auf das eigentliche Endgerät, also das Mobiltelefon,
- der Zugriff auf bestimmte Funktionen des Mobiltelefons, z. B. das Telefonbuch,
- der Zugriff auf die Mailbox, also die Anrufbeantworterfunktion, oder andere Dienstleistungen des Netzbetreibers,
- der Zugriff auf Daten beim Netzbetreiber (bei Fragen an die Hotline wegen der Abrechnung muss unter Umständen ein Kennwort genannt werden).

Alle diese Sicherheitsmechanismen sollten auch genutzt werden (siehe auch M 4.114 *Nutzung der Sicherheitsmechanismen von Mobiltelefonen*). Am wichtigsten ist dabei sicherlich der Schutz der SIM-Karte, da deren Missbrauch zu hohen finanziellen Schäden führen kann. Die persönliche Geheimzahl (PIN) darf keinesfalls zusammen mit der zum Mobiltelefon gehörigen SIM-Karte aufbewahrt werden.

Bei Verlust der SIM-Karte sollte sofort beim Netzbetreiber eine Kartensperre veranlasst werden, um einen eventuellen Missbrauch und damit auch einen finanziellen Schaden abzuwehren (siehe M 2.189 *Sperrung des Mobiltelefons bei Verlust*).

Um die missbräuchliche Nutzung der SIM-Karte rechtzeitig zu bemerken, sollte in jedem Fall der Einzelverbindungsnachweis auf unerklärliche Gebühren und Zielrufnummern geprüft werden.

Einzelverbindungsnachweis

Der Netzbetreiber speichert die Anrufdaten für die Abrechnung. In Deutschland darf er sie nur bis zur Rechnungsstellung speichern, maximal aber 80 Tage gemäß TDSV (Telekommunikationsdienstunternehmen-Datenschutzverordnung - Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen). Es kann aber für den Kunden sinnvoll sein, dem Netzbetreiber zu erlauben, die Anrufdaten länger zu speichern, falls nachträglich Probleme mit der Rechnung auftreten.

Jeder Kunde sollte einen Einzelverbindungsnachweis verlangen, um die Mobiltelefon-Nutzung kontrollieren zu können. In Deutschland haben die Kunden das Recht auf einen kostenlosen Einzelverbindungsnachweis. Aus diesem können z. B. folgende Daten entnommen werden:

- Rechnungsdatum,
- angerufene Rufnummer (vollständig bzw. die letzten Ziffern unkenntlich),
- Beginn, Ende oder Dauer der Verbindung,
- Kosten des Gesprächs.

Alle Mitbenutzer des Telefons müssen darüber informiert werden, dass ein Einzelverbindungsnachweis beantragt wurde und welche Daten dadurch erfasst werden.

Wenn in einer Behörde bzw. einem Unternehmen zur Kostenkontrolle Einzelverbindungsnachweise geführt und ausgewertet werden, ist das Verfahren mit dem Betriebs- bzw. Personalrat und dem Datenschutzbeauftragten abzustimmen und den Benutzern bekannt zu geben.

Die Einzelverbindungsnachweise sollten immer nach Erhalt überprüft werden, ob sie korrekt sind. Hierdurch lässt sich auch ersehen, wo evtl. Kosten reduziert werden können.

Weitergabe der Rufnummer

Es kann gewählt werden, ob und welche Daten über den Mobiltelefon-Anschluss in öffentliche Telefonbücher eingetragen werden bzw. für Abfragen über Telefonauskünfte zur Verfügung gestellt werden. Ein Rufnummerneintrag erleichtert es Kommunikationspartnern anzurufen. Dies ist aber nicht für alle Einsatzzwecke sinnvoll, z. B. bei Mobiltelefonen aus einem Pool oder wenn die Zahl der Anrufer klein gehalten werden soll.

Wenn die Rufnummernanzeige aktiviert ist, können die Gesprächspartner (je nach Ausstattung) sehen, von welcher Telefonnummer sie angerufen werden. Dieser Dienst kann vom Netzbetreiber generell für ein Mobiltelefon an- oder abgeschaltet werden.

Rufnummernunterdrückung

Im GSM-Netz können den beteiligten Kommunikationspartnern die jeweiligen Rufnummern signalisiert werden. Wenn dies nicht gewünscht ist, sollte M 5.79 *Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung* beachtet werden.

Schutz vor Abhören von Telefonaten

Der einzige wirksame Schutz gegen das Abhören des Inhaltes von Telefonaten ist die interoperable, netzübergreifende Ende-zu-Ende-Verschlüsselung. Da diese Verschlüsselung nicht realisiert ist, kann jede Verbindung, ob im Festnetz oder im Mobilfunknetz, potentiell abgehört werden. Die Kommunikation zwischen Mobiltelefon und Basisstation wird aber in Deutschland und den meisten anderen Ländern automatisch verschlüsselt.

Folgende Maßnahmen können zur Verringerung der Gefährdung empfohlen werden:

- Es sollte nicht immer und überall telefoniert werden. Zum Telefonieren sollte ein ungestörter Bereich aufgesucht werden (dadurch werden auch andere weniger gestört).
- Grundsätzlich sollten keine Telefongespräche mit vertraulichem Inhalt geführt werden.
- Manche Mobiltelefone zeigen auf dem Display an, wenn die Übertragung zwischen Mobiltelefon und Basisstation nicht verschlüsselt wird. Wenn diese Anzeige vorgesehen ist, sollten die Benutzer darüber informiert werden. Ab und zu sollten sie sich durch einen Blick auf das Display davon überzeugen, dass tatsächlich verschlüsselt wird. So gibt es z. B. einige Länder, in denen die Kommunikation zwischen Mobiltelefon und Basisstation nicht verschlüsselt wird.

- Es gibt auch einige wenige und verhältnismäßig teure Mobiltelefone, mit denen die Kommunikation von Ende zu Ende verschlüsselt werden kann. Dafür müssen aber beide Gesprächspartner kompatible Geräte einsetzen. Wenn häufiger hochsensitive Informationen über Mobiltelefon weitergegeben werden sollen, kann dies sinnvoll sein.
- Bei der Datenübertragung z. B. von einem Laptop über GSM sollten die übertragenen Daten vorher auf dem Endgerät verschlüsselt werden. Hierzu gibt es eine Vielzahl von Programmen, die dies einfach ermöglichen.
- Wenn Mobiltelefone bzw. SIM-Karten gewechselt werden, ist es enorm aufwendig, gezielt Telefonate abzuhören. Dies kann daher bei der Übertragung hochsensitiver Information bzw. Daten zweckmäßig sein.
- Es sollte geprüft werden, ob alle Gesprächsgebühren dem Teilnehmer in Rechnung gestellt wurden. Fehlende Gebühren für bestimmte Verbindungen können auf Abhören hindeuten.

Sensibilisierung der Benutzer

Da oft leichtfertig mit der Abhörgefahr im Telekommunikationsbereich umgegangen wird, sollten Behörden bzw. Unternehmen prüfen, inwieweit die bisherigen Maßnahmen zur Aufklärung ihrer Mitarbeiter über Gefährdungen im Telekommunikationssektor ausreichen. Gegebenenfalls ist es angebracht, die Mitarbeiter regelmäßig über die Abhörgefahren zu informieren und damit auch zu sensibilisieren.

Sorgfalt bei der Weitergabe von Informationen

Die Mitarbeiter sollten auch darüber aufgeklärt werden, dass sie vertrauliche Informationen nicht ohne weiteres telefonisch weitergeben sollten. Insbesondere sollte die Identität des Kommunikationspartners hinterfragt werden, bevor detaillierte Auskünfte gegeben werden (siehe auch G 3.45 *Unzureichende Identifikationsprüfung von Kommunikationspartnern*). Bei der Benutzung von Mobiltelefonen sollten sie außerdem darauf achten, dass vertrauliche Mitteilungen nicht in der Öffentlichkeit besprochen werden.

Immer wieder kursieren spektakuläre, aber falsche Warnmeldungen (siehe auch G 5.80 *Hoax*). Damit nicht wertvolle Arbeitszeit auf die Prüfung des Wahrheitsgehaltes solcher Nachrichten verschwendet wird, sollten alle Mitarbeiter schnellstmöglich über das Auftreten eines neuen Hoax informiert werden. Es gibt verschiedene Informationsdienste, die entsprechende Warnungen weitergeben.

Regelungen zur Mobiltelefon-Nutzung

Bei der Nutzung von Mobiltelefonen in einer Behörde oder einem Unternehmen sind einige Punkte zu regeln. Dies betrifft sowohl die Nutzung von privaten als auch von dienstlichen Mobiltelefonen.

Nutzung von privaten Mobiltelefonen

Aufgrund einer unzureichenden Ausstattung kann es vorkommen, dass private Mobiltelefone für dienstliche Zwecke benutzt werden. Hierbei sind aber folgende Aspekte vorher zu regeln:

- Wer bezahlt dienstliche Gespräche und wie werden sie abgerechnet?
- Moderne Mobiltelefone beinhalten Terminkalender, Adressbücher, E-Mail-Unterstützung und mehr. Die sinnvolle Nutzung dieser Funktionen erfordert im Allgemeinen eine Synchronisation mit einem PC. Daher muss geklärt werden, ob die Installation der dafür benötigten Hard- und Software erlaubt wird.

Nutzung von dienstlichen Mobiltelefonen

Ebenso sind bei der Nutzung von dienstlichen Mobiltelefonen diverse Punkte zu regeln:

- Es muss geklärt werden, ob bzw. in welcher Menge Privatgespräche mit dienstlichen Mobiltelefonen geführt werden dürfen.
- Es sollte überlegt werden, ob die Nutzung der Mobiltelefone auf bestimmte Kommunikationspartner eingeschränkt werden sollte, z. B. um unnötigen Kosten vorzubeugen oder auch um die Informationsweitergabe einzuschränken (siehe auch M 2.42 *Festlegung der möglichen Kommunikationspartner*). Hierzu kann eine organisatorische Vorgabe erfolgen, es kann aber auch technisch geregelt werden, wie weiter unten unter den Stichworten "Anrufsperrungen" und "Geschlossene Benutzergruppe" beschrieben.
- Auch bei dienstlichen Mobiltelefonen sollten die Benutzer über die entstehenden Kosten informiert werden, damit diese möglichst gering gehalten werden können. So sollten die Benutzer über die Tarifstruktur und Roaming-Abkommen unterrichtet sein, damit sie beispielsweise im Ausland die günstigsten Netzbetreiber auswählen können.
- Die Benutzer sollten darauf hingewiesen werden, wie sie sorgfältig mit den Mobiltelefonen umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten (z. B. Akkupflege, Aufbewahrung außerhalb von Büro- oder Wohnräumen, Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen).
- Die Verwaltung, Wartung und Weitergabe von Mobiltelefonen sollte geregelt werden. Hierzu empfiehlt sich die Einrichtung eines Mobiltelefon-Pools (siehe M 2.190 *Einrichtung eines Mobiltelefon-Pools*).
- Bei jedem Benutzerwechsel müssen alle benötigten PINs gesichert weitergegeben werden (siehe M 2.22 *Hinterlegen des Passwortes*).

Allgemeine Regelungen

Unabhängig davon, ob privat oder dienstlich angeschaffte Mobiltelefone genutzt werden, sollte der Arbeitgeber schriftlich regeln,

- dass der Fahrer in dienstlich genutzten Fahrzeugen während der Fahrt nicht telefonieren darf, da sonst bei einem Unfall Mithaftung droht.
- dass Dienstgeheimnisse nicht über das Mobiltelefon weitergegeben werden dürfen. Gefahr droht hier weniger durch Mithören der Kommunikation auf der Verbindungsstrecke (über das Netz) als durch die Personen in der unmittelbaren Umgebung.

- dass man sich von der Identität seiner Gesprächspartner überzeugen sollte bzw. keine voreiligen Schlussfolgerungen ziehen sollte, bevor Interna weitergegeben werden.

Ein Mobiltelefon sollte möglichst nicht unbeaufsichtigt bleiben. Falls ein Mobiltelefon in einem Kraftfahrzeug zurückgelassen werden muss, so sollte das Gerät von außen nicht sichtbar sein. Das Abdecken des Gerätes oder das Einschließen in den Kofferraum bieten Abhilfe. Ein Mobiltelefon stellt einen Wert dar, der potentielle Diebe anlocken könnte.

Wird das Mobiltelefon in fremden Büroräumen vor Ort benutzt, so sind die Sicherheitsregelungen der besuchten Organisation zu beachten.

In fremden Räumlichkeiten wie Hotelzimmern sollte ein Mobiltelefon nicht ungeschützt ausliegen. Alle Passwort-Schutzmechanismen sollten spätestens jetzt aktiviert werden. Das Verschließen des Gerätes in einem Schrank behindert Gelegenheitsdiebe.

Information über Kosten

GSM-Telefonate werden zwar jedes Jahr preiswerter, es gibt aber einige Optionen, die auf Dauer hohe Kosten verursachen können. Da sich die Gebührenstruktur häufig ändert, sollten sich die Benutzer regelmäßig informieren, was welche Verbindungsarten, welche Verbindungszeiten und andere Optionen kosten.

So kann bei der Nutzung von Mobilfunktelefonen auch die Entgegennahme eines Anrufs Geld kosten, wenn sich der Angerufene z. B. im Ausland befindet oder eine Anrufweiterleitung ins Festnetz geschaltet hat. Da der Anrufer nicht wissen kann, wo sich der Angerufene befindet, werden ihm die Weiterleitungskosten auch nicht in Rechnung gestellt.

Regelung der Erreichbarkeit

Auch mit einem Mobiltelefon kann oder will ein Benutzer nicht jederzeit angerufen werden. So macht es einen schlechten Eindruck, wenn Mobiltelefone bei jeder Gelegenheit benutzt werden. Bei Besprechungen oder Vorträgen sollten Mobiltelefone möglichst ausgeschaltet werden. Zumindest sollte der Klingelton abgeschaltet oder leise und unauffällig eingestellt sein. Bei allen Gelegenheiten, bei denen ohnehin nicht frei gesprochen werden kann (Besprechungen, Restaurant, etc.) sollte die Benutzung des Mobiltelefons von vorneherein vermieden werden.

Andererseits sollte auch die Erreichbarkeit des Benutzers sichergestellt werden. Dafür bieten sich verschiedene Möglichkeiten an, beispielsweise

- können Erreichbarkeits-Zeiten festgelegt werden,
- kann die Anrufbeantworter-Funktionalität genutzt werden oder
- es kann eine Rufumleitung auf ein Sekretariat eingerichtet werden.

Nutzungsverbot von Mobiltelefonen

Es sollte überlegt werden, ob die Nutzung oder sogar das Mitbringen von Mobiltelefonen in allen oder bestimmten Bereichen einer Behörde oder eines Unternehmens eingeschränkt werden sollte. Dies kann z. B. für Besprechungs-

räume sinnvoll sein (siehe dazu auch M 5.80 *Schutz vor Abhören der Raumgespräche über Mobiltelefone*). Wenn die IT-Sicherheitspolitik der Institution es nicht zulässt, dass Mobiltelefone mitgebracht werden, muss an allen Eingängen deutlich darauf hingewiesen werden. Dies sollte dann auch regelmäßig kontrolliert werden.

Mobiltelefon nicht auf Server legen!

Durch die Nutzung von Mobiltelefonen können unter Umständen auch andere technische Geräte in ihrer Funktionsfähigkeit beeinträchtigt werden. Deswegen müssen z. B. in Flugzeugen oder Intensivstationen Mobiltelefone ausgeschaltet werden. Auch andere, empfindliche IT-Systeme können durch Mobiltelefone gestört werden. Dies ist z. B. schon in Serverräumen und Rechenzentren beobachtet worden. Mögliche Störungen sind umso unwahrscheinlicher, je geringer die Sendeleistung des Mobiltelefons ist bzw. je weiter dieses entfernt ist.

Schutz vor der Datenweitergabe über Mobiltelefone

Bei IT-Systemen, auf denen sensitive Daten verarbeitet werden oder die an ein Rechner-Netz angebunden sind, sollten keine Mobilfunkkarten zugelassen werden (siehe auch M 5.81 *Sichere Datenübertragung über Mobiltelefone*).

Einen absoluten Schutz gegen unberechtigte Datenweitergabe über Mobiltelefone - insbesondere bei Innentätern - gibt es nicht. Es sollte aber die Mitnahme von Mobiltelefonen in sensitive Bereiche untersagt und die Umsetzung dieses Verbotes regelmäßig überprüft werden.

Telefonbuch

Im Telefonbuch eines Mobiltelefons können Rufnummern und zugehörige Namen oder weitere Details gespeichert werden. Ein Telefonbuch kann im Endgerät, also dem Mobiltelefon, oder auf der SIM-Karte gespeichert werden. Deren Inhalte müssen nicht übereinstimmen. Dementsprechend kann über PINs auch wahlweise der Zugriff auf das Telefonbuch im Speicher des Endgeräts und/oder der SIM-Karte geschützt werden.

Ob Telefonnummern bevorzugt im Endgerät oder auf der SIM-Karte gespeichert werden, hängt von verschiedenen Erwägungen ab, beispielsweise wie einfach das Sichern der Daten auf anderen Medien ist (siehe M 6.72 *Ausfallvorsorge bei Mobiltelefonen*). Im Allgemeinen bietet sich das Speichern der Daten auf der SIM-Karte an, da

- diese damit bei einem Wechsel der SIM-Karte auch auf anderen Geräten zur Verfügung stehen und
- diese eventuell sensitiven Daten leicht aus dem Gerät entfernt werden können (wichtig z. B. bei Reparaturarbeiten oder Benutzerwechsel).

Es sollte möglichst nur eine Art der Speicherung gewählt werden. In diesem Telefonbuch sollten alle wichtigen Rufnummern gespeichert werden, damit diese jederzeit verfügbar sind. Die gespeicherten Rufnummern sollten gelegentlich kontrolliert werden, ob sie noch korrekt bzw. notwendig sind. Alle Rufnummern sollten so gespeichert werden, dass sie weltweit angerufen werden können, d. h. inklusive Landes- und Ortsvorwahl. Da nur der Ländercode international abgestimmt ist, nicht die Null, sollte dazu jede Rufnummer mit einem "+" am Anfang, gefolgt vom Ländercode (z. B. +49 für Deutschland), Ortsvorwahl ohne führende Null und dann Telefonnummer eingegeben

werden. Ein Eintrag könnte also wie folgt aussehen: *+4922895825369 GS-Hotline*.

Wenn das Mobiltelefon von mehreren Benutzern eingesetzt wird, sollten hier nur die gemeinsam genutzten Telefonnummern gespeichert werden. Außerdem sollte die Möglichkeit genutzt werden, über die vorhandenen Sperrmöglichkeiten Änderungen am Telefonbuch zu verhindern.

Nutzung der Anrufbeantworter-Funktionalität

Über die Netzbetreiber kann im Allgemeinen zu einem Mobiltelefon eine Anrufbeantworter-Funktionalität aktiviert werden. Eingehende Anrufe werden dabei beim Netzbetreiber in einer so genannten Mail- oder Mobilbox gespeichert, die vom Benutzer jederzeit abgerufen werden kann. Dies kann sehr sinnvoll sein, verursacht aber in der Regel zusätzliche Kosten.

Der Zugriff auf die Mailbox sollte durch eine PIN geschützt werden. Selbst wenn die Mailbox nicht genutzt wird, sollte die voreingestellte PIN schnell geändert werden, um eine Fremdnutzung zu verhindern.

Eingegangene Aufzeichnungen sollten regelmäßig abgehört werden. Alle Benutzer müssen darüber informiert werden, wie dies funktioniert.

Rufumleitung

Mit der Funktion Rufumleitung können eingehende Anrufe auf die Mailbox oder auf eine andere Rufnummer weitergeleitet werden. Dafür gibt es mehrere Varianten:

- Es können alle eingehenden Anrufe weitergeleitet werden.
- Anrufe werden nur dann weitergeleitet, wenn besetzt ist.
- Anrufe werden nur dann weitergeleitet, wenn der Anschluss nicht erreichbar ist, z. B. wegen eines Funklochs oder weil das Mobiltelefon ausgeschaltet ist.
- Es können bestimmte Arten von Anrufen weitergeleitet werden, z. B. Sprach-, Daten- oder Faxanrufe.

Dabei sollte allerdings berücksichtigt werden, dass Rufumleitungen auf Festnetzanschlüsse hohe Kosten verursachen können, da der Angerufene die Weiterleitungskosten selbst tragen muss.

Anrufsperrungen

Über Anrufsperrungen können Gespräche zu oder von einer Rufnummer gesperrt werden. Diese Funktionen werden über den Netzbetreiber zur Verfügung gestellt und können über das Mobiltelefon geändert werden. Dafür ist im Allgemeinen die Eingabe eines Passwortes erforderlich.

Anrufsperrungen können sinnvoll sein, wenn das Mobiltelefon an Dritte weitergegeben werden soll. Es gibt verschiedene Möglichkeiten von Anrufsperrungen:

- Sperren aller abgehenden Anrufe

  Damit können nur noch Anrufe empfangen, aber keine Rufnummern mit Ausnahme von Notruf-Nummern mehr angerufen werden.

- Sperren aller abgehenden internationalen Anrufe

  Mit dieser Sperrung können nur noch Nummern innerhalb des Landes angewählt werden, in dem man sich gerade befindet. Anrufe aus dem Ausland können weiterhin empfangen werden.

- Sperren aller abgehenden internationalen Anrufe außer ins Heimatland

  Damit können im Ausland Gespräche in das Heimatland (des Netzbetreibers) geführt werden. Das Anrufen in andere Länder ist gesperrt.

- Sperren aller ankommenden Anrufe

  Jede beliebige Nummer kann angewählt werden. Störungen durch eingehende Anrufe sind ausgeschlossen.

- Sperren aller ankommenden Anrufe bei Aufenthalt im Ausland

  Innerhalb des Heimatlandes kann weiterhin wie gewohnt telefoniert werden. Im Ausland können dagegen keine Telefonate mehr empfangen werden. Diese Option kann sinnvoll sein, da für den Empfang von Gesprächen im Ausland teilweise hohe Gebühren anfallen.

Ob und welche Art von Anrufsperrungen gewählt werden sollte, hängt von der Einsatzart des jeweiligen Mobiltelefons ab.

Geschlossene Benutzergruppe

Über den Dienst "Geschlossene Benutzergruppe" kann die Kommunikation auf die Mitglieder dieser Gruppe beschränkt werden (siehe auch M 5.47 *Einrichten einer Closed User Group*).

Die Gruppenmitglieder müssen beim Netzbetreiber eingetragen werden. Die Option "Geschlossene Benutzergruppe" kann am Mobiltelefon aktiviert werden. Die Einrichtung von geschlossenen Benutzergruppen kann z. B. sinnvoll sein, um die Datenübertragung über Mobilfunk einzuschränken.

Ergänzende Kontrollfragen:

- Existiert eine aktuelle Sicherheitsrichtlinie für die Mobiltelefon-Nutzung?
- Wie wird die Einhaltung der Sicherheitsrichtlinie für die Mobiltelefon-Nutzung überprüft?
- Besitzt jeder Mobiltelefon-Benutzer ein Exemplar dieser Mobiltelefon-Richtlinie oder ein Merkblatt mit einem Überblick der wichtigsten Sicherheitsmechanismen?
- Ist die Sicherheitsrichtlinie für die Mobiltelefon-Nutzung Inhalt der Schulungen zu IT-Sicherheitsmaßnahmen?
- Werden die Benutzer von Mobiltelefonen auf die Regelungen hingewiesen, die von ihnen einzuhalten sind?
- Werden die Benutzer von Mobiltelefonen auf die geeignete Aufbewahrung hingewiesen?

M 2.189 Sperrung des Mobiltelefons bei Verlust

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Benutzer

Verantwortlich für Umsetzung: Benutzer

Bei Verlust der SIM-Karte bzw. des Mobiltelefons trägt der Inhaber der SIM-Karte die Kosten für eine missbräuchliche Nutzung des Mobiltelefonanschlusses. Daher sollte sofort beim Netzbetreiber eine Sperrung der SIM-Karte veranlasst werden, um einen eventuellen Missbrauch, und damit einen zusätzlichen finanziellen Schaden, abzuwehren.

Darüber hinaus sollte die PIN-Abfrage der SIM-Karte stets aktiviert sein (siehe M 4.114 *Nutzung der Sicherheitsmechanismen von Mobiltelefonen*). Bei einem Diebstahl oder Verlust verhindert dies, dass die SIM-Karte von einem Unbefugten benutzt oder ausgewertet werden kann. Die PIN wird allerdings nur abgefragt, wenn das Mobiltelefon eingeschaltet wird. Wird ein eingeschaltetes Mobiltelefon gestohlen, kann hiermit zumindest solange missbräuchlich telefoniert werden, bis der Akku leer ist!

Bei Verlust oder Diebstahl des Mobiltelefons kann der Netzbetreiber außerdem die weitere Nutzung des Mobiltelefons unterbinden, indem er es auf eine "schwarze Liste" setzt. Hierzu benötigt er die Angabe der Gerätenummer (IMEI - International Mobile Equipment Identifier). Sie steht häufig auf der Rückseite des Gerätes und sollte daher notiert und unabhängig vom Gerät aufbewahrt werden.

Bereits beim Kauf sollte darauf geachtet werden, dass die zum Mobiltelefon gehörende IMEI schriftlich mitgeteilt wurde. Sie kann auch aus dem Mobiltelefon ausgelesen werden, allerdings ist das Verfahren nicht für alle Geräte einheitlich. Die Gerätenummer steht häufig auf dem Typenschild unter dem Akku oder kann mit der Eingabe "*#06#" angezeigt werden.

Um die missbräuchliche Nutzung der SIM-Karte rechtzeitig zu bemerken, sollte in jedem Fall der Einzelverbindungsnachweis auf unerklärliche Gebühren und Zielrufnummern geprüft werden.

SIM-Karte bei Verlust sofort sperren lassen!

Alle Daten, die für die Sperrung der SIM-Karte bzw. des Mobiltelefons benötigt werden, sollten griffbereit, aber getrennt vom Mobiltelefon aufbewahrt werden. Das sind

- die Rufnummer des Mobilfunkanschlusses sowie die zugehörige SIM-Kartennummer,
- die Seriennummer des Mobiltelefons,
- die Servicenummer des Netzbetreibers, unter der der Sperrwunsch gemeldet werden kann sowie
- das Servicenummer-Passwort und Kundennummer, also die Daten, die für die Authentikation gegenüber dem Netzbetreiber benötigt werden.

M 2.190 Einrichtung eines Mobiltelefon-Pools

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Einrichtung eines Mobiltelefon-Pools

Sind in einer Behörde bzw. einem Unternehmen eine Vielzahl von Mobiltelefonen im Einsatz und wechseln die Benutzer häufig, kann es angebracht sein, die zeitweise nicht genutzten Mobiltelefone in einer Sammelaufbewahrung (Pool) zu halten.

Für alle Mobiltelefone ist die Stromversorgung sicherzustellen, damit die Akkus dieser Geräte den sofortigen Einsatz erlauben. Dabei ist zu beachten, dass sich ein Akku im Laufe der Zeit entlädt, auch wenn er nicht verwendet wird. Wenn die Mobiltelefone häufiger über längere Zeiträume eingesetzt werden, sollten zusätzlich Ersatzakkus vorrätig gehalten werden.

Hinweis: Die Ladegeräte sollten den Mobiltelefonen eindeutig und leicht erkennbar zugeordnet werden. Die Ladegeräte sehen sich zwar alle sehr ähnlich, sind aber leider meist nicht austauschbar.

Zusätzlich müssen die Rücknahme und die Ausgabe von Mobiltelefonen dokumentiert werden, so dass jederzeit nachvollziehbar ist, welche Geräte bei wem im Einsatz sind. Jeder Benutzer sollte mit Namen, Organisationseinheit, Datum und Uhrzeit in das Übergabejournal eingetragen werden.

Bei der Übergabe und Rücknahme von Mobiltelefonen sind außerdem folgende Punkte zu beachten:

Übergabe:

- Der neue Benutzer erhält alle benötigten PINs und Passwörter für die Nutzung des Mobiltelefons. Wenn diese auf selbstgewählte Werte geändert werden, müssen die neuen Werte bei der Rückgabe dokumentiert werden.
- Außerdem erhält er die Rufnummer des Mobiltelefons.
- Dem neuen Benutzer wird ein Merkblatt für den sicheren Umgang mit dem Mobiltelefon übergeben. Der Benutzer sollte außerdem die Bedienungsanleitung des Mobiltelefons bekommen. Neben der normalen Bedienung seines Telefons sollte der Benutzer vor allem in der Lage sein, etwaige Warnanzeigen (wie Piktogramme im Display) zu interpretieren.
- Das Mobiltelefon sollte geladen und zusammen mit dem passenden Ladegerät übergeben werden. Wenn das Mobiltelefon über längere Zeitspannen einsetzbar sein soll, sollte ein geladener Ersatzakku mit übergeben werden.

Rücknahme bzw. Weitergabe:

- Der Benutzer gibt die zuletzt benutzten PINs und Passwörter bekannt. Es muss überprüft werden, ob diese korrekt sind. Sie müssen notiert (und sicher verwahrt) werden.
- Die Vollständigkeit des Gerätes, des Zubehörs und der Dokumentation ist zu überprüfen. Das Gerät sollte auf Defekte überprüft werden.

- Der Benutzer muss sicherstellen, dass vor Rückgabe des Gerätes sämtliche Daten, die der Benutzer noch benötigt, auf ihm zugängliche Datenträger (z. B. seinen PC) übertragen werden. Darüber hinaus hat der Benutzer selber dafür Sorge zu tragen, dass sämtliche von ihm erzeugten Daten (z. B. Telefonnummern) gelöscht sind.
- Im Nummernspeicher des Mobiltelefons werden die zuletzt angerufenen Rufnummern gespeichert. Ebenso werden die Rufnummern der letzten Anrufer gespeichert, wenn die Funktion Anruferkennung verfügbar und aktiviert ist. Diese sollten vor einem Benutzerwechsel gelöscht werden. Außerdem können in Telefonbüchern sowohl im Mobiltelefon selbst als auch auf der SIM-Karte Rufnummern gespeichert werden. Persönliche Rufnummern sollten vor der Weitergabe ebenfalls gelöscht werden. Die für die dienstliche Kommunikation wichtigen Rufnummern sollten allen Benutzern dauerhaft zur Verfügung stehen.
- Im Mobiltelefon bzw. auf der SIM-Karte können außerdem Kurznachrichten, Faxe oder E-Mails gespeichert sein. Auch diese sollten vor einer Weitergabe gelöscht werden.

Ergänzende Kontrollfragen:

- Werden die Benutzer bei der Ausgabe von Mobiltelefonen auf die Regelungen und Sicherheitsmaßnahmen hingewiesen, die von ihnen einzuhalten sind?
- Werden die Benutzer bei der Ausgabe von Mobiltelefonen auf deren geeignete Aufbewahrung hingewiesen?
- Wird die Ausgabe und Rücknahme der Mobiltelefone dokumentiert?

M 2.191 Etablierung des IT-Sicherheitsprozesses

Diese Maßnahme ist mit Version 2005 entfallen.

M 2.192 Erstellung einer IT-Sicherheitsleitlinie

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter

Die Leitaussagen zur IT-Sicherheitsstrategie sollten in einer IT-Sicherheitsleitlinie zusammengefasst werden, um die zu verfolgenden IT-Sicherheitsziele und das angestrebte IT-Sicherheitsniveau für alle Mitarbeiter zu dokumentieren. Mit der IT-Sicherheitsleitlinie bekennt sich die Behörden- bzw. Unternehmensleitung sichtbar zu ihrer Verantwortung für IT-Sicherheit.

Bei der Erstellung der IT-Sicherheitsleitlinie müssen folgende Punkte beachtet werden:

Verantwortung der Behörden- bzw. Unternehmensleitung

Wichtig ist, dass die Behörden- bzw. Unternehmensleitung in vollem Umfang hinter der IT-Sicherheitsleitlinie und den darin festgehaltenen Zielen steht. Daher muss die IT-Sicherheitsleitlinie von der Behörden- bzw. Unternehmensleitung unterschrieben und in deren Namen veröffentlicht werden. Selbst wenn einzelne Aufgaben im Rahmen des IT-Sicherheitsprozesses an Personen oder Organisationseinheiten delegiert werden, die dann für die Umsetzung zuständig sind, bleibt die Gesamtverantwortung immer bei der Behörden- bzw. Unternehmensleitung.

Festlegung des Geltungsbereichs

Für die Feststellung von Rahmenbedingungen, IT-Sicherheitsanforderungen, Einflussfaktoren und weiteren sicherheitsrelevanten Aspekten muss der Geltungsbereich der IT-Sicherheitsleitlinie klar definiert werden. Dieser kann die gesamte Institution umfassen oder aus einzelnen Teilbereichen bestehen. Um einen sinnvollen IT-Sicherheitsprozess aufzusetzen ist es jedoch wichtig, dass im betrachteten Geltungsbereich die zugehörigen Fachaufgaben und Geschäftsprozesse komplett enthalten sind.

Festlegung von Sicherheitszielen

Zu Beginn des Sicherheitsprozesses muss die Behörden- bzw. Unternehmensleitung die Sicherheitsziele festlegen, abstimmen und dokumentieren. Diese lassen sich aus den Geschäftsaufgaben und Fachaufgaben, gesetzlichen Rahmenbedingungen und allgemeinen Behörden- oder Unternehmenszielen ableiten. Die Sicherheitsziele dienen als Grundlage der Sicherheitsleitlinie.

Inhalt der IT-Sicherheitsleitlinie

Die IT-Sicherheitsleitlinie sollte kurz und übersichtlich sein, dabei aber mindestens die folgenden Aspekte enthalten:

- Der Stellenwert der IT-Sicherheit und die Bedeutung der IT für die Institution müssen dargestellt werden.
- Die IT-Sicherheitsziele und der Bezug der IT-Sicherheitsziele zu den Geschäftszielen und Aufgaben der Institution müssen dabei erläutert werden.
- Die Kernelemente der IT-Sicherheitsstrategie sollten genannt werden.

- Die Leitungsebene muss allen Mitarbeitern aufzeigen, dass die IT-Sicherheitsleitlinie von ihr getragen und durchgesetzt wird. Ebenso muss es Leitaussagen zur Erfolgskontrolle geben.
- Die für die Umsetzung des IT-Sicherheitsprozesses etablierte Organisationsstruktur muss beschrieben werden (siehe M 2.193 *Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit*).

Bekanntgabe der IT-Sicherheitsleitlinie

IT-Sicherheitsmaßnahmen und organisatorische Regelungen werden erfahrungsgemäß nur dann von allen Mitarbeitern befolgt, wenn diese ihren Sinn erkennen. Die IT-Sicherheitsleitlinie muss daher veröffentlicht werden, um die Strategie des verantwortlichen Managements zu dokumentieren. Dies sollte so erfolgen, dass der Stellenwert der IT-Sicherheit deutlich wird. Es ist wichtig, dass alle Mitarbeiter die Inhalte der IT-Sicherheitsleitlinie kennen und nachvollziehen können. Neue Mitarbeiter sollten auf die IT-Sicherheitsleitlinie hingewiesen werden, bevor sie Zugang zur Informationsverarbeitung erhalten. Deren Bedeutung wird unterstrichen, wenn alle Mitarbeiter die Kenntnis der IT-Sicherheitsleitlinie schriftlich bestätigen müssen.

Generell sollte die IT-Sicherheitsleitlinie so allgemein gehalten sein, dass sich alle Mitarbeiter aus den verschiedenen Organisationsbereichen einer Institution davon angesprochen fühlen. Es ist aber auch möglich, die IT-Sicherheitsleitlinie für spezielle Anwendungen oder Bereiche innerhalb einer Institution um Inhalte zu ergänzen, die nur für einen eingeschränkten Personenkreis relevant oder die vertraulich sind. Es empfiehlt sich, diese Abschnitte in eine Anlage zur Leitlinie zu verlagern, um so flexibler und zeitnah auf erforderliche Änderungen zu reagieren zu können, ohne das der allgemeine Teil der Leitlinie angepasst werden muss. Falls erforderlich, kann die Anlage separat als vertraulich gekennzeichnet und besonders geschützt werden.

Aktualisierung der IT-Sicherheitsleitlinie

Die IT-Sicherheitsleitlinie muss regelmäßig bei Änderungen von Rahmenbedingungen, Geschäftszielen, Aufgaben oder der IT-Sicherheitsstrategie überprüft und gegebenenfalls aktualisiert werden.

Ergänzende Kontrollfragen:

- Gibt es eine von der Leitungsebene verabschiedete IT-Sicherheitsleitlinie?
- Enthält die Leitlinie Aussagen zu allen in dieser Maßnahme genannten Aspekten?
- Ist die IT-Sicherheitsleitlinie allen Mitarbeitern bekannt?
- Wann wurde die IT-Sicherheitsleitlinie das letzte Mal überprüft?

M 2.193 Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement-Team

Planung und Einrichtung der IT-Sicherheitsorganisation

Um einen IT-Sicherheitsprozesses erfolgreich planen, umsetzen und aufrechterhalten zu können, muss eine geeignete Organisationsstruktur vorhanden sein. Es müssen also Rollen definiert sein, die die verschiedenen Aufgaben für die Erreichung der IT-Sicherheitsziele wahrnehmen müssen. Außerdem müssen Personen benannt sein, die qualifiziert sind und denen ausreichend Ressourcen zur Verfügung stehen, um diese Rollen auszufüllen.

Zu Beginn eines IT-Sicherheitsprozesses kann sich herausstellen, dass es keine übergreifende Struktur für IT-Sicherheit gibt. In den meisten Behörden und Unternehmen gibt es allerdings bereits Personen, die für verschiedene Aspekte der IT-Sicherheit zuständig sind. Hier muss eine geeignete, übergreifende IT-Sicherheitsorganisation aufgebaut werden. Auch wenn bereits eine IT-Sicherheitsorganisation etabliert ist, sollte regelmäßig überlegt werden, ob diese noch angemessen ist oder an neue Rahmenbedingungen angepasst werden muss.

Funktion des IT-Sicherheitsbeauftragten

Die Art und Ausprägung einer IT-Sicherheitsorganisation hängt von der Größe, Beschaffenheit und Struktur der jeweiligen Institution ab. In jeder Institution muss allerdings die Funktion des IT-Sicherheitsbeauftragten eingerichtet werden, der für alle Belange der IT-Sicherheit zuständig ist. Die Aufgaben des IT-Sicherheitsbeauftragten sind unter anderem:

- den IT-Sicherheitsprozess zu steuern und zu koordinieren,
- die Erstellung von IT-System-Sicherheitsrichtlinien zu initiieren und zu koordinieren,
- die Erstellung des IT-Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte zu koordinieren,
- den Realisierungsplan für die IT-Sicherheitsmaßnahmen zu erstellen und deren Realisierung zu initiieren und zu überprüfen,
- der Leitungsebene und dem IT-Sicherheitsmanagement-Team zu berichten,
- sicherheitsrelevante Projekte zu koordinieren und den Informationsfluss zwischen Bereichs-IT-, IT-Projekt- sowie IT-System-Sicherheitsbeauftragten sicherzustellen,
- sicherheitsrelevante Zwischenfälle zu untersuchen sowie
- Sensibilisierungs- und Schulungsmaßnahmen zu IT-Sicherheit zu initiieren und zu steuern.

Der IT-Sicherheitsbeauftragte muss bei allen Projekten mit IT-Bezug beteiligt werden, damit sichergestellt ist, dass sicherheitsrelevante Aspekte ausreichend

beachtet werden. Dazu gehören z. B. die Beschaffung von IT-Systemen oder die Gestaltung von IT-gestützten Geschäftsprozessen.

Um den direkten Zugang zur Behörden- bzw. Unternehmensleitung sicherzustellen, ist es empfehlenswert, diese Rolle als Stabsstelle einzurichten.

In kleinen Organisationen kann die Funktion des IT-Sicherheitsbeauftragten auch von einem qualifizierten Mitarbeiter neben anderen Aufgaben wahrgenommen werden. Maßgeblich ist, dass dem IT-Sicherheitsbeauftragten ausreichend Zeit für seine Aufgaben zugebilligt wird. Vor allem bei der erstmaligen Einrichtung des IT-Sicherheitsprozesses müssen hierfür auch hinreichende zeitliche Ressourcen eingeplant werden. Ebenfalls wichtig bei der Planung der IT-Sicherheitsorganisation ist die Benennung eines qualifizierten Vertreters des IT-Sicherheitsbeauftragten.

Auswahl des IT-Sicherheitsbeauftragten

Der IT-Sicherheitsbeauftragte sollte über Wissen und Erfahrung in den Gebieten Informationstechnik und IT-Sicherheit verfügen. Weiterhin sollte er über die folgenden Qualifikationen und Eigenschaften verfügen:

- Identifikation mit den Zielsetzungen der Institution
- Einsicht in die Notwendigkeit von IT-Sicherheit
- Kooperations- und Teamfähigkeit (wenige andere Aufgaben erfordern so viel Fähigkeit und Geschick im Umgang mit anderen Personen)
- Fähigkeit zum selbständigen Arbeiten
- Durchsetzungsvermögen
- Erfahrungen im Projektmanagement

Ein IT-Sicherheitsbeauftragter alleine kann nicht für angemessene Sicherheit in allen Bereichen einer Institution sorgen. Daher sind Kommunikations- und Präsentationsfähigkeiten wichtig. Die Leitungsebene muss in zentralen Fragen des IT-Sicherheitsprozesses immer wieder eingebunden werden, außerdem müssen Entscheidungen eingefordert werden. Die Zusammenarbeit mit den IT-Benutzern verlangt viel Geschick, da diese von der Notwendigkeit der (für sie manchmal etwas lästigen) IT-Sicherheitsmaßnahmen überzeugt werden müssen. Mindestens genauso heikel ist die Befragung der Mitarbeiter nach sicherheitskritischen Vorkommnissen und Schwachstellen. Um bei diesen Befragungen nützliche Ergebnisse zu erzielen, müssen die Mitarbeiter davon überzeugt werden, dass ehrliche Antworten nicht zu Problemen für sie selbst führen.

Aufbau eines IT-Sicherheitsmanagement-Teams

In größeren Organisationen ist es sinnvoll, ein IT-Sicherheitsmanagement-Team aufzubauen, das den IT-Sicherheitsbeauftragten unterstützt und sämtliche übergreifende Belange der IT-Sicherheit regelt und Pläne, Vorgaben und Richtlinien erarbeitet. Die Größe und die Zusammenstellung des IT-Sicherheitsmanagement-Teams sollten in Abhängigkeit vom Umfang des IT-Sicherheitsprozesses und der dafür benötigten Ressourcen und Expertisen definiert werden. In BSI-Standard 100-2 *IT-Grundschutz-Vorgehensweise* sind verschiedene Varianten dargestellt, wie eine Aufbauorganisation des IT-Sicherheitsmanagements aussehen kann.

Auswahl des IT-Sicherheitsmanagement-Teams

Um die verschiedenen Sichten der IT-Sicherheit in der Organisation zu berücksichtigen, sollten im IT-Sicherheitsmanagement-Team folgende Vertreter zusammenarbeiten:

- IT-Sicherheitsbeauftragter
- IT-Verantwortliche
- Vertreter der IT-Anwender
- Datenschutzbeauftragte
- IT-Revision
- Juristische Vertretung der Organisation
- Personalrat

Benennung eines verantwortlichen Managers

Auf Leitungsebene sollte die Aufgabe IT-Sicherheit eindeutig einem verantwortlichen Manager zugeordnet sein, an den der IT-Sicherheitsbeauftragte direkt berichtet. In kleinen Organisationen kann auch ein Geschäftsführer diese Aufgabe übernehmen.

Überprüfung der IT-Sicherheitsorganisation

Eine einmal aufgebaute IT-Sicherheitsorganisation ist nicht statisch. Geschäftsprozesse und Umfeldbedingungen ändern sich permanent, so dass auch die IT-Sicherheitsorganisation immer wieder überdacht werden muss. Dabei sollte beispielsweise beleuchtet werden, ob die Aufgaben und Kompetenzen innerhalb des IT-Sicherheitsprozesses ausreichend klar definiert waren, aber auch, ob vorgesehene Aufgaben nicht wahrgenommen werden konnten. Vor allem sollten die folgenden Punkte abgeklopft werden:

- Überwachung von Verantwortlichkeiten im laufenden Betrieb

  Es muss regelmäßig überprüft werden, ob alle Verantwortlichkeiten und Zuständigkeiten eindeutig zugewiesen wurden und ob diese beachtet werden.

- Überprüfung der Einhaltung von Vorgaben

  Es muss regelmäßig geprüft werden, ob alle Prozesse und Abläufe der IT-Sicherheitsorganisation wie vorgesehen angewendet und durchgeführt werden. Außerdem sollte dabei überdacht werden, ob die aufgebauten Strukturen der IT-Sicherheitsorganisation den Anforderungen gerecht werden.

- Beurteilung der Effizienz von Prozessen und organisatorischer Regelungen

  Es muss regelmäßig überprüft werden, ob Prozesse und organisatorische Regelungen des IT-Sicherheitsmanagements praxistauglich und effizient sind. Wenn Prozesse oder Regelungen, die aus Sicherheitsgründen eingerichtet wurden, zu kompliziert oder zeitaufwendig sind, werden sie häufig nicht beachtet oder umgangen, was zu Sicherheitsvorfällen führen kann.

- Managementbewertungen

  Das Management ist über die Ergebnisse der oben genannten Überprüfungen regelmäßig zu informieren. Die Berichte sind nicht nur not-

wendig, um dringende oder zeitkritische Probleme zu lösen, sondern enthalten wichtige Informationen, die das Management für die Steuerung des IT-Sicherheitsprozesses benötigt.

Anpassung und Verbesserung der IT-Sicherheitsorganisation

Die IT-Sicherheitsorganisation muss regelmäßig in Bezug auf Effizienz und Effektivität optimiert werden. Hat sich herausgestellt, dass Prozesse oder Regelungen für die IT-Sicherheitsorganisation Schwächen haben, müssen diese abgestellt werden.

Dokumentation

Die Aufgaben, Verantwortungen und Kompetenzen im IT-Sicherheitsmanagement müssen nachvollziehbar dokumentiert sein. Dazu gehören auch die wesentlichen Arbeitsanweisungen und organisatorischen Regelungen.

Ergänzende Kontrollfragen:

- Ist ein IT-Sicherheitsbeauftragter benannt worden?
- Besteht die Notwendigkeit, den IT-Sicherheitsbeauftragten durch ein IT-Sicherheitsmanagement-Team zu unterstützen?
- Sind die Aufgaben und Kompetenzen innerhalb des IT-Sicherheitsprozesses klar definiert?
- Wird die Effizienz der IT-Sicherheitsorganisation regelmäßig überprüft? Wie?

M 2.194 Erstellung einer Übersicht über vorhandene IT-Systeme

Diese Maßnahme ist mit Version 2005 entfallen.

M 2.195 Erstellung eines IT-Sicherheitskonzepts

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement-Team

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement-Team

Zielsetzung

Ein IT-Sicherheitskonzept dient zur Umsetzung der IT-Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das IT-Sicherheitskonzept ist das zentrale Dokument im IT-Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Maßnahme muss sich letztlich darauf zurückführen lassen. Aus diesem Grund muss ein IT-Sicherheitskonzept sorgfältig geplant und umgesetzt sowie regelmäßig überarbeitet werden. Die einzelnen, im folgenden kurz angerissenen Aspekte werden ausführlich im BSI-Standard 100-2 *IT-Grundschutz-Vorgehensweise* behandelt.

Geltungsbereich

Nicht alle Bereiche einer Institution müssen durch ein einziges IT-Sicherheitskonzept abgedeckt werden. Wenn die Umsetzung des IT-Grundschutzes in einem großen Schritt eine unübersichtliche Aufgabe darstellt, dann kann es sinnvoll sein, zunächst nur in ausgewählten Bereichen das erforderliche Sicherheitsniveau umzusetzen. Von dieser Basis ausgehend sollte sich dann der IT-Sicherheitsprozess auf die Gesamtorganisation ausweiten. Vor allem bei großen Behörden und Unternehmen kann es mehrere IT-Sicherheitskonzepte geben, die verschiedene Organisationsbereiche abdecken. Es muss gewährleistet sein, dass alle Bereiche einer Institution durch angemessene IT-Sicherheitskonzepte abgedeckt werden.

Auch komplexe Geschäftsprozesse oder Anwendungen können in eigenen IT-Sicherheitskonzepten behandelt werden. Dies empfiehlt sich vor allem bei der Einführung neuer Aufgaben oder Anwendungen.

IT-Verbund

Der festgelegte Geltungsbereich wird im Weiteren als IT-Verbund bezeichnet und stellt detailliert den Bereich dar, für den das IT-Sicherheitskonzept umgesetzt werden soll. Ein IT-Verbund kann sich somit auf Fachaufgaben, Geschäftsprozesse oder Organisationseinheiten beziehen. Er umfasst alle infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in diesem Anwendungsbereich der Informationsverarbeitung dienen.

Der IT-Verbund muss so festgelegt sein, dass die betrachteten Geschäftsprozesse und Informationen diesem Bereich vollständig zugeordnet werden können. Die Abhängigkeiten aller sicherheitsrelevanten Prozesse sind zu berücksichtigen. Die Schnittstellen zu den anderen Bereichen müssen klar definiert werden, so dass der IT-Verbund im Gesamtunternehmen eine sinnvolle Mindestgröße einnimmt.

Risikobewertung

Das IT-Sicherheitsmanagement muss eine Methode zur Risikobewertung auswählen, die es ermöglicht, potentielle Schäden durch IT-Sicherheitsvorfälle zu analysieren und zu bewerten. Es können auch mehrere, aufeinander aufbauende Verfahren zur Risikobewertung gewählt werden.

In der Vorgehensweise nach IT-Grundschutz wird implizit eine Risikobewertung für Bereiche mit normalem Schutzbedarf durchgeführt. Falls der betrachtete IT-Verbund Komponenten mit hohem oder sehr hohem Schutz-

bedarf enthält, muss im Anschluss an die IT-Grundschutz-Analyse eine ergänzende IT-Sicherheitsanalyse durchgeführt werden.

Übersicht IT-Verbund

Basis jeder Risikobewertung ist die Beschreibung der zu schützenden Informationen und Geschäftsprozesse. Um einen Überblick über die für die Geschäftsprozesse wichtigen IT-Strukturen zu bekommen, ist der IT-Verbund strukturiert zu erfassen. Neben den technischen Komponenten, den IT-Anwendungen und den verarbeitenden Informationen sind hierbei auch die räumliche Infrastruktur und die Vernetzung zu erfassen. Dabei müssen auch die Abhängigkeiten der verschiedenen Komponenten untereinander festgehalten werden.

Schutzbedarfsfeststellung

In der Schutzbedarfsfeststellung sind folgende Schritte enthalten:

- Es wird analysiert, welche Gefährdungen bzw. Risiken für die Institution als Folge unzureichender IT-Sicherheit bestehen.
- Mögliche Schäden durch Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit werden identifiziert.
- Die potentiellen Auswirkungen auf die Geschäftstätigkeit oder die Aufgabenerfüllung durch IT-Sicherheitsvorfälle und andere IT-Sicherheitsrisiken werden analysiert und bewertet.

Anhand dieser Betrachtungen lässt sich das Risiko für das Unternehmen bzw. die Behörde abschätzen und der Schutzbedarf für Informationen, IT-Anwendungen und IT-Systemen festlegen.

Soll-Ist-Vergleich

Aus den allgemeinen IT-Sicherheitszielen, dem identifizierten Schutzbedarf und der Risikobewertung werden konkrete IT-Sicherheitsmaßnahmen passend zum betrachteten IT-Verbund abgeleitet. Hierfür müssen konkrete Bausteine der IT-Grundschutz-Kataloge für die Sicherheitsanforderungen eines IT-Verbundes ausgewählt werden, um so ein spezifisches Paket von IT-Sicherheitsmaßnahmen als Soll-Vorgabe zu erhalten.

Um zu ermitteln, welche der Sicherheitsmaßnahmen bereits umgesetzt und an welchen Stellen noch Lücken sind, wird ein Basis-Sicherheitscheck durchgeführt.

Ergänzende Sicherheitsanalyse

Die Umsetzung der nach IT-Grundschutz vorgeschlagenen Maßnahmen ist für den normalen, in manchen Fällen auch für den höheren Schutzbedarf ausreichend. Für Bereiche mit hohem oder sehr hohem Schutzbedarf ist in einer ergänzenden Sicherheitsanalyse zu entscheiden, ob eine weiterführende Risikobetrachtung erforderlich ist. Für die identifizierten Bereiche sollte eine Risikoanalyse auf der Basis von IT-Grundschutz durchgeführt werden.

Konsolidierung der Maßnahmen

Vor der Fertigstellung eines Sicherheitskonzeptes müssen die in der ergänzenden Risikoanalyse zusätzlich identifizierten Maßnahmen mit den IT-Grundschutzmaßnahmen konsolidiert werden. Dabei ist für alle neu ermittelten IT-Sicherheitsmaßnahmen zu überprüfen, ob sie die vorhandenen Maßnahmen ersetzen, ergänzen oder in ihrer Wirkung beeinträchtigen.

Umsetzungsplanung

Bei der Erstellung eines IT-Sicherheitskonzepts sollte auch direkt bei der Auswahl der einzelnen Sicherheitsmaßnahmen die Umsetzungsplanung vorgenommen werden. Dafür ist festzuhalten, in welchem Zeitraum die einzelnen Maßnahmen umzusetzen sind, welche vernünftigerweise gemeinsam umge-

setzt werden sollten und welche Maßnahmen zeitkritisch sind. Die Umsetzungsplanung sollte entweder im IT-Sicherheitskonzept oder in einem beigefügten Realisierungsplan festgehalten werden. Hierin sollten vor allem Umsetzungsreihenfolge und Verantwortlichkeiten enthalten sein:

Realisierungsplan

- Festlegung von Prioritäten (Umsetzungsreihenfolge): Alle IT-Sicherheitsmaßnahmen sollten nach Wichtigkeit und Effektivität priorisiert werden. Grundsätzlich sollten Maßnahmen gegen besonders schwerwiegende Gefährdungen vorrangig umgesetzt werden. Dies ist besonders wichtig, wenn gegen diese Gefährdungen bisher nur wenig Schutz besteht. Wenn (z. B. aus finanziellen Gründen) nicht sofort alle Maßnahmen umgesetzt werden können, sollte geprüft werden, welche Maßnahmen die größte Breitenwirkung haben, also gegen besonders viele Gefährdungen wirken. Diese Maßnahmen sollten zuerst umgesetzt werden.
- Bei der Umsetzungsreihenfolge sollten auch mögliche Zusammenhänge zwischen Maßnahmen berücksichtigt werden.
- Verantwortlichkeiten: Für jede Maßnahme ist festzulegen, wer für Initialisierung, Umsetzung und Kontrolle (z. B. Audit) oder Revision verantwortlich ist.

Bei der Auswahl von Sicherheitsmaßnahmen ist auch immer deren Angemessenheit und Wirtschaftlichkeit zu beachten. Es muss nachvollziehbar sein, warum die ausgewählten Maßnahmen geeignet sind, die IT-Sicherheitsziele und -anforderungen zu erreichen. Die Dokumentation sollte daher konkrete Angaben über Verantwortlichkeiten und Zuständigkeiten sowie geplante Aktivitäten zur Kontrolle, Revision, Überwachung enthalten. Die Reihenfolge für die Umsetzung offener Aktivitäten ist festzuhalten. Außerdem sind die geplanten bzw. eingesetzten Ressourcen für die Umsetzung der einzelnen IT-Sicherheitsmaßnahmen zu dokumentieren.

Aufrechterhaltung der Sicherheit und Verbesserung

Da IT-Sicherheit ein kontinuierlicher Prozess ist, genügt es nicht, alle Sicherheitsmaßnahmen einmal umzusetzen. Der Sicherheitsprozess muss kontinuierlich verbessert werden, auf neue technische Entwicklungen reagieren und vor allem müssen Schwachstellen und aufgedeckte Sicherheitslücken berücksichtigt werden. Daher ist der Sicherheitsprozess regelmäßig zu überprüfen, zu aktualisieren und Änderungen zu dokumentieren. Wichtige Verfahren sind dabei die Einführung von regelmäßigen Berichten (siehe M 2.200 *Managementreporte und -bewertungen der IT-Sicherheit*) und Meldeprozesse.

Eine Zertifizierung des IT-Sicherheitsprozesses dokumentiert die Einhaltung einer definierten Vorgehensweise und kann als unabhängiges Review-Verfahren in den Sicherheitsprozess integriert werden.

Strukturierung des IT-Sicherheitskonzepts

Das IT-Sicherheitskonzept wird in der Praxis häufig herangezogen, um konkrete Sicherheitsmaßnahmen bezüglich ihrer Umsetzung oder ihrer Aktualität zu überprüfen. Daher sollte es so strukturiert sein, dass

- spezifische Bereiche schnell gefunden werden können, und
- es mit minimalem Aufwand aktualisiert werden kann (hierfür bietet sich die Nutzung eines Tools an).

Außerdem sollten die einzelnen Sicherheitsmaßnahmen ausreichend konkret beschrieben sein, damit im Vertretungsfall ein Dritter sicherheitsspezifische Aufgaben übernehmen kann.

Ein Sicherheitskonzept kann Informationen beinhalten, die nicht beliebig weitergegeben werden sollten. Dies können zum Beispiel Angaben über noch nicht beseitigte Schwachstellen oder Informationen zu Maßnahmen sein, die geeignet sind, die Maßnahmen zu umgehen oder zu überwinden. Die Vertraulichkeit dieser Informationen ist sicherzustellen, indem ausschließlich den Betroffenen die für sie relevanten Teile zugänglich gemacht werden. Eine entsprechende Gliederung des Sicherheitskonzeptes kann dies unterstützen.

Es ist wichtig, ein gemeinsames Verständnis für Informationssicherheit in einer Institution herzustellen. Dazu gehört auch die Verwendung einheitlicher und klarer Begriffe. Daher sollte frühzeitig ein Glossar mit den wichtigsten Begriffen rund um IT-Sicherheit erstellt werden. Dieses Glossar sollte bei der Erstellung aller sicherheitsrelevanten Dokumente herangezogen werden. Es kann im IT-Sicherheitkonzept oder auch einzeln veröffentlicht werden.

Ergänzende Kontrollfragen:

- Existiert ein IT-Sicherheitskonzept?
- Wann wurde das IT-Sicherheitskonzept zuletzt aktualisiert?
- Wo befindet sich das IT-Sicherheitskonzept?
- Wer darf darauf zugreifen?
- Ist jeder Mitarbeiter zumindest über die ihn unmittelbar betreffenden Teile des IT-Sicherheitskonzeptes informiert?

M 2.196 Umsetzung des IT-Sicherheitskonzepts nach einem Realisierungsplan

ist mit Version 2006 entfallen

M 2.196 Umsetzung des IT-Sicherheitskonzepts nach einem Realisierungsplan

Diese Maßnahme ist mit Version 2006 entfallen.

M 2.197 Integration der Mitarbeiter in den Sicherheitsprozess

Verantwortlich für Initiierung: IT-Sicherheitsmanagement-Team

Verantwortlich für Umsetzung: Vorgesetzte, IT-Sicherheitsmanagement-Team

IT-Sicherheit betrifft ohne Ausnahme alle Mitarbeiter. Jeder Einzelne muss durch verantwortungs- und qualitätsbewusstes Handeln Schäden vermeiden und zum Erfolg beitragen. Zur Integration der Mitarbeiter in den Sicherheitsprozess gehören folgende Aufgaben:

Motivation und Arbeitsbedingungen

Die Behörden- oder Unternehmensleitung muss ein positives Arbeitsklima schaffen und das Engagement der Mitarbeiter für die IT-Sicherheit fördern. Dazu gehören unter anderem folgende Aspekte:

- Es müssen angemessene und bedienungsfreundliche IT-Sicherheitsprodukte eingesetzt werden.
- IT-Sicherheitskonzepte und -Richtlinien müssen realistisch sein.
- IT-Sicherheit muss von der Leitungsebene praktiziert werden, um eine hohe Akzeptanz bei den Mitarbeitern zu gewährleisten.

Schulung und Sensibilisierung

Eine weitere Aufgabe, die den gesamten IT-Sicherheitsprozess begleiten muss, ist die Organisation und Durchführung von Schulungs- und Sensibilisierungsmaßnahmen. Das Unternehmen oder die Behörde sollte ein Schulungs- und Sensibilisierungskonzept erarbeiten. Eine ausführliche Behandlung dieses Themas ist im Baustein B 1.13 *IT-Sicherheitssensibilisierung und -schulung* genauer nachzulesen.

Beteiligung von Mitarbeitern

Mitarbeiter müssen über den Sinn von Sicherheitsmaßnahmen aufgeklärt werden. Weiterhin sollten Mitarbeiter frühzeitig bei der Planung von IT-Sicherheitsmaßnahmen oder der Gestaltung organisatorischer Regelungen beteiligt werden.

Personelle Sicherheitsmaßnahmen

Es gibt eine Vielzahl von personellen Sicherheitsaspekten, die bei allen Mitarbeitern, internen wie externen, berücksichtigt werden sollten. Dies beginnt bei der Personalauswahl und geht über die Einarbeitung neuer Mitarbeiter bis zu deren Weggang. Die erforderlichen Sicherheitsmaßnahmen sind in Baustein B 1.2 *Personal* beschrieben.

Ergänzende Kontrollfragen:

- Werden die Mitarbeiter bei der Einführung von IT-Sicherheitsrichtlinien und Sicherheitswerkzeugen beteiligt und vorher informiert?
- Gibt es Schulungs- und Sensibilisierungskonzepte?

M 2.198 Sensibilisierung der Mitarbeiter für IT-Sicherheit

Verantwortlich für Initiierung: IT-Sicherheitsmanagement-Team

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement-Team, Vorgesetzte

Viele Sicherheitsvorfälle werden nicht durch organisationsfremde Angreifer, sondern durch unsachgemäßes Verhalten eigener Mitarbeiter hervorgerufen. Daher sollte Wert darauf gelegt werden, dass alle Mitarbeiter die für ihren Arbeitsplatz erforderlichen IT-Sicherheitskenntnisse haben, Zwischenfälle frühzeitig als solche erkennen können und eigenverantwortlich sinnvolle Maßnahmen bei Sicherheitsproblemen ergreifen können. Eine der wichtigsten Aufgaben des IT-Sicherheitsmanagements besteht daher in der Durchführung von Veranstaltungen, um die Mitarbeiter für das Thema IT-Sicherheit zu sensibilisieren. Diese sollten unter anderem folgende Themen umfassen:

IT-Sicherheit in unserer Organisation

- die Aufgaben und Ziele der Organisation,
- wie die Aufgaben der Organisation durch den IT-Einsatz unterstützt werden,
- Gefährdungen und Risiken durch den IT-Einsatz,
- Werte für die Organisation,
- Erläuterung der Grundprinzipien der IT-Sicherheit: Vertraulichkeit, Integrität, Verfügbarkeit,
- die IT-Sicherheitsrichtlinien des Hauses,
- Ziel und Inhalt des IT-Sicherheitskonzeptes,
- Verpflichtung von IT-Benutzern, System- und Aufgabenverantwortlichen zur Umsetzung des IT-Sicherheitskonzeptes,
- Anpassung des IT-Sicherheitskonzeptes an neue Entwicklungen und Aufgaben.

Alle diese Themen sollen zum besseren Verständnis anhand von Beispielen untermauert werden.

Jeder Mitarbeiter sollte diese Inhalte kennen, sinnvollerweise findet die Sensibilisierung im Rahmen der Einarbeitung statt. Da die Sensibilisierung für IT-Sicherheit der wichtigste Garant für die Umsetzung (manchmal lästiger) IT-Sicherheitsmaßnahmen ist, empfiehlt es sich, solche Veranstaltungen für alle Mitarbeiter regelmäßig anzubieten.

Zur Umsetzung von IT-Sicherheit bedarf es nicht nur abstrakter Regularien, sondern auch eines praxisorientierten Sicherheitsbewusstseins. Wie sich an vielen konkreten Beispielen - wie den Schadensstatistiken von Elektronik-Versicherern - belegen lässt, resultieren IT-Schäden oft schlicht aus der Unkenntnis elementarer Sicherheitsmaßnahmen. Umgekehrt können Mitarbeiter oft bereits durch die Beachtung einfacher Vorsichtsmaßregeln dazu beitragen, dass Schäden vermieden werden.

Neben der regelmäßigen Sensibilisierung für grundsätzliche Aspekte der IT-Sicherheit müssen die Mitarbeiter auch für die IT-Sicherheitsmaßnahmen

sensibilisiert werden, die sie in ihrer täglichen Arbeit zu beachten haben. Dies sollte unter anderem die folgenden Themenschwerpunkte umfassen:

Themenschwerpunkte

- Zutritts- und Zugangsschutz: Verschließen von Büro- und Serverräumen, Sperren der Arbeitsstation auch bei kurzfristiger Abwesenheit (z. B. durch Bildschirmschoner mit Passwortschutz), Clean Desk Policy, Beaufsichtigen von Externen, etc...
- Zugriffsschutz: Umgang mit Passwörtern und anderen Zugriffsmitteln (nicht weitergeben, sicher aufbewahren, etc.), Auswahlregeln für sichere Passwörter, etc...
- Technische Sicherheit: keine Abdeckung von Lüftungsöffnungen durch Akten, Kleider oder ähnliches, Vermeiden gefährlicher "Fallbrücken" durch unsachgemäße Aufstellung von Geräten oder über den Fußboden verlegte Kabel, keine unsachgemäßen Reparaturversuche an der Elektroinstallation, etc...
- Sicherheitsmaßnahmen bei Nutzung von E-Mail und Internet: Sensibilisierung für die fehlende Vertraulichkeit unverschlüsselter E-Mails (wenn sie vorhanden sind, sollte die Nutzung von Verschlüsselungs- und Signaturkomponenten geschult werden), sichere Konfiguration des Internet-Browsers (z. B. Deaktivierung von ActiveX und Java-Script), kein sorgloses Herunterladen ausführbarer Programme wegen möglicher Schadensfunktionen, etc...
- Schad-Software: Erläuterung der Begriffe Viren, Trojanische Pferde, Würmer usw., Surfen im Internet nur bei aktiviertem Virenschutz, Virenprüfung vor dem Öffnen von E-Mail-Anhängen, etc...
- Umgang mit Sicherheitsvorfällen: Woran sind sie zu erkennen, was sollen Benutzer machen, an wen sollen sie sie melden, etc...
- Rechtliche Aspekte: Grundlagen des Datenschutzes, keine Installation unlizenzierter Software, Urheberrecht (z. B. bezüglich der Nutzung von Material aus dem Internet), etc...

Die hier angegebenen Themen stellen lediglich eine Auswahl dar. Ein Aktionsprogramm zur "IT-Sicherheit" sollte stets den individuellen Gegebenheiten der Behörde oder des Unternehmens angepasst sein.

Möglichkeiten zur Sensibilisierung

Um wirkungsvoll das Bewusstsein für IT-Sicherheit zu schärfen und eingeschliffene Verhaltensweisen dauerhaft zu ändern, ist ein fortwährender Lernprozess erforderlich. Sinnvolle kontinuierliche Sensibilisierungsmaßnahmen müssen dabei auf das Arbeitsumfeld und Zielpublikum angepasst sein. Um die Lerneffekte zu verstärken, ist es empfehlenswert, regelmäßig Aspekte zur IT-Sicherheit in den Köpfen der Mitarbeiter zu verankern, z. B. durch E-Mail-aktionen, Hinweise im Intranet und Integration von Sicherheitsthemen in internen Veranstaltungen. Andere wirksame Möglichkeiten zur Sensibilisierung für IT-Sicherheit sind auch

- die regelmäßige Information über aktuelle Bedrohungen und Schwachstellen, beispielsweise

  - des IT-Sicherheitsbeauftragten durch entsprechende Informationsdienste oder
  - der Mitarbeiter durch den IT-Sicherheitsbeauftragten.
- der Aufbau eines Kommunikationsforums, um Mitarbeiter zu ermutigen, aktuelle Sicherheitsthemen zu diskutieren, Fragen zu stellen und auch Sicherheitsprobleme vorzubringen.
- die regelmäßige Befragung von Mitarbeitern zu IT-Sicherheitsaspekten, wodurch nicht nur der vorhandene Wissenstand ermittelt, sondern dieser auch verbessert werden kann. Außerdem werden dadurch IT-Sicherheitsprobleme besser wahrgenommen und IT-Sicherheitsmaßnahmen besser umgesetzt (Beispiel: "Wie oft sichern Sie Ihre Daten? ").
- die Durchführung von Simulationsspielen, z. B. über die Auswirkungen von Schwachstellen auf die konkrete Arbeitsumgebung.
- Mitarbeiter-Workshops, um Schwachstellen aufzudecken und passende Sicherheitsmaßnahmen zu finden.
- Einrichtung eines Sicherheitspools im Intranet, wo über aktuelle IT-Sicherheitsvorfälle und Lösungsansätze berichtet wird. Hier sollte auch darüber informiert werden, wie sie zuhause ihre IT schützen können. Dies motiviert zusätzlich und reduziert die Sicherheitsprobleme, die über private IT-Nutzung entstehen können.

Positive Einstellung zu IT-Sicherheit

Programme zur Sensibilisierung für IT-Sicherheitsaspekte haben zunächst den generellen Effekt, dass die Beteiligten über die IT-Sicherheitsbelange aufgeklärt und dafür aufgeschlossen werden. Damit auch ein Verhaltenswandel eintritt, muss IT-Sicherheit auch in das allgemeine Wertebild des Unternehmens bzw. der Behörde eingebunden werden. Das bezüglich IT-Sicherheit erwünschte Verhalten muss also genauso bewertet werden wie das zu anderen Zielvorgaben. Seitens der Vorgesetzten muss Interesse daran gezeigt und auch positive oder negative Rückmeldungen (Lob bzw. Tadel) gegeben werden. Die Vorgesetzten sollten außerdem als gutes Vorbild agieren, ebenso wie Administratoren und Support-Mitarbeiter wichtige Multiplikatoren sind. Wenn diese Gruppen die Sicherheitsrichtlinien nicht einhalten oder nicht als wichtig erachten, wird es der Rest der Mitarbeiter auch nicht tun.

Die einzelnen Themen sollten durchgängig mit Beispielen unterlegt werden, die dem Tagesgeschäft der Teilnehmer entnommen oder daran angelehnt sind. Dadurch werden die Inhalte für die Teilnehmer einprägsamer vermittelt und leichter umsetzbar.

Beispiel:

In einem Unternehmen wird zur Verbesserung der E-Mail-Sicherheit ein Produkt zur Verschlüsselung und Signatur von E-Mails eingeführt. Damit diese Mechanismen sinnvoll und kontinuierlich genutzt werden, sollten

- die Mitarbeiter zunächst zu Wirkung und Funktion geschult werden, **Aufklärung**
- die Vorgesetzten auch intern verschlüsselte und signierte E-Mails senden, **Vorbildfunktion**

- Reiseabrechnungen per E-Mail abgegeben werden können, aber nur noch elektronisch signiert akzeptiert werden und **Anreiz schaffen**
- Mitarbeiter seitens der Vorgesetzten angesprochen werden, wenn diese trotzdem noch unverschlüsselte E-Mails verschicken. **Aufmerksamkeit zeigen**

Der offene Umgang mit IT-Sicherheitsfragen muss in der gesamten Institution gelebt werden. Eine vertrauensvolle und offene Kommunikationskultur ist wichtig, damit Sicherheitsvorfälle auch umgehend weitergemeldet und offen angegangen werden. Dazu gehört auch, dass die Mitarbeiter über organisationsinterne IT-Sicherheitsvorkommnisse informiert werden und was diese für ihren Arbeitsplatz bedeuten. Dies sollte zeitnah erfolgen und nicht erst, wenn diese öffentlich bekannt geworden sind.

Materialien zur IT-Sicherheit

Zur Sensibilisierung können auch attraktive Werbematerialen bzw. -aktionen beitragen. Hierzu gehören zielgerichtete Mitteilungen und Slogans zur IT-Sicherheit. Damit sie lange im Blickfeld der Mitarbeiter verbleiben, können kurze IT-Sicherheitshinweise beispielsweise auf Kalendern, Kaffeetassen, Merkzetteln, Frisbees, Mousepads oder Screensavern untergebracht werden.

Über Plakate können Botschaften ebenfalls effektiv vermittelt werden. Diese sollten an auffälligen Stellen aufgehängt werden, z. B. in der Kantine, im Aufzug und in Besprechungsräumen, und regelmäßig gewechselt werden. Poster zu IT-Sicherheitsthemen gibt es beispielsweise von diversen Herstellern von Sicherheitsprodukten und Werbemittelherstellern.

Merksprüche zur IT-Sicherheit sollten einfach und einprägsam sein und können (je nach Organisationskultur) auch lustig sein, beispielsweise **Werbung für IT-Sicherheit**

- Die Sicherung ist null und nichtig, nimmt man das Passwort nicht so wichtig!
- Viel Ärger hat sich der erspart, der heikle Dinge gut verwahrt!
- Verzichte auf den Mailversand, ist der Inhalt sehr pikant!
- Fremder Zugriff wird erschwert, bleibt der Zugang stets verwehrt!

Bei allen Aktivitäten zur Sensibilisierung der Mitarbeiter für IT-Sicherheit dürfen auch die Personen nicht vergessen werden, die keinen direkten IT-Zugang haben, wie Reinigungskräfte oder Hausarbeiter. Auch bei diesen kann eine angemessene Aufklärung über Sicherheitsvorgaben helfen, Schäden zu vermeiden.

Ergänzende Kontrollfragen:

- Wie wird sichergestellt, dass eine kontinuierliche Sensibilisierung zu IT-Sicherheit erfolgt?
- Stehen den IT-Sicherheitsverantwortlichen und allen interessierten Mitarbeitern Fachzeitschriften bzw. andere aktuelle Informationen zur IT-Sicherheit zur Verfügung?

- Wird in geeigneter Form auf organisationsinterne oder öffentlich bekannt gewordene IT-Sicherheitsvorkommnisse hingewiesen? Werden, wo möglich,Wege zu deren Vermeidung aufgezeigt?
- Existieren allgemein akzeptierte und genutzte Foren zur organisations-internen Kommunikation über Belange der IT-Sicherheit?

M 2.199 Aufrechterhaltung der IT-Sicherheit

Verantwortlich für Initiierung: IT-Sicherheitsmanagement-Team

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement-Team

Im IT-Sicherheitsprozess geht es nicht nur darum, das angestrebte IT-Sicherheitsniveau zu erreichen, sondern dieses auch dauerhaft zu gewährleisten. Um das bestehende IT-Sicherheitsniveau aufrechtzuerhalten und fortlaufend zu verbessern, sollten alle IT-Sicherheitsmaßnahmen regelmäßig überprüft werden.

Sowohl die korrekte Umsetzung als auch die Umsetzbarkeit eines IT-Sicherheitskonzepts müssen regelmäßig überprüft werden. Dabei ist zu unterscheiden zwischen der Prüfung, ob bestimmte Maßnahmen geeignet und effizient sind, um die gesteckten Sicherheitsziele zu erreichen (Vollständigkeits- bzw. Aktualisierungsprüfung), und der Kontrolle, inwieweit Sicherheitsmaßnahmen in den einzelnen Bereichen umgesetzt wurden (IT-Sicherheitsrevision).

Die im IT-Sicherheitskonzept geplanten IT-Sicherheitsmaßnahmen müssen gemäß des Realisierungsplans umgesetzt werden. Der Umsetzungsstatus muss dokumentiert werden. Zieltermine und Ressourceneinsatz müssen überwacht und gesteuert werden. Die Leitungsebene ist dazu regelmäßig zu informieren.

Regelmäßige und anlassbezogene Prüfungen

Diese Überprüfungen sollten zu festgelegten Zeitpunkten (mindestens jährlich) durchgeführt werden und können bei gegebenem Anlass auch zwischenzeitlich erfolgen. Insbesondere Erkenntnisse aus sicherheitsrelevanten Zwischenfällen, Veränderungen im technischen oder technisch-organisatorischen Umfeld sowie Änderungen von Sicherheitsanforderungen bzw. Bedrohungen erfordern eine Anpassung der bestehenden IT-Sicherheitsmaßnahmen. Die in den einzelnen Überprüfungen ermittelten Ergebnisse sollten dokumentiert werden, und es muss festgelegt sein, wie mit den Überprüfungsergebnissen zu verfahren ist. Hervorzuheben ist hierbei, dass Überprüfungen nur dann wirksam die IT-Sicherheit aufrechterhalten können, wenn aufgrund der Überprüfungsergebnisse auch die erforderlichen Korrekturmaßnahmen ergriffen werden.

Koordinierte Vorgehensweise

Es sollte in der Behörde bzw. im Unternehmen festgelegt werden, wie die Tätigkeiten im Zusammenhang mit diesen Überprüfungen zu koordinieren sind. Dazu ist zu regeln, welche IT-Sicherheitsmaßnahmen wann und von wem zu überprüfen sind. Somit wird zum einen Doppelarbeit vermieden und zum anderen verhindert, dass bestimmte Bereiche innerhalb einer Organisation unberücksichtigt bleiben.

Die vorhandenen IT-Sicherheitsmaßnahmen sollten mindestens einmal im Jahr überprüft werden. Darüber hinaus sind sie immer dann zu prüfen, wenn

- neue IT-Komponenten oder Prozesse implementiert werden,
- größere Änderungen der Infrastruktur vorgenommen werden(z. B. Umzug),
- größere organisatorischen Änderungen anstehen (z. B. Outsourcing),
- die Gefährdungslage sich wesentlich ändert,
- wenn gravierende Schwachstellen oder Schadensfälle bekannt werden.

Einhaltung des IT-Sicherheitskonzeptes (IT-Sicherheitsrevision)

Hierbei muss geprüft werden, ob IT-Sicherheitsmaßnahmen tatsächlich so umgesetzt sind und eingehalten werden, wie sie im IT-Sicherheitskonzept vorgegeben wurden. Hierbei ist auch zu untersuchen, ob technische Maßnahmen korrekt implementiert und konfiguriert wurden und ob alle vorgesehenen Detektionsmaßnahmen (z. B. Auswertung von Protokolldateien) tatsächlich durchgeführt werden.

Dabei kann sich zeigen, dass beispielsweise IT-Sicherheitsmaßnahmen nicht umgesetzt worden sind oder dass sie in der Praxis nicht greifen. In beiden Fällen sollten die Ursachen für die Abweichungen ermittelt werden. Als mögliche Korrekturmaßnahmen kommen - je nach Ursache - in Frage:

- organisatorische Maßnahmen sind anzupassen,
- personelle Maßnahmen, z. B. Schulungs- und Sensibilisierungsmaßnahmen, sind zu ergreifen oder disziplinarische Maßnahmen einzuleiten,
- infrastrukturelle Maßnahmen, z. B. bauliche Veränderungen, sind zu initiieren,
- technische Maßnahmen, z. B. Änderungen an Hardware und Software oder Kommunikationsverbindungen und Netzen, sind vorzunehmen,
- Entscheidungen des verantwortlichen Vorgesetzten (bis hin zur Leitungsebene) sind einzuholen.

Auf jeden Fall sollte für jede Abweichung eine Korrekturmaßnahme vorgeschlagen werden. Außerdem sollte festgelegt werden, wer für die Umsetzung der Korrekturmaßnahme zuständig und bis wann die Umsetzung durchzuführen ist.

Kontinuierliche Verbesserung des IT-Sicherheitskonzeptes (Vollständigkeits- bzw. Aktualisierungsprüfung)

Eignung und Wirksamkeit von IT-Sicherheitsmaßnahmen

Das IT-Sicherheitskonzept muss regelmäßig aktualisiert, verbessert und an neue Rahmenbedingungen angepasst werden. Es muss regelmäßig geprüft werden, ob die IT-Sicherheitsmaßnahmen geeignet sind, um die IT-Sicherheitsziele zu erreichen. Dazu gehört auch, technische und regulatorische Entwicklungen zu verfolgen. Hierfür sollten externe Wissensquellen, wie Standards oder Fachpublikationen, verfolgt werden.

Außerdem sollte überlegt werden, Kontakte mit Gremien und Interessengruppen aufzunehmen, die sich mit Sicherheitsaspekten beschäftigen, die für die eigene Institution von Interesse sind. Dies unterstützt das IT-Sicherheitsmanagement-Team dabei, das Wissen über sicherheitsrelevante Methoden und Lösungen zu erweitern und aktuell zu halten. Außerdem werden dabei auch wertvolle Kontakte mit anderen IT-Sicherheitsbeauftragten geknüpft, um Lösungen anderer Institutionen kennen zu lernen und Praxiserfahrungen auszutauschen. Es werden dadurch auch Wege geebnet, um frühzeitig Warnungen über aufkommende Sicherheitsprobleme zu erhalten. Das IT-Sicherheitsmanagement-Team sollte einen Überblick besitzen, bei welchen Gremien und Interessengruppen aktiv mitgearbeitet werden sollte und bei welchen die Ergebnisse regelmäßig beobachtet und ausgewertet werden sollten.

Außerdem muss regelmäßig überprüft werden, ob die eingesetzten IT-Sicherheitsmaßnahmen effizient sind oder ob die IT-Sicherheitsziele mit anderen Maßnahmen ressourcenschonender erreicht werden könnten.

Effizienz der IT-Sicherheitsmaßnahmen

Durchführung der Prüfungen

Entsprechend dem Prüfungszweck sind Umfang und Tiefe der Überprüfung festzulegen. Als Grundlage für die Überprüfung dient das IT-Sicherheitskonzept und die vorhandene Dokumentation des IT-Sicherheitsprozesses. Die Überprüfung, die von internen oder externen Personen durchgeführt werden kann, ist sorgfältig zu planen. Während der Durchführung sind alle relevanten Feststellungen von den Prüfenden zu dokumentieren und auszuwerten.

Alle Prüfungen müssen von geeigneten Personen durchgeführt werden. Vollständigkeitsprüfungen sollten nicht durch die Ersteller der Konzepte durchgeführt werden. Prüfer bzw. Auditoren müssen die notwendigen Qualifikationen mitbringen. Außerdem sollten Prüfer möglichst unabhängig sein.

Die Ergebnisse sind in einem Bericht festzuhalten. Dieser sollte auch die vorgeschlagenen Korrekturmaßnahmen aus fachlicher Sicht enthalten. Der Bericht sollte dem Leiter des überprüften Bereiches sowie dem IT-Sicherheitsmanagement-Team zur Kenntnis gegeben werden. Bei schwerwiegenden Problemen sollte die Leitungsebene mit einbezogen werden, damit auch weitreichende Entscheidungen zeitnah getroffen werden können.

Bei Prüfungen werden oft spezielle Werkzeuge eingesetzt. Ebenso wie bei den Berichten muss sichergestellt sein, dass nur dazu autorisierte Personen darauf Zugriff haben. Diagnose- und Prüftools sowie die Prüfergebnisse müssen daher besonders geschützt werden.

Korrekturmaßnahmen

Erkannte Fehler und Schwachstellen müssen abgestellt werden. Der identifizierte Optimierungsbedarf bei Effizienz und Effektivität von IT-Sicherheitsmaßnahmen muss umgesetzt werden.

Daher sind aufgrund der Überprüfungsergebnisse Entscheidungen über das weitere Vorgehen zu treffen. Insbesondere sind alle erforderlichen Korrekturmaßnahmen zu beschließen und in Form eines Umsetzungsplans festzuhalten. Auch hierfür sind die Verantwortlichen für die Umsetzung der Korrekturmaßnahmen zu benennen und mit den notwendigen Ressourcen auszustatten.

Ergänzende Kontrollfragen:

- Wird eine regelmäßige IT-Sicherheitsrevision durchgeführt?
- Werden regelmäßig Vollständigkeits- und Aktualisierungsprüfungen durchgeführt?
- Werden IT-Sicherheitsrevisionen gegebenenfalls auch von einer Revisionsabteilung oder mit externer Unterstützung durchgeführt?

M 2.200 Managementreporte und -bewertungen der IT-Sicherheit

Verantwortlich für Initiierung: IT-Sicherheitsmanagement-Team, IT-Sicherheitsbeauftragter,

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement-Team, Behörden-/Unternehmensleitung

Zu den Aufgaben des IT-Sicherheitsbeauftragten gehört es, die Behörden- oder Unternehmensleitung bei der Wahrnehmung ihrer Gesamtverantwortung für die IT-Sicherheit zu unterstützen. Eine wichtige Grundlage für die zu treffenden Entscheidungen sind übersichtliche und aussagekräftige Informationen zur aktuellen Lage der IT-Sicherheit in der Institution.

Um den IT-Sicherheitsprozess zu steuern und aufrecht zu erhalten, muss mindestens einmal im Jahr eine Managementbewertung der IT-Sicherheit durchgeführt werden. Ziel der Managementbewertung der IT-Sicherheit ist, das weitere Vorgehen im IT-Sicherheitsprozess mit der Leitungsebene abzustimmen. Die Managementreporte dienen dabei als Entscheidungsgrundlage für die Managementbewertung.

In der Managementbewertung müssen alle erforderlichen Änderungen am Sicherheitsprozess aufgezeigt und festgelegt werden, beispielsweise in den Sicherheitszielen oder der Sicherheitsleitlinie. Alle Ergebnisse der Managementbewertung müssen dokumentiert und Aufzeichnungen gepflegt werden.

Managementreporte

Grundsätzlich ist zwischen zwei verschiedenen Formen von Managementreporten zu unterscheiden:

Regelmäßige Managementreporte

Durch regelmäßige Managementreporte wird sichergestellt, dass die Leitungsebene die Informationen erhält, die sie zur Managementbewertung benötigt.

Ein Managementreport IT-Sicherheit sollte aufzeigen:

- inwieweit die Vorgaben des IT-Sicherheitskonzepts im Unternehmen oder in der Behörde bereits abgedeckt sind,
- an welchen Stellen noch Lücken - und damit Restrisiken - bestehen,
- welche IT-Sicherheitsvorfälle aufgetreten sind, welche Schäden entstanden sind und welche Schäden verhindert werden konnten,
- welche Ergebnisse interne Überprüfungen und Audits erbracht haben (siehe M 2.199 *Aufrechterhaltung der IT-Sicherheit*),
- inwieweit das IT-Sicherheitsniveau den Sicherheitsanforderungen und der Bedrohungslage der Institution genügt,
- ob sich Rahmenbedingungen geändert haben, so dass weitere Maßnahmen erforderlich sind,
- ob die Aktivitäten im Rahmen der IT-Sicherheit Erfolg hatten,
- ob sich die IT-Sicherheitsmaßnahmen zur Erreichung der IT-Sicherheitsziele als geeignet erwiesen haben oder ob Maßnahmen geändert oder ergänzt werden müssen,
- welche Rückmeldungen es von Kunden, Geschäftspartnern, Mitarbeitern oder der Öffentlichkeit zu IT-Sicherheitsaspekten gab,

Verbesserungsvorschläge

- welche Ressourcen für IT-Sicherheit aufgewendet wurden,
- ob und wie die Entscheidungen der letzten Managementbewertung umgesetzt wurden und ob die Aktivitäten im Rahmen der IT-Sicherheit Erfolg hatten.

Nachverfolgung der letzten Management-bewertung

Daneben sollte auch ein Ausblick auf die zu erwartende Weiterentwicklung der organisationsweiten IT-Sicherheit gegeben werden und es sollte dargestellt werden, ob es technische Entwicklungen oder Verfahrensweisen gibt, die zur Verbesserung des IT-Sicherheitsprozesses beitragen können.

Anlassbezogene Managementreporte

Neben den regelmäßigen Managementreporten kann es auch notwendig sein, bei überraschend auftretenden IT-Sicherheitsproblemen oder aufgrund von Risiken, die aus neuen technischen Entwicklungen resultieren, anlassbezogene Managementreporte zu erstellen. Dies ist vor allem dann der Fall, wenn sich herausstellt, dass diese Probleme nicht auf der Arbeitsebene beseitigt werden können, weil z. B. materielle Ressourcen außerhalb des bewilligten Rahmens benötigt werden oder weitergehende personelle Regelungen getroffen werden müssen.

Immer wieder erregen IT-Sicherheitsvorfälle wie globale Computer-Virenattacken die Aufmerksamkeit der Massenmedien. Es hat sich als sinnvoll erwiesen, auch in diesen Fällen Managementreporte zu erstellen, um aufzuzeigen, inwieweit die eigene Organisation von diesen Sicherheitsvorfällen betroffen wurde. Auch wenn sich die IT-Sicherheitslage ändert (z. B. neue Bedrohungen, neue Technologien, neue Gesetze) kann ein anlassbezogener Managementreport sinnvoll sein.

kurz und verständlich

Bei der Abfassung der Managementreporte sollte berücksichtigt werden, dass sich der Leserkreis in der Regel nicht aus technischen Experten zusammensetzt. Entsprechend sollte sich der Text durch größtmögliche Verständlichkeit und Knappheit auszeichnen. Es sollten also gezielt die wesentlichen Punkte, insbesondere also bestehende Schwachstellen, aber auch erreichte Erfolge, herausgearbeitet werden.

Entscheidungsvorlage

Zum Abschluss des Managementreports, vor allem bei anlassbezogenen Berichten, sollten immer klar priorisierte und mit realistischen Abschätzungen des zu erwartenden Umsetzungsaufwands versehene Maßnahmenvorschläge stehen. Hierdurch wird sichergestellt, dass eine notwendige Entscheidung der Leitungsebene ohne unnötige Verzögerungen herbeigeführt werden kann.

Zusammenarbeit mit der Leitungsebene

Wenn irgend möglich, sollte der Managementreport zur IT-Sicherheit der Leitungsebene nicht nur schriftlich unterbreitet, sondern auch durch ein Mitglied des IT-Sicherheitsmanagement-Teams präsentiert werden. Eine solche persönliche Übergabe eröffnet zum einen die Möglichkeit, auf wesentliche Schwerpunkte, insbesondere auf bestehende oder drohende Sicherheitsmängel mit besonderem Nachdruck hinzuweisen. Zum anderen steht der anwesende IT-Sicherheitsverantwortliche auch direkt für Nachfragen oder weitergehende Erläuterungen zur Verfügung, was wiederum erfahrungsgemäß zu einer Beschleunigung des Entscheidungsvorgangs führt. Nicht zuletzt bietet ein solcher persönlicher Kontakt die Möglichkeit, einen "kleinen Dienstweg" zu

etablieren, dessen Existenz sich in dringenden Notfällen als sehr hilfreich erweisen kann. Alternativ bzw. ergänzend zur persönlichen Präsentation des Managementreports sollte überlegt werden, ob ein Mitglied der Leitungsebene des Unternehmens oder der Behörde mit entsprechendem fachlichen Hintergrund und Interesse vorab als Ansprechpartner zur Verfügung steht. Auch so können Leitungsentscheidungen besser vorbereitet und Probleme schon im Voraus entschärft werden.

Managementbewertung

In der Managementbewertung werden auf Grundlage des Managementreports Entscheidungen hinsichtlich der weiteren Vorgehensweise in Bezug auf den IT-Sicherheitsprozess getroffen. Dabei wird die Behörden- oder Unternehmensleitung gegebenenfalls vom IT-Sicherheitsbeauftragten unterstützt.

Die Managementbewertung sollte Entscheidungen zu folgenden Punkten vorbereiten und dokumentieren:

- Erforderliche Aktionen zur Verbesserungen der Effektivität des IT-Sicherheitskonzepts sowie die dafür benötigten Ressourcen
- Höhe des Schutzbedarfs sowie die Behandlung des Restrisikos in der ergänzenden Risikoanalyse
- Veränderungen von sicherheitsrelevanten Prozessen, um internen oder externen Ereignissen zu begegnen, die Einfluss auf das IT-Sicherheitskonzept haben könnten, z. B. in Hinsicht auf Änderungen bei
  - Geschäftszielen
  - Sicherheitsanforderungen
  - Geschäftsprozessen
  - externen Rahmenbedingungen (wie dem gesetzlichen Umfeld oder vertraglichen Verpflichtungen)

Dokumentation

Zur kontinuierlichen Verfolgung des IT-Sicherheitsprozesses sollten sämtliche Managementreporte und Managementbewertungen zur IT-Sicherheit zusammen mit Vermerken über die getroffenen Entscheidungen in geordneter Weise archiviert werden. Diese Dokumentation sollte den Verantwortlichen bei Bedarf kurzfristig zugänglich sein (siehe M 2.201 *Dokumentation des IT-Sicherheitsprozesses*).

Vertraulichkeit

Da die Managementreporte zur IT-Sicherheit im Allgemeinen sensitive Informationen über bestehende Sicherheitslücken und Restrisiken enthalten, ist deren Vertraulichkeit zu schützen. Es müssen angemessene Schutzvorkehrungen getroffen werden, damit keine unbefugten Personen Kenntnis über den Inhalt der Managementreporte erlangen.

Ergänzende Kontrollfragen:

- Beinhalten die Managementreporte die wesentlichen relevanten Informationen des IT-Sicherheitsprozesses?
- Werden die Managementreporte aussagekräftig bewertet und unterschrieben?
- Werden die Managementreporte und Managementbewertungen archiviert?

M 2.201 Dokumentation des IT-Sicherheitsprozesses

Verantwortlich für Initiierung: IT-Sicherheitsmanagement-Team

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement-Team

Ein angemessenes Sicherheitsniveau lässt sich nur dann erreichen, wenn eine verständliche, angemessene, aktuelle und konsistente Dokumentation des IT-Sicherheitsprozesses vorhanden ist und eine geordnete Dokumentenverwaltung besteht.

Der Ablauf des IT-Sicherheitsprozesses sowie wichtige Entscheidungen und die Arbeitsergebnisse in den einzelnen Phasen sollten dokumentiert werden. Eine solche Dokumentation ist eine wesentliche Grundlage für die Aufrechterhaltung der IT-Sicherheit und damit entscheidende Voraussetzung für die effiziente Weiterentwicklung des Prozesses. Sie hilft dabei, die Ursachen von Störungen und fehlgeleiteten Abläufen zu finden und zu beseitigen. Wichtig ist dabei, dass nicht nur die jeweils aktuelle Version der betreffenden Unterlagen griffbereit gehalten wird, sondern auch eine zentrale Archivierung der Vorgängerversionen vorgenommen wird. Erst hierdurch ist eine kontinuierliche Rückverfolgung der Entwicklung im Bereich IT-Sicherheit, bei der die getroffenen Entscheidungen nachvollziehbar werden, gewährleistet.

Arten von Dokumentationen

Neben Dokumenten zum IT-Sicherheitsmanagement und dem IT-Sicherheitsprozess gibt es weitere für das IT-Sicherheitsmanagement relevante Dokumente. Abhängig vom Gegenstand und vom Verwendungszweck sind folgende Arten von Dokumentationen zu betrachten:

Berichte an die Leitungsebene

Damit die oberste Leitungsebene einer Behörde oder eines Unternehmens die richtigen Entscheidungen treffen kann, um IT-Sicherheit auf einem angemessenen Niveau zu gewährleisten, benötigt sie die dafür notwendigen Informationen. Hierfür sollte der IT-Sicherheitsbeauftragte bzw. das IT-Sicherheitsmanagement-Team regelmäßig sowie anlassbezogen Management-Reporte zum Status der IT-Sicherheit (siehe auch M 2.200 *Managementreporte und -bewertungen der IT-Sicherheit*) erstellen.

Dokumente zum IT-Sicherheitsprozess

Folgende Arten von Dokumentationen zum IT-Sicherheitsprozess sollten erstellt werden:

IT-Sicherheitsziele und die IT-Sicherheitsstrategie

- Die oberste Leitungsebene muss die IT-Sicherheitsleitlinie der Behörde bzw. des Unternehmens festlegen und veröffentlichen. Diese enthält unter anderem die IT-Sicherheitsziele und die IT-Sicherheitsstrategie.

IT-Sicherheitskonzept

- Im IT-Sicherheitskonzept werden die erforderlichen IT-Sicherheitsmaßnahmen beschrieben und deren Umsetzung festgelegt.

Sicherheitsrichtlinien

- Auf der Sicherheitsleitlinie aufbauend gibt es bereichs- und systemspezifische Sicherheitsrichtlinien und Regelungen für den ordnungsgemäßen und sicheren IT-Einsatz.

- Die wesentlichen Arbeiten des IT-Sicherheitsmanagement-Teams sollten ebenfalls dokumentiert sein, dazu gehören z. B. Sitzungsprotokolle und Beschlüsse.
- Ergebnisse von Audits und Überprüfungen (z. B. Prüflisten und Befragungsprotokolle).

Dokumentation von Arbeitsabläufen

Arbeitsabläufe, organisatorische Vorgaben und technische IT-Sicherheitsmaßnahmen müssen so dokumentiert werden, dass IT-Sicherheitsvorfälle durch Unkenntnis oder Fehlhandlungen vermieden werden.

Es muss bei Störungen oder IT-Sicherheitsvorfällen möglich sein, den gewünschten Soll-Zustand der IT wiederherzustellen. Technische Einzelheiten und Arbeitsabläufe sind daher so zu dokumentieren, dass dies in angemessener Zeit möglich ist.

Dokumentation von Sicherheitsvorfällen

Sicherheitsrelevante Vorfälle müssen so aufbereitet werden, dass alle damit verbundenen Vorgänge und Entscheidungen nachvollziehbar sind. Ebenso soll es die Dokumentation ermöglichen, Verbesserungen an den Notfallstrategien vorzunehmen und bekannte Fehler zu vermeiden. Zur Bearbeitung von Sicherheitsvorfällen sind außerdem technische Unterlagen, wie Protokolle oder für den Vorfall besonders relevante System-Meldungen, zu speichern und zu archivieren. Die Regelungen des Datenschutzes müssen eingehalten werden.

Technische Dokumentation

Zu dieser Art von sicherheitsrelevanten Dokumentationen gehören:

- Installations- und Konfigurationsanleitungen,
- Anleitungen für den Wiederanlauf nach einem Sicherheitsvorfall,
- Dokumentation von Test- und Freigabeverfahren und
- Anweisungen für das Verhalten bei Störungen und IT-Sicherheitsvorfällen.

Anleitungen für IT-Benutzer

IT-Sicherheitsmaßnahmen müssen für die IT-Benutzer verständlich dokumentiert werden. Den Benutzern müssen also

- die geltenden Sicherheitsrichtlinien,
- übersichtliches Merkblätter für die sichere Nutzung von IT-Systemen und Anwendungen sowie zum Verhalten bei Sicherheitsvorfällen,
- Handbücher und Anleitungen für die eingesetzten IT-Systeme und Anwendungen

zur Verfügung stehen.

Ausnahmeregelungen

Es kann in seltenen Fällen vorkommen, dass ein Verstoß gegen eine Sicherheitsrichtlinie sinnvoll und notwendig ist. Ein solcher Verstoß muss aber auf jeden Fall durch eine autorisierte Stelle genehmigt werden. Ausnahmegenehmigungen dürfen nur nach gründlicher Prüfung und in den seltensten Fällen erteilt werden. Anschließend muss eine schriftliche Begründung verfasst werden, die vom Verantwortlichen zu unterzeichnen ist.

Informationsfluss und Meldewege

Wichtig für die Aufrechterhaltung des IT-Sicherheitsprozesses ist die Beschreibung und zeitnahe Aktualisierung der Meldewege und der Vorgehensweise für den Informationsfluss.

Dokumentationswesen

Formale Anforderungen an Dokumentationen und Berichte

Es ist Aufgabe des IT-Sicherheitsbeauftragten bzw. des IT-Sicherheitsmanagement-Teams, stets aktuelle und aussagekräftige Dokumentationen zur IT-Sicherheit vorzuhalten. Für alle Dokumentationen im Rahmen des IT-Sicherheitsprozesses sollte es daher eine geregelte Vorgehensweise geben. Dazu gehören z. B. folgende Punkte:

- Dokumentationen müssen verständlich sein. Das bedeutet auch, dass sie zielgruppengerecht gestaltet werden müssen. Berichte an die Leitungsebene haben andere Anforderungen als technische Dokumentationen für Administratoren.

  Lesbarkeit

- Dokumentationen müssen aktuell und ihre Pflege muss festgelegt sein. Sie müssen so bezeichnet und abgelegt werden, dass sie im Bedarfsfall auch schnell gefunden werden können. Es müssen Angaben zu Erstellungsdatum, Version, Quellen und Autoren vorhanden sein. Veraltete Unterlagen müssen sofort aus dem Umlauf genommen und archiviert werden.

  Aktuell und auffindbar

- Es sollte ein definiertes Verfahren existieren, um Änderungsvorschläge (inklusive der Erstellung neuer Dokumente) einzubringen, zu beurteilen und gegebenenfalls zu berücksichtigen.
- Neben der schnellen Informationsweitergabe an Berechtigte ist andererseits die Vertraulichkeit von organisationsinternen Details sicherzustellen. Vertrauliche Inhalte müssen als solche klassifiziert werden und die Dokumente sicher verwahrt und bearbeitet werden (siehe auch M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*).

Bei der Pflege der Vielzahl sicherheitsrelevanter Dokumente kann ein Dokumentenmanagement hilfreich sein (siehe auch M 2.259 *Einführung eines übergeordneten Dokumentenmanagements*).

Dokumentationen müssen nicht immer in Papierform vorliegen. Das Dokumentationsmedium kann je nach Bedarf gewählt werden. Zur Dokumentation können Übersichtsdiagramme (z. B. Netzplan), kurze Sitzungsprotokolle (z. B. jährliche Sitzung der Geschäftsführung zur Diskussion der IT-Sicherheitsstrategie), handschriftliche Notizen oder Software-Tools (z. B. zur Dokumentation des IT-Sicherheitskonzepts) genutzt werden.

Ergänzende Kontrollfragen:

- Sind für alle Phasen des IT-Sicherheitsprozesses ausreichende Dokumentationen vorhanden?
- Existieren Regelungen, um die Vertraulichkeit der Dokumentationen zu wahren?
- Sind die vorhandenen Dokumente auf dem neuesten Stand?

M 2.202 Erstellung eines Handbuchs zur IT-Sicherheit

Diese Maßnahme ist mit Version 2006 entfallen.

M 2.203 Aufbau einer Informationsbörse zur IT-Sicherheit

Diese Maßnahme ist mit Version 2005 entfallen.

M 2.204 Verhinderung ungesicherter Netzzugänge

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Revisor

Jeder ungesicherte Zugang zu einem Netz stellt eine enorme Sicherheitslücke dar. Daher muss jede Kommunikation in das interne Netz ausnahmslos über einen gesicherten Zugang geführt werden. Dies kann beispielsweise eine Firewall sein (siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)*).

Es müssen Regelungen getroffen werden, dass keine weiteren externen Verbindungen unter Umgehung der Firewall geschaffen werden dürfen. Alle Benutzer müssen darauf hingewiesen werden, welche Gefahren mit der Schaffung "wilder" Zugänge, z. B. über mitgebrachte Modems, verbunden sind.

Dokumentation der Netzzugänge

Sämtliche externen Netzzugänge sollten zentral erfasst werden (siehe Baustein 2.1). Weiterhin sollte durch Stichproben überprüft werden, ob über Modems oder anderweitig zusätzliche Netzzugänge geschaffen wurden. Dafür können z. B. automatisiert vorgegebene Rufnummerbereiche getestet werden, ob sich dort Datenübertragungseinrichtungen melden.

Die Datenübertragung sollte in allen Organisationen klar geregelt sein. Alle Datenübertragungseinrichtungen sollten genehmigt sein und deren Nutzung klaren Regelungen unterliegen. Dies betrifft nicht nur Router, Modems und ISDN-Karten, sondern auch Infrarot- oder Funk-Schnittstellen.

Die Datenübertragung sollte in allen Organisationen klar geregelt sein. Insbesondere sollten die folgenden Punkte festgelegt sein:

- Zuständigkeiten für Installation, Wartung und Betreuung
- Festlegung des Benutzerkreises und der Nutzungsberechtigungen
- Vorgaben und Sicherheitsmaßnahmen für die Benutzung
- Festlegung der möglichen Kommunikationspartner
- Nutzungszeiten
- Vertretungsregelung
- Protokollierung
- Sichere Konfiguration der Datenübertragungseinrichtungen

Beispiele hierfür finden sich in M 2.61 *Regelung des Modem-Einsatzes* oder M 2.179 *Regelungen für den Faxserver-Einsatz*.

Ergänzende Kontrollfragen:

- Sind alle externen Netzzugänge dokumentiert?
- Sind Regelungen für die Nutzung von Datenübertragungseinrichtungen festgelegt worden?
- Werden die Regelungen für die Nutzung von Datenübertragungseinrichtungen regelmäßig an das Einsatzumfeld und die technische Entwicklung angepasst?

M 2.205 Übertragung und Abruf personenbezogener Daten

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Datenschutzbeauftragter

Verantwortlich für Umsetzung: Leiter IT, Datenschutzbeauftragter

Erfolgt eine Übertragung personenbezogener Daten vom Standort des Arbeit- bzw. Auftraggebers zu einem "entfernten" Arbeitsplatz (z. B. eines Telearbeiters), so müssen die datenschutzrechtlichen Bestimmungen Beachtung finden. Gemäß § 9 BDSG muss in solchen Fällen insbesondere verhindert werden, dass Unbefugte mit Hilfe von Einrichtungen zur Datenübertragung IT-Systeme nutzen (Benutzerkontrolle). Weiterhin ist zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle).

Der Transportweg bzw. die Übertragungsmethode sollten so gewählt sein, dass sowohl die Vertraulichkeit und Integrität als auch die Authentizität (Herkunftsnachweis) der personenbezogenen Daten gewährleistet werden kann.

Erfolgt die Übertragung personenbezogener Daten im Rahmen eines automatisierten Abrufverfahrens, sind die besonderen Zulässigkeitsvoraussetzungen in den einschlägigen Gesetzen zu beachten:

Allgemeine Aspekte

- Anlass und Zweck sowie beteiligte Stellen am Abrufverfahren sind festzulegen.
- Abrufberechtigungen sind festzulegen und zu kontrollieren.
- Art und Umfang der bereitgehaltenen Daten sind festzulegen.
- Sperr- und Löschfristen für Daten sind zu definieren.
- Es ist festzulegen, in welchen Fällen die speichernde Stelle von der abrufenden Stelle zu informieren ist.
- Der Transportweg ist festzulegen, z. B. Zugriff über ISDN-Wählleitung, gesichert über Callback basierend auf CLIP bzw. COLP (siehe M 5.49 *Callback basierend auf CLIP/COLP*).
- Es sollten geeignete kryptographische Verfahren (z. B. symmetrische und asymmetrische Verschlüsselung, digitale Signatur) eingesetzt werden, um Verletzungen des Datenschutzes beim Transport schutzwürdiger Daten zu verhindern. Wie entsprechende Verfahren und Produkte ausgewählt werden können, ist in Baustein B 1.7 *Kryptokonzept* beschrieben.
- Werden über einen Transportweg regelmäßig oder dauerhaft personenbezogene Daten ausgetauscht, sollte die Übertragung mit Hilfe eines virtuellen privaten Netzes (VPN) gesichert werden (siehe M 5.76 *Einsatz geeigneter Tunnel-Protokolle für die RAS-Kommunikation* und M 5.83 *Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN*

Maßnahmen gegen unbefugten Abruf

Der Abruf von Daten durch nicht Abrufberechtigte ist durch geeignete Vorkehrungen zu verhindern:

- Jeder Benutzer muss sich gegenüber den IT-Systemen, von denen die personenbezogenen Daten abgerufen werden, eindeutig identifizieren und authentisieren.
- Nach einer festgelegten Anzahl von Fehlversuchen ist die Berechtigung zu sperren.
- Passwörter müssen in regelmäßigen Abständen gewechselt werden. Soweit möglich, ist dies durch die entsprechenden Programme zu erzwingen.
- Zur Überprüfung der Protokolldateien sollten programmgesteuerte Prüfungsverfahren eingesetzt werden.
- Art und Umfang der Protokollierung müssen festgelegt werden (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*).
- Es sollten zufallsgesteuerte Stichprobenkontrollen oder eine Dauerprotokollierung durchgeführt werden.
- Es ist festzulegen, an welcher Stelle die Protokollierungen durchgeführt werden (abrufende und/oder speichernde Stelle).
- Die Protokollierung muss so konzipiert sein, dass nachträglich festgestellt werden kann, aufgrund wessen Abrufberechtigung Daten abgerufen wurden.
- Die Gründe des Abrufs müssen protokolliert werden.
- Beim Abruf von Daten sollte protokolliert werden, über welchen Anschluss und welche Endgeräte die Übertragung stattfindet.

Maßnahmen zur Organisationskontrolle

- Alle Mitarbeiter, insbesondere die der abrufenden Stelle, sind auf das Datengeheimnis zu verpflichten. Eine Weitergabe von Daten an Dritte ist vertraglich zu untersagen.

Ergänzende Kontrollfragen:

- Wurden die umgesetzten technischen und organisatorischen Maßnahmen dokumentiert?
- Liegt ein Konzept zur Überprüfung und Feststellung der Zulässigkeit der im Rahmen automatisierter Abrufe erfolgten Datenübertragungen vor?

M 2.206 Planung des Einsatzes von Lotus Notes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Vor der Einführung von Lotus Notes muss entschieden werden, für welche Einsatzzwecke Lotus Notes genutzt werden soll. Die Nutzungsart hat zum einen Einfluss auf die zu beschaffende Software (z. B. Domino Application Server oder Domino Mail Server), die festzulegenden Sicherheitsrichtlinien und auch auf die Art und den Umfang der Planungen für die Einsatzszenarien.

Generell kann grob zwischen drei verschiedenen Varianten unterschieden werden:

1. Einsatz als Intranetserver und Zugriff über Notes-Clients

   In diesem Szenario liegt der Hauptaugenmerk auf dem Einsatz als internes System zur Bürokommunikation (Datenverwaltung, E-Mail, Terminvereinbarung, Koordination von Gruppenarbeit).

2. Einsatz als Intranetserver und Zugriff über Browser

   In diesem Szenario liegt das Hauptaugenmerk auf dem Web-Zugriff auf einen Notes-Server. Da an der Web-Schnittstelle des Notes-Servers gänzlich andere Sicherheitsmechanismen als in Variante 1 genutzt werden, wird die sichere Konfiguration dieser Schnittstelle als eigenes Szenario betrachtet.

3. Einsatz als Internet-Server und Zugriff über Browser

   Neben dem primären Einsatz eines Notes-Servers als Intranet-Server kann auch die Nutzung als öffentlich zugreifbarer Informations-Server über das Internet gewünscht sein. Diese Nutzungsart erfordert aufgrund der exponierten Stellung eines solchen Servers besondere Aufmerksamkeit bei der Systemkonfiguration. Insbesondere muss hierbei der Notes-Server in einer DeMilitarisierten Zone (DMZ) aufgestellt sein, also in einem durch Firewalls gegen unbefugte Zugriffe von innen und außen geschütztem Bereich (siehe auch M 2.211 *Planung des Einsatzes von Lotus Notes in einer DMZ*).

Welche Funktionen sollen genutzt werden

Innerhalb der Einzelszenarien kann weiter dahingehend unterschieden werden, welche Notes-Funktionen genutzt werden sollen (z. B. Datenbankzugriff, Notes-Mail, Internet-Mail, LDAP-Server, HTML-Server). Eine Unterscheidung auf dieser Ebene soll hier nicht erfolgen. Grundsätzlich gilt jedoch, dass für die Nutzung jeder Funktionalität eine eigene Planung erforderlich ist, bei der auch Sicherheitsgesichtspunkte zu berücksichtigen sind. Für einige der genannten Funktionen existieren auch eigene Bausteine in den IT-Grundschutz-Katalogen, die bei deren Nutzung beachtet werden sollten, z. B. Baustein B 5.3 *E-Mail* und B 5.4 *Webserver*.

Grundsätzlich müssen bei der Einsatzplanung folgende Aspekte betrachtet werden:

- Lotus Notes baut einen eigenen Namensraum auf, der die Aufteilung in sogenannte Notes-Domänen ermöglicht. Damit dieser effizient genutzt werden kann, muss eine Planung der Domänen erfolgen. Daneben wird durch die Notes-Zertifikate eine hierarchische Zertifikatsstruktur aufgebaut, die unabhängig von der Domänenaufteilung ist und daher eine eigene Planung erfordert. Die dabei zu berücksichtigenden Aspekte sind in der Maßnahme M 2.208 *Planung der Domänen und der Zertifikatshierarchie von Lotus Notes* beschrieben.

Domänen- und Zertifikatsstruktur planen

- Begleitend zur Planung des Namensraumes von Lotus Notes und des gewünschten Einsatzszenarios ist eine Notes-spezifische Sicherheitsrichtlinie zu entwerfen. Die dabei zu berücksichtigenden Aspekte sind in der Maßnahme M 2.207 *Festlegen einer Sicherheitsrichtlinie für Lotus Notes* zusammengefasst.

Sicherheitsrichtlinien festlegen

- Die Detailplanung für das gewünschte Einsatzszenario ist durchzuführen. Für jedes Szenario sind die relevanten Empfehlungen in den folgenden Maßnahmen erfasst:
  - M 2.209 *Planung des Einsatzes von Lotus Notes im Intranet*
  - M 2.210 *Planung des Einsatzes von Lotus Notes im Intranet mit Browser-Zugriff*
  - M 2.211 *Planung des Einsatzes von Lotus Notes in einer DMZ*

  Die Planung des Notes Systems darf nur dann als abgeschlossen betrachtet werden, wenn auch das sogenannte "Roll-out" im Detail geplant worden ist. Durch die Roll-out-Planung wird die Installationsreihenfolge der einzelnen Notes-Server und aller Notes-Clients festgelegt. Insbesondere das Roll-out der Zertifizierungsstellen muss genau geplant werden, um die Zertifizierungshierarchie korrekt nutzen zu können.

Roll-out planen

Die bei der Planung getroffenen richtungsweisenden Entscheidungen sollten dokumentiert werden, damit später überprüft werden kann, ob diese vollständig umgesetzt worden sind. Insbesondere sollten sie so aufgeschrieben werden, dass die Gründe für diese Entscheidungen nachvollziehbar sind.

Entscheidungen dokumentieren

Ergänzende Kontrollfragen:

- Wurde eine Anforderungsanalyse für den Einsatz von Lotus Notes durchgeführt?

M 2.207 Festlegen einer Sicherheitsrichtlinie für Lotus Notes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Wie für jedes in einem Unternehmen eingesetzte Software-Produkt muss auch für den Einsatz von Lotus Domino Servern eine geeignete Sicherheitsrichtlinie festgelegt werden. Lotus Domino kann als eigenes Netzkommunikationssystem angesehen werden, welches das darunter liegende Betriebssystem lediglich als Ablaufumgebung nutzt und auf administrativer Ebene über eigenständige Mechanismen verfügt. Daher ist für das Festlegen einer Sicherheitsrichtlinie ein ähnlich umfangreiches Themenspektrum zu bedenken, wie für ein Netzbetriebssystem.

Im Rahmen der Sicherheitsrichtlinie sind folgende Aspekte zu berücksichtigen:

- Die Sicherheitsrichtlinie für Lotus Notes muss konform zu den geltenden generellen Sicherheitsrichtlinien der Behörde bzw. des Unternehmens sein (siehe M 2.192 *Erstellung einer IT-Sicherheitsleitlinie*).
- Es müssen Zugriffsregeln festgelegt werden, **Zugriffsregeln**
  - welcher Benutzer auf welchen Server zugreifen darf und welche Benutzer auf welche Server **nicht** zugreifen sollen (Ausschlussliste),
  - welcher Benutzer mit welchen Rechten auf welche Datenbank zugreifen darf,
  - welche Datenbank von welchem Server aus administriert wird,
  - welche anderen Server auf einen Server zugreifen dürfen,
  - wie Datenbanken repliziert werden,
  - welche Datenbankbestandteile (Datensätze, Ansichten, Scripten usw.) repliziert werden,
  - von wo aus auf einen Notes-Server zugegriffen werden darf.
- Außerdem muss festgelegt werden,
  - wie Notes-ID-Dateien zu behandeln sind, beispielsweise in bezug auf Erzeugung, Verteilung, Speicherung und Vier-Augen-Prinzip (siehe dazu auch Maßnahme M 4.129 *Sicherer Umgang mit Notes-ID-Dateien*), **Notes-ID-Dateien**
  - ob und unter welchen Bedingungen das Wiederherstellen von Passwörtern für Notes-ID-Dateien bzw. ganzer Notes-ID-Dateien erfolgt,
  - ob eine Kommunikationsabsicherung (z. B. für Netzkommunikation, E-Mail-Kommunikation) eingesetzt werden soll, welcher Mechanismus genutzt wird und welche Kommunikationsverbindungen geschützt werden sollen. **Verschlüsselung und Signatur**
- Es muss ein Auditing- und Protokollierungskonzept entworfen werden. Es ist darauf zu achten, dass der Datenschutzbeauftragte in die Planung mit **Audit und Protokollierung**

einbezogen wird, da im Rahmen der Überwachung auch personenbezogene Daten anfallen können.

- Die Planung der Notes Domänen muss erfolgen, die Zugriffsberechtigungen zwischen den Domänen müssen festgelegt werden (benutzerorientiert und serverorientiert) und es muss eine Planung der Replikation von Datenbanken erfolgen.
- Für jedes aktivierte Funktionsmodul des Domino Applikation Servers ist eine Sicherheitsplanung erforderlich. Es müssen u. a. Zugriffsbeschränkungen, Zugriffsarten, zu benutzende Authentisierungsmechanismen und Reaktionen auf Sicherheitsverstöße festgelegt werden.

Alle Benutzer müssen die Vorgaben kennen.

Die Sicherheitsrichtlinie für die Nutzung von Lotus Notes muss organisationsweit abgestimmt sein und allen Benutzern bekannt gegeben worden sein. Hierbei empfiehlt es sich, für die Endbenutzern die wichtigsten Inhalte in einer kurzen und prägnanten Form aufzubereiten, z. B. in Form eines Faltblattes oder einer Webseite. Wenn sich Sicherheitsvorgaben verändern, müssen alle Benutzer hierüber informiert werden.

Im Rahmen von bestehenden Sicherheitsrichtlinien kann die Situation entstehen, dass bestimmte Sicherheitsanforderungen mit den Mechanismen von Lotus Notes nicht realisiert werden können. In diesem Fall muss entschieden werden, ob die bestehenden Sicherheitsrichtlinien angepasst werden oder ob das Einsatzszenario von Lotus Notes so stark eingeschränkt wird, dass die Richtlinien umgesetzt werden können.

Ergänzende Kontrollfragen:

- Existiert eine aktuelle Sicherheitsrichtlinie für die Nutzung von Lotus Notes?
- Können alle relevanten Sicherheitsvorschriften der organisationsweiten Sicherheitsrichtlinie auf Lotus Notes abgebildet werden?
- Werden alle Benutzer über neue oder veränderte Sicherheitsvorschriften informiert?

M 2.208 Planung der Domänen und der Zertifikatshierarchie von Lotus Notes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Ein Notes-System besteht aus einem oder mehreren Lotus Notes Servern und vielen Notes- und/oder Web-Clients. Die einzelnen Server eines Notes-Systems können einzelnen Notes-Domänen zugeordnet werden. Domänen legen - ähnlich wie in anderen Netz-Betriebssystemen - die administrativen Grenzen und die Gültigkeit von Sicherheitseinstellungen (z. B. Zugriffskontrollen) fest. Zusätzlich wird durch jede Domäne ein eigener Namensraum aufgespannt. Der Planung der Notes-Domänen und dem durch sie definierten Namensraum kommt daher eine wichtige Bedeutung zu.

Domänen an Organisationsstruktur anpassen

Eine Domäne korrespondiert mit einem Notes-Verzeichnis und kann in grober Vereinfachung als Mittel zur E-Mail-Verteilung angesehen werden. Der Namensraum einer Domäne kann hierarchisch in sogenannten Organisationseinheiten strukturiert sein, so dass Benutzer, Gruppen und Server, die in einer Domäne zusammengefasst sind, weiter unterteilt werden können. Die Aufteilung einer Domäne muss an die Anforderungen der Behörde bzw. des Unternehmens angepasst werden. Es empfiehlt sich jedoch eine Aufteilung, die die Organisationsstruktur widerspiegelt.

Die E-Mail-Kommunikation kann unter Lotus Notes durch den Einsatz von Verschlüsselung und digitalen Signaturen abgesichert werden (siehe M 5.85 *Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail*). Für die Verteilung der kryptographischen Schlüssel sollte eine Zertifikatshierarchie (Public Key Infrastruktur - PKI) aufgebaut werden, die unabhängig von der Domänenplanung sein kann. Dies hat zur Folge, dass in einer Notes-Domäne mehrere unabhängige Zertifikatshierarchien existieren können oder eine Zertifikatshierarchie mehrere Domänen umfasst.

Bei der Planung von Domänen ist zu überlegen, ob ein Ein- oder Mehr-Domänen-Konzept konzipiert werden soll.

Ein-Domänen-Konzept

Ein Ein-Domänen-Konzept besitzt folgende Vorteile:

- Die E-Mail-Adressen aller Benutzer besitzen die gleiche Domänenkennung (*Benutzer@Domäne*). Eine Kenntnis der Notes-Domänenzugehörigkeit bei der Nutzung mehrerer Domänen in einem Unternehmen ist für den Sender nicht notwendig.
- Die Administration vereinfacht sich wesentlich, da nur ein Namens- und Adressbuch (NAB) gepflegt werden muss. Werden mehrere Domänen benutzt, so sind im NAB zusätzlich z. B. die Verbindungs-Einträge und Domänen-Definitionen enthalten, die die Schnittstellen der jeweiligen Domäne mit den anderen Domänen festlegen. Diese müssen für jede Domäne einzeln gepflegt werden. Beim Ein-Domänen-Konzept fällt diese Arbeit nicht an.

Ein Mehr-Domänen-Konzept besitzt folgende Vorteile:

Mehr-Domänen-Konzept

- Große Benutzermengen lassen sich besser in mehreren Domänen verwalten, da mit zunehmender Größe des NAB die Performance sinkt und auch die Verwaltung unübersichtlicher wird. Wird das NAB zusätzlich auf Clients repliziert (z. B. für mobile Benutzer) kann dies bei entsprechender Größe durch den zunehmenden Bedarf an Speicherplatz bzw. der wachsenden Replikationszeit, insbesondere bei langsamen Verbindungen, problematisch werden. Das Aufbrechen in mehrere Domänen und damit mehrere NABs besitzt daher Vorteile und bietet auch einen gewissen Ausfallschutz.
- Vielfach sind Organisationsstrukturen nicht homogen und lassen sich daher schlecht auf genau eine Notes-Domäne abbilden. Insbesondere ist vielfach auch die administrative Trennung einzelner Bereiche sinnvoll oder zwingend erforderlich, z. B. wenn unterschiedliche Sicherheitsvorschriften umzusetzen sind oder länderspezifische Eigenschaften, wie Sprache oder Zeichensätze, berücksichtigt werden müssen. Diese Trennung lässt sich nur durch ein Mehr-Domänen-Konzept erreichen.
- Durch Zusammenlegung von Organisationseinheiten werden vorher eigenständige Notes-Domänen weitergeführt, da eine Integration einen hohen administrativen Aufwand bedeutet oder der etablierte Namensraum weiter verwendet werden soll.
- Es können spezielle Domänen angelegt werden, die zur Isolation oder Abgrenzung gegen andere Domänen genutzt werden können, beispielsweise Test-Domänen, Domänen für Software-Entwicklung oder Domänen mit Einwahl-Zugängen.

Nachträgliche Änderungen sind aufwändig.

Bei der Planung des Domänenkonzeptes ist zu bedenken, dass eine nachträgliche Veränderung im Domänenmodell zwar generell möglich, jedoch in der Regel mit hohem administrativen Aufwand verbunden ist, da u. a. alle von einem Domänenwechsel betroffenen Server und Benutzer innerhalb der Notes-Domänen umgesiedelt werden müssen. Dabei sind auch Rezertifizierungen notwendig, sowie das Umstellen von Datenbank-ACLs.

Zertifikatshierarchien

Bei der Planung von Zertifikatshierarchien ist generell folgendes zu beachten:

- Es muss zwischen Notes-Zertifikaten und den von Notes benutzten Internet-Zertifikaten (X.509-Zertifikate) unterschieden werden. Es sind daher u. U. zwei Zertifikatshierarchien parallel zu verwalten.
- Zur Zertifizierung von Notes-Benutzern (Notes-ID) können nur Notes-Zertifikate und keine Internet-Zertifikate genutzt werden.
- Die Vergabe und Kontrolle von Zugriffsberechtigungen (auch zwischen verschiedenen Domänen) bei Lotus Notes basiert auf den Notes-Zertifikaten.
- Zwischen verschiedenen Zertifikatshierarchien (ohne gemeinsame Zertifizierungsinstanz) können Vertrauensstellungen eingetragen werden, indem eine sogenannte Cross-Zertifizierung erfolgt (Anerkennen fremder Zertifikate). Die leichtfertige Vergabe von Cross-Zertifikaten (meist können diese automatisch erzeugt werden, wenn ein unbekanntes Zertifikat

"entdeckt" wird) vermindert die Systemsicherheit. Dies gilt sowohl für Notes-Zertifikate, als auch für X.509-Zertifikate. Dabei können Cross-Zertifikate auch von Benutzern einfach im persönlichen lokalen Adressbuch erzeugt werden. Das Anlegen von Cross-Zertifikaten im NAB kann dagegen nur durch einen berechtigten Administrator erfolgen.

- Zur Identifizierung von Benutzern bei Zugriffen über die Web-Schnittstelle von Lotus Notes können nur Internet-Zertifikate benutzt werden.
- Notes Zertifikatsstrukturen können flach oder hierarchisch sein. In einer flachen Zertifikatsstruktur gibt es eine Zertifizierungsstelle, die die Zertifikate für alle Benutzer ausstellt. In einer hierarchischen Zertifikatsstruktur gibt es verschiedene Zertifizierungsstellen, wobei die Zertifikate der einzelnen Zertifizierungsstellen von einer übergeordneten Zertifizierungsinstanz signiert werden.

  Flache Zertifikatsstrukturen sind einfacher zu administrieren, hierarchische Strukturen besitzen allerdings den Vorteil, dass eine Delegation der Administration möglich ist (so können z. B. Abteilungen neue Benutzer selbst zertifizieren). Dies ermöglicht es auch einzelnen Organisationseinheiten, eigene Zertifikate auszustellen und zu verwalten.
- Die Zertifikatshierarchie ist zu planen. Es muss u. a. festgelegt werden, welche Zertifikate ausgestellt werden, wer zertifizieren darf und was zertifiziert werden darf. Die Zuständigkeiten und Verantwortlichkeiten müssen geplant werden.

gründliche Abstimmung mit allen beteiligten Stellen

Das Aufsetzen einer Zertifikatshierarchie stellt in der Regel weniger ein technisches als ein organisatorisches und politisches Problem dar. Eine entsprechend lange Planungsphase, in die alle beteiligten Stellen (technisch und organisatorisch) eingebunden sind und an deren Ende ein von allen Beteiligten verabschiedetes Konzept vorliegt, sollte daher vorgesehen werden.

Ergänzende Kontrollfragen:

- Ist die Domänenplanung dokumentiert?
- Wird bereits eine Zertifikatsinfrastruktur (PKI) betrieben?
- Kann oder muss die PKI zur Ausstellung von X.509-Zertifikaten benutzt werden?

M 2.209 Planung des Einsatzes von Lotus Notes im Intranet

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Lotus Domino ist hauptsächlich für den Einsatz im Intranet konzipiert, was durch die Integration von Internet-Technologien weiter unterstützt wird. Soll ein Notes-System eingesetzt werden, so ist ein Betriebskonzept zu entwerfen. Ohne festgelegtes Konzept kann in der Regel keine IT-Sicherheit gewährleistet werden. Bei der Planung eines Notes-Systems ist folgendes aus Sicherheitssicht zu beachten:

- Die umzusetzenden Sicherheitsvorschriften müssen geplant werden (siehe M 2.207 *Festlegen einer Sicherheitsrichtlinie für Lotus Notes*).
- Die Domänenplanung und die Planung der Zertifikatshierarchie ist durchzuführen (siehe M 2.208 *Planung der Domänen und der Zertifikatshierarchie von Lotus Notes*).
- **sichere Aufstellung der Server**

  Die Standorte der Notes-Server ist festzulegen. Alle Notes-Server sollten in Serverräumen aufgestellt werden. Hierbei zu realisierende Maßnahmen sind in Baustein B 2.4 *Serverraum* beschrieben. Wenn kein Serverraum zur Verfügung steht, kann ein Notes-Server alternativ in einem Serverschrank aufgestellt werden (vergleiche Baustein B 2.7 *Schutzschränke*).
- Neben den Notes-spezifischen Sicherheitsmaßnahmen sind für die Server die relevanten Bausteine aus dem Baustein 3 umzusetzen.
- Die Verteilung von Datenbanken auf Server ist zu planen. Dabei muss auch die Lastverteilung berücksichtigt werden. Ausgangspunkt ist dabei die Frage, welche Clients auf welchen Server zugreifen.
- **Rechtekonzept für Server**

  Für die Server sind die Zugangs- und Zugriffsbeschränkungen zu planen. Dabei sollten nur die Rechte vergeben werden, die auch wirklich benötigt werden.
- Für die Datenbanken eines Servers ist die Zugriffskontrolle zu planen: Welche Benutzer (oder Benutzergruppen) sollen mit welchen Rechten auf Datenbanken zugreifen?
- Es sollte ein Notes-spezifisches Gruppenkonzept entworfen werden, so dass die Zugriffskontrolle gruppenbasiert konzipiert werden kann.
- Ein einzelner Notes-Server integriert sich durch die zur Verfügung stehenden Funktionsmodule in viele Anwendungen (z. B. E-Mail, News, Web) und kann dadurch eine zentrale Rolle in jedem System spielen. Dies macht einen Notes-Server jedoch auch zu einer kritischen Ressource. Fällt ein solcher Server aus, so sind u. U. alle diese Anwendungen teilweise oder ganz funktionsunfähig. Es sollte daher überlegt werden, verschiedenen Notes-Servern dedizierte Rollen zuzuweisen.
- **nicht benötigte Module deaktivieren**

  Für jeden Server ist festzulegen, welche Funktionsmodule aktiviert werden. Nicht benötigte Module sind zu deaktivieren.

- Jedes Funktionsmodul erfordert eine eigene Planung, die die Einbindung in das lokale Netz berücksichtigt (z. B. E-Mail-System mit Domino Mail Servern, Notes-Server als LDAP-Server oder LDAP-Client, gemischtes News-System mit Notes-NNTP-Servern und Unix-NNTP-Servern).

Die Sicherheit des Notes-Systems hängt von vielen Faktoren ab, die wichtigsten sind jedoch:

- Die Sicherheit jedes Notes-Servers.
- Die Sicherheit jedes Notes-Clients.
- Die Sicherheit jeder Kommunikationsverbindung zwischen Notes-Servern und Clients.

Detaillierte Maßnahmen zu Absicherung dieser Hauptkomponenten finden sich in den Notes-spezifischen Maßnahmen der Maßnahmenkataloge 4 "Hardware/Software" und 5 "Kommunikation".

M 2.210 Planung des Einsatzes von Lotus Notes im Intranet mit Browser-Zugriff

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Soll auf einen Notes-Server im Intranet auch über einen Browser zugegriffen werden, so ist eine Planung insbesondere unter Sicherheitsgesichtspunkten notwendig.

Die Web-Schnittstelle bietet im Vergleich zum Zugriff mittels Notes-Client in der Regel weniger Funktionalitäten. Insbesondere ist zu beachten, dass an der Web-Schnittstelle im Vergleich zum Zugriff mittels Notes-Client gänzlich andere Sicherheitsmechanismen für die Authentisierung zum Einsatz kommen. Auch die Datensicherheit auf Datenbankebene wird hier nur eingeschränkt unterstützt. Die Ent- bzw. Verschlüsselung von Dokumentenfeldern an der Web-Schnittstelle wird zur Zeit nicht angeboten. Eine weitere Einschränkung ist die fehlende Möglichkeit, Datenbanken lokal auf Clients zu replizieren, um eine Offline-Verarbeitung zu ermöglichen.

Da der Browser-Zugriff verschiedene Einschränkungen der IT-Sicherheit mit sich bringt, ist dieser nicht zu empfehlen. Daher sollte er möglichst restriktiv gehandhabt werden, also nur ermöglicht werden, wenn dies unbedingt erforderlich ist.

Soll trotz der zusätzlichen Sicherheitsprobleme der Browser-Zugriff ermöglicht werden, müssen für die Planung die nachstehend aufgeführten Fragestellungen berücksichtigt werden:

- Welche Benutzer sollen über die Web-Schnittstelle auf welche Server zugreifen dürfen? Diese Entscheidung hat Einfluss auf die Konfiguration des Datenbankzugriffs, die dann entsprechend angepasst werden muss (siehe M 4.120 *Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken* und M 4.125 *Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken*).
- Soll ausschließlich über die Web-Schnittstelle auf Lotus Notes zugegriffen werden? Ist dies der Fall, müssen gewisse Einschränkungen, z. B. in bezug auf Verschlüsselungsmechanismen, in Kauf genommen werden, da nicht alle Funktionen und Sicherheitsmechanismen an der Webschnittstelle verfügbar sind. Es ist daher zu entscheiden, ob diese Einschränkungen in Kauf genommen werden können.
- Können alle notwendigen Datenbanken über die Web-Schnittstelle genutzt werden? Datenbanken, die Funktionen über clientseitiges LotusScript und Agenten anbieten, verlieren diese Funktionalität beim Web-Zugriff, da LotusScript nicht durch Browser unterstützt wird. Aus diesem Grund muss überprüft werden, ob solche Datenbanken genutzt werden.
- Auf welche Daten soll über die Web-Schnittstelle zugegriffen werden? Es kann grob zwischen öffentlichen Daten, internen Daten, z. B. Kundendaten, Projektdaten, Personaldaten, und den Bürodaten der Mitarbeiter, z. B. Terminkalender, E-Mail, Todo-Listen, unterschieden werden. Eine

weitere Unterteilung, z. B. nach einer Schutzbedarfsfeststellung, ist sinnvoll. Nur Daten ohne besonderen Schutzbedarf sollten für den Zugriff über die Web-Schnittstelle freigegeben werden.

- Können die Daten, auf die über die Web-Schnittstelle zugegriffen werden soll, auf dedizierten Servern gehalten werden? Dies erleichtert die Konfiguration von Servern, da kein Mischzugriff (Notes-Client und Browser) erfolgt. Die Daten sollten daher möglichst getrennt gehalten werden.
- Welche Datenbanken sollen über die Web-Schnittstelle zugreifbar sein? Für solche Datenbanken müssen spezielle Sicherheitseinstellungen vorgenommen werden (siehe M 4.120 *Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken*, M 4.125 *Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken*).
- Müssen die Daten beim Transport über die Web-Schnittstelle geschützt werden? In diesem Fall muss die Kommunikation abgesichert werden (siehe M 5.86 *Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes*). Der ungeschützte Transport von Daten sollte grundsätzlich vermieden werden. Nur bei Daten, auf die anonym zugegriffen werden darf, kann auf Verschlüsselung verzichtet werden.
- Ist der anonyme Zugriff über die Web-Schnittstelle notwendig? In diesem Fall muss der jeweilige Server und die betroffenen Datenbanken entsprechend angepasst werden (siehe M 4.119 *Einrichten von Zugangsbeschränkungen auf Lotus Notes Server*, M 4.120 *Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken*, M 4.124 *Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes*). Öffentliche Daten, auf die anonym zugegriffen werden soll, sollten möglichst auf einem speziellen Server vorgehalten werden. Anonyme Zugriffe auf alle anderen Server sind dann zu deaktivieren.
- Soll der Zugriff auf Datenbanken über die Web-Schnittstelle mit eingeschränkten Rechten erfolgen? Dies ist auf Grund der eingeschränkten Sicherheitsfunktionalität dringend zu empfehlen. In diesem Fall ist allerdings auf Grund der damit einhergehenden Funktionseinbuße in der Regel keine ausschließliche Nutzung der Web-Schnittstelle möglich. Die Datenbanken müssen entsprechend konfiguriert werden (siehe M 4.125 *Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken*).
- Soll eine eigene Zertifizierungsstelle (CA) zum Ausstellen von Internetzertifikaten betrieben werden? Hierzu müssen das Aufsetzen einer eigenen Zertifizierungsstelle (z. B. einer Notes-CA) und die Zertifikatshierarchien geplant werden. Zusätzlich muss für die Verteilung der Zertifikate an Server und Benutzer gesorgt werden.
- Kann die Sicherheit der Computer, die als Client fungieren, gewährleistet werden? Das Sicherheitsniveau dieser Computer hat Einfluss auf die benutzten Authentisierungsverfahren an der Web-Schnittstelle (siehe M 4.124 *Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes*).

- Welcher Browser wird für den Web-Zugriff genutzt? Auch die Sicherheitsmechanismen des Browsers haben Einfluss auf die benutzten Authentisierungsverfahren an der Web-Schnittstelle (siehe M 4.124 *Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes*, M 4.127 *Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes*).
- Sollen Server über die Web-Schnittstelle administriert werden? Die Administration über die Web-Schnittstelle sollte nur nach einer gewissenhaften Risikoabwägung erfolgen. Der administrative Zugriff muss alle Sicherheitsmechanismen nutzen (siehe M 4.123 *Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes*, M 4.125 *Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken*).
- Sollen Benutzer auf ihre E-Mail-Datenbanken über die Web-Schnittstelle zugreifen dürfen? Dies erfordert eine entsprechende Konfiguration der Zugriffsmechanismen der einzelnen E-Mail-Datenbanken (siehe M 4.123 *Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes*, M 4.125 *Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken*).
- Müssen E-Mails verschlüsselt werden? In diesem Fall kann die Web-Schnittstelle nicht als alleiniger Zugang zum Notes-Server verwendet werden, wenn auch Notes-Verschlüsselung benutzt werden muss. Auch die S/MIME-Verschlüsselung ist an der Web-Schnittstelle nicht verfügbar. Daher müssen alle Benutzer einen S/MIME-fähigen E-Mail-Client verwenden und mit einem "Internet-Zertifikat" ausgestattet sein, das mit S/MIME benutzt werden kann (siehe M 5.85 *Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail*).

Je nach konkretem Einsatzszenario, sind weitere Fragestellungen beim Einsatz von Lotus Notes im Intranet mit Browser-Zugriff zu beachten.

Ergänzende Kontrollfragen:

- Gibt es zwingende Gründe Browser-Zugriffe auf Notes-Server zuzulassen?
- Existiert eine Konzeption für den Einsatz von Lotus Notes mit Browser-Zugriffen?

M 2.211 Planung des Einsatzes von Lotus Notes in einer DMZ

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Die in den Datenbanken eines Notes-Servers gespeicherten Daten können auch für den öffentlichen Zugriff aus dem Internet bereitgestellt werden. Dies stellt besondere Anforderungen an die Sicherheit des dazu benutzten Notes-Servers.

Für den direkten Zugriff auf einen Notes-Server aus dem Internet ist generell folgendes zu beachten:

keine direkten Zugriffe aus dem Internet ins LAN zulassen

- Direkte Zugriffe aus dem Internet auf einen Notes-Server im lokalen Netz dürfen nicht erfolgen. Alle internen Notes-Server sind vor direkten Zugriffen aus dem Internet mit einer Firewall zu schützen (siehe auch Baustein B 3.301 *Sicherheitsgateway (Firewall)*).

aus dem Internet erreichbare Notes-Server in DMZ platzieren

- Notes-Server, auf die direkt aus dem Internet zugegriffen wird, müssen in einem separaten Netz (einer sogenannten DeMilitarisierten Zone, DMZ) angesiedelt sein. Der Zugriff auf den Server muss durch eine Firewall abgesichert werden (siehe auch M 2.77 *Integration von Servern in das Sicherheitsgateway*).

Bei einer Anbindung an das Internet können auftretende Sicherheitsprobleme gravierende Folgen haben (siehe G 5.100 *"Hacking Lotus Notes"*). Daher sollte darauf verzichtet werden, Notes-Server für Zugriff aus dem Internet zu öffnen. Kommt trotzdem ein Notes-Server in der DMZ zum Einsatz, so muss die Konfiguration der Sicherheitseinstellungen besonders sorgfältig erfolgen. Dabei sind insbesondere die folgenden Punkte zu beachten:

Regelungen für Internet-Anbindung von Notes-Servern

- Es muss eine Sicherheitskonzeption für die Anbindung von Notes-Servern an das Internet erarbeitet werden, in dem u. a. die Sicherheitsziele und die grundlegenden Voraussetzungen festgelegt sind, die erforderliche Netzstruktur beschrieben ist und alle organisatorischen Regelungen festgehalten sind.
- Der Notes-Server sollte in einer separaten Notes-Domäne angesiedelt werden.
- Es sollte eine eigene Zertifizierung des Servers erfolgen, die keine Berechtigungen im Intranet der Behörde bzw. des Unternehmens besitzt.
- Der Notes-Server in der DMZ darf nicht mit internen Notes-Servern replizieren. Für den Datentransfer können dateibasierte Mechanismen, z. B. ftp, zum Einsatz kommen.
- Die Firewall-Konfiguration muss das Initiieren von Verbindungen vom Notes-Server in das interne Netz unterbinden. Ist ein Datenaustausch zwischen internen Systemen und dem Notes-Server in der DMZ notwendig, so dürfen Verbindungen nur von den internen Systemen initiiert werden können. Auch hier sollte auf die Verwendung von Notes-Mecha-

nismen zum Datenaustausch verzichtet werden, um einen bewussten Protokollbruch zu erzeugen.

- Datenbanken enthalten auch ausführbaren Programmcode, wie Agenten und Skripten, die zur Kompromittierung des internen Netzes genutzt werden können. Datenbanken, die vom Notes-Server in der DMZ in das interne Netz zur Weiterverarbeitung transferiert werden, sollten daher einer Sicherheitsüberprüfung unterzogen werden.
- Sollen nur HTML-Seiten (und keine Notes-Datenbanken) durch den Server angeboten werden, so ist ein reines WWW-Server-Produkt zu verwenden. Durch einen Notes-Server werden komplexe Funktionen und Mechanismen angeboten, die sich nicht alle deaktivieren lassen und damit als mögliche Angriffspunkte genutzt werden können. Beispielsweise ist immer eine Verbindung über das Notes-Protokoll möglich.

Notes nicht als Ersatz für einen reinen WWW-Server verwenden

- Das Notes-System sollte ebenso wie andere existierende Systeme in der DMZ überwacht werden.

Neben den hier aufgeführten Aspekten können sich durch die Nutzung eines Notes-Systems in exponierter Stellung weitere Probleme ergeben. Es wird empfohlen, eine individuelle Risikoabwägung durchzuführen, die den Schutzbedarf der IT-Anwendungen und Informationen berücksichtigt.

Ergänzende Kontrollfragen:

- Gibt es zwingende Gründe Internet-Zugriffe auf Notes-Server zuzulassen?
- Ist das IT-Sicherheitsmanagement in diese Entscheidung einbezogen worden?
- Existiert ein Sicherheitskonzept für den Einsatz von Lotus Notes in der DMZ?

M 2.212 Organisatorische Vorgaben für die Gebäudereinigung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Innerer Dienst

Die Gebäudereinigung erfordert im Normalfall den Zutritt von Betriebsfremden. Dies kann insbesondere in Bereichen mit höheren Sicherheitsanforderungen wie Rechenzentren, Serverräumen, Technikräumen oder Kommunikationszentralen problematisch sein und daher zusätzliche Sicherheitsmaßnahmen erfordern.

Bereits in der Ausschreibung und der Vertragsformulierung ist die Sonderbehandlung sensitiver Bereiche einzubeziehen. Zum Beispiel sind bei Rechenzentren stichprobenartige Kontrollen von Taschen oder Transportgut im Zugangs- oder Zufahrtsbereich für betriebsfremdes Personal in den Verträgen festzuschreiben.

Reinigungspersonal einweisen

Da bei Reinigungskräften IT-Kenntnisse nicht vorausgesetzt werden können, sollten diese daher in allen Bereichen mit geschäftskritischen IT-Systemen dahingehend eingewiesen werden, welche Tätigkeiten zu Schäden an IT-Einrichtungen oder Problemen beim IT-Betrieb führen können. Beispiele für solche Problemfelder sind:

- Bei der Reinigung von Tastaturen können unbeabsichtigt Eingaben an Servern oder anderen zentralen Komponenten erfolgen, die den IT-Betrieb beeinträchtigen.
- IT-Systeme können versehentlich ausgeschaltet werden.
- Stromversorgungs- oder Kommunikationskabel können durch Staubsauger beschädigt oder aus den Endpunkten gerissen werden.
- Durch Wasser oder Reinigungsflüssigkeit können Kurzschlüsse in Hardware-Komponenten verursacht werden.

Zutritt der Reinigungskräfte regeln

Wenn Vertrauen in die Reinigungsfirma besteht, sollte der Zutritt der Reinigungskräfte über die vorhandene Zutrittskontrolle bzw. das Schließsystem geregelt werden. Jedoch können dies nur wirksame Sicherungsmaßnahmen sein, wenn z. B. Ausweis oder Schlüssel gegen Unterschrift und nur zeitlich begrenzt benannten bzw. bekannten Mitarbeitern der Reinigungsfirma ausgegeben werden. Bei der Vereinbarung über die Verwendung von Stammpersonal kann über das Ausweissystem eine wirksame Kontrolle der Vertragseinhaltung erreicht werden.

Ansprechpartner der Reinigungsfirma

Für die Koordination, aber auch bei auftretenden Problemen ist vom Auftragnehmer ein Objektverantwortlicher zu benennen, der jederzeit ansprechbar ist. Er muss Entscheidungsbefugnis über das einzusetzende (vor allem auch über nicht mehr einzusetzendes, weil unerwünschtes) Personal haben.

Bereiche mit einem erhöhten Sicherungsbedarf wie Maschinensaal oder Datenträgerarchiv sind nur unter Anwesenheit von Verantwortlichen des Auftraggebers oder in einigen Fällen auch unter Anwesenheit einer Vertrauensperson des Auftragnehmers, z. B. im Vier-Augen-Prinzip, zu reinigen.

Ergänzende Kontrollfragen:

- Wird kontrolliert, ob die Mitarbeiter der beauftragten Reinigungsfirma die ausgegebenen Schlüssel bzw. Ausweise vertragsgemäß verwenden?
- Sind die Reinigungskräfte über den Umgang mit der IT ausreichend informiert?
- Werden die Reinigungskräfte in besonders sensitiven Bereichen bei der Arbeit beaufsichtigt?

M 2.213 Wartung der technischen Infrastruktur

Verantwortlich für Initiierung: Leiter Haustechnik

Verantwortlich für Umsetzung: Haustechnik

Die von den Herstellern empfohlenen Wartungsintervalle und -vorschriften sollten unbedingt eingehalten werden. Neben der normalen Wartung sollten ältere Anlagen einer größeren Inspektion unterzogen werden, bei denen insbesondere verschlissene Teile erkannt und rechtzeitig ausgetauscht werden. Dies betrifft insbesondere größere Aggregate der Gebäudetechnik, beispielsweise zentrale Heizungs- und Klimatisierungsanlagen, sowie mechanisch stark beanspruchte Anlagen, z. B. Lastenaufzüge für Rechenzentren. Gegebenenfalls sollte die Unterstützung durch technische Sachverständige in Anspruch genommen werden.

Besondere Beanspruchung oder außergewöhnliche Betriebsbedingungen können zu zusätzlichem Wartungsaufwand führen. Zum Beispiel müssen Luftfilter während und nach Bauarbeiten in erheblich kürzeren Intervallen geprüft werden.

Ergänzende Kontrollfragen:

- Werden die Wartungsvorschriften eingehalten?
- Werden die Wartungsintervalle bei besonderen Beanspruchungen diesen angepasst?

M 2.214 Konzeption des IT-Betriebs

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Um einen ordnungsgemäßen und sicheren IT-Betrieb gewährleisten zu können, ist eine übergreifende Konzeption unabdingbar. Es sollten Regelungen bzw. Vorgaben für den Einsatz von IT-Systemen und IT-Produkten in den verschiedenen Bereichen existieren, die gut aufeinander abgestimmt sind und die Sicherheitsziele der Behörde bzw. des Unternehmens widerspiegeln.

Richtlinien für IT-Verfahrensabläufe und IT-Sicherheitsprinzipien

grundlegende IT-Sicherheitsprinzipien abstimmen

Alle an der IT-Planung und am IT-Betrieb beteiligten Organisationseinheiten müssen sich auf grundlegende IT-Sicherheitsprinzipien verständigen, die auf alle Bereiche anzuwenden sind (z. B. Anforderungen an Passwörter). Es muss eine übergreifende Regelung der Authentisierung und Rechtevergabe (siehe M 2.220 *Richtlinien für die Zugriffs- bzw. Zugangskontrolle*) erfolgen.

Verantwortlichkeiten festlegen

Die Verantwortlichkeiten für den Betrieb aller IT-Komponenten müssen klar festgelegt werden. Dazu gehört die Benennung von Administratoren und Ansprechpartnern für die Benutzer (siehe auch M 2.79 *Festlegung der Verantwortlichkeiten im Bereich Standardsoftware*).

Integration neuer Komponenten

Jeder Beschaffung von neuen IT-Komponenten sollte eine Konzeption für deren Einsatz zugrunde liegen. Dabei sollte auch deren Integration in den vorhandenen IT-Verbund betrachtet werden und welche Auswirkungen dies auf vorhandene IT-Sicherheitsmechanismen hat, die evtl. angepasst werden müssen (siehe M 2.216 *Genehmigungsverfahren für IT-Komponenten*).

Test neuer Hard- und Software

Ebenso wie der Ablauf bei der Bestellung von IT muss auch der Umgang mit den gelieferten IT-Komponenten geregelt sein (siehe M 2.90 *Überprüfung der Lieferung*). Bevor neue Hardware-Komponenten oder neue Software zum Einsatz kommen, müssen diese getestet werden (siehe M 4.65 *Test neuer Hard- und Software*).

geregelte Installation und Konfiguration

Jede Installation von IT-Komponenten sollte den grundlegenden IT-Sicherheitszielen der Behörde bzw. des Unternehmens folgen und auf geregelten Verfahren basieren. Abhängig von der jeweiligen IT-Komponente und deren Sicherheitsanforderungen müssen hierbei Zugriffsregelungen, Benutzerrechte und andere sicherheitsrelevante Konfigurationen eingerichtet werden. Grundsätzlich sollte jede Installation nachvollziehbar dokumentiert werden (siehe M 2.87 *Installation und Konfiguration von Standardsoftware*).

Richtlinien für den sicheren IT-Betrieb

Um auch im laufenden Betrieb die Sicherheit aller IT-Systeme aufrechterhalten zu können, müssen eine Vielzahl von Faktoren berücksichtigt werden. Daher sollten alle zur Aufrechterhaltung eines ordnungsgemäßen und sicheren Betriebs notwendigen Aufgaben beschrieben und klar zugeordnet werden. Dies betrifft unter anderem die folgenden Aspekte:

- Die Informationsverarbeitung muss kontinuierlich in allen ihren Phasen, allen Anwendungen und allen Systemen dokumentiert werden (siehe M 2.219 *Kontinuierliche Dokumentation der Informationsverarbeitung*).
- Der Zugang zu allen IT-Systemen sollte geschützt sein, z. B. durch Passwörter.
- Die Funktionen derjenigen IT-Komponenten, die nicht zum Einsatz kommen sollen oder dürfen, sind - wenn möglich - zu sperren (siehe auch M 4.95 *Minimales Betriebssystem*).
- Die Protokollierungsdateien sind in regelmäßigen Abständen auf Anomalien (z. B. Ausführung von Funktionen, die nicht zum Einsatz kommen sollen) zu untersuchen.
- Nach Möglichkeit sollten die IT-Systeme in Abständen einem Integritätstest unterzogen werden, so dass unberechtigte Änderungen so früh wie möglich entdeckt werden können. Dies gilt insbesondere für Konfigurationsdaten.
- Für alle IT-Systeme sollten geeignete Verfahren zur Datensicherung eingesetzt werden.
- Die Einhaltung der IT-Sicherheitsmaßnahmen muss regelmäßig kontrolliert werden (siehe M 2.182 *Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen*).

Standardlösungen für verwendete Hard- oder Software-Komponenten

möglichst einheitliche Komponenten verwenden

Je größer eine Institution ist, desto wichtiger ist es, für die IT-Ausstattung und den IT-Betrieb möglichst einheitliche Komponenten zu verwenden. Dies betrifft sowohl Hardware-Komponenten, wie z. B. Router, Drucker und Grafikkarten, als auch Software-Produkte, wie Betriebssysteme, Textverarbeitungsprogramme und Tools. Anderenfalls besteht die Gefahr, dass das Gesamtsystem aufgrund von Interoperabilitätsproblemen und ausufernder Komplexität nicht mehr administriert werden kann.

Hausstandards definieren

Es sollten daher Hausstandards für Hardware- und Software-Komponenten festgelegt und dokumentiert werden, die bei der Beschaffung zu berücksichtigen sind. Dies erlaubt es, auf bewährte Lösungen zurückzugreifen und Interoperabilitäts- und Kompatibilitätsprobleme möglichst zu vermeiden. Weiterhin wird hierdurch der administrative Aufwand und das erforderliche Fachwissen verringert. In vielen Fällen können auch die Lagerkosten für Verbrauchsmaterial gesenkt werden. In Verbindung mit Rahmenverträgen oder Mengenrabatt können oft auch weitere finanzielle Einsparungen erreicht werden.

Kompatibilität sicherstellen

Aufgrund der schnellen technischen Fortentwicklung im Bereich der Informationsverarbeitung müssen Hausstandards für IT-Komponenten regelmäßig aktualisiert werden. Dies führt in der Regel dazu, dass ein Mischbetrieb zwischen verschiedenen "Generationen" von Hausstandards erforderlich ist. Daher ist bei der Überarbeitung der Hausstandards zu berücksichtigen, dass neue und alte IT-Komponenten bzw. Produkte kompatibel sind und gemeinsam verwendet werden können.

Hausstandards für Arbeitsplatz-PCs

Ein besonders wichtiger Anwendungsfall für Hausstandards sind Arbeitsplatz-PCs. Hier sollte sowohl für die Hardware-Komponenten in den PCs, wie Prozessor, Arbeitsspeicher, Grafikkarte, usw., als auch für die installierte Software und deren Konfigurationen Hausstandards festgelegt werden. Anderenfalls besteht aufgrund der Vielzahl von Konfigurationsmöglichkeiten, die PCs bieten, die Gefahr, dass die eingesetzten Arbeitsplatz-PCs unüberschaubar und somit nicht mehr administrierbar werden. Allein die Pflege der notwendigen Hardware-Treiber für die Betriebssysteme ist in mittelgroßen Behörden und Unternehmen ohne verbindliche Festlegung von Hausstandards nicht mehr leistbar. Durch Hausstandards für Arbeitsplatz-PCs wird auch der Einsatz von Systemmanagement-Produkten erleichtert.

Hinweis: Bei der Definition von Hausstandards für Hardware- oder Software-Komponenten sollte keinesfalls nur das marktgängigste Produkt in Betracht gezogen werden. Vielmehr sollte sich die Auswahl nach den funktionalen Anforderungen und den (IT-)Sicherheitsanforderungen richten. Eine "Monokultur", d. h. die weitgehende Dominanz eines einzelnen Produktes am Markt, kann unter Umständen sogar zu Sicherheitsproblemen führen. In diesem Fall sind nämlich auch die in dem Produkt evtl. vorhandenen Software-Schwachstellen besonders weit verbreitet und können daher, wenn sie ausgenutzt werden, zu hohen Gesamtschäden führen. Computer-Viren, Trojanische Pferde und andere Gefährdungen durch vorsätzliche Handlungen richten sich in vielen Fällen auf weit verbreitete Produkte.

Konventionen für Namens-, Adress- und Nummernräume

Innerhalb einer Institution existieren meist eine ganze Reihe unterschiedlicher Namens- und Nummernräume nebeneinander. Besonders populär sind diejenigen, die auch außerhalb der Behörde bzw. des Unternehmens verwendet werden, beispielsweise E-Mail-Adressen, DNS-Namen, Telefonnummern und Bezeichnungen von Organisationseinheiten. Aber auch rein interne Bezeichnungskonventionen, wie Inventarnummern, IP-Adressen und Ausweisnummern, spielen oft eine wichtige Rolle für die Organisation und das IT-Management.

übergreifendes Konzept für Namens- und Nummernräume

Für einen reibungslosen Ablauf der Informationsverarbeitung und für die Administrierbarkeit der eingesetzten IT ist es erforderlich, dass ein übergreifendes Konzept für die verwendeten Namens- und Nummernräume erstellt wird. Bei der Konzeption sollten folgende Aspekte berücksichtigt werden:

- Möglichst wenig unterschiedliche Namens- und Nummernräume sollten parallel verwendet und gepflegt werden.
- Das Konzept muss Vergabe, Entzug, gegebenenfalls Sperrung von Namen und Nummern sowie das Zusammenspiel der einzelnen Namens- und Nummernräume regeln.
- Namen und Nummern, die nur für Teilbereiche (Organisationseinheiten, Teilnetze, Liegenschaften, usw.) benötigt werden, sollten möglichst aus allgemeinen, behörden- bzw. unternehmensweiten Namens- bzw. Nummernräumen abgeleitet werden.

- Die Struktur der verwendeten Namens- und Nummernräume sollte möglichst einfach, allgemein und ohne unnötige Ausnahmen sein, auch wenn dies bedeutet, dass die Bezeichnungen länger werden (z. B. mehr Ziffern enthalten). Anderenfalls besteht die Gefahr, dass die Bezeichnungen fehlinterpretiert oder von gängigen Produkten nicht verarbeitet werden können.

unnötige Ausnahmen vermeiden

- Bei der Konzeption ist das absehbare mittelfristige Wachstum zu berücksichtigen, das durch den Namens- bzw. Nummernraum versorgt werden muss. In jedem Fall sind großzügige Reserven einzuplanen. Nachträgliche Erweiterungen oder Migrationen auf größere Namens- oder Nummernräume sind oft zeit- und kostenintensiv.

Reserven einplanen

- Wenn Kollisionen, d. h. mehrfache Vergabe des gleichen Bezeichners oder der gleichen Nummer, durch das generelle Vergabesystem möglich sind, so ist im Konzept festzulegen, wie diese aufgelöst werden. Ein wichtiges Beispiel ist die Konvention *Vorname.Nachname* für E-Mail-Adressen. Hier muss im Konzept definiert werden, welche Adressen ersatzweise vergeben werden, wenn in der Behörde bzw. im Unternehmen zwei oder mehr Mitarbeiter mit gleichen Vor- und Nachnamen beschäftigt werden.

Kollisionen auflösen

Schnittstellendefinitionen für das Zusammenspiel der Komponenten

Die Informationsverarbeitung geschieht in der Regel durch eine Vielzahl kleiner Verarbeitungsschritte, die durch geeignete Hardware- oder Software-Komponenten unterstützt werden. Der Datentransfer zwischen diesen Komponenten erfolgt in der Regel über Dateien, Datenbanken oder Netze.

Um einen reibungslosen IT-Betrieb gewährleisten zu können ist es daher erforderlich, die Schnittstellen für das Zusammenspiel der einzelnen Komponenten klar zu definieren. Alle Schnittstellendefinitionen sollten dokumentiert werden, sofern sie nicht von den verwendeten Komponenten her selbstverständlich sind.

Schnittstellen definieren und dokumentieren

Wichtige Aspekte von Schnittstellendefinitionen zwischen IT-Komponenten sind beispielsweise Datei- und Datenformate sowie Netzprotokolle. Um bei Bedarf einzelne Komponenten möglichst problemlos austauschen zu können (Investitionsschutz) und um auf praxisbewährte Lösungen zurückgreifen zu können, sollten so weit wie möglich Standardformate und Standardprotokolle verwendet werden, beispielsweise EDI, XML und HTTP.

Standardformate und Standardprotokolle verwenden

Alle Änderungen an Schnittstellendefinitionen zwischen den verwendeten IT-Komponenten müssen dokumentiert und in Bezug auf Auswirkungen auf die Sicherheit des IT-Verbunds geprüft werden. Falls erforderlich ist das IT-Sicherheitskonzept entsprechend zu ergänzen bzw. anzupassen.

Auswirkungen auf die IT-Sicherheit prüfen

Ergänzende Kontrollfragen:

- Gibt es Richtlinien für IT-Verfahrensabläufe und den sicheren IT-Betrieb?
- Wurden Hausstandards für verwendete Hardware- und Software-Komponenten festgelegt?
- Existiert ein übergreifendes Konzept für den Einsatz von Namens-, Adress- und Nummernräumen?

M 2.215 Fehlerbehandlung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Benutzer, Administrator

Alle Fehler, die IT-Systeme oder Kommunikationsverbindungen betreffen, müssen gemeldet und protokolliert werden. Hiervon sind natürlich alle Fehlermeldungen ausgenommen, die aufgrund von Plausibilitätsprüfungen angezeigt werden, also z. B. durch fehlerhafte Benutzereingaben hervorgerufen werden. Es muss gewährleistet sein, dass die gemeldeten Fehler schnellstmöglich behoben werden.

Information der Benutzer

Die Untersuchung und Beseitigung von Fehlern sollte nur von entsprechend geschultem Personal durchgeführt werden. Alle Benutzer sollten darüber informiert sein, wer beim Auftreten von Fehlern oder Problemen mit IT-Systemen zu benachrichtigen ist. Außerdem sollten die Benutzer über Fehler, die das Arbeiten mit IT-Systemen beeinträchtigen können, informiert werden, ebenso über deren Behebung.

Protokollierung

Die Protokolle über gemeldete Fehler sollten folgende Angaben enthalten:

- Bezeichnung und Versionsnummer der betroffenen IT-Systeme und Software,
- den Zeitpunkt der Meldung,
- eine Beschreibung, ob bzw. inwiefern die Nutzung der betroffenen IT-Systeme eingeschränkt ist,
- den Namen des für die Behebung Verantwortlichen sowie
- den Zeitpunkt der Fehlerbehebung.

In einigen Fällen kann es sinnvoll oder notwendig sein, aufgetretene Fehler nicht zu beheben, z. B. wenn kein zuverlässiger Patch vorhanden ist oder ein Ersatzteil nicht beschafft werden kann. Dann sollte im Protokoll vermerkt werden, ob die betroffene IT-Komponente mit Funktionseinschränkungen weiter betrieben werden kann.

Diese Protokolle sollten regelmäßig daraufhin überprüft werden, ob sie aktuell sind und ob alle gemeldeten Fehler behoben wurden.

sorgfältige Bereinigung der Fehler

Fehler sollten nur von den dafür benannten Verantwortlichen korrigiert werden. Die Fehlerbeseitigung muss im Rahmen der IT-Sicherheitsrichtlinien der jeweiligen Institution erfolgen. Wenn für die Fehlerbehebung Patches oder Updates benötigt werden, sollten diese direkt vom Hersteller oder von vertrauenswürdigen Stellen bezogen werden (siehe auch M 4.107 *Nutzung von Hersteller-Ressourcen*). Größere Korrekturmaßnahmen müssen zunächst auf vom Wirknetz getrennten Systemen getestet werden, da diese auch unerwünschte Nebeneffekte haben können. Nach der Fehlerbeseitigung müssen eventuell die geänderten IT-Systeme bzw. Komponenten erneut abgenommen und freigegeben werden (siehe M 2.62 *Software-Abnahme- und Freigabe-Verfahren*).

Ergänzende Kontrollfragen:

- Gibt es ein festgelegtes Verfahren für die Fehlerbehandlung?
- Werden Fehler ausschließlich von der fachlich zuständigen Stelle beseitigt?

M 2.216 Genehmigungsverfahren für IT-Komponenten

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Die Beschaffung, die Installation und der Betrieb von IT-Komponenten **aller Art** muss koordiniert und genehmigt sein. Es muss geregelt sein, wie IT-Komponenten abgenommen, freigegeben, installiert bzw. benutzt werden. Dies betrifft beispielsweise den Einsatz von Modems, Diskettenlaufwerken, Software und Mobiltelefonen. Eine entsprechende Vorgehensweise für den Bereich Standardsoftware ist in Baustein B 1.10 *Standardsoftware* beschrieben. Dabei wird der gesamte Lebenszyklus von Standardsoftware betrachtet: Erstellung eines Anforderungskataloges, Vorauswahl eines geeigneten Produktes, Test, Freigabe, Installation, Lizenzverwaltung und Deinstallation. Um eine analoge Vorgehensweise für andere IT-Komponenten zu entwickeln, kann sich ebenfalls an diesem Baustein orientiert werden.

Im Rahmen des Genehmigungsverfahrens von neuen IT-Komponenten müssen

- die generelle Funktionstüchtigkeit untersucht werden (siehe auch M 4.65 *Test neuer Hard- und Software*),
- deren Sicherheitseigenschaften bewertet werden,
- mögliche Sicherheitsrisiken, die durch diese IT-Komponenten entstehen könnten, untersucht und bewertet sowie weitestgehend behoben werden,
- alle ihre Sicherheitseigenschaften (sowohl die positiven als auch die negativen) sorgfältig dokumentiert werden,
- auf dieser Basis Installationsanweisungen erarbeitet werden.

Dokumentation aller sicherheitsrelevanten Einstellungen

Während des Genehmigungsverfahrens sollten außerdem Installations- bzw. Konfigurationsanleitungen erarbeitet werden, in denen auch alle sicherheitsrelevanten Einstellungen dokumentiert sind. Auch nach der Erstinstallation von IT-Komponenten müssen diese weitergepflegt werden (siehe auch M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen*). Vor der Inbetriebnahme neuer IT-Komponenten sind (sofern erforderlich) die Administratoren bzw. die Benutzer in deren Anwendung zu schulen.

Die Installation und Benutzung nicht freigegebener IT-Komponenten muss verboten und die Einhaltung dieses Verbotes regelmäßig kontrolliert werden.

Ergänzende Kontrollfragen:

- Gibt es Genehmigungs- und Registrierverfahren für IT-Komponenten **aller Art**?
- Werden alle Schritte bei der Abnahme und Freigabe von IT-Komponenten sorgfältig dokumentiert?

M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Grundsätzlich sollten Mitarbeiter natürlich sorgfältig mit allen Informationen umgehen. Darüber hinaus gibt es aber in vielen Bereichen Daten, die einen höheren Schutzbedarf haben oder besonderen Restriktionen unterliegen, z. B. personenbezogene, finanzrelevante, vertrauliche oder Copyright-geschützte Daten. Für diese gelten je nach ihrer Kategorisierung unterschiedliche Beschränkungen im Umgang mit ihnen. Daher ist es wichtig, alle Mitarbeiter auf die für diese Daten geltenden Restriktionen hinzuweisen (siehe auch M 3.2 *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*).

Der Schutzbedarf von Daten wirkt sich natürlich unmittelbar auf alle Medien aus, auf denen diese gespeichert oder verarbeitet werden. Daten mit besonderem Schutzbedarf können in den unterschiedlichsten Bereichen anfallen, z. B. bei Fax oder E-Mail. Es sollte also in allen Bereichen Regelungen geben, in denen beispielsweise auch festgelegt ist, wer solche Daten lesen, bearbeiten bzw. weitergeben darf (siehe z. B. M 2.42 *Festlegung der möglichen Kommunikationspartner*). Dazu gehört auch die regelmäßige Überprüfung auf Korrektheit und Vollständigkeit der Daten (siehe auch M 4.64 *Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen*).

Einschränkung der Weitergabe

Viele Informationen, aber auch IT-Anwendungen, unterliegen Copyright-Vermerken oder Weitergaberestriktionen ("Nur für den internen Gebrauch"). Alle Mitarbeiter müssen darauf hingewiesen werden, dass weder Dokumente, noch Dateien oder Software ohne Berücksichtigung evtl. Copyright-Vermerke oder Lizenzbedingungen kopiert werden dürfen.

Schutz geschäftskritischer Informationen

Ein besonderes Augenmerk muss auch auf alle Informationen gelegt werden, die die Grundlage für die Aufgabenerfüllung bilden. Dazu gehören alle geschäftsrelevanten Daten, also z. B. diejenigen Daten, bei deren Verlust die Institution handlungsunfähig wird, die die wirtschaftlichen Beziehungen zusammenarbeitender Unternehmen beeinträchtigen können oder aus deren Kenntnis ein Dritter (z. B. Konkurrenzunternehmen) finanzielle Vorteile ziehen kann. Jede Behörde und jedes Unternehmen sollte eine Übersicht darüber haben, welche Daten als geschäftskritisch einzustufen sind. Neben den allgemeinen Sorgfaltspflichten können auch hier für diese Daten bei der Speicherung, Verarbeitung, Weitergabe und Vernichtung besondere Vorschriften und Regelungen gelten. Geschäftskritische Informationen müssen vor Verlust, Manipulation und Verfälschung geschützt werden. Längerfristig gespeicherte oder archivierte Daten müssen regelmäßig auf ihre Lesbarkeit getestet werden. Nicht mehr benötigte Informationen müssen zuverlässig gelöscht werden (siehe auch M 2.167 *Sicheres Löschen von Datenträgern*).

Ergänzende Kontrollfragen:

- Werden die Mitarbeiter regelmäßig auf den sorgfältigen Umgang mit Informationen hingewiesen?
- Sind alle Informationen entsprechend ihrem Schutzbedarf eingestuft worden?

M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Die IT-Komponenten, die innerhalb einer hauseigenen Liegenschaft eingesetzt werden, sind im Allgemeinen durch infrastrukturelle Sicherheitsmaßnahmen ausreichend vor Missbrauch und Diebstahl geschützt. Häufig sollen aber IT-Systeme oder Datenträger auch außer Haus eingesetzt werden, z. B. bei Dienstreisen oder Telearbeit. Um auch diese ausreichend schützen zu können, muss die Mitnahme von Datenträgern und IT-Komponenten klar geregelt werden.

Dabei muss festgelegt werden, **Regelung**

- welche IT-Komponenten bzw. Datenträger außer Haus mitgenommen werden dürfen, **Welche Komponenten?**
- wer IT-Komponenten bzw. Datenträger außer Haus mitnehmen darf, **Wer darf?**
- welche grundlegenden IT-Sicherheitsmaßnahmen dabei beachtet werden müssen (Virenschutz, Verschlüsselung sensitiver Daten, Aufbewahrung, etc.). **Was ist zu beachten?**

Die Art und der Umfang der anzuwendenden IT-Sicherheitsmaßnahmen für extern eingesetzte IT-Komponenten hängt einerseits vom Schutzbedarf der darauf gespeicherten IT-Anwendungen und Daten und andererseits von der Sicherheit der Einsatz- bzw. Aufbewahrungsorte ab.

Grundsätzlich sollte für alle IT-Komponenten, die extern eingesetzt werden sollen, eine entsprechende Genehmigung eingeholt werden.

Bei größeren Institutionen, bei denen der Zutritt zu den Liegenschaften durch Pförtner bzw. Wachdienste kontrolliert wird, sollte überlegt werden, ob diese angewiesen werden sollten, in Stichproben zu überprüfen, inwieweit die Regelungen für die Mitnahme von Datenträgern und IT-Komponenten eingehalten werden. **ggf. Stichprobe veranlassen**

Außerhalb der organisationseigenen Liegenschaften sind die Benutzer für den Schutz der ihnen anvertrauten IT verantwortlich. Darauf und auf die zu ergreifenden Vorsichtsmaßnahmen sind sie hinzuweisen. Dazu gehören folgende Regeln:

- IT-Systeme müssen stets sicher aufbewahrt werden. Bei Dienstreisen sollten sie nicht unbeaufsichtigt gelassen werden. Insbesondere sollten sie nicht in Fahrzeugen zurückgelassen werden (siehe auch M 1.33 *Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz*). **Aufbewahrung**
- IT-Systeme wie Laptops oder Mobiltelefone und deren Anwendungen können im Allgemeinen durch PINs oder Passwörter abgesichert werden. Diese Mechanismen sollten auch genutzt werden. **Zugriffsschutz**

- IT-Systeme oder Datenträger, die sensitive Daten enthalten, sollten möglichst komplett verschlüsselt werden (siehe auch M 4.29 *Einsatz eines Verschlüsselungsprodukte für tragbare PCs*). **Verschlüsselung**
- Die Verwaltung, Wartung und Weitergabe von extern eingesetzten IT-Systemen sollte geregelt werden. Hierzu können beispielsweise Pools eingerichtet werden (siehe auch M 1.35 *Sammelaufbewahrung mehrerer tragbarer PCs* bzw. M 2.190 *Einrichtung eines Mobiltelefon-Pools*). **Verwaltung**
- Es sollte protokolliert werden, wann und von wem welche IT-Komponenten außer Haus eingesetzt wurden. **Protokollierung**

Ergänzende Kontrollfragen:

- Gibt es Regelungen für die Mitnahme von IT-Komponenten aller Art?
- Werden die Benutzer von extern eingesetzten IT-Komponenten auf die Regelungen hingewiesen, die von ihnen einzuhalten sind?
- Werden die Benutzer von extern eingesetzten IT-Komponenten auf deren geeignete Aufbewahrung hingewiesen?

M 2.219 Kontinuierliche Dokumentation der Informationsverarbeitung

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Die Informationsverarbeitung muss kontinuierlich in allen Phasen, allen Anwendungen und allen Systemen dokumentiert werden, um einen ordnungsgemäßen IT-Betrieb gewährleisten zu können. Dazu gehören:

- eine aktuelle Dokumentation aller vorhandenen IT-Systeme und deren Konfiguration (siehe M 2.25 *Dokumentation der Systemkonfiguration*), **Konfiguration**
- die Dokumentation der auf den jeweiligen IT-Systemen eingerichteten Benutzer und deren Rechteprofile (siehe M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*), dies umfasst auch eine Beschreibung und Begründung aller Einschränkungen bei der Nutzung von IT-Systemen (Rechte und Ressourcen), **Rechteprofile**
- die neu hinzugekommenen Hard- und Softwarekomponenten müssen in der Systemdokumentation aufgeführt werden (siehe M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*), **Veränderungen**
- die Dokumentation aller sicherheitsrelevanten Abläufe wie der Datensicherung (siehe M 6.37 *Dokumentation der Datensicherung*) oder der Vernichtung von Datenträgern, **sicherheitsrelevante Abläufe**
- die Dokumentation der Wartungsmaßnahmen (siehe M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*), **Wartung**
- eine Beschreibung aller gefundenen und behobenen Fehler (siehe M 2.215 *Fehlerbehandlung*). **Fehlerbehandlung**

Die Benennung der Systemverantwortlichen (siehe M 2.26 *Ernennung eines Administrators und eines Vertreters*) sollte ebenfalls schriftlich erfolgen und den Benutzern bekannt gegeben werden.

Für Problemfälle sollte dokumentiert sein, wer helfen kann und wo Informationen zu finden sind (M 6.59 *Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen*). **Ansprechpartner**

Ergänzende Kontrollfragen:

- Wird die Informationsverarbeitung in allen Phasen, allen Anwendungen und allen Systemen dokumentiert?
- Gibt es Regelungen für die Dokumentation der Informationsverarbeitung?

M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Fachverantwortliche

Um IT-Systeme bzw. System-Komponenten und Netze nutzen zu können bzw. um dort gespeicherte Informationen abrufen zu können, muss die Zugriffs- bzw. Zugangskontrolle geregelt sein. Neben den an den einzelnen IT-Komponenten einzurichtenden Zugriffs- bzw. Zugangskontrollen sollte eine übergreifende Richtlinie hierzu existieren, in der die Grundsatzfragen geregelt sind. Die Regelungen zur Zugriffs- bzw. Zugangskontrolle müssen den Schutzbedarf der Behörde bzw. des Unternehmens widerspiegeln. Insbesondere ist hier auf die Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen, also z. B. Datenschutz- und Urheberrechtsgesetze bzw. Lizenzregelungen, zu verweisen.

Standard-Rechteprofile

Es empfiehlt sich, dabei Standard-Rechteprofile für nutzungsberechtigte Personen aufgrund ihrer Funktionen und Aufgaben festzulegen (siehe auch M 2.8 *Vergabe von Zugriffsrechten*). Die Benutzerrechte für Zugriffe auf Dateien und Programme müssen abhängig von der jeweiligen Rolle, dem Need-to-Know und der Sensitivität der Daten definiert sein. Falls Rechte vergeben werden, die über den Standard hinausgehen, sollte dies begründet werden.

Die Richtlinien für die Zugriffs- bzw. Zugangskontrolle sollte allen Verantwortlichen für IT-Anwendungen vorliegen. Darauf aufbauend können dann Zugriffsregelungen für die einzelnen IT-Systeme abgeleitet und eingerichtet werden.

Regelungen auf IT-Systeme anpassen

Für jedes einzelne IT-Systeme und jede IT-Anwendung sollten schriftliche Zugriffsregelungen und die Dokumentation der Einrichtung von Benutzern und der Rechtevergabe vorhanden sein (siehe M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*). Hierbei müssen die system- bzw. anwendungsspezifischen Besonderheiten und Sicherheitsanforderungen berücksichtigt werden. Verantwortlich für die Erstellung und Aktualisierung der system- bzw. anwendungsspezifischen Vorgaben sind die IT-Verantwortlichen.

Restriktive Rechtevergabe

Werden an Mitarbeiter besonders weitgehende Rechte vergeben (z. B. an Administratoren), so sollte dies möglichst restriktiv erfolgen. Hierbei sollte zum einem der Kreis der privilegierten Benutzer möglichst eingeschränkt werden und zum anderen nur die für die Durchführung der Arbeit benötigten Rechte vergeben werden (siehe auch M 2.38 *Aufteilung der Administrationstätigkeiten*). Für alle Aufgaben, die ohne erweiterte Rechte durchgeführt werden können, sollten auch privilegierte Benutzer unter Accounts mit Standard-Rechten arbeiten.

kein Zugriff ohne Authentikation

Der Zugriff auf alle IT-Systeme oder Dienste muss durch Identifikation und Authentikation des zugreifenden Benutzers oder IT-Systems abgesichert werden. Beim Zugriff aus externen Netzen sollten starke Authentisierungs-

verfahren eingesetzt werden, also solche die z. B. auf dem Einsatz von Einmalpasswörtern oder dem Besitz von Chipkarten basieren.

Beim Anmeldevorgang sollten keine Informationen über das IT-System oder den Fortschritt der Anmeldeprozedur angezeigt werden, bis dieser erfolgreich abgeschlossen ist. Es sollte dabei darauf hingewiesen werden, dass der Zugriff nur autorisierten Benutzern gestattet ist. Die Authentikationsdaten dürfen erst dann überprüft werden, wenn sie vollständig eingegeben wurden. Weitere Anforderungen an die Authentikationsmechanismen finden sich in M 4.133 *Geeignete Auswahl von Authentikations-Mechanismen*.

Ergänzende Kontrollfragen:

- Gibt es Richtlinien für die Zugriffs- bzw. Zugangskontrolle?
- Gibt es Standard-Rechteprofile für verschiedene Funktionen bzw. Aufgaben?

M 2.221 Änderungsmanagement

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Fachverantwortliche

Bei der Komplexität heutiger IT-Systeme können bereits kleine Änderungen an laufenden Systemen zu Sicherheitsproblemen führen, z. B. durch unerwartetes Systemverhalten oder Systemausfälle.

In bezug auf IT-Sicherheit ist es Aufgabe des Änderungsmanagements, neue Sicherheitsanforderungen zu erkennen, die sich aus Änderungen an IT-Systemen ergeben. Sind signifikante Hardware- oder Software-Änderungen an einem IT-System geplant, so sind die Auswirkungen auf die Sicherheit des Gesamtsystems zu untersuchen. Änderungen an einem IT-System dürfen nicht zu einer Verringerung der Effizienz von einzelnen Sicherheitsmaßnahmen und damit einer Gefährdung der Gesamtsicherheit führen.

Richtlinien für Änderungen

Daher sollte es Richtlinien für die Durchführung von Änderungen an IT-Komponenten, Software oder Konfigurationsdaten geben (siehe M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen*). Alle Änderungen an IT-Komponenten, Software oder Konfigurationsdaten sollten geplant, getestet, genehmigt und dokumentiert werden. Es ist dafür Sorge zu tragen, dass auf alle sicherheitsrelevanten Änderungen angemessen reagiert wird. Dazu gehören zum Beispiel:

- Änderungen an IT-Systemen (neue Applikationen, neue Hardware, neue Netzwerkverbindungen, Modifikationen an der eingesetzten Software, Einspielen von Sicherheitspatches, Aufrüstung der Hardware, ...),
- Änderungen in der Aufgabenstellung oder in der Wichtigkeit der Aufgabe für die Institution,
- Änderungen in der Benutzerstruktur (neue, etwa externe oder anonyme, Benutzergruppen),
- räumliche Änderungen, z. B. nach einem Umzug.

Rückfalllösung

Bevor Änderungen genehmigt und durchgeführt werden, muss durch Prüfung und Test der geplanten Aktionen sichergestellt werden, dass das Sicherheitsniveau während und nach der Änderung erhalten bleibt. Wenn Risiken, insbesondere für die Verfügbarkeit, nicht ausgeschlossen werden können, muss die Planung auch eine Rückfalllösung vorsehen und Kriterien vorgeben, wann diese zum Tragen kommen soll.

Dokumentation der Änderungen

Alle Änderungen und die dazugehörigen Entscheidungsgrundlagen sind zu dokumentieren. Dies gilt sowohl in der Betriebs- als auch in einer Testumgebung.

Beim Änderungsmanagement ist das Berechtigungskonzept zur Durchführung von Änderungen ein wichtiger Punkt:

- Nur diejenigen, die Änderungen durchführen dürfen, sollten Zugriffsberechtigungen auf die dafür relevanten Systembereiche haben.

- Es sollte Mechanismen geben, die sicherstellen, dass alle wesentlichen Änderungen vorher abgestimmt wurden.

Hinweis: Bei der Durchführung von Änderungen sollte immer beachtet werden, dass Änderungen eines IT-Systems oder seiner Einsatzbedingungen

- Änderungen in der Umsetzung des IT-Sicherheitsplanes,
- die Erstellung eines neuen IT-Sicherheitskonzepts oder sogar
- die Überarbeitung der organisationsweiten IT-Sicherheitspolitik

erforderlich machen können. Bei größeren Änderungen sollte daher das IT-Sicherheitsmanagement involviert werden.

Ergänzende Kontrollfragen:

- Gibt es Richtlinien für die Durchführung von Änderungen an IT-Komponenten, Software oder Konfigurationsdaten?
- Werden alle Änderungen getestet und dokumentiert?
- Wird bei größeren Änderungen das IT-Sicherheitsmanagement beteiligt?

M 2.222 Regelmäßige Kontrollen der technischen IT-Sicherheitsmaßnahmen

Diese Maßnahme ist entfallen.

M 2.223 Sicherheitsvorgaben für die Nutzung von Standardsoftware

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

In den meisten Büroumgebungen wird für die typischen Büroaufgaben Standardsoftware eingesetzt. Dazu gehören z. B. Textverarbeitungsprogramme (Word, WordPerfect, StarOffice), Tabellenkalkulation, Büro-Kommunikationssysteme, E-Mail-Programme und Datenbanken. Da diese häufig komplett von einem Anbieter gekauft werden, wird hier auch von Office-Paketen gesprochen. Durch die hohe Verbreitung gleichartiger Software können Sicherheitslücken in diesen Programmen große Auswirkungen haben, da sie an vielen IT-Systemen ausgenutzt werden können und sich Schadprogramme sehr schnell weiterverbreiten. Ein typisches Beispiel hierfür sind Makro-Viren (siehe G 5.43 *Makro-Viren*).

Um solche Probleme vermeiden bzw. reduzieren zu können, sollten daher Sicherheitsrichtlinien bei der Nutzung von Standardsoftware festgelegt werden.

Benutzer über Eignung und Sicherheitsfunktionen informieren

Standardsoftware ist im Allgemeinen nicht auf ein hohes IT-Sicherheitsniveau ausgelegt. Alle Mitarbeiter sollten daher darauf hingewiesen werden, dass besonders schutzbedürftige Informationen nicht ohne weitere IT-Sicherheitsmaßnahmen auf einem Standard-Büroarbeitsplatz verarbeitet werden sollten. Einige der Standardprodukte bieten aber trotzdem eine Reihe von IT-Sicherheitsfunktionen an, die aber meist deutlich weniger Sicherheit bieten als spezielle Sicherheitsprodukte. Die Benutzer sollten über diese Sicherheitsfunktionen und deren Wirksamkeit informiert werden (siehe auch M 4.30 *Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen*). Dabei ist vor allen Dingen sicherzustellen, dass die Benutzer sich nicht in einer falschen, trügerischen Sicherheit wiegen und dass die Nutzung dieser Sicherheitsfunktionen keine Sicherheitslücken öffnet. Benutzer sollten darüber informiert werden, dass Office-Produkte nicht für jeden beliebigen Einsatzzweck geeignet sind.

Daneben bieten Office-Pakete häufig Funktionen, die den Austausch von Informationen erleichtern sollen, die aber häufig bereits in der Konzeption große Sicherheitsprobleme mit sich bringen.

Beispiele:

- **Nutzung gemeinsamer Terminkalender**

  Um die Koordination innerhalb von Arbeitsgruppen zu erleichtern, lassen sich die meisten elektronischen Terminkalender untereinander vernetzen. Neben vielen Vorteilen bringt dies aber auch einige Probleme mit sich. So will nicht jeder Mitarbeiter alle seine Termine den Kollegen offen legen. Darauf haben die Hersteller reagiert, in dem sie hier die Möglichkeit bieten, anderen nur die freien bzw. belegten Zeiten anzuzeigen. Viele Mitarbeiter glauben aber zum einen, dass es einen schlechten Eindruck macht, wenn hier viel freie Zeit angezeigt wird, und befürchten zum anderen, dass

jede freie Minute von Kollegen mit Terminen besetzt wird. Dies führt dann dazu, dass große Zeiträume auf Vorrat blockiert werden.

Daneben kann es auch zu anderen Problemen kommen, z. B. durch zu großzügige Rechtevergabe (siehe auch G 3.20 *Ungewollte Freigabe des Leserechtes bei Schedule+*).

Es sollte daher Richtlinien für die Verwendung vernetzter Terminkalender und die hierbei zu beachtenden Zugriffsrechte geben. Diese sollten frühzeitig mit dem Personal- bzw. Betriebsrat abgestimmt werden. Bei der Einführung von vernetzten Terminkalendern sollten außerdem alle Mitarbeiter in den richtigen Umgang damit eingewiesen werden.

- **automatischer Start von CD-ROMs**

  Unter allen neueren Windows-Betriebssystemen können CD-ROMs automatisch erkannt und gestartet werden. Dadurch können auch Schadprogramme wie Viren oder Trojanische Pferde auf den Rechner gelangen werden. Die automatische CD-ROM-Erkennung sollte daher ausgeschaltet werden (siehe M 4.57 *Deaktivieren der automatischen CD-ROM-Erkennung*).

- **OLE (Object Linking And Embedding, Dienst zum Verknüpfen und Einbetten von Objekten)**

  Über OLE-Funktionen können Objekte in Dateien eingebettet werden. Diese werden in vielen Office-Produkten benutzt, um Informationen anderen Programmen zur Verfügung zu stellen. Hierüber kann beispielsweise eine in Excel erstellte Tabelle in einem Word-Dokument eingebettet werden. Damit werden aber nicht nur die in dem Tabellenausschnitt dargestellte Informationen, sondern u. U. alle in der Excel-Datei enthaltenen Informationen in die Word-Datei übertragen. Wenn die Word-Datei dann weitergegeben wird, kann der Empfänger dann auch die Excel-Datei einsehen und sogar verändern, auch wenn diese durch ein Passwort lese- oder schreibgeschützt war.

  Um dies zu verhindern, sollte in diesem Beispiel die Tabelle als Text in die Word-Datei kopiert werden. Nur wenn die Ursprungs-Excel-Datei keine anderen Informationen enthält, als solche, die weitergegeben werden sollen, sollte sie in einer andere Datei eingebettet werden. Dies kann z. B. durch Anlegen einer neuen Excel-Datei erreicht werden (siehe auch M 4.64 *Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen*).

- **PostScript /ghostscript**

  In PostScript-Dateien kann es zu Problemen ähnlich wie bei Makro-Viren kommen. Bei Anzeige-Programmen für PostScript handelt es sich um Interpreter, die die PostScript-Sprache abarbeiten. Ab Level 2.0 der PostScript-Spezifikation gibt es auch PostScript-Befehle, um Dateien zu schreiben. Dadurch ist es möglich, PostScript-Dateien zu erzeugen, die während der Bearbeitung durch einen Interpreter, auch bereits bei der Anzeige am Bildschirm, andere Dateien modifizieren, löschen oder umbenennen können.

Konkrete Probleme existieren bei dem Programm *ghostscript* (*gs*). In den Unix-Versionen können die Schreibmöglichkeiten auf Dateien mit der Option *-dSAFER* abgeschaltet werden. Allerdings ist dies nicht die Voreinstellung. In Versionen für andere Betriebssysteme heißt diese Option ähnlich.

Die Verwendung der Option *-dSAFER* wird dem Benutzer überlassen. Dies hat auch zur Folge, dass zahlreiche andere Programme, die intern *ghostscript* (*gs*) aufrufen (z. B. *netscape*, *xdvi*, *xfig*, *xv* etc.), dies unterschiedlich realisieren. Die Option sollte daher als Default eingestellt werden. Beschreibungen, wie dies zu realisieren ist, finden sich in den Sicherheitsbulletins des DFN-CERT DSB-95:02 und DSB-95:03 vom 24. August 1995 (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*).

Bei älteren *ghostscript*-Versionen kann es daneben weitere PostScript-Befehle geben, mit denen Dateien modifiziert werden können. Es sollten nur *ghostscript*-Versionen eingesetzt werden, bei denen diese Probleme beseitigt wurden.

Das Programm *ghostview*, mit dem sich PostScript-Dateien anzeigen lassen, bietet ab der Version 1.5 eine Option *-safer* an, die die Sicherheitsfunktionen von *ghostscript* aktiviert. Versionen vor 1.5 bieten diesen Schutz nicht und sollten durch die aktuelle Version ersetzt werden. Ein ähnliches Programm zur Anzeige von PostScript-Dateien ist *gv*. Hier sollte im Dialogfeld "Ghostscript Options" die Schaltfläche "Safer" aktiviert sein. Beim PostScript-Viewer *GSview*, der für Windows und OS/2 zur Verfügung steht, sollte die Option "Schreibschutz für Dateien" eingeschaltet sein.

- **PDF (Portable Document Format)**

  Auch bei PDF-Dateien kann es zu ähnlichen Problemen kommen, wenn zum Anzeigen dieser Dateien ältere Versionen des Acrobat Readers eingesetzt werden. In PDF-Dateien lassen sich Funktionen wie Programmaufrufe einbetten, die ein Sicherheitsrisiko für die Dateien des lokalen IT-Systems darstellen. Daher sollte zur Anzeige von PDF-Dateien ein Viewer verwendet werden, der

  - diese Funktionalität nicht unterstützt oder
  - geeignete Sicherheitsmechanismen für die Ausführung von Makros bereitstellt (beispielsweise aktuelle Versionen des Acrobat Readers).

  Anderenfalls besteht die Gefahr, dass die eingebetteten Funktionen bereits beim Öffnen des Dokuments oder durch das Bewegen im Dokument über so genannte *Action Trigger* gestartet werden, ohne dass sich der Leser dessen bewusst ist.

- **Schnellspeicherung unter Word**

  Word besitzt die Möglichkeit der Schnellspeicherung von erstellten Texten. Dies führt dazu, dass nur die aktuell vorgenommenen Änderungen an einem Dokument gespeichert werden. Dieser Vorgang nimmt nicht so viel Zeit in Anspruch wie ein vollständiger Speichervorgang, bei dem

Word das vollständige überarbeitete Dokument speichert. Ein vollständiger Speichervorgang erfordert jedoch weniger Festplattenspeicher als eine Schnellspeicherung. Der entscheidende Nachteil der Schnellspeicherung ist aber, dass die Datei unter Umständen Textfragmente enthalten kann, die der Verfasser nicht weitergeben möchte.

Grundsätzlich sollte daher die Option "Schnellspeicherung zulassen" abgeschaltet werden. Des weiteren sollte die Option "Erstellung einer Sicherungskopie" aktiviert sein. Das System sollte regelmäßig durch Löschen der nicht mehr benötigten Sicherungskopien gesäubert werden.

Entscheidet sich der Benutzer trotzdem für die Schnellspeicheroption, sollte er bei folgenden Situationen immer einen vollständigen Speichervorgang durchführen:

- Sobald die Bearbeitung eines Dokuments abgeschlossen worden ist.
- Bevor eine Aufgabe ausgeführt wird, die viel Speicherplatz in Anspruch nimmt, z. B. die Suche nach Text oder das Kompilieren eines Indexes.
- Bevor der Dokumenttext in eine andere Anwendung übertragen wird.
- Bevor das Dokument in ein anderes Dateiformat konvertiert wird.

Informationen über Sicherheitslücken einholen

Um gegen Konzeptionsschwächen und bekannt gewordene Sicherheitslücken rechtzeitig Maßnahmen ergreifen zu können, sollte sich der Administrator bzw. das IT-Sicherheitsmanagement regelmäßig über solche Probleme informieren (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*).

Ergänzende Kontrollfragen

- Wurden die Benutzer über die Sicherheitsfunktionen in Anwendungsprogrammen und deren Wirksamkeit informiert?
- Wurde überprüft, dass die Option *-dSAFER* bei den eingesetzten PostScript-Interpretern aktiviert ist?

M 2.224 Vorbeugung gegen Trojanische Pferde

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Ein Trojanisches Pferd ist ein Programm mit einer Schadensfunktion, das in ein anderes Programm verdeckt eingebettet ist. Trojanische Pferde werden verbreitet, indem sie in möglichst "attraktive" Wirtsprogramme integriert werden, die dann beispielsweise zum Download angeboten oder als Anhang an E-Mails verschickt werden. Neben unmittelbaren Schäden können über Trojanische Pferde Informationen nicht nur über den einzelnen Rechner, sondern auch über das lokale Netzwerk ausspäht werden.

Benutzer immer wieder informieren!

Es ist schwierig, sich gegen Trojanische Pferde zu schützen, da diese in vielerlei Dateien versteckt sein können. Daher ist es wichtig, alle Benutzer immer wieder über die Problematik Trojanischer Pferde aufzuklären. Wichtige Verhaltensregeln sind aus diesem Grunde:

- Daten und Programme, die aus dem Internet abgerufen werden, stellen einen Hauptverbreitungsweg für Computer-Viren und Trojanische Pferde dar, um Benutzerdaten auszuspähen, weiterzuleiten, zu verändern oder zu löschen. Aber nicht nur Programme im eigentlichen Sinn, sondern auch Office-Dokumente (Text-, Tabellen- und Präsentations-Dateien) können über Makros Viren und Trojanische Pferde enthalten.

  Software aus vertrauenswürdigen Quellen beziehen

  Es sollten keine Programme aus unbekannter Quelle installiert werden (siehe auch M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*).

  Viele Daten und Programme sind über verschiedene Quellen verfügbar, z. B. über Mirror-Server im Internet oder über CD-ROMs von Zeitschriften. Daten und Programme sollten nur von vertrauenswürdigen Seiten geladen werden, also insbesondere von den Originalseiten des Erstellers.

- **ggf. beim Absender nachfragen**

  Es sollten keine E-Mail-Anhänge oder andere Dateien von Kommunikationspartnern geöffnet werden, wenn diese nicht erwartet wurden oder merkwürdige Namen tragen. Im Zweifelsfall sollte bei diesen nachgefragt werden, ob sie die Nachrichten wirklich geschickt haben.

  Hinweis: Eingehende E-Mail ist das größte Einfalltor für Computer-Viren und Trojanische Pferde. Bei E-Mail auch von vermeintlich bekannten bzw. vertrauenswürdigen Absendern ist zu prüfen, ob der Text der Nachricht auch zum Absender passt (englischer Text von deutschem Partner, zweifelhafter Text oder fehlender Bezug zu konkreten Vorgängen etc.) und ob die Anlage (Attachment) auch erwartet wurde.

- **möglichst Größe und Prüfsumme überprüfen**

  Die Angabe der Größe von Dateien, sowie einer evtl. auch angegebenen Prüfsumme, sollte nach einem Download immer überprüft werden. Bei Abweichungen von der vorgegebenen Größe oder Prüfsumme ist zu vermuten, dass unzulässige Veränderungen vorgenommen worden sind. Daher sollten solche Dateien sofort gelöscht werden.

- Beim Austausch von E-Mails sollten möglichst Digitale Signaturen eingesetzt werden, um die Echtheit und Korrektheit der E-Mail-Inhalte überprüfen zu können (M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*).
- **aktuellen Virenscanner verwenden**
  Alle von Dritten erhaltenen Dateien und Programme sollten vor der Aktivierung mit aktuellem Virenscanner überprüft werden. Diese überprüfen auch, ob (bekannte) Trojanische Pferde vorhanden sind (siehe dazu auch Baustein B 1.6 *Computer-Viren-Schutzkonzept*).
- Grundsätzlich sollten alle Programme vor Installation und Freigabe auf Testsystemen überprüft werden (M 4.65 *Test neuer Hard- und Software*).
- Bei CERTs bzw. anderen sicherheitsbezogenen Informationsdiensten sollte regelmäßig recherchiert werden, ob eingesetzte Programme dahingehend aufgefallen sind, dass sie Daten vom IT-System des Benutzers ohne dessen Wissen übertragen (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*). Neben einigen Office-Programmen und freier Zusatzsoftware sind hier auch Programmbibliotheken aufgefallen, die Nutzerinformationen an Dritte weitergegeben haben, ohne das dies den Programmierern, die sie eingesetzt hatten, bekannt gewesen wäre.
- Bei der Installation von Programmen sollten die Programmhinweise und Nutzungsbedingungen sorgfältig durchgelesen werden. Oftmals wird in diesen sogar (mehr oder weniger deutlich) darauf hingewiesen, dass bei deren Nutzung Benutzer- oder Systemdaten erhoben und weitergegeben werden.
- **Vorsicht bei aktiven Inhalten**
  Trojanische Pferde können auch in aktive Inhalte von WWW-Seiten (Java, JavaScript und besonders ActiveX) eingebettet sein, da sie zusammen mit WWW-Seiten geladen werden, häufig ohne das es der Benutzer bemerkt. Ein gewisser Schutz kann aber schon dadurch erreicht werden, dass sichergestellt wird, dass - besonders zu den Zeiten, zu denen man online arbeitet - nur Prozesse und Programme laufen, die wirklich notwendig sind und so die zusätzlichen Aktivitäten des Rechners oder der Festplatte bemerkt werden. Weiterhin können die Einstellmöglichkeiten des verwendeten Internet Browsers konsequent ausgenutzt werden, so dass beispielsweise aktive Inhalte gar nicht erst auf den eigenen Rechner geladen werden können.
- **Passwörter nicht abspeichern**
  Trojanische Pferde verfolgen häufig den Zweck, Passwörter oder andere Zugangsdaten auszuspähen. Daher sollten Passwörter nie auf den IT-Systemen abgespeichert werden.

Darüber hinaus bietet es sich an, die genutzten Speichermedien regelmäßige auf unerwartete Veränderungen (neue oder veränderte Dateien, ungewöhnliches Verhalten) zu kontrollieren.

M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Fachverantwortliche, Administrator, Mitarbeiter

Um zu einer umfassenden Gesamtsicherheit zu gelangen, ist die Beteiligung aller Mitarbeiter einer Organisation an der Umsetzung der erforderlichen IT-Sicherheitsmaßnahmen erforderlich. Für alle Informationen, Anwendungen und IT-Komponenten sollte daher festgelegt werden, wer für diese und deren Sicherheit verantwortlich ist. Hierfür sollte immer eine konkrete Person (inklusive Vertreter) und keine abstrakte Gruppe benannt werden, damit die Zuständigkeit jederzeit deutlich erkennbar ist. Bei komplexeren Informationen, Anwendungen und IT-Komponenten sollten alle Verantwortlichen und deren Vertreter namentlich genannt sein.

Umgekehrt sollten natürlich alle Mitarbeiter wissen, für welche Informationen, Anwendungen und IT-Komponenten sie in welcher Weise verantwortlich sind.

Jeder Mitarbeiter ist dabei für das verantwortlich, was in seinem Einflussbereich liegt, es sei denn, es ist explizit anders geregelt. Beispielsweise ist die Leitungsebene der Organisation verantwortlich für alle grundsätzlichen Entscheidungen bei der Einführung einer neuen Anwendung, der Leiter IT zusammen mit dem IT-Sicherheitsmanagement für die Ausarbeitung von Sicherheitsvorgaben, die Administratoren für deren korrekte Umsetzung und die Benutzer für den sorgfältigen Umgang mit den zugehörigen Informationen, Anwendungen und Systemen.

Die Fachverantwortlichen als die "Eigentümer" von Informationen und Anwendungen müssen sicherstellen, dass

- der Schutzbedarf der Informationen, Anwendungen und IT-Komponenten korrekt festgestellt wurde,
- die erforderlichen Sicherheitsmaßnahmen umgesetzt werden,
- dies regelmäßig (z. B. täglich, wöchentlich, monatlich) überprüft wird,
- die Aufgaben für die Umsetzung der Sicherheitsmaßnahmen klar definiert und zugewiesen werden,
- der Zugang bzw. Zugriff zu den Informationen, Anwendungen und IT-Komponenten geregelt ist,
- die Sicherheit gefährdende Abweichungen schriftlich dokumentiert werden.

Die Fachverantwortlichen müssen zusammen mit dem IT-Sicherheitsmanagement entscheiden, wie mit eventuellen Restrisiken umgegangen wird.

M 2.226 Regelungen für den Einsatz von Fremdpersonal

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung,

Verantwortlich für Umsetzung: Leiter IT, Leiter Personal

Häufig wird in Behörden oder Unternehmen auf externe Unterstützung zurückgegriffen, falls die entsprechenden personellen Ressourcen nicht im eigenen Haus vorhanden sind. Dies kann im Extremfall dazu führen, dass Fremdpersonal über so lange Zeiträume im eigenen Haus eingesetzt wird, dass viele Mitarbeiter schon nicht mehr genau wissen, ob es sich um eigene oder externe Mitarbeiter handelt.

Einhaltung von Gesetzen und Vorschriften

Externe Mitarbeiter, die über einen längeren Zeitraum in einer oder für eine Organisation tätig sind und eventuell Zugang zu vertraulichen Unterlagen und Daten bekommen könnten, sind schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen zu verpflichten (siehe auch M 3.2 *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen)*.

Einarbeitung und Einweisung

Beim Einsatz von externen Mitarbeiter muss außerdem auf jeden Fall sichergestellt sein, dass sie bei Beginn ihrer Tätigkeit - ähnlich wie eigene Mitarbeiter - in ihre Aufgaben eingewiesen werden (siehe M 3.1 *Geregelte Einarbeitung/Einweisung neuer Mitarbeiter*). Sie sind - so weit es zur Erfüllung ihrer Aufgaben und Verpflichtungen erforderlich ist - über hausinterne Regelungen und Vorschriften zur IT-Sicherheit sowie die organisationsweite IT-Sicherheitspolitik zu unterrichten. Dies gilt in besonderem Maß, wenn sie innerhalb der Liegenschaften des Auftraggebers arbeiten.

Vertretungsregelungen

Daneben sollte sichergestellt sein, dass auch für externe Mitarbeiter Vertretungsregelungen existieren (siehe M 3.3 *Vertretungsregelungen*). Ebenso sollte gewährleistet sein, dass sich diese mit den von ihnen eingesetzten IT-Anwendungen auskennen und auch die erforderlichen IT-Sicherheitsmaßnahmen beherrschen.

geregeltes Verfahren bei Ende des Auftrags

Bei Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Unterlagen und Betriebsmittel erfolgen. Es sind außerdem sämtliche eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Außerdem sollte der Ausscheidende explizit darauf hingewiesen werden, dass die Verschwiegenheitsverpflichtung auch nach Beendigung der Tätigkeit bestehen bleibt (siehe auch M 3.6 *Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern*).

Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal ist wie Besucher zu behandeln, d. h. beispielsweise dass der Aufenthalt in sicherheitsrelevanten Bereichen nur in Begleitung von Mitarbeitern der Behörde bzw. des Unternehmens erlaubt ist (siehe auch M 2.16 *Beaufsichtigung oder Begleitung von Fremdpersonen*).

Ergänzende Kontrollfragen:

- Werden externe Mitarbeiter mit längerfristigen Aufgaben auf die Einhaltung der einschlägigen Gesetze und Vorschriften verpflichtet?
- Werden externe Mitarbeiter geregelt in ihre Aufgaben eingearbeitet und über bestehende Regelungen zur IT-Sicherheit unterrichtet?
- Werden bei sämtlichen eingerichteten Zugangsberechtigungen die Zugriffsrechte bei Auftragsende entzogen bzw. gelöscht?

M 2.227 Planung des Windows 2000 Einsatzes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Vor der Einführung eines Windows 2000 Systems, welches aus vernetzten, einzelnen Windows-Rechnern aufgebaut ist, sind umfangreiche Planungen durchzuführen, damit eine geregelte und auch sichere Einführung sowie in Folge ein sicherer Betrieb ermöglicht wird. Im Rahmen der Windows 2000 Planung sind abhängig von den geplanten Einsatzszenarien für Windows 2000 Systeme verschiedene Gesamt- und Einzelkonzepte zu erstellen. Dabei ist aus Sicherheitssicht jeweils zu gewährleisten, dass die festgelegten Sicherheitsrichtlinien (siehe M 2.228 *Festlegen einer Windows 2000 Sicherheitsrichtlinie*) eingehalten und in der Planung berücksichtigt werden, so dass eine richtlinienkonforme Umsetzung erfolgen kann.

Planung vom Grobkonzept zu Teilkonzepten

Die Planung eines Windows 2000 Systems erfolgt in mehreren Schritten nach dem Prinzip des Top-Down-Entwurfes: Ausgehend von einem Grobkonzept für das Gesamtsystem werden konkrete Planungen für Teilkomponenten in spezifischen Teilkonzepten festgelegt.

Im Grobkonzept werden beispielsweise folgende typische Fragestellungen behandelt:

- Wird ein neues Netz aufgebaut oder wird ein bestehendes Netz migriert?
- Soll ein existierendes Windows Netz (z. B. Windows NT basiert) vollständig oder nur teilweise nach Windows 2000 migriert werden?
- Welche Komponenten, z. B. Server, Druckserver, Arbeitsplatzrechner, werden ersetzt, welche bleiben erhalten?
- **Integration in bestehende Umgebung**

  Müssen existierende Verfahren oder Komponenten, wie z. B. ein bestehendes Kerberos-System oder auch eine bestehende PKI, in Windows 2000 integriert werden? Hier ist u. a. die Interoperabilität sowie der angebotene Funktionsumfang zu berücksichtigen.
- **Mischbetrieb mit anderen Systemen**

  Ist ein Mischbetrieb von Windows 2000 und anderen Betriebssystemen, wie Windows 9x/ME/NT/WfW, OS/2, Novell oder Unix, notwendig? Ist dies der Fall, so hat dies u. a. Einfluss auf die im System verwendeten Authentisierungsverfahren, die je nach den anderen eingesetzten Betriebssystemen auch Schwachstellen aufweisen und damit die Sicherheit des gesamten Windows 2000 Systems schwächen können.
- **mixed mode oder native mode**

  Muss Windows 2000 mit existierenden Windows NT Domänen, z. B. mit Backup-Domänen-Controllern, zusammenarbeiten? Dies hat Einfluss auf den Modus (Mixed-Mode, Native-Mode), in dem eine Domäne betrieben werden muss. Je nach Modus sind dann einige Sicherheitsmechanismen nicht verfügbar.

Die folgenden typischen Teilkonzepte sind für Windows 2000 zu berücksichtigen, wobei sich die jeweiligen Empfehlungen zu den Teilkonzepten in spezifischen Maßnahmen befinden:

- Das Active Directory Konzept: Mit Windows 2000 wurde das Active Directory (AD) als zentraler Datenspeicher zur Systemverwaltung

eingeführt. Technisch gesehen ist die AD-Installation einfach und problemlos durchzuführen. Durch die zentrale Stellung des AD innerhalb von Windows 2000 und insbesondere dadurch, dass Domänen unter Windows 2000 nun global verwaltet, sowie hierarchisch und baumartig angeordnet werden können, ergeben sich allerdings eine Vielzahl organisatorischer und unternehmenspolitischer Problemstellungen. Diese erfordern eine ausgedehnte Planungsphase für das AD-Konzept. Dabei ist ein Zeitrahmen von ein bis zwei Jahren für global operierende Unternehmen und Behörden durchaus als minimaler Planungszeitraum einzukalkulieren.

Active Directory als Schaltzentrale

Aus Sicherheitssicht stellt das AD eine wichtige Schaltzentrale für ein Windows 2000 System dar, da durch die Berechtigungen im AD administrative Delegationen erreicht werden können. Zudem erlaubt der Mechanismus der Gruppenrichtlinien (vergleichbar mit den Windows NT Systemrichtlinien) eine feingranulare Konfiguration auch der Sicherheitseinstellungen eines Windows 2000 Systems. Auch hier ist eine zentrale Verwaltung der Sicherheitseinstellungen möglich.

Das AD erfordert neben der eigentlichen Planung der AD-Struktur (siehe M 2.229 *Planung des Active Directory*) noch die Planung weiterer Teilkonzepte für die im AD verwendeten Sicherheitsmechanismen. Es sind dies das Konzept für die AD-Administration (siehe M 2.230 *Planung der Active Directory-Administration*), in dem u. a. auch die Rechtevergabe auf AD-Objekten geregelt wird, sowie das Konzept für die Gruppenrichtlinien (siehe M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000*), in denen u. a. die Sicherheitseinstellungen für alle Windows 2000 Systeme und deren Verteilung geregelt werden. Des Weiteren müssen im Rahmen des AD-Administrationskonzeptes insbesondere auch Regeln für die Zugehörigkeit zu den verschiedenen administrativen Gruppen erstellt werden. Hier ist u. a. festzugelegen, wer Mitglied in den von Windows 2000 vordefinierten Gruppen, wie z. B. *Organisations-Admins*, und den selbst definierten Gruppen sein soll.

- Das PKI-Konzept: Windows 2000 bietet PKI-Komponenten im Standardlieferumfang an, die zum Aufbau einer unternehmensweiten PKI (Public Key Infrastruktur) genutzt werden können. Die dabei verwendeten Zertifikatsausgabestellen (Certificate Authority, CA) können sowohl von Windows 2000 Systemkomponenten, z. B. von den EFS-Komponenten, als auch von externen Komponenten, also z. B. bei Kunden oder Geschäftspartnern, und von Komponenten von Drittherstellern, wie z. B. E-Mail-Programmen, verwendet werden. Im Rahmen des PKI-Konzeptes (siehe M 2.232 *Planung der Windows 2000 CA-Struktur*) ist dabei die hierarchische Struktur von CAs, deren Vertrauensstellungen zueinander, sowie der Einsatzzweck und die Verteilung von Zertifikaten an Benutzer und innerhalb des Systems zu regeln.

PKI-Konzept

- Das DNS/WINS/DHCP-Konzept: Neben dem AD ist eine weitere grundsätzliche Neuerung innerhalb von Windows 2000, dass als primärer Namensdienst zur Zuordnung von Rechnernamen zu IP-Adressen DNS (Domain Name Service) genutzt wird. Insbesondere gilt, dass ohne DNS kein Windows 2000 AD aufgebaut werden kann. Dabei muss jedoch nicht

DNS, WINS und DHCP

zwingend die Windows 2000 DNS-Komponente eingesetzt werden, sondern es kann auch eine externe DNS-Implementierung (z. B. Unix-basiert) zum Einsatz kommen. Allerdings muss die Fremdimplementierung gewissen Anforderungen genügen. So müssen z. B. so genannte SRV-Records und dynamische Updates von DNS-Einträgen unterstützt werden. Da die Domänennamen einer Windows 2000 Domänenhierarchie mit dem hierarchischen DNS-Namensraum übereinstimmen, beeinflussen sich AD-Konzept und DNS-Konzept maßgeblich. Zusätzlich muss im DNS-Konzept berücksichtigt werden, ob der bisherige Namensdienst WINS (Windows Internet Naming Service) - der für den Betrieb von Windows 2000 Systemen nicht mehr notwendig ist - aus Gründen der Rückwärtskompatibilität weiter betrieben werden muss. Gründe hierfür können z. B. Applikationen sein, die zwingend WINS benötigen.

Außerdem ist die Integration des DNS mit dem DHCP (Dynamic Host Configuration Protocol) zu planen, mit dem der Rechner automatisch nach dem Einschalten für den Netzzugriff konfiguriert wird. Unter dem Gesichtspunkt der Sicherheit sind jeweils die berechtigten Administratoren und die Verwendung der einzelnen komponentenspezifischen Sicherheitsmechanismen festzulegen. Hinweise zu den Einzelkonzepten werden genauer in M 4.140 *Sichere Konfiguration wichtiger Windows 2000 Dienste* und den darin referenzierten Maßnahmen gegeben.

- Das RAS-Konzept: Auch Windows 2000 bietet Komponenten, um den entfernten Zugang zu einem lokalen Netz zu realisieren. Im Vergleich zu der aus Windows NT bekannten Lösung sind keine gravierenden Änderungen zu verzeichnen. Insbesondere aus Sicherheitssicht ergeben sich kaum Unterschiede. Als wesentliche Neuerung ist lediglich die Verfügbarkeit starker Verschlüsselung zu nennen, die nach Einspielen des so genannten "High-Encryption-Pack" und des "Service Pack 1" zur Verfügung steht. Alternativ kann auch das mittlerweile verfügbare Service Pack 2 genutzt werden, das die stärkere Verschlüsselung integriert enthält. Für die Konfiguration der Zugangskontrolle steht eine neue regelgesteuerte Möglichkeit zur Verfügung, die in Maßnahme M 4.145 *Sichere Konfiguration von RRAS unter Windows 2000* erläutert wird. Für generelle Empfehlungen und Maßnahmen zum Themenkomplex *Remote Access* existiert ein entsprechender Baustein in Baustein B 4.4 *Remote Access*.

RAS-Konzept

- Das NTFS-Konzept: Auch unter Windows 2000 wird das Windows NT-File System (NTFS) eingesetzt, das im Vergleich zu der unter Windows NT eingesetzten Vorgängerversion einige Neuerungen auch sicherheitstechnischer Art bietet. Einerseits können Dateiberechtigungen und Überwachungseinstellungen unter Windows 2000 nun wesentlich detaillierter erfolgen, andererseits besteht mit dem Dateisystem EFS die Möglichkeit der Dateiverschlüsselung. Daneben steht das verteilte Dateisystem DFS, das auch schon unter Windows NT verwendet werden konnte, unter Windows 2000 integriert zur Verfügung. Entsprechende Maßnahmen für die sicherheitsrelevanten Neuerungen finden sich unter M 3.28 *Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer*, M 4.140 *Sichere Konfiguration wichtiger Windows 2000 Dienste*,

NTFS-Konzept

M 4.147 *Sichere Nutzung von EFS unter Windows 2000/XP*, sowie unter M 4.148 *Überwachung eines Windows 2000/XP Systems.*

- Das Migrations-Konzept: Der völlige Neuaufbau eines Windows 2000 Systems stellt normalerweise nicht den Regelfall dar. Vielmehr besteht regelmäßig der Wunsch oder die Notwendigkeit, existierende, meist Windows NT-basierte Netze auf Windows 2000 umzustellen. Dabei muss die so genannte Migration sorgfältig geplant, vorbereitet und durchgeführt werden. Eine allgemeine Empfehlung, welche der verschiedenen Migrationskonzepte zur Anwendung kommen sollen, kann nicht gegeben werden, da dies vom zu migrierenden Netz abhängt. Generell muss jedoch schon bei der Planung des Windows 2000 Netzes bedacht werden, dass das Netz über einen längeren Zeitraum als heterogenes Netz betrieben werden muss, das migrierte und auch nicht migrierte Komponenten enthalten wird. Insbesondere ist zu beachten, dass während der Migration die Sicherheit des Systems - im Vergleich zu einem reinen Windows 2000 System - gefährdet sein kann. Dies geschieht u. U. durch Fehler bei der Migration, durch nicht kompatible Konfigurationsparameter oder aber durch die Notwendigkeit der Rückwärtskompatibilität für Sicherheitseinstellungen. Hinweise zu typischen Sicherheitsproblemen bei der Migration sind in M 2.233 *Planung der Migration von Windows NT auf Windows 2000* zu finden.

Migrations-Konzept

- Das Auditing/Protokollierungs-Konzept: Um die Sicherheit in einem Windows 2000 System gewährleisten zu können, muss das Einhalten der festgelegten Sicherheitsrichtlinien (siehe M 2.228 *Festlegen einer Windows 2000 Sicherheitsrichtlinie*) überwacht werden. Dazu stellt Windows 2000, wie auch schon Windows NT, einen ereignisbasierten Protokollierungs-Mechanismus zur Verfügung. Die im Rahmen eines Auditing-Konzeptes zu beachtenden Sicherheitsaspekte sind in der Maßnahme M 4.148 *Überwachung eines Windows 2000/XP Systems* zusammengefasst.

Auditing und Protokollierung

- Das IPSec-Konzept: Für die Kommunikationsabsicherung auf Transportebene stellt Windows 2000 eine IPSec-konforme Implementierung zur Verfügung. Durch IPSec können alle IP-basierten Kommunikationsverbindungen von und zu einem Rechner abgesichert werden. Dabei ist es möglich, die Endpunkte der Kommunikation zu authentisieren und die Datenpakete signiert und verschlüsselt zu übertragen, so dass die Integrität und Vertraulichkeit der Daten gewährleistet werden kann. Empfehlungen für die Konfiguration der IPSec-Komponenten sind in Maßnahme M 5.90 *Einsatz von IPSec unter Windows 2000/XP* zusammengefasst.

IPSec-Konzept

Neben diesen Teilkonzepten können je nach Einsatzszenario auch weitere Konzepte notwendig werden, wie z. B. Internet-Konzept oder Softwareverteilungs-Konzept, die dann in der Planungsphase berücksichtigt werden müssen. So basiert beispielsweise die Windows 2000 Authentisierung auf dem Kerberos-Protokoll. Hierbei werden Zeitstempel benutzt, um u. a. die Gültigkeit von Authentisierungsdaten zu beschränken. Daher müssen die Systemuhren aller Rechner, die mit Kerberos arbeiten, innerhalb eines Toleranzintervalls synchronisiert sein. Standardmäßig erfolgt der regelmäßige Uhrenabgleich automatisch durch Windows 2000 selbst. Sofern jedoch auf eine externe Zeitquelle synchronisiert werden soll, ist dazu ein Konzept zu

entwerfen, das alle notwendigen Randbedingungen umfasst. Dies sind beispielsweise Zeitserver, Verfahren beim Ausfall des Zeitservers und Toleranzintervalle.

Ergänzende Kontrollfragen:

- Wurde die Windows 2000 Planung bedarfsgerecht durchgeführt?
- Sind alle für den konkreten Einsatz notwendigen Teilkonzepte entworfen?
- Wurde die AD-Struktur mit allen Betroffenen abgestimmt?

M 2.228 Festlegen einer Windows 2000 Sicherheitsrichtlinie

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Das Festlegen einer Sicherheitsrichtlinie für Windows 2000 ist eine der organisatorischen Hauptaufgaben bei der Windows 2000 Planung. Durch die Sicherheitsrichtlinie wird festgelegt, welche Sicherheitsbestimmungen in einem Windows 2000 System gelten sollen und bei der Windows 2000 Installation umgesetzt werden müssen.

Durch die Windows 2000 Sicherheitsrichtlinie werden sämtliche sicherheitsbezogenen Themenbereiche eines Windows 2000 Systems geregelt. Die folgende Liste gibt einen groben Überblick über die abzudeckenden Bereiche. Die Liste muss je nach Unternehmen und Windows 2000 Einsatzszenarien entsprechend angepasst, ausgestaltet und erweitert werden.

Eine Windows 2000 Sicherheitsrichtlinie sollte für folgende Windows 2000 spezifischen Bereiche Regelungen treffen:

Allgemein:

- Wie sollen Windows 2000 Rechner physikalisch abgesichert werden?
- Welche Windows 2000 Komponenten, z. B. RAS, IIS, sollen genutzt werden?
- Welcher Benutzer darf welche Rechte ausüben?
- Welcher Administrator darf welche Rechte ausüben?
- Welche Datenkommunikation ist abgesichert abzuwickeln, also wo muss Vertraulichkeit und Integrität sichergestellt sein?
- Wo ist Authentikation erforderlich? Welche Authentisierungsverfahren sollen gewählt werden?

Active Directory (AD):

- Welche Rechner sind Domänen-Controller und halten eine AD Kopie?
- Wer hat welchen Zugriff auf das AD?
- Wer darf welche administrativen Aufgaben auf Objekten im AD ausführen?
- Welche Domänenstruktur (Domäne, Baum, Wald) soll gewählt werden?
- Welche Vertrauensstellungen zwischen Domänen dürfen bzw. müssen existieren?
- Sollen Berechtigungen domänenübergreifend vergeben werden?

DNS/DHCP/WINS:

- Welche DNS-Server sollen Daten miteinander austauschen?
- Welcher Server ist für welche DNS-Zone verantwortlich?
- Welche Rechner sollen DHCP verwenden dürfen?

- Dürfen DHCP-Clients eigenständig DNS-Updates machen?
- Soll neben DNS auch WINS weiter betrieben werden?
- Wer verwaltet DNS, DHCP und WINS?

Kerberos:

- Welche Kerberos-Parameter sind zu verwenden?
- Wer darf Kerberos-Einstellungen ändern?

Dateisystem:

- Welche Berechtigungen auf Systemdateien gelten für die verschiedenen Administratoren und Benutzer?
- Soll das verschlüsselnde Dateisystem (EFS) eingesetzt werden?
- Für welche Daten soll EFS eingesetzt werden?

RAS:

- Welche Rechner sollen als RAS-Einwahlrechner fungieren?
- Welche Benutzer dürfen sich unter welchen Bedingungen über RAS einwählen?
- Welche RAS-Sicherheitsmechanismen sollen benutzt werden, um die RAS-Kommunikation abzusichern?
- Welches Authentisierungsverfahren (z. B. MS-CHAP, PAP, RADIUS) soll für RAS eingesetzt werden?

Netz-Zugriff:

- Auf welche Rechner darf vom Netz aus zugegriffen werden?
- Welche Ressourcen sind aus dem Netz von welchen Benutzern zugreifbar?
- Welchen Rechnern wird für die Delegation, d. h. das stellvertretende Handeln unter einer Benutzeridentität, vertraut?
- Welche Authentisierungsverfahren sollen eingesetzt oder erlaubt werden (Kerberos, NTLM Version 1 oder 2, LanMan)?
- Welche Benutzer dürfen welche externen Dienste, z. B. den Internetzugriff, nutzen?

Diese für Windows 2000 Komponenten spezifische Auflistung von Themengebieten kann in folgende zeitliche Abfolge gebracht werden:

1. Definition der Client-Server-Netzstruktur

Im ersten Schritt ist die logische Struktur des Client-Server-Netzes, insbesondere die Zuordnung der Server und der Netz-Domänen festzulegen (siehe M 2.227 *Planung des Windows 2000 Einsatzes*). Nach Möglichkeit sollte auf die Verwendung von Peer-to-Peer-Funktionalitäten verzichtet werden, da diese die Sicherheit des Client-Server-Netzes beeinträchtigen können. Sofern sich dies jedoch nicht vermeiden lässt, sind verbindliche Regelungen für die Nutzung von Peer-to-Peer-Funktionalitäten zu treffen (siehe M 2.67 *Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste*).

2. Regelung der Verantwortlichkeiten

Ein Client-Server-Netz sollte von geschulten Netzadministratoren sicher betrieben werden. Dabei ist im Rahmen der Notfallvorsorge für eine geeignete Stellvertreterregelung zu sorgen. Nur die berechtigten Administratoren dürfen Windows 2000 Sicherheitsparameter verändern. Sie sind z. B. dafür zuständig, auf den Servern den entsprechenden Verantwortlichen Administrationsrechte und -werkzeuge zur Verfügung zu stellen, damit diese die Vergabe von Datei- und Verzeichnisberechtigungen, die Freigabe der von anderen benötigten Verzeichnissen bzw. Anwendungen, den Aufbau von Benutzergruppen und -konten sowie die Einstellung der Systemrichtlinien für Benutzer, Zugriffskontrolle und Überwachung vornehmen können.

Die Verantwortlichkeiten der einzelnen Administratoren und Benutzer im Client-Server-Netz sind unter Schritt 11 dargestellt.

3. Festlegung von Namenskonventionen

Um die Verwaltung des Client-Server-Netzes zu erleichtern, sollten eindeutige Namen für die Rechner, Benutzergruppen und die Benutzer verwendet werden.

Zusätzlich sollten Namenskonventionen für die Freigabenamen von Verzeichnissen oder Druckern eingeführt werden. Sollen keine Rückschlüsse auf den Inhalt eines freigegebenen Verzeichnisses möglich sein, sind entsprechende Pseudonyme zu verwenden. Soll eine freigegebene Ressource nicht als solche erkennbar sein, ist dem Freigabenamen das Zeichen "$" anzuhängen. Letzteres empfiehlt sich immer dann, wenn Verzeichnisse nur zum bilateralen Austausch von Informationen zwischen zwei Anwendern oder zum Zugriff auf Ressourcen, die nur einzelnen Benutzern bekannt sein sollen, freigegeben werden. Es wird explizit darauf hingewiesen, dass das "Verstecken" von Netzfreigaben nicht als Sicherheitsmechanismus angesehen oder benutzt werden kann. Die Sicherheit der über eine Netzfreigabe verfügbar gemachten Daten muss durch entsprechende Zugriffsrechte gewährleistet werden.

4. Festlegung der Regeln für Benutzerkonten

Vor der Einrichtung von Benutzerkonten sollten die Restriktionen, die für alle bzw. für bestimmte Konten gelten sollen, festgelegt werden. Dies betrifft insbesondere die Regelungen für Passwörter und für die Reaktion des Systems auf fehlerhafte Login-Vorgänge. Unter Windows 2000 erfolgen diese Einstellungen bevorzugt über Gruppenrichtlinien im Active Directory (siehe M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000*) oder für nicht vernetzte Systeme über die Konfiguration der lokalen Sicherheitsrichtlinien in der Programmgruppe *Verwaltung*.

5. Einrichtung von Gruppen

Zur Vereinfachung der Administration sollten Benutzerkonten, für die die gleichen Anforderungen gelten, zu Gruppen zusammengefasst werden. Benutzerrechte sowie Datei-, Verzeichnis- und Freigabeberechtigungen und ggf. weitere vordefinierte Funktionen werden dann den Gruppen und nicht einzelnen Benutzerkonten zugeordnet. Die Benutzerkonten erben die Rechte und Berechtigungen der Gruppen, denen sie angehören. So ist es z. B. denkbar, alle Mitarbeiter einer Abteilung in einer Gruppe zusammenzufassen. Eine

Zuweisung von Benutzerrechten und -berechtigungen an einzelne Benutzer sollte nur erfolgen, wenn dies ausnahmsweise unumgänglich ist.

Die Verwaltung von Gruppen von Benutzern oder Rechnern erfolgt unter Windows 2000 über das Active Directory (siehe M 2.229 *Planung des Active Directory*).

6. Festlegung der Benutzerrechte

Rechte gestatten einem Benutzer die Ausführung bestimmter Aktionen auf dem System. Sie beziehen sich auf das gesamte System, sind keinem speziellen Objekt zugeordnet und können die Berechtigungen für ein Objekt außer Kraft setzen, da ein Recht Vorrang vor allen Datei- und Verzeichnisberechtigungen hat. Wenn sich ein Benutzer bei einem Konto anmeldet, dem die gewünschten Rechte entweder direkt oder über die Gruppenmitgliedschaft erteilt wurden, kann er die entsprechenden Aktionen ausführen. Besitzt ein Benutzer nicht die geeigneten Rechte, so verhindert Windows 2000 jeden Versuch, die betreffenden Aktionen auszuführen.

Die Konfiguration der Benutzerrechte erfolgt unter Windows 2000 vorzugsweise über Gruppenrichtlinien im Active Directory (siehe M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000*) oder bei nicht vernetzten Rechnern über die Konfiguration der lokalen Sicherheitsrichtlinie.

7. Festlegung der Vorgaben für Protokollierung

Windows 2000 stellt sehr ausführliche Möglichkeiten der Protokollierung sicherheitsrelevanter Ereignisse zur Verfügung. Diese sind bei vollständiger Nutzung in der Lage, das System weitgehend mit der Protokollierung auszulasten und dabei große Mengen an Plattenplatz zu verbrauchen. Dabei kann ein Spektrum von Ereignisarten aufgezeichnet werden, das sich von systemweiten Ereignissen, wie zum Beispiel dem Anmelden eines Benutzers bis hin zum Versuch eines Benutzers, eine bestimmte Datei zu lesen, erstreckt. Sowohl die erfolgreichen als auch die fehlgeschlagenen Versuche, eine Aktion durchzuführen, lassen sich aufzeichnen. Bei der Festlegung der jeweils rechnerlokalen Protokolleinstellungen ist auf die Verträglichkeit mit dem Gesamtkonzept der Systemüberwachung (siehe M 4.148 *Überwachung eines Windows 2000/XP Systems*) zu achten.

Die Konfiguration der Protokolleinstellungen (z. B. Aktivierung der Protokollmöglichkeit, Größe der Protokolldateien, Protokolleinstellungen pro Datei) erfolgt unter Windows 2000 vorzugsweise über Gruppenrichtlinien im Active Directory (siehe M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000*) oder bei nicht vernetzten Rechnern über die Konfiguration der lokalen Sicherheitsrichtlinie.

8. Regelungen zur Datenspeicherung

Es ist festzulegen, wo Benutzerdaten gespeichert werden (siehe M 2.138 *Strukturierte Datenhaltung*). So ist es denkbar, dass Benutzerdaten nur auf einem Server abgelegt werden. Eine Datenspeicherung auf der lokalen Festplatte ist bei diesem Modell nicht erlaubt. Möglich ist aber auch, bestimmte Benutzerdaten nur auf der lokalen Festplatte abzulegen. Nach welcher Strategie verfahren werden soll, muss an den konkreten Umständen

des Einzelfalles festgelegt werden. Eine generelle Empfehlung auszusprechen, ist nicht möglich.

9. Einrichtung von Projektverzeichnissen

Um eine saubere Trennung von Benutzer- und projektspezifischen Daten untereinander sowie von den Programmen und Daten des Betriebssystems durchzusetzen, sollte eine geeignete Verzeichnisstruktur festgelegt werden, mit der eine projekt- und benutzerbezogene Dateiablage unterstützt wird. So können beispielsweise zwei Hauptverzeichnisse *\Projekte* und *\Benutzer* angelegt werden, unter denen dann die Dateien und Verzeichnisse der Projekte bzw. Benutzer in jeweils eigenen Unterverzeichnissen abgelegt werden.

10. Vergabe der Zugriffsrechte

Für die Server ist festzulegen, welche Verzeichnisse - und bei Nutzung von NTFS-Partitionen - welche Dateien für den Betrieb freizugeben und welche Zugriffsrechte ihnen zuzuweisen sind (siehe M 4.145 *Sichere Konfiguration von RRAS unter Windows 2000*). Zusätzlich ist bei Nutzung von Peer-to-Peer-Funktionalitäten auf der Ebene der Clients zu entscheiden, welche Verzeichnisse für Netzzugriffe freizugeben sind. Gleiches gilt für die Freigabe von Druckern.

11. Verantwortlichkeiten für Administratoren und Benutzer im Client-Server-Netz

Neben der Wahrnehmung der Netzmanagement-Aufgaben (siehe Nr. 2) müssen weitere Verantwortlichkeiten festgelegt werden. Es ist festzulegen, welche Verantwortung die einzelnen Administratoren im Client-Server-Netz übernehmen müssen. Dies können zum Beispiel Verantwortlichkeiten sein für

- die Verwaltung des Active Directory oder einzelner Active Directory Teilkomponenten,
- die Auswertung der Protokolldateien auf den einzelnen Servern oder Clients,
- die Vergabe von Zugriffsrechten,
- das Hinterlegen und den Wechsel von Passwörtern und
- die Durchführung von Datensicherungen.

Auch die Endbenutzer müssen in einem Client-Server-Netz bestimmte Verantwortlichkeiten übernehmen, sofern ihnen Rechte zur Ausführung administrativer Funktionen gegeben werden. In der Regel beschränken sich diese Verantwortlichkeiten jedoch auf die Vergabe von Zugriffsrechten auf die eigenen Dateien, sofern diese explizit festgelegt und nicht von Voreinstellungen des übergeordneten Verzeichnisses übernommen werden.

12. Schulung

Abschließend muss festgelegt werden, welche Benutzer zu welchen Punkten geschult werden müssen. Erst nach ausreichender Schulung kann der Wirkbetrieb aufgenommen werden. Insbesondere die Administratoren sind hinsichtlich der Verwaltung und der Sicherheit von Windows 2000 gründlich zu schulen.

Die daraus entwickelten Sicherheitsrichtlinien sind zu dokumentieren und im erforderlichen Umfang den Benutzern des Client-Server-Netzes mitzuteilen.

Bei der Definition der Sicherheitsrichtlinie ist zu beachten, dass sich die für Windows 2000 festgelegten Richtlinien an den bisher geltenden Sicherheitsrichtlinien der Organisation orientieren, diesen nicht widersprechen (Konsistenz) und auch nicht im Widerspruch zu geltendem Recht stehen. In der Regel wird eine Windows 2000 Sicherheitsrichtlinie existierende Regelungen Windows 2000-spezifisch anpassen oder aber sinngemäß erweitern. Dabei sind unter Umständen neue Regelungen für neue Windows 2000 spezifische Funktionalitäten, z. B. für das Active Directory, zu treffen. Generell gilt, dass sich die Planung der Windows 2000 Infrastruktur an den jeweiligen Sicherheitsrichtlinien orientiert, dabei jedoch auch Einfluss auf die Sicherheitsrichtlinien besitzt (Feedback-Prozess).

Ergänzende Kontrollfragen:

- Sind alle für den geplanten Einsatz von Windows 2000 relevanten Bereiche durch die Sicherheitsrichtlinien abgedeckt?
- Wurden zeitliche Abhängigkeiten für die Umsetzung der Sicherheitsrichtlinien berücksichtigt?
- Sind alle Benutzer auf die Windows 2000 Sicherheitsrichtlinien vorbereitet worden?

M 2.229 Planung des Active Directory

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Das Active Directory (AD) ist der zentrale Datenspeicher für sämtliche Verwaltungsdaten einer Windows 2000 Domäne. Abstrakt gesehen, bildet das AD eine hierarchisch und baumartig organisierte, Objekt-basierte Datenbank. Es ist an den Verzeichnisdienst-Standard X.500 angelehnt, von dem es die interne Struktur und den internen Aufbau entliehen hat. Es ist jedoch kein X.500 kompatibler Verzeichnisdienst.

Domänen

Das Windows 2000 Domänenkonzept gleicht auf Domänenebene prinzipiell dem Windows NT Domänenkonzept: in einer Domäne werden Rechner und Benutzer zusammengefasst und können durch den Domänenadministrator verwaltet werden. Eine Domänengrenze bildet grundsätzlich eine administrative Grenze und begrenzt auch den Wirkungsbereich von Berechtigungen. Zusätzlich zu diesem Konzept bietet Windows 2000 an, Domänen baumartig miteinander in Beziehung zu setzen, so dass Vater-Kind-Beziehungen zwischen Domänen bestehen können. Eine Kind-Domäne wird dabei auch als Sub-Domäne bezeichnet, da sich der Name der Kind-Domäne aus dem Namen der übergeordneten Domäne ableitet, indem diesem Namen der Name der Domäne durch einen Punkt getrennt angehängt wird.

Beispiel:

Name der Vater-Domäne: unternehmen.de

Name der Sub-Domäne: verwaltung.unternehmen.de

Tree

Der so aufgespannte Namensraum ist mit dem zugehörigen DNS Namensraum identisch und kann auch nicht verschieden von diesem gebildet werden. Domänen, die einen gemeinsamen Namensstamm besitzen, bilden einen Baum (englisch Tree).

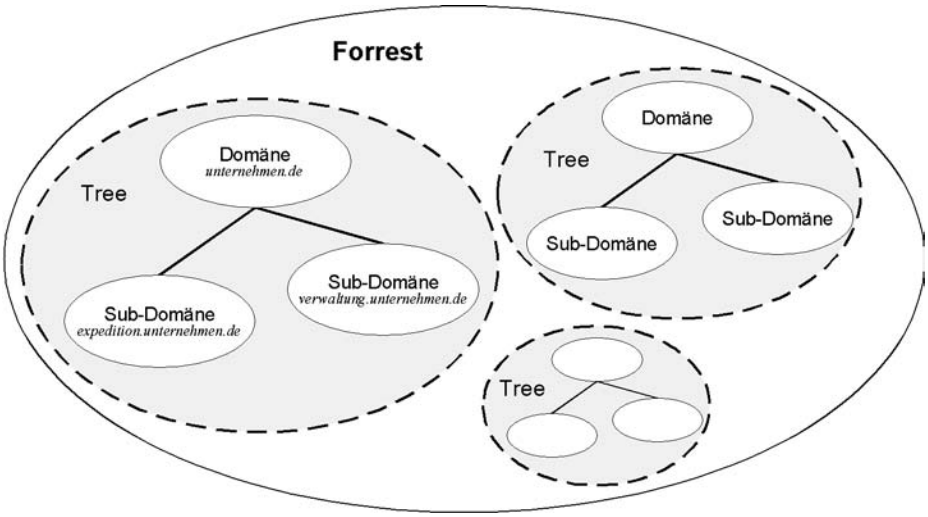


Abbildung: Zu einem Wald (Forrest) zusammengeschlossene Domänenbäume

Forest

Domänen, die in mehreren Bäumen angesiedelt sind - also unterschiedliche Namensräume aufspannen - können dennoch gemeinsam verwaltet werden. Derart zusammengeschlossene Domänenbäume bilden einen Wald (englisch *Forest*). Insbesondere bildet eine einzige alleinstehende Domäne auch einen Baum und gleichzeitig auch einen Wald.

Forest-Root-Domäne

In einem Wald gibt es immer eine ausgezeichnete Domäne, die eine gewisse Sonderstellung besitzt. Es ist die als erstes erzeugte Domäne, die auch als *Forest-Root-Domäne* (FRD, Wurzel-Domäne des Waldes) bezeichnet wird. Die Sonderstellung besteht darin, dass Administratoren der FRD im gesamten Forest weitreichende Berechtigungen besitzen. Für die Mitglieder der Gruppe Organisations-Admins stellen die Domänengrenzen keine administrativen Grenzen dar, da sie in allen Domänen Zugriffsrechte besitzen. Beim Aufbau eines Windows Domänenverbundes ist zu bedenken, dass die zuerst erzeugte Domäne immer die FRD ist. Insbesondere kann die "Rolle" der FRD nachträglich nicht auf eine andere Domäne "übertragen" werden, so dass die Domänenstruktur ggf. vollständig in der gewünschten Form neu erzeugt werden muss.

Active Directory Objekte

Das AD besteht aus verschiedenen Objekten, den Active Directory Objekten (ADOs). Jedes Objekt besitzt einen ausgezeichneten Typ, wie z. B. Benutzerobjekt oder Rechnerobjekt, und ist gemäß dieses Typs aus verschiedenen Attributen zusammengesetzt. Die verschiedenen Objektattribute können verschiedene Werte aufnehmen, wie z. B. Telefonnummer oder IP-Adresse. Das AD kennt verschiedene vordefinierte Objekttypen:

- Domänen-Objekt: Dieses Objekt ist die Wurzel aller AD-Objekte einer Domäne und enthält Informationen über die Domäne, wie z. B. den Namen. Unterhalb eines Domänen-Objektes können andere Objekte angeordnet sein.
- Gruppierungs-Objekte: Diese Objekte dienen dazu, andere Objekte zu gruppieren. Standardmäßig steht das Objekt Organisations-Einheit (Organizational Unit, OU) zur Verfügung. Unterhalb eines OU-Objektes können weitere OU-Objekte enthalten sein, sowie Rechner-, Benutzer- und Benutzer-Gruppen-Objekte.
- Rechner-Objekt: Durch dieses Objekt werden Windows 2000/XP Rechner repräsentiert. Unterhalb eines Rechner-Objektes können keine weiteren Objekte mehr angeordnet sein. Das Windows 2000 Active Directory ist nur auf die Verwaltung von Windows Rechnern ausgelegt, so dass Rechner-Objekte ausschließlich Windows Rechner repräsentieren können, die mit dem Active Directory zusammenarbeiten. Dies sind standardmäßig Rechner mit den Betriebssystemen Windows NT/2000/XP. Für andere Versionen von Windows, wie z. B. Windows 98, stehen Active Directory Anmeldekomponenten zur Verfügung.
- Benutzer-Objekt: Durch dieses Objekt werden Domänenbenutzer repräsentiert. Unterhalb eines Benutzer-Objektes können keine weiteren Objekte mehr angeordnet sein.

- Benutzer-Gruppen-Objekte: Durch diese so genannten Sicherheits-Gruppen werden Windows Gruppen repräsentiert. Es gibt verschiedene Gruppentypen, die sich im Geltungsbereich (domänen-, forestweit) und in den möglichen Gruppenmitgliedern (Domänen-, Forest-Objekte) unterscheiden. Es wird unterschieden zwischen lokalen, domänen-lokalen, globalen und universalen Gruppen. Sicherheits-Gruppen werden dazu benutzt, Berechtigungen zu vergeben. Im Vergleich zu Windows NT ist in einem Windows 2000/XP System mit einer deutlich höheren Anzahl von Gruppen zu rechnen (mehrere zehntausend für größere Unternehmen), so dass u. U. über eine werkzeuggestützte Verwaltung nachgedacht werden muss. Diese kann sowohl über selbst geschriebene Skripte, als auch über Produkte von Drittherstellern erfolgen. Ob und welche Werkzeuge hier sinnvoll sind, muss jedoch im Einzelfall entschieden werden.

Der generelle AD-Aufbau lässt sich wie folgt darstellen:

- Das Domänen-Objekt ist die Wurzel des AD-Baumes einer Domäne.
- Unter dem Domänen-Objekt werden OU-Objekte erzeugt, um Rechner-, Benutzer- und Benutzer-Gruppen-Objekte strukturiert zusammenzufassen. Da OU-Objekte geschachtelt werden können, ergibt sich eine organisationsspezifische Baumstruktur.

Anpassung an administrative Gegebenheiten

Nach einer Standardinstallation existiert eine einfache und flache AD-Struktur, die von Windows 2000 angelegt wird und dann entsprechend der AD-Planung verändert werden muss. Da das AD primär der Verwaltung eines Windows 2000/XP Systems dient, sollte beim Aufbau der AD-Struktur darauf geachtet werden, dass die Struktur vornehmlich auf administrative Gegebenheiten abgestimmt wird. Wenn stattdessen zwanghaft die organisatorische Behörden- bzw. Unternehmensstruktur bis ins Kleinste nachgebildet wird, kann dies zu Problemen in der Administration führen.

AD-Schema

Die möglichen Anordnungen von AD-Objekten, d. h. die Festlegung welches Objekt welche anderen Objekte enthalten darf, welche Attribute existieren und aus welchen Attributen Objekte zusammengesetzt werden, wird durch das so genannte AD-Schema definiert. Das von Microsoft vorgegebene AD-Schema kann auch verändert werden. Dies stellt jedoch einen gravierenden Eingriff in das AD dar, der nur nach sorgfältiger Planung durchgeführt werden darf. Eine Schema-Änderung wirkt sich in allen gemeinsam verwalteten Domänen, d. h. im Wald bzw. Forest, aus. Da die Schemaänderung eine kritische Operation ist, kann diese nur an genau einem Rechner, dem so genannten Schema-Master, durch Mitglieder der Gruppe *Schema-Admins* durchgeführt werden. Schemaänderungen können zudem u. U. nicht mehr rückgängig gemacht werden. Die Mitgliedschaft in dieser Gruppe ist daher unbedingt restriktiv zu vergeben und streng zu kontrollieren.

Global Catalog

Das AD wird auf Domänen Controllern gehalten und innerhalb einer Domäne zwischen diesen durch Replikation synchronisiert. Das AD einer Domäne enthält nur domänenbezogene Informationen. Um in einem Forest schnell auf Informationen aus dem gesamten Forest zugreifen zu können, wird der so genannte *Global Catalog* (GC) aufgebaut. Er besteht aus Teilinformationen von AD-Objekten und wird im gesamten Forest repliziert, so dass über den

GC in einer Domäne auch direkt auf Informationen aus anderen Domänen zugegriffen werden kann.

Sites

Neben der beschriebenen baumartigen und hierarchischen Struktur baut Windows 2000 automatisch eine zusätzliche und orthogonale Struktur auf. Räumlich nahe Rechner - dies bestimmt Windows 2000 über Netzlaufzeiten - werden zu so genannten Standorten (englisch *Sites*) zusammengefasst. Über Sites wird u. a. auch die Replikationsstruktur von Domänen Controllern gesteuert. Pro Site muss mindestens ein Rechner existieren, der eine Kopie des Global Catalogs hält. Der Global Catalog muss im Rahmen des Anmeldeprozesses eines Benutzers angefragt werden, so dass bei der Anmeldung immer ein Global Catalog-Server zugreifbar sein muss. Die von Windows 2000 automatisch aufgebaute Standortstruktur sollte an die behörden- oder unternehmensinternen Gegebenheiten, wie z. B. Standorte in verschiedenen Städten oder Ländern, individuell angepasst werden. Da dies Einfluss auf die AD-Replikationsbeziehungen hat, ist dazu jedoch ein Konzept zu erstellen.

Im Rahmen der AD Planung sind folgende Aspekte zu berücksichtigen:

- Welche AD-Struktur im Sinne der Aufteilung in Domänen und welche Anordnung der Domänen in Bäume und Wälder soll gewählt werden?
- Welche Benutzer und Rechner sollen in welchen Domänen zusammengefasst werden?

Für jede Domäne muss entschieden werden,

- welche OU-Objekte existieren sollen, wie diese hierarchisch angeordnet werden und welche Objekte diese jeweils aufnehmen sollen,
- welche Sicherheitsgruppen benötigt werden und wie diese in OUs zusammengefasst werden,
- welches administrative Modell umgesetzt wird (zentrale/dezentrale Verwaltung),
- ob und an wen administrative Aufgaben delegiert werden sollen,
- welche Sicherheitseinstellungen für verschiedene Typen von Rechnern und Benutzergruppen gelten sollen,
- welche Einstellungen bei den Gruppenrichtlinien benötigt werden und nach welchem Konzept die Gruppenrichtlinien verteilt werden (siehe M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000* und M 2.326 *Planung der Windows XP Gruppenrichtlinien*),
- welche Vertrauensstellungen von Windows 2000 automatisch generiert werden und welche zusätzlichen Vertrauensstellungen (z. B. zu NT-Domänen oder externen Kerberos-Realms) eingerichtet werden müssen,
- auf welche AD-Informationen über die verschiedenen AD-Schnittstellen (z. B. ADSI, LDAP) von wem zugegriffen werden dürfen,
- welche AD-Objekte in den so genannten Global Catalog übernommen werden sollen, auf den in einem Forest global zugegriffen werden kann,

- in welchem Modus die Domäne betrieben werden muss: müssen in einer Domäne noch Windows NT Backup-Domänen-Controller (BDCs) betrieben werden, so muss die Domäne im "Mixed-Mode" betrieben werden. Sind keine BDCs vorhanden, kann die Domäne im "Native-Mode" betrieben werden.

Generell muss die geplante AD-Struktur dokumentiert werden, dies trägt maßgeblich zur Stabilität, konsistenten Administration und damit zur Systemsicherheit bei. Es empfiehlt sich insbesondere festzuhalten, welche Schemaänderungen durchgeführt werden. Dabei sollten auch die Gründe für die Änderung dokumentiert sein.

Für jedes AD-Objekt sollte dokumentiert sein:

- Name und Position im AD-Baum (z. B. "StandortBerlin", Vater-Objekt: OU "Filialen-Deutschland")
- welchem Zweck das Objekt dient (z. B. Gruppe der Benutzer mit RAS-Zugang auf RAS-Server 1)
- welche administrativen Zugriffsrechte für das Objekt und dessen Attribute vergeben werden sollen (z. B. vollständig verwaltet von "Admin1")
- wie die Vererbung von AD-Rechten konfiguriert werden soll, z. B. Blockieren der Rechtevererbung (siehe auch M 2.230 *Planung der Active Directory-Administration*, M 3.27 *Schulung zur Active Directory-Verwaltung*)
- welche Gruppenrichtlinienobjekte auf dieses Objekt wirken (siehe M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000*)

Der Planung der AD-Administration und des benutzten administrativen Modells kommt eine wichtige Aufgabe zu. Empfehlungen dazu finden sich zusammengefasst in Maßnahme M 2.230 *Planung der Active Directory-Administration*.

Die sicherheitsrelevanten Kernaspekte der AD-Planung sind zusammengefasst:

- **Domänen sind administrative Grenzen**

  Domänen begrenzen die administrative Macht von Administratoren. Administratoren können daher nur innerhalb einer Domäne verwaltend tätig werden, so dass ihre Verwaltungsbefugnis standardmäßig nicht über die Domänengrenze reicht. Dies gilt insbesondere im Verbund mit mehreren Domänen (Baum, Wald), so dass die oft geäußerten Bedenken, dass durch das standardmäßig transitive Vertrauensmodell auch administrative Berechtigungen über Domänengrenzen hinweg möglich sind, für normale Administratorenkonten ausgeräumt werden können (siehe jedoch *Organisations-Admins* unten).

- **domänenübergreifende Zugriffe**

  Domänenübergreifende Zugriffe setzen voraus, dass in der Ziel-Domäne explizit Zugriffsberechtigungen für den Zugreifer aus einer anderen Domäne eingerichtet werden. Standardmäßig sind daher keine domänenübergreifenden Zugriffe möglich. Dies bedeutet, dass in einem Baum oder Wald ein Administrator einer Domäne "A" nur dann administrativ auf eine beliebige andere Domäne "B" zugreifen kann, falls der Domänen

administrator von "B" dem Administrator der Domäne "A" explizit Berechtigungen dazu einräumt (siehe jedoch *Organisations-Admins*).

- Die Mitglieder der Gruppe *Organisations-Admins* genießen einen Sonderstatus, da sie im gesamten Forest Administratorrechte auf dem AD besitzen. Insbesondere werden gesetzte Zugriffsrechte auf AD-Objekte bei Zugriffen von Organisations-Admins ignoriert. Die Mitgliedschaft in der Gruppe der Organisations-Admins muss daher restriktiv vergeben und strikt kontrolliert werden. Es ist zu beachten, dass ein Organisations-Admin benötigt wird, um beispielsweise eine Subdomäne anzulegen.

Organisations-Admins

- Administrative Delegation wird durch die Vergabe von Zugriffsrechten auf AD-Objekte und deren Attribute erreicht. Die Verteilung der Zugriffsrechte muss gemäß dem administrativen Modell erfolgen. Durch die Mechanismen für Zugriffsrechte im AD (Vererbung, Kontrolle der Vererbung, Wirkungsbereich von Zugriffseinstellungen) können sehr komplexe Berechtigungsstrukturen aufgebaut werden. Diese können sehr schnell unübersichtlich und nicht mehr administrierbar werden, so dass sich durch Fehlkonfigurationen im AD Sicherheitslücken ergeben können. Eine möglichst einfache Berechtigungsstruktur ist daher vorzuziehen.

Administrative Delegation

- Schemaänderungen sind kritische Operationen und dürfen nur von autorisierten Administratoren nach sorgfältiger Planung durchgeführt werden.

Schemaänderungen sorgfältig planen

Abschließend sei darauf hingewiesen, dass Fehler in der AD-Planung und den zugrunde liegenden Konzepten nach erfolgter Installation nur mit beträchtlichem Aufwand zu berichtigen sind. Nachträgliche Veränderungen in der AD-Struktur, wie z. B. die Anordnung von Domänen in Bäume und Forests, ziehen u. U. das komplette Neuaufsetzen von Domänen nach sich.

Ergänzende Kontrollfragen:

- Wurde eine AD-Planung durchgeführt?
- Sind alle Beteiligten in die Planung einbezogen worden?
- Ist ein bedarfsgerechtes AD-Berechtigungskonzept entworfen worden?
- Sind administrative Delegationen mit restriktiven und bedarfsgerechten Berechtigungen ausgestattet?

M 2.230 Planung der Active Directory-Administration

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Das Active Directory (AD) besteht aus verschiedenen Objekten, die baumartig organisiert sind. Jedes Objekt besteht aus bestimmten Attributen, die die Objektinformationen speichern. Durch Objekte geschieht die Verwaltung eines Windows 2000/XP Systems, die durch einen berechtigten Administrator erfolgen muss. Für alle AD-Objekte können Berechtigungen vergeben werden, die den Zugriff auf die Objekte steuern. Damit kann festgelegt werden, welche Objekte von welchen Benutzern in einer bestimmten Art und Weise verändert werden können, wie beispielsweise das Anlegen von Benutzern oder das Zurücksetzen von Benutzerpasswörtern.

Bei einer Standardinstallation von Windows 2000 besitzen nur Administratoren das Recht, Veränderungen an Objekten vorzunehmen und damit eine Domäne zu verwalten. Benutzer besitzen in der Regel maximal Leserecht.

Generell gilt auch unter Windows 2000, dass an der Domänengrenze auch die administrative Macht der Administratoren der Domäne endet. Lediglich die Mitglieder der Gruppe *Organisations-Admins* besitzen in jeder Domäne eines Forests Vollzugriff auf alle AD-Objekte, und zwar unabhängig von den für diese Objekte eingestellten Zugriffsrechten. Standardmäßig sind dies die Mitglieder der Administratorengruppe der Forest-Root-Domain (FRD).

Delegation administrativer Aufgaben

In großen Domänen empfiehlt sich die Delegation administrativer Aufgaben, so dass die administrative Last auf mehrere Administratoren verteilt ist oder auch, unter Umständen zusätzlich, eine Rollentrennung umgesetzt werden kann. Die Delegation administrativer Aufgaben erfolgt im AD durch die Vergabe von entsprechenden Zugriffsrechten auf AD-Objekte für die jeweiligen Adminstratorengruppen. Dabei erlaubt die AD-Rechtestruktur eine feingranulare Vergabe von Rechten. Auf diese Weise kann z. B. einem Administrator erlaubt werden, Benutzerkonten anzulegen und Benutzerpasswörter zurückzusetzen, jedoch nicht Benutzerkonten zu löschen oder in andere Organizational Units (OU, Organisationseinheiten) zu verschieben. Um die Vergabe gleichförmiger Rechte innerhalb eines kompletten Teilbaums zu vereinfachen, besteht zusätzlich die Möglichkeit, Rechte eines Objektes an Objekte im Unterbaum zu vererben. Da die Übernahme von vererbten Rechten durch bestimmte Objekte im Unterbaum unter Umständen nicht gewünscht ist, lässt sich die Übernahme für Objekte auch blockieren, so dass sich hier durchaus komplexe Szenarien für die Verteilung von Berechtigungen ergeben können (siehe auch M 3.27 *Schulung zur Active Directory-Verwaltung*).

Aus Sicherheitssicht ergeben sich folgende Aspekte, die bei der Planung der AD-Administration zu berücksichtigen sind:

restriktive Rechtevergabe

- Wird Delegation eingesetzt, so sollten nur die unbedingt notwendigen Rechte vergeben werden, die zur Ausübung der delegierten administrativen Tätigkeiten erforderlich sind.

Delegationsmodell dokumentieren

- Das Delegationsmodell und die daraus resultierenden Rechtezuordnungen müssen dokumentiert werden.

- Die administrativen Tätigkeiten sollten so delegiert werden, dass sich möglichst keine Überschneidungen ergeben. Ansonsten können durch zwei Administratoren sich widersprechende Veränderungen durchgeführt werden. Dies führt dann zu Replikationskonflikten, die von Windows 2000 automatisch aufgelöst werden, so dass sich eine der Änderungen auf jeden Fall durchsetzt. Es gibt jedoch für diesen Fall keine Warnungen. Es empfiehlt sich daher, das Administrationsmodell so zu entwerfen, dass möglichst überschneidungsfreie Zuständigkeiten existieren. Auf diese Weise kann die Gefahr von Replikationskonflikten verringert werden. Sind Replikationskonflikte zu erwarten oder bereits aufgetreten, so sollte in regelmäßigen Abständen oder nach wichtigen Änderungen eine manuelle Überprüfung erfolgen, ob sich immer die korrekten Werte durchgesetzt haben. Ob das Führen einer Evidenzdatenbank mit den Active Directory Soll-Daten unter Umständen organisatorisch sinnvoll ist, muss im Einzelfall entschieden werden.

- Wird für die Verwaltung des AD Delegation eingesetzt, so wird dies durch die Vergabe von entsprechenden Zugriffsrechten innerhalb des AD erreicht. Dabei wird in der Regel der Vererbungsmechanismus eingesetzt, um Berechtigungen auf Objekte in Teilbäumen zu verwalten. Komplexe Szenarien mit Delegation und damit Rechtevererbung sollten jedoch unbedingt vermieden werden, da sonst leicht Sicherheitslücken entstehen können. Beispielsweise kann der Fall eintreten, dass ein Benutzer zu wenige oder zu viele Rechte hat.

Komplexität reduzieren

- Es muss ein Konzept für die Mitgliedschaft in den verschiedenen administrativen Gruppen entworfen werden. Dabei sind vor allem die Bedingungen und Verfahren zu definieren, die festlegen, ob, wann und wie lange ein Benutzer oder eine Benutzergruppe in eine administrative Gruppe aufgenommen wird. Es muss insbesondere dafür Sorge getragen werden, die Mitgliedschaft in der Gruppe der Organisations-Admins restriktiv zu handhaben und zu kontrollieren. Falls es der organisatorische Ablauf zulässt, kann erwogen werden, alle Mitglieder in dieser Gruppe nach Aufbau der Domänenstruktur zu entfernen und nur bei Bedarf und unter Einhaltung des Vier-Augen-Prinzips entsprechende Mitglieder hinzuzufügen. Es muss jedoch berücksichtigt werden, dass ein Mitglied der Gruppe der Organisations-Admins immer dann benötigt wird, wenn eine neue Domäne im Forest angelegt werden soll.

Konzept für Gruppenmitgliedschaft schaffen

- Die Administratoren sind über die AD-Struktur und die organisatorischen Abläufe im Rahmen ihrer administrativen Tätigkeit zu informieren und entsprechend zu schulen, um zu verhindern, dass nicht-konforme Änderungen zu Sicherheitslücken führen. Beispielsweise kann es erforderlich sein, beim Anlegen eines neuen Benutzers diesen in entsprechende Sicherheitsgruppen aufzunehmen oder sogar zusätzlich eine neue Sicherheitsgruppe mit einem speziellen Namen anzulegen. Wird dies vergessen, so erhalten Benutzer unter Umständen fehlerhafte Berechtigungen.

Administratoren informieren und schulen

Tools verwenden

- Für große Domänen sollte über die Möglichkeit der werkzeuggestützten Verwaltung nachgedacht werden. Es gibt verschiedene kommerzielle und auch frei verfügbare Werkzeuge, die die AD-Verwaltung erleichtern. Es sollte überlegt werden, diese einzusetzen. Werden solche Werkzeuge verwendet, so muss sichergestellt werden, dass die AD-Verwaltung ausschliesslich durch diese Werkzeuge erfolgt.

Ergänzende Kontrollfragen:

- Wurde eine Planung der administrativen Gruppen zur AD-Verwaltung durchgeführt?
- Ist das Delegationsmodell überschneidungsfrei?
- Sind alle administrativen Aufgabenbereiche und Berechtigungen dokumentiert?
- Wurden die Administratoren durch Schulungen auf die AD-Verwaltung vorbereitet?

M 2.231 Planung der Gruppenrichtlinien unter Windows 2000

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Zur Konfiguration von Windows 2000 Rechnern steht der Mechanismus der so genannten Gruppenrichtlinien zur Verfügung. Schon unter Windows NT gab es mit den Gruppenrichtlinien ein ähnliches, aber deutlich weniger leistungsfähiges Instrument. Gruppenrichtlinien dienen im Active Directory dazu, einen Satz von Konfigurationseinstellungen, zu denen insbesondere auch Sicherheitseinstellungen gehören, auf eine Gruppe von Objekten anzuwenden. Durch ein so genanntes Gruppenrichtlinienobjekt (englisch *Group Policy Object, GPO*) wird ein vorgegebener Satz von Konfigurationsparametern (standardmäßig über 700) zusammengefasst. Für jeden Parameter kann ein konkreter Wert angegeben werden, der u. U. nur aus einem beschränkten Wertebereich stammt. Generell kann auch immer der Wert *nicht definiert* gewählt werden, so dass dann automatisch die Windows Standardeinstellungen für diese Parameter gelten. Die Standardeinstellungen sind in der Hilfedatei zu Gruppenrichtlinien, u. a. im Windows 2000 Server Resource Kit, dokumentiert.

Rechner- und Benutzereinstellungen

Die Parameter innerhalb eines Gruppenrichtlinienobjektes sind baumartig oder dateisystemartig thematisch zusammengefasst. Dabei ergibt sich eine generelle Zweiteilung auf oberster Ebene in Einstellungen für Rechner sowie für Benutzer. Aus Sicherheitssicht sind insbesondere die Einstellungen interessant, die sich unterhalb der folgenden "Pfade" finden:

- *Rechnereinstellungen\WindowsEinstellungen\Sicherheitseinstellungen*
- *Rechnereinstellungen\Administrative Einstellungen\ Windows Komponenten\Windows Installer*
- *Rechnereinstellungen\Administrative Vorlagen\System\Gruppenrichtlinien*
- *Benutzereinstellungen\Administrative Vorlagen\ Windows Komponenten\Microsoft Management Konsole*
- *Benutzereinstellungen\Administrative Einstellungen\ Windows Komponenten\Windows Installer*

Berechnung der jeweils gültigen Einstellungen

Windows 2000 berechnet generell für jeden an einer Domäne angemeldeten Rechner und für jeden angemeldeten Benutzer die jeweils gültigen Einstellungen für jeden Gruppenrichtlinienparameter. Diese Berechung ist nötig, da die Vorgaben für die Parametereinstellungen durch unterschiedliche Gruppenrichtlinienobjekte definiert sein können, die sich gegenseitig überlagern können. Folgende Gruppenrichtlinienobjekte können definiert werden:

1. Jeder Rechner besitzt ein lokal definiertes Gruppenrichtlinienobjekt. Dies erlaubt die Definition von Parametereinstellungen lokal auf dem Rechner, z. B. wenn keine Netzverbindung besteht.
2. Gruppenrichtlinienobjekte können über Windows 2000 Standorte (Sites) definiert werden. Damit können Einstellungen standortspezifisch adaptiert werden.

3. Innerhalb der Active Directory Struktur können Gruppenrichtlinienobjekte für das Domänenobjekt definiert werden, so dass damit Parametereinstellungen für Rechner und Benutzer innerhalb der gesamten Domäne gesteuert werden können.
4. Auf jedem OU-Objekt können Gruppenrichtlinien definiert werden, deren Einstellungen dann auf alle Rechner und Benutzer unterhalb dieses OU-Objektes wirken.

Reihenfolge LSDO

Für die Berechnung der jeweils für einen konkreten Rechner oder Benutzer geltenden Parametereinstellungen wird folgendes Berechnungs- bzw. Überdeckungsschema (Lokal <- Standort <- Domäne <- Organisationseinheit, LSDO) angewandt: Zunächst werden die lokalen Einstellungen berücksichtigt (L, Lokal). Dann werden diese Einstellungen durch die Einstellungen des Gruppenrichtlinienobjektes, das auf dem zugehörigen Standort definiert ist, überdeckt (S, Standort). Danach erfolgt die Überdeckung durch die auf dem relevanten Domänenobjekt definierten Gruppenrichtlinienobjekte (D, Domäne). Schließlich werden die Gruppenrichtlinienobjekte der OU-Objekte in der Reihenfolge angewandt, wie sie auf dem Weg vom Domänenobjekt zu dem OU-Objekt, das den jeweiligen Rechner oder Benutzer enthält, definiert sind (O, Organisationseinheit).

Blockieren und Erzwingen der Überdeckung

Die Überdeckung kann durch die Optionen *blockieren* bzw. *erzwingen* beeinflusst werden. Stehen die Einstellungen *blockieren* und *erzwingen* im Konflikt, so wird die Einstellung *erzwingen* durchgesetzt. Zusätzlich ist es auf OU-Ebene möglich, mehrere Gruppenrichtlinienobjekte für ein OU-Objekt zu definieren. Dabei erfolgt die Überdeckung gemäß der angegebenen Reihenfolge. Es ist dabei außerdem möglich, jedes einzelne Gruppenrichtlinienobjekt für ein OU-Objekt zu aktivieren oder zu deaktivieren.

Gruppenrichtlinienobjekte können im Active Directory nur auf OU-Objekten definiert werden, nicht jedoch auf einzelnen Rechnern oder Benutzerobjekten. Das lokal definierte Gruppenrichtlinienobjekt wird nicht im Active Directory gespeichert. Soll ein Gruppenrichtlinienobjekt, das auf einem OU-Objekt definiert ist, das Rechnerobjekte zusammenfasst, nicht auf alle enthaltenen Rechnerobjekte wirken, so besteht die Möglichkeit, durch die Vergabe von Zugriffsrechten auf das Gruppenrichtlinienobjekt die Anwendung auf ein konkretes Rechnerobjekt zu unterbinden. Hierzu ist diesem Rechnerobjekt das Zugriffsrecht *Anwenden* auf das Gruppenrichtlinienobjekt zu entziehen.

Links zwischen GPOs und OUs

Die bisher benutzte Darstellung der Definition von Gruppenrichtlinienobjekten auf OU-Objekten war jedoch vereinfacht: Gruppenrichtlinienobjekte werden separat im Active Directory gespeichert und bilden einen Pool von Objekten. Jedes definierte Gruppenrichtlinienobjekt kann nun einem oder auch mehreren OU-Objekten assoziiert werden. Man spricht dann von einem *Link*. Durch das Kennzeichnen eines Links als aktiviert oder deaktiviert wird das jeweilige Gruppenrichtlinienobjekt bei der Berechnung für das OU-Objekt herangezogen oder nicht (siehe oben). Für jedes Gruppenrichtlinienobjekt kann über den Eigenschaftsdialog festgestellt werden, mit welchen OU-Objekten ein *Link* besteht, d. h. auf welche Objekte sie potentiell wirken.

Aus Sicherheitssicht sind bei der Planung und im Umgang mit Gruppenrichtlinienobjekten folgende Aspekte zu berücksichtigen:

- Das Gruppenrichtlinienkonzept muss so einfach wie möglich gehalten werden. Komplexe Strukturen aus Mehrfachüberdeckungen sind zu vermeiden. Insbesondere sollte auf die Möglichkeit der Vergabe von Zugriffsrechten auf Gruppenrichtlinienobjekte nur in Ausnahmefällen zurückgegriffen werden. Generell muss das Gruppenrichtlinienkonzept so dokumentiert sein, dass Ausnahmeregelungen einfach zu erkennen sind.

GPO-Konzept möglichst einfach halten

- Das Gruppenrichtlinienkonzept und die OU-Objektstruktur beeinflussen sich gegenseitig wesentlich, da Gruppenrichtlinienobjekte im Active Directory nur auf OU-Objekte angewandt werden können und nicht auf Rechner- oder Benutzerobjekte. Beim Aufbau der OU-Gruppierungen ist daher darauf zu achten, dass nur Objekte, die mit gleichen GPO-Einstellungen versehen werden sollen, in einem OU-Objekt oder untergeordneten OU-Objekten zusammengefasst werden.

GPO-Konzept bei OU-Gruppierung beachten

- Durch die Rechteberechnung ist es möglich, die Verwaltung der Parametereinstellungen auf unterschiedliche "Orte" (Lokal, Standort, Domänen-Objekt, OU-Objekte) zu verteilen. Es muss daher für jeden Parameter entschieden werden, wo er definiert wird. Es ist dabei zu beachten, dass einige Parameter nur dann wirksam werden, wenn sie an bestimmten "Orten" definiert werden. So können z. B. die Passworteinstellungen nur auf Domänen-Objekten definiert werden.

Wo wird welcher Parameter definiert?

- Gruppenrichtlinienobjekte müssen vor unberechtigter Veränderung geschützt werden. Dazu müssen einerseits entsprechende Berechtigungen im Active Directory vergeben werden (siehe auch M 2.230 *Planung der Active Directory-Administration*, M 3.27 *Schulung zur Active Directory-Verwaltung*) und andererseits kann der Gebrauch von entsprechenden Verwaltungswerkzeugen, wie z. B. MMC-Gruppenrichtlinien-Snap-In oder Registrierungseditoren, für Benutzer unterbunden werden.

GPOs schützen

- Insbesondere für die sicherheitsrelevanten Parameter innerhalb eines Gruppenrichtlinienobjektes sind die Einstellungen festzulegen. Neben den oben angegebenen Einstellungen können je nach Anwendungsszenario auch weitere Parameter sicherheitsrelevant sein. Dazu zählen z. B. Internet-Explorer-Einstellungen.

sicherheitsrelevante Parameter festlegen

Die Einstellungen der verschiedenen Gruppenrichtlinienobjekte müssen sich dabei generell an den Sicherheitsrichtlinien des Unternehmens bzw. der Behörde orientieren und diese umsetzen.

Im Folgenden werden Vorgaben für die Sicherheitseinstellungen aufgezeigt, die als Ausgangsbasis für die Sicherheitseinstellungen innerhalb einer Gruppenrichtlinie dienen können. Die angegebenen Werte müssen auf jeden Fall an die lokalen Bedingungen angepasst werden. Im Rahmen des Gruppenrichtlinienkonzeptes sind die einzelnen Werte zudem auf unterschiedliche Gruppenrichtlinienobjekte zu verteilen und jeweils an den Verwendungszweck anzupassen (z. B. GPO für Server, GPO für Arbeitsplatzrechner). Dadurch können für einzelne Einträge auch jeweils unterschiedliche Werte zustande kommen.

Kennwortrichtlinie	
Richtlinie	**Computereinstellung**
Kennwortchronik erzwingen	6 Gespeicherte Kennwörter
Kennwörter müssen den Komplexitätsanforderungen entsprechen.	Aktiviert
Kennwörtern für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern	Deaktiviert
Maximales Kennwortalter	90 Tage
Minimale Kennwortlänge	6 Zeichen
Minimales Kennwortalter	1 Tag

Kontosperrungsrichtlinien	
Richtlinie	**Computereinstellung**
Kontensperrungsschwelle	3 Ungültige Anmeldeversuche
Kontosperrdauer	0 (Hinweis: Konto ist gesperrt, bis Administrator Sperrung aufhebt)
Kontosperrungszähler zurücksetzen nach	30 Minuten

Kerberos-Richtlinie	
Richtlinie	**Computereinstellung**
Benutzeranmeldeeinschränkungen erzwingen	Aktiviert
Max. Gültigkeitsdauer des Benutzertickets	8 Stunden
Max. Gültigkeitsdauer des Diensttickets	60 Minuten
Max. Toleranz für die Synchronisation des Computertakts	5 Minuten
Max. Zeitraum, in dem ein Benutzerticket erneuert werden kann	1 Tag

Überwachungsrichtlinie	
Richtlinie	**Computereinstellung**
Active Directory-Zugriff überwachen	Erfolgreich, Fehlgeschlagen
Anmeldeereignisse überwachen	Erfolgreich, Fehlgeschlagen
Anmeldeversuche überwachen	Erfolgreich, Fehlgeschlagen
Kontenverwaltung überwachen	Erfolgreich, Fehlgeschlagen
Objektzugriffsversuche überwachen	Fehlgeschlagen
Prozessverfolgung überwachen	Keine Überwachung
Rechteverwendung überwachen	Fehlgeschlagen
Richtlinienänderungen überwachen	Erfolgreich, Fehlgeschlagen
Systemereignisse überwachen	Erfolgreich, Fehlgeschlagen

Zuweisen von Benutzerrechten	
Richtlinie	**Computereinstellung**
Als Dienst anmelden	Definiert, aber leer
Ändern der Systemzeit	Administratoren
Anheben der Zeitplanungspriorität	Administratoren
Anheben von Quoten	Administratoren
Anmelden als Stapelverarbeitungsauftrag	Definiert, aber leer
Anmeldung als Batchauftrag verweigern	Nicht definiert
Anmeldung als Dienst verweigern	Nicht definiert
Auf diesen Computer vom Netzwerk aus zugreifen	Jeder, Administratoren, Authentisierte Benutzer, Sicherungs-Operatoren
Auslassen der durchsuchenden Überprüfung	Jeder
Debuggen von Programmen	Nicht definiert
Einsetzen als Teil des Betriebssystems	Definiert, aber leer
Entfernen des Computers von der Dockingstation	Administratoren
Ermöglichen, dass Computer- und Benutzerkonten für Delegierungszwecke vertraut wird	Administratoren
Ersetzen eines Tokens auf Prozessebene	Definiert, aber leer
Erstellen einer Auslagerungsdatei	Administratoren
Erstellen eines Profils der Systemleistung	Administratoren
Erstellen eines Profils für einen Einzelprozess	Administratoren
Erstellen eines Tokenobjekts	Definiert, aber leer
Erstellen von dauerhaft freigegebenen Objekten	Definiert, aber leer
Erzwingen des Herunterfahrens von einem Remote-system aus	Administratoren
Generieren von Sicherheitsüberwachungen	Definiert, aber leer
Herunterfahren des Systems	Administratoren
Hinzufügen von Arbeitsstationen zur Domäne	Definiert, aber leer
Laden und Entfernen von Gerätetreibern	Administratoren
Lokal anmelden	Administratoren, Sicherungs-Operatoren
Lokale Anmeldung verweigern	Nicht definiert
Sichern von Dateien und Verzeichnissen	Sicherungs-Operatoren
Sperren von Seiten im Speicher	Definiert aber leer
Synchronisieren von Verzeichnisdienstdaten	Definiert, aber leer Hinweis: Gemäß der Dokumentation zum Ressorce-Kit findet diese Einstellung in der gegenwärtigen Version von Windows 2000 keine Anwendung.

Übernehmen des Besitzes von Dateien und Objekten	Administratoren
Verändern der Firmwareumgebungsvariablen	Administratoren
Verwalten von Überwachungs- und Sicherheits-protokollen	Administratoren
Wiederherstellen von Dateien und Verzeichnissen	Administratoren
Zugriff vom Netzwerk auf diesen Computer verwei-gern	Nicht definiert

Sicherheitsoptionen	
Richtlinie	**Computereinstellung**
Administrator umbenennen	Nicht definiert
Anwender vor Ablauf des Kennworts zum Ändern des Kennworts auffordern	7 Tage
Anwendern das Installieren von Druckertreibern nicht erlauben	Aktiviert
Anzahl zwischenzuspeichernder vorheriger Anmel-dungen (für den Fall, dass der Domänencontroller nicht verfügbar ist)	0 Anmeldungen
Auslagerungsdatei des virtuellen Arbeitspeichers beim Herunterfahren des Systems löschen	Aktiviert
Auswerfen von NTFS-Wechselmedien zulassen	Administratoren
Benutzer automatisch abmelden, wenn die Anmelde-zeit überschritten wird (lokal)	Aktiviert
Benutzer nach Ablauf der Anmeldezeit automatisch abmelden	Aktiviert
Clientkommunikation digital signieren (immer)	Deaktiviert
Clientkommunikation digital signieren (wenn möglich)	Aktiviert
Die Verwendung des Sicherungs- und Wieder-herstellungsrechts überprüfen	Deaktiviert
Gastkonto umbenennen	Nicht definiert
Herunterfahren des Systems ohne Anmeldung zulassen	Deaktiviert
LAN Manager-Authentisierungsebene	Nur NTLMv2-Antworten senden\LM verweigern
Leerlaufzeitspanne bis zur Trennung der Sitzung	15 Minuten
Letzten Benutzernamen nicht im Anmeldedialog anzeigen	Aktiviert
Nachricht für Benutzer, die sich anmelden wollen	Nicht definiert
Nachrichtentitel für Benutzer, die sich anmelden wollen	Nicht definiert
Serverkommunikation digital signieren (immer)	Deaktiviert

Sicherheitsoptionen (Fortsetzung)	
Richtlinie	**Computereinstellung**
Serverkommunikation digital signieren (wenn möglich)	Aktiviert
Serveroperatoren das Einrichten von geplanten Tasks erlauben (Nur für Domänencontroller)	Nicht definiert
Sicherer Kanal: Daten des sicheren Kanals digital signieren (wenn möglich)	Aktiviert
Sicherer Kanal: Daten des sicheren Kanals digital verschlüsseln (wenn möglich)	Aktiviert
Sicherer Kanal: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)	Deaktiviert
Sicherer Kanal: Starker Sitzungsschlüssel erforderlich (Windows 2000 oder höher)	Deaktiviert (Hinweis: In reinen Windows 2000 Umgebungen aktivieren)
Standardberechtigungen globaler Systemobjekte (z. B. symbolischer Verknüpfungen) verstärken	Aktiviert
STRG+ALT+ENTF-Anforderung zur Anmeldung deaktivieren	Deaktiviert (Hinweis: D. h. STRG+ALT+ENTF ist erforderlich)
System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können	Deaktiviert
Systemwartung des Computerkontokennworts nicht gestatten	Deaktiviert
Unverschlüsseltes Kennwort senden, um Verbindung mit SMB-Servern von Drittanbietern herzustellen	Deaktiviert
Verhalten bei der Installation von nichtsignierten Dateien (außer Treibern)	Warnen, aber Installation zulassen
Verhalten bei der Installation von nichtsignierten Treibern	Warnen, aber Installation zulassen
Verhalten beim Entfernen von Smartcards	Computer sperren
Weitere Einschränkungen für anonyme Verbindungen	Kein Zugriff ohne explizite anonyme Berechtigung
Wiederherstellungskonsole: Automatische administrative Anmeldungen zulassen	Deaktiviert
Wiederherstellungskonsole: Kopieren von Disketten und Zugriff auf alle Laufwerke und alle Ordner zulassen	Deaktiviert
Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken	Aktiviert
Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken	Aktiviert
Zugriff auf globale Systemobjekte prüfen	Deaktiviert

Ereignisprotokoll	
Richtlinie	**Computereinstellung**
Anwendungsprotokoll aufbewahren für	Nicht definiert
Aufbewahrungsmethode des Anwendungsprotokolls	Ereignisse bei Bedarf überschreiben
Aufbewahrungsmethode des Sicherheitsprotokolls	Ereignisse bei Bedarf überschreiben Hinweis: Im Hochsicherheitsbereich ist folgende Einstellung zu wählen: Ereignisse nicht überschreiben (Protokoll manuell aufräumen)
Aufbewahrungsmethode des Systemprotokolls	Ereignisse bei Bedarf überschreiben
Gastkontozugriff auf Anwendungsprotokoll einschränken	Aktiviert
Gastkontozugriff auf Sicherheitsprotokoll einschränken	Aktiviert
Gastkontozugriff auf Systemprotokoll einschränken	Aktiviert
Maximale Größe des Anwendungsprotokolls	30080 Kilobytes
Maximale Größe des Sicherheitsprotokolls	100992 Kilobytes
Maximale Größe des Systemprotokolls	30080 Kilobytes
Sicherheitsprotokoll aufbewahren für	Nicht definiert
System bei Erreichen der max. Sicherheitsprotokoll-größe herunterfahren	Deaktiviert (Hinweis: Für Hochsicherheitssysteme aktivieren)
Systemprotokoll aufbewahren für	Nicht definiert

Ergänzende Kontrollfragen:

- Wurde das GPO-Konzept bedarfsgerecht entworfen?
- Sind alle GPOs durch restriktive Zugriffsrechte geschützt?
- Sind für alle GPO-Parameter in allen GPOs Vorgaben festgelegt?

M 2.232 Planung der Windows 2000/2003 CA-Struktur

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator

Windows 2000/2003 wird mit eigenen PKI-Komponenten ausgeliefert, die den Aufbau einer unternehmensweiten Zertifikatshierarchie ermöglichen. Kernstück einer PKI (Public Key Infrastruktur) ist die so genannte Zertifizierungsstelle (Certificate Authority, CA), die Zertifikate ausstellen kann. Für den Betrieb von Windows 2000/2003 ist der Betrieb einer CA zwar generell nicht notwendig, jedoch immer dann zwingend, wenn bestimmte Eigenschaften oder Funktionen genutzt werden sollen, wie z. B. Anmeldung mit Chipkarte oder abgesicherte Kommunikation zwischen Windows Systemkomponenten über SSL. Windows 2000 und Windows Server 2003 bieten zwei Ausprägungen einer CA an:

1. Stand-alone-CA (alleinstehende Zertifizierungsstelle) und
2. Enterprise-CA (Organisationsweite Zertifizierungsstelle).

Der Hauptunterschied zwischen den beiden CA-Versionen ist, dass die Enterprise-CA im Active Directory integriert ist und damit vom Active Directory als Verzeichnisdienst profitiert. Beispielsweise werden Zertifizierungsstellen im Active Directory veröffentlicht, und Zertifikate können in großem Umfang automatisch ausgestellt und verteilt werden. Bei der Stand-alone-CA wird die Zertifikatsanforderung immer vom Administrator der CA geprüft. Die Zertifikatserzeugung muss durch den Administrator von Hand angestoßen werden. Die Stand-alone-CA kann auch auf einem nicht vernetzten Rechner installiert und betrieben werden, wohingegen die Enterprise-CA sinnvoll nur auf einem vernetzten Rechner ablaufen kann. Ab Windows Server 2003 Enterprise Edition können bei der Enterprise-CA die Zertifikatsvorlagen individuell angepasst werden.

Beide CA-Versionen eignen sich für den Aufbau von Zertifikatshierarchien und können daher auch als untergeordnete CA fungieren. Für viele infrastrukturelle Zwecke eines LANs ist die Enterprise-CA besser geeignet und sollte im Normalfall bevorzugt werden.

Insbesondere bei der Planung einer behörden- oder unternehmensweiten PKI sollte darauf geachtet werden, dass alle Einsatzszenarien und die dadurch betroffenen Applikationen bekannt sind. Um die technische Machbarkeit abschätzen zu können, empfiehlt es sich, alle Komponenten, die eingesetzt werden sollen, im Vorfeld auf ihre Interoperabilität zu überprüfen.

Eine Auflistung struktureller Planungsaspekte ist auf den BSI-Webseiten unter den Hilfsmittel zum IT-Grundschutz zu finden (siehe Hilfsmittel für die Planung der Windows 2000/2003 CA-Struktur). Generell gilt, dass alle für den Betrieb einer CA relevanten organisatorischen, technischen und auch sicherheitstechnischen Rahmenbedingungen in einem entsprechenden Konzept dokumentiert werden müssen.

Planung des Einsatzes geeigneter Zertifizierungsstellen

Organisatorische Aspekte:

Zuständigkeiten regeln

- Die Planung einer PKI erfordert Zeit. In der Regel müssen insbesondere innerorganisatorische Zuständigkeiten geregelt und festgeschrieben werden.
- Der Verwendungszweck von Zertifikaten spielt bei der Planung der CA-Struktur eine wichtige Rolle. So bereitet der Aufbau einer generellen, organisationsweiten Zertifikatsinfrastruktur meist mehr Schwierigkeiten, als der Aufbau einer applikationsbezogenen PKI. Eine applikationsbezogene PKI kann beispielsweise eingesetzt werden, wenn im Rahmen einer netzbasierten Anwendung nur die betroffenen Mitarbeiter zuverlässig identifiziert werden müssen. Ein Beispiel hierfür ist das elektronische Einreichen und Bearbeiten von Urlaubsanträgen, wobei die Anträge nacheinander von verschiedenen Personen digital abgezeichnet, also signiert, werden müssen.
- Werden Zertifikate nur innerhalb einer Behörde bzw. eines Unternehmens genutzt, so sollten diese nur von CAs vergeben werden, die ausschließlich intern genutzte Zertifikate ausstellen. Solche internen CAs dürfen keine Zertifikate nach "außen" geben, z. B. an Personen oder Geräte, die nicht in der Behörde oder dem Unternehmen eingesetzt werden. Eine interne CA sollte nicht von außen über das Internet erreichbar sein, deshalb ist auch keine Überprüfung von nach außen gegebenen Zertifikaten möglich.

Nutzungsrichtlinien dokumentieren

- Für extern genutzte Zertifikate und die ausstellenden CAs sind die Nutzungsrichtlinien zu definieren und zu dokumentieren. Es ist dabei insbesondere darauf zu achten, dass entsprechende Anforderungen an die Qualität der Identitätsprüfung gestellt und umgesetzt werden.

Technische Aspekte:

Mangelnde Interoperabilität

- Es muss geplant werden, welche kryptographischen Verfahren und Algorithmen und welche Schlüssellängen zum Einsatz kommen sollen (siehe auch M 2.162 *Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte*).

CAs besonders schützen

- Das Vertrauen in Zertifikate einer CA hängt wesentlich von deren Sicherheitsgrad ab. Daher ist für CAs, die sicherheitskritische Zertifikate erzeugen, besonders auf die physikalische und softwaretechnische Sicherheit zu achten. Sicherheitskritisch sind insbesondere solche Zertifikate, die einen großen Anwenderkreis haben oder von deren Korrektheit weitere sicherheitskritische Anwendungen abhängen.
- Für Zertifikate mit unterschiedlichem Sicherheitsbedarf sollten unterschiedliche CAs eingesetzt werden.
- Beim Einsatz von CA-Hierarchien muss das Gültigkeitsmodell festgelegt werden. Dabei ist es wichtig festzulegen, wie nachgeordnete Zertifikate zu behandeln sind, wenn z. B. das Root-CA-Zertifikat (aus welchen Gründen auch immer) gesperrt werden muss.

- Für die verschiedenen Zertifikatstypen (z. B. Root-CA-Zertifikat, Benutzer-E-Mail-Zertifikat) muss jeweils die maximale Gültigkeitsdauer festgelegt werden. Im Allgemeinen ist es sinnvoll, dass die Gültigkeitsdauer der Zertifikate nicht die Gültigkeitsdauer des Zertifikates der ausstellenden CA überschreitet. Es gibt hier allerdings verschiedene Gültigkeitsmodelle (z. B. so genannte "Kettenmodelle" und "Schalenmodelle"). Beispielsweise kann bei Signaturen nach dem deutschen Signaturgesetz die Gültigkeit der einzelnen Zertifikate länger sein als die Gültigkeit des CA-Zertifikates.
- Die Möglichkeiten und Verfahren nach Ablauf der Gültigkeit eines Zertifikates sind festzulegen. Sind z. B. Verlängerungen möglich oder müssen neue Zertifikate ausgestellt werden?

Sind Verlängerungen möglich?

Neben der Planung einer PKI spielt insbesondere die Sicherheit im laufenden Betrieb der einzelnen PKI-Komponenten eine große Rolle. Die Absicherung einer Zertifizierungsstelle muss dem Schutzbedarf der jeweiligen Anwendung genügen, in der Zertifikate verwendet werden. Empfehlungen dazu finden sich in M 4.144 *Nutzung der Windows 2000 CA* und unter den Hilfsmittel zum IT-Grundschutz (siehe *Hilfsmittel für den Schutz der Zertifikatsdienste unter Windows Server 2003)*.

Versionsspezifische Planungsaspekte für eine Windows-Server-2003 CA

Verteilung von Zertifikaten:

Auto-Enrollment

Der Vorgang des Anforderns und Austellens (kurz: der Verteilung) von Zertifikaten kann automatisch (ohne Benutzereingriff) oder manuell erfolgen. Die automatische Verteilung von Zertifikaten (*Auto-Enrollment*) basiert auf Active Directory und Gruppenrichtlinien (vergleiche M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000* Auto-Enrollment ist ein mächtiges Werkzeug, das die Verwaltung von Zertifikaten von Benutzern (ab Windows Server 2003 Enterprise Edition) und Computern für bestimmte Anwendungen im Organisationsumfeld stark vereinfacht. Häufiges Beispiel ist das Verteilen von Verschlüsselungszertifikaten für das *Encrypting File System* (EFS) auf Clients. Das Zertifikats-Enrollment wird nur für autentisierte Clients durchgeführt und ist mit entsprechenden Sicherheitsmechansimen und Berechtigungen versehen. Die Einstellungen sind im Gruppenrichtlinienobjekt-Editor unter

Computerkonfiguration | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Richtlinien öffentlicher Schlüssel* | *Eigenschaften* von *Einstellungen für die automatische Registrierung*

und

Benutzerkonfiguration | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Richtlinien öffentlicher Schlüssel* | *Eigenschaften* von *Einstellungen für die automatische Registrierung*

zu finden. Standardmäßig fordern nur Domänencontroller automatisch ein Computerzertifikat an. Einige optionale Windows-Komponenten fordern ebenfalls automatisch ein Zertifikat an, z. B. erhält jeder Client mit aktiviertem EFS automatisch ein EFS-Zertifikat. Auto-Enrollment sollte jedoch nur im tatsächlich benötigten Umfang eingesetzt werden, da sonst

die Verwaltung erschwert wird und unter anderem auch die Gefahr des Abfangens von Schlüsseln besteht.

Es sollte auf Grundlage der geplanten Applikationen bzw. Windows-Komponenten überlegt werden, welche Zertifikatstypen für welche Benutzer bzw. Computer zugelassen sind und auf welche Weise die Verteilung stattfindet. Entsprechend sind die Gruppenrichtlinien und die Berechtigungen in den Zertifikatsdiensten zu planen.

Archivierung von privaten Schlüsseln:

Die Archivierung von privaten Schlüsseln in der Zertifizierungsstelle (ab Windows Server 2003 Enterprise Edition) sollte nur dann aktiviert werden, wenn ein geeignetes Konzept zur Rollentrennung der PKI-Verwaltung geplant und umgesetzt wurde. Die Archivierung kann die Gefahr des Schlüsselverlusts einzelner Benutzer verringern, allerdings wird das Risiko des Missbrauchs erhöht. Deshalb ist sie nicht zu empfehlen. Die geeignete Strategie ist abhängig von den eingesetzten Anwendungen und Komponenten und sollte durch die PKI-Planung und in einer IT-Sicherheitsrichtlinie festgelegt werden.

Rollentrennung:

Rollentrennung durchsetzen

Rollentrennung bedeutet, dass die Konzentration mehrerer oder aller kritischer Verwaltungsrollen im Zusammenhang mit PKI auf eine Person, bzw. ein Benutzerkonto, verhindert wird. Dazu muss zunächst die Rollentrennung auf organisatorischer Ebene definiert sein (siehe oben). Auf technischer Seite kann die Rollentrennung durch das System erzwungen werden (ab Windows Server 2003 Enterprise Edition). Die vier Rollen sind:

- Zertifizierungsstellenadministrator
- Zertifikatverwaltung
- Sicherungs-Operator
- Prüfer

Details zu den Rollen sind im Hilfethema *Rollenbasierte Verwaltung* der integrierten Windows-Hilfe zu finden.

Ein Benutzerkonto, das vorher zwei oder mehr der genannten Rollen inne hatte, wird durch die Rollentrennung von allen Verwaltungstätigkeiten an der CA ausgeschlossen. Die Rollen müssen durch einen Administrator neu zugeteilt werden. Bei einer fehlerhaften Konfiguration der Rollentrennung ist die CA nicht mehr nutzbar. Wenn diese Funktion eingesetzt werden soll, ist hierfür zunächst ein geeignetes Berechtigungskonzept zu erstellen, welches dann in einem Testszenario erprobt werden sollte.

Ergänzende Kontrollfragen:

- Wurde eine bedarfsgerechte PKI-Planung durchgeführt?
- Ist die CA-Hierarchie mit allen Verantwortlichkeiten und Nutzungsbestimmungen dokumentiert?
- Sind alle Zertifizierungsstellen bzw. Zertifizierungsdienste gemäß dem Schutzbedarf der jeweiligen Anwendungen abgesichert?
- Wurde festgelegt, welcher Benutzer welche Zertifikate erhält?

- Wurden alle Parameter wie etwa die Gültigkeit für alle Zertifikatstypen definiert?
- Wurde ein Berechtigungskonzept für die Trennung der Verwaltungsrollen erstellt?

M 2.233 Planung der Migration von Windows NT auf Windows 2000

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

In der Regel wird ein auf Windows 2000 basierendes Netz nicht vollständig neu aufgebaut, sondern es existiert bereits ein Behörden- oder Unternehmensnetz, welches meist auf Vorgängerversionen wie Windows NT beruht. Auch eine Umstellung von einer alten Windows-Version auf Windows 2000 ist in der Regel schon für Netze mittlerer Größe nur in mehreren Schritten und über einen längeren Zeitraum hin möglich. Diese Migration erfordert sorgfältige Planung, da sich in der Zeit der Umstellung leicht Sicherheitslücken ergeben können.

Für die Migration stehen verschiedene Migrationsverfahren zur Verfügung. Eine generelle Empfehlung für eines der Verfahren kann jedoch nicht gegeben werden, da das günstigste Verfahren sehr von den lokalen Gegebenheiten abhängt und zusätzlich darauf zugeschnitten werden muss.

Für die Migration auf Windows 2000 kann unterschieden werden zwischen

- Migration einer Domäne,
- Migration von Servern und
- Migration von Clients.

Die Umstellung einer Domäne von Windows NT auf Windows 2000 erfolgt dabei durch die Umstellung von Domänen-Controllern auf Windows 2000. Generell kann bei der Migration von Domänen zwischen zwei Varianten unterschieden werden:

1. Dem so genannten *Domain Upgrade* oder *In-place Upgrade*, bei dem die existierenden Domänenstrukturen eins-zu-eins nach Windows 2000 übernommen werden. Dies hat den Vorteil, dass die Umstellung keine großen Restrukturierungen mit sich bringt, und aus Benutzersicht lediglich ein Betriebssystem-Update erfolgt. Nachteilig kann jedoch sein, dass dadurch auch existierende Unzulänglichkeiten automatisch in das Windows 2000 System übernommen werden.

Domain Upgrade

2. Der so genannten *Domänen Restrukturierung*, *Domain Restructure* oder *Domain Consolidation*, bei der eine neue Windows 2000 Domänenstruktur aufgebaut wird. Hier wird die Umstellung auf Windows 2000 genutzt, um existierende Unzulänglichkeiten in der zurzeit benutzten Domänenstruktur durch Reorganisation zu verbessern. Dieses Vorgehen entspricht meist einem völligen Neuaufbau. Es bietet den Vorteil, dass hierbei alte und schwer administrierbare Strukturen durch neue ersetzt werden können. So sind einige unter Windows NT geltende Limitierungen aufgehoben worden. Außerdem ist es möglich, u. U. veränderten Geschäftsanforderungen und lokalen Gegebenheiten besser zu entsprechen. Es ist dabei jedoch zu beachten, dass die Planung und Umsetzung der neuen Struktur meist mit großem Aufwand verbunden ist.

Domain Restructure

native mode oder mixed mode

Im Rahmen der Migration einer Domäne ist zusätzlich von Bedeutung, ob nach Abschluss der Migration weiterhin Windows NT Backup-Domänen-Controller (BDC) innerhalb der Domäne betrieben werden oder nicht. Davon hängt ab, ob die Windows 2000 Domäne im so genannten "nativen Modus" (*native mode*) oder im so genannten "gemischten Modus" (*mixed mode*) betrieben werden kann. Im gemischten Modus unterstützen die Windows 2000 Domänen-Controller weiterhin alle Mechanismen und Protokolle, um mit den BDCs wie ein Windows NT Primärer Domänen-Controller (PDC) zu kommunizieren. Dies hat jedoch den Nachteil, dass auch unter Windows 2000 bestimmte Funktionen, die von Windows NT nicht unterstützt werden, nicht genutzt werden können. Existieren nach der Migration keine Windows NT BDCs im Netz, so kann die Windows 2000 Domäne in den nativen Modus geschaltet werden. Es sei an dieser Stelle darauf hingewiesen, dass auch Client- oder Server-Rechner mit älteren Windows Versionen durchaus Mitglied in einer Windows 2000 Domäne sein können, die im nativen Modus betrieben wird. Vor der Umstellung einer Domäne auf den nativen Modus ist zu beachten, dass diese Umstellung nicht wieder rückgängig gemacht werden kann. Eine Rückkehr zu einer Windows NT-Domäne ist dann nicht mehr möglich.

Die wesentlichen Einschränkungen des gemischten Modus sind:

- Es existiert eine Größeneinschränkung der Windows NT SAM.
- Folgende, unter Windows 2000 neu eingeführte Gruppentypen und Funktionen stehen nicht zur Verfügung:
  - Universelle Sicherheitsgruppen
  - Domänen-lokale Gruppen
  - Verschachtelte Gruppen
  - Transitive Kerberos-Vertrauensstellungen

Vorteilhaft am gemischten Modus ist, dass jederzeit wieder auf Windows NT umgestellt werden kann, indem ein vorhandener Windows NT BDC zum PDC heraufgestuft wird, nachdem alle Windows 2000 Domänen-Controller vom Netz genommen worden sind.

Für die eigentliche Rechnerumstellung auf Windows 2000 kann grob zwischen folgenden Verfahren unterschieden werden, die sich im wesentlichen im zusätzlichen Hardware-Bedarf unterscheiden:

In-place-Umstellung

1. In-place-Umstellung: Bei dieser Umstellungsart kommt die jeweilige Update-Version von Windows 2000 zum Einsatz. Auf die Rechner wird - nach vorheriger Datensicherung - Windows 2000 aufgespielt. Dabei wird das Vorgängersystem durch Windows 2000 ersetzt und analog zur existierenden Version konfiguriert. Bei dieser Variante ist keine zusätzliche Hardware notwendig. Nachteilig ist jedoch, dass der umzustellende Rechner während der Umstellung nicht zur Verfügung steht.

separates Netz

2. Migration durch parallelen Aufbau eines separaten Windows 2000 Netzes: Bei dieser Migrationsart wird parallel zum existierenden Netz ein äquivalentes Windows 2000 Netz aufgebaut. Nach erfolgreichem Aufbau des Parallelnetzes wird dieses genutzt. Vorteilhaft ist hierbei, dass das existie-

rende System nicht beeinflusst wird. Nachteilig ist hier jedoch der hohe Bedarf an zusätzlicher Hardware.

3. Rollende Migration: Bei dieser Variante der parallelen Migration wird das existierende Netz in Teilbereiche aufgeteilt. Die Teilbereiche werden dann nacheinander auf Windows 2000 umgestellt. Dabei wird zunächst jeweils für das Teilnetz eine parallele Struktur aufgebaut, die dann nach erfolgtem Aufbau genutzt wird. Die so freigesetzte Hardware des Altsystems kann dann für den Aufbau des parallelen Systems des nächsten Teilsystems genutzt werden.

rollende Migration

Für die Migrationsreihenfolge von Rechnern kann unterschieden werden zwischen:

1. Client-Update-first: Hierbei werden zunächst die Arbeitsplatzrechner auf Windows 2000 umgestellt und innerhalb der existierenden NT Domäne betrieben. Danach werden die Server und die Domäne nach Windows 2000 migriert. Vorteil dieser Umstellungsart ist, dass Benutzer bereits mit der neuen Bedienoberfläche arbeiten können, ohne dass serverseitig wichtige Systemdienste umgestellt werden müssen.
2. Server-Update-first: Hierbei werden zunächst die Server auf Windows 2000 umgestellt. In der Regel erfolgt dabei zunächst eine Domänen-Umstellung und die Server werden in die Windows 2000 Domäne integriert. Danach erfolgt die Umstellung der Clients. Vorteil dieser Umstellungsart ist, dass Benutzer mit dem gewohnten Client-Betriebssystem arbeiten können und die Umstellung der wichtigen Systemdienste im Hintergrund vollzogen werden kann.

Wie bereits erwähnt, kann an dieser Stelle keine Empfehlung für eine der Migrationsvarianten gegeben werden. Generell sind für die Planung der Migration jedoch folgende Aspekte zu bedenken:

Zeitplan erstellen

- Es muss ein realistischer Zeitplan für die Migration erstellt werden. Im Laufe der Migrationsplanung muss mit Angleichungen des Zeitplanes gerechnet werden.
- Es muss sichergestellt sein, dass die existierenden Betriebssysteme auf Windows 2000 umgestellt werden können: So ist es z. B. nicht möglich, Windows NT 3.51 direkt auf Windows 2000 umzustellen. Hier muss eine Zwischenumstellung, z. B. auf Windows 95/98 oder NT 4.0, eingeplant werden.
- Die existierende Domänenstruktur muss erfasst werden. Nur so kann eine korrekte Planung der Windows 2000 Domänenstruktur erfolgen.

Notfallplan erstellen

- Es muss ein Notfallplan erstellt werden, der sicherstellt, dass bei einem fehlgeschlagenen Migrationsversuch ein operatives System schnell wiederhergestellt werden kann.
- Der Migrationsplan muss eine Strategie zur Umstellung der Domain Controller festlegen (In-place-Upgrade, Parallel-Upgrade, Reihenfolge).
- Die Reihenfolge, in der die existierenden Domänen umgestellt werden sollen, muss festgelegt werden. Da die erste umgestellte Domäne die Rolle der so genannten Forest-Root-Domäne (FRD) erhält, ist die Wahl der

Domäne, die als erste umgestellt werden soll, besonders wichtig. Es kann u. U. sinnvoll sein, keine der existierenden Domänen mit der Rolle der FRD zu betrauen und die FRD völlig neu zu erzeugen.

- Für jede Domäne muss entschieden werden, ob und wann diese in den nativen Modus umgeschaltet wird. Ziel einer Migration sollte immer die vollständige Umschaltung aller Domänen in den nativen Modus sein.
- Im Rahmen der Migrationsplanung sollte entschieden werden, ob eine Restrukturierung der Domänen notwendig oder gewünscht ist. Ist dies der Fall, muss der Restrukturierungsprozess geplant werden.

Sollen Domänen restrukturiert werden?

- Für jede Domäne muss die Migration von Benutzern und Benutzergruppen geplant werden. Es ist dabei darauf zu achten, dass die Migration Einfluss auf die Zugriffsberechtigungen hat, da sich die SID eines Benutzerkontos bei der Migration ändert. Windows 2000 bietet hier den Mechanismus der so genannten SID-History an, der es einem nach Windows 2000 migrierten Benutzerkonto erlaubt, unter der Prä-Windows 2000 Identität (SID) auf Ressourcen zuzugreifen. Es ist hierbei darauf zu achten, dass einerseits die SID-History nach der vollständigen Migration für alle Benutzerkonten gelöscht wird und andererseits nicht alle Windows 2000 Vorgängerversionen SID-Histories unterstützen, z. B. Windows NT 3.51.

Wie und wann werden Benutzer und Gruppen migriert?

- Für jede Domäne muss die Migration von Rechnern, also Clients und Servern, geplant werden. Es ist dabei darauf zu achten, ob insbesondere die Migration von Applikationsservern problemlos möglich ist, oder ob bestimmte Applikationen eine Migration verhindern, weil diese beispielsweise auf einem BDC installiert sein müssen. Werden Clients vor Servern auf Windows 2000 umgestellt und ohne Windows 2000 Active Directory Unterstützung betrieben, so muss berücksichtigt werden, dass nach Umstellung der Server auf Windows 2000 und Einführung des Active Directory u. U. eine nochmalige Neuinstallation der Clients notwendig ist, um deren gewünschte Systemkonfiguration sicherzustellen.

Wie und wann werden Clients und Server migriert?

- Während der Migration existieren Windows 2000 Domänen und (meist) Windows NT Domänen nebeneinander. Der Zugriff auf Ressourcen der NT Domäne kann dabei auch über schon nach Windows 2000 migrierte Benutzerkonten erfolgen. Zwischen Windows 2000 Domänen und Windows NT Domänen muss jedoch eine explizite Vertrauensstellung definiert werden, damit der Zugriff erfolgen kann. Es sollten hierbei nur die notwendigen Vertrauensstellungen erzeugt werden. Es empfiehlt sich außerdem, NT-Kontendomänen vor NT-Ressourcendomänen auf Windows 2000 umzustellen. Dadurch muss die Vertrauensstellung nur einseitig von den NT-Ressourcendomänen für eine Windows 2000 Domäne erfolgen.

Vertrauensstellung zwischen alten und neuen Domänen

- Bei der Durchführung der Migration werden in der Regel diverse Migrationswerkzeuge eingesetzt. In der Migrationsplanung muss auch der Werkzeugeinsatz geplant werden. Es ist festzulegen, welche Werkzeuge für welche Migrationsschritte zum Einsatz kommen sollen.

Welche Tools werden eingesetzt?

- Während der technischen Migrationsvorbereitung findet in der Regel eine Informationssammelphase statt, bei der - meist werkzeuggestützt - Systeminformationen, wie Benutzerkonten, Zugriffsrechte usw., zusammengetragen werden. Damit die benutzten Werkzeuge auf diese Infor-

mationen zugreifen können, ist es je nach Vorgehensweise notwendig, zusätzliche Vertrauensstellungen zwischen den existierenden NT-Domänen einzurichten. Es ist dabei zu beachten, dass dadurch potentielle Sicherheitslücken erzeugt werden können.

- Oft wird ein spezielles Migrationsteam mit der Aufgabe der Migration betraut. Die Mitglieder dieses Teams müssen dafür jedoch mit weitreichenden Berechtigungen sowohl innerhalb des existierenden Systems als auch innerhalb des Windows 2000 Systems ausgestattet werden. Es ist daher in solchen Fällen darauf zu achten, dass nur vertrauenswürdige Personen mit diesen Aufgaben betraut werden. Im Migrationskonzept sollte außerdem festgelegt sein, welche Aufgaben nur im Vier-Augen-Prinzip erfolgen dürfen.

Migrationsteam benennen

- Nach Abschluss der Migration empfiehlt sich ein Soll-Ist-Vergleich aller Sicherheitseinstellungen, wie z. B. der Zugriffsberechtigungen und der Gruppenmitgliedschaften. Dies ist in der Regel jedoch nur werkzeuggestützt möglich.

abschließender Soll-Ist-Vergleich

Die hier aufgeführten Aspekte dienen als Leitfaden für ähnliche und weitergehende Fragestellungen, die im Rahmen des Migrationskonzeptes adressiert werden müssen. Es ist zu beachten, dass ein Migrationsplan immer auf ein konkretes System zugeschnitten sein muss und die jeweiligen lokalen Anforderungen an die Migration reflektiert.

Ergänzende Kontrollfragen:

- Wurde eine bedarfsgerechte Migrationsplanung durchgeführt?
- Sind alle Werkzeuge, die im Rahmen der Migration benötigt werden, bekannt und getestet?
- Wurde ein zeitliche Migrationsreihenfolge entworfen?
- Ist sichergestellt, dass die weitreichenden Berechtigungen des Migrationsteams nach Abschluss der Migration wieder zurückgesetzt werden?

M 2.234 Konzeption von Internet-PCs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsbeauftragter

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsbeauftragter

Nach der Entscheidung, einen oder mehrere Internet-PCs für die Nutzung von Internet-Angeboten und -Diensten zur Verfügung zu stellen, sollte ein Konzept für die konkrete Realisierung erstellt werden. In diesem Konzept sollten die funktionale Anforderungen, IT-Sicherheitsanforderungen, erforderliche Regelungen, Zuständigkeiten sowie Vorgaben für die technische Realisierung und Nutzung festgelegt werden.

Es wird empfohlen, bei der Konzeption mindestens die folgenden Teilaspekte zu berücksichtigen. Je nach den vorliegenden organisatorischen Randbedingungen müssen unter Umständen weitere Punkte in das Konzept aufgenommen werden. Hinweise hierzu können den Bausteinen B 3.301 *Sicherheitsgateway (Firewall)* und B 5.4 *Webserver* entnommen werden.

Funktionale Anforderungen

Welche Dienste sollen genutzt werden?

Als Erstes sollte festgelegt werden, welche im Internet angebotenen Dienste, z. B. World Wide Web (WWW), E-Mail, News oder Instant Messaging, genutzt werden sollen. Dies hat weitgehende Auswirkungen auf die zu installierende Software und die erforderlichen Sicherheitsmaßnahmen.

Um einen geeigneten Internet Service Provider (ISP) und eine zweckmäßige Anschlusstechnik auswählen zu können, sollten weiterhin die benötigten Bandbreiten und Antwortzeiten für die einzelnen Internet-Dienste dokumentiert werden.

Um Kriterien für die Aufstellungsorte der Internet-PCs zu erhalten, sollte anschließend im Konzept dokumentiert werden, wie hoch das voraussichtliche Nutzeraufkommen ist und welche Anforderungen hinsichtlich der räumlichen Nähe des Internet-PCs zum Mitarbeiter bestehen.

Weiterhin sollte festgelegt werden, wie mit Daten aus dem Internet, z. B. heruntergeladenen Dateien, umgegangen wird, ob diese z. B. auf anderen Systemen weiterverarbeitet werden dürfen oder archiviert werden müssen. Ein Datenaustausch zwischen Internet-PC und Hausnetz erfordert zusätzliche IT-Sicherheitsmaßnahmen und Regelungen.

IT-Sicherheitsanforderungen

Hinsichtlich der IT-Sicherheitsanforderungen sollte im Konzept festgelegt werden, ob die Informationen, die aus dem Internet abgerufen oder an andere Computer im Internet gesendet werden, gegen unbefugtes Mitlesen oder unerlaubte Veränderung geschützt werden müssen.

Weiterhin ist im Konzept zu dokumentieren, ob auf dem Internet-PC schützenswerte Daten abgespeichert und längere Zeit vorgehalten werden müssen. Dies ist besonders dann relevant, wenn der Internet-PC auch für E-Mail verwendet wird.

Im Hinblick auf Zurechenbarkeit und Schutz vor unerlaubter Nutzung sollte festgelegt werden, ob sich Benutzer am Internet-PC authentisieren müssen, bevor sie den Internet-Zugang verwenden können.

Das Einsatzkonzept sollte auch Aussagen zu Anforderungen an die Verfügbarkeit enthalten. Es ist daher festzulegen, ob ein Ausfall des Internet-PCs für längere Zeit tolerabel ist oder ob für diesen Fall Ausweichlösungen geschaffen werden müssen.

Erforderliche Regelungen

Im Hinblick auf die Nutzung eines Internet-PCs müssen bestehende Regelungen angepasst oder neu festgelegt werden. Dazu gehören insbesondere das IT-Sicherheitskonzept und die Benutzerrichtlinie (siehe auch M 2.235 *Richtlinien für die Nutzung von Internet-PCs*). Je nach Standort kann der Einsatz eines Internet-PCs aber beispielsweise auch Auswirkungen auf bestehende Zutrittsregelungen haben.

Zuständigkeiten

Ansprechpartner für Benutzer

Auch Internet-PCs müssen durch fachkundiges Personal administriert und gewartet werden. Im Einsatzkonzept sollte daher festgelegt werden, welche Mitarbeiter bzw. Rollen für Administration und Betrieb des Internet-PCs zuständig sind und wer zu benachrichtigen ist, wenn der Internet-PC ausfällt oder wenn Anzeichen für einen Sicherheitsvorfall entdeckt werden.

Da sich das Nutzungsprofil und die Einsatzumgebung von Internet-PCs schnell ändern können, muss das Konzept fortgeschrieben werden. Es sollte dokumentiert werden, wer hierfür zuständig ist.

Vorgaben für die technische Realisierung (Hardware)

Im Konzept sollte vorgegeben werden, wie viele Internet-PCs zum Einsatz kommen und ob diese untereinander vernetzt und mit einer gemeinsamen Internet-Anbindung ausgestattet werden sollen. In diesem Fall sollte auch festgelegt werden, was für Komponenten zur Vernetzung verwendet werden.

Weiterhin sollte die Hardware-Ausstattung der Internet-PCs definiert werden. Dazu gehören z. B. die Hardware-Plattform, Laufwerke, Schnittstellen und Peripheriegeräte.

Falls eine Datensicherung des Internet-PCs erforderlich ist, sollte im Konzept festgelegt werden, über welche Medien oder Schnittstellen diese erfolgt.

Vorgaben für die technische Realisierung (Software)

Standardisierung reduziert Betreuungsaufwand

Um die Administration zu vereinfachen, sollten alle Internet-PCs möglichst gleich ausgestattet sein. Die Software-Ausstattung sollte daher im Konzept weitgehend vorgegeben werden.

Das verwendete Betriebssystem sollte auf jeden Fall im Einsatzkonzept festgelegt werden. Falls eine Authentisierung der Benutzer erforderlich ist, sollten nur Betriebssysteme mit einer wirksamen Benutzertrennung, z. B. Windows NT/2000 oder Linux, eingesetzt werden. Windows 9x/ME sind in diesem Fall ungeeignet.

Weiterhin sollte dokumentiert werden, welche Client-Programme für Internet-Dienste zum Einsatz kommen sollen. In vielen Fällen wird zumindest ein WWW-Browser und ein E-Mail-Client benötigt. Weitere Beispiele sind News-Clients und Instant Messaging-Programme.

Sicherheitstools installieren

Um die IT-Sicherheitsanforderungen erfüllen zu können, müssen meist zusätzliche Sicherheitstools installiert werden, z. B. für den Schutz vor Computer-Viren, zur Datensicherung oder zur Verschlüsselung. Im Konzept sollte festgelegt werden, welche Produkte hierfür ggf. verwendet werden.

Vorgaben für die technische Realisierung (Internet-Anbindung)

Das Einsatzkonzept sollte detaillierte Vorgaben zur technischen Realisierung der Internet-Anbindung machen, um die Anforderungen an Bandbreite, Antwortzeiten und Verfügbarkeit erfüllen zu können (siehe auch M 5.92 *Sichere Internet-Anbindung von Internet-PCs*). Hierzu gehört einerseits die Frage, über welchen oder welche Internet Service Provider (ISP) der Zugang zum Internet erfolgen soll (siehe auch M 2.176 *Geeignete Auswahl eines Internet Service Providers*).

Andererseits muss auch festgelegt werden, über welche Zugangstechnik, z. B. ISDN oder DSL, die Internet-Anbindung erfolgen soll und welche Schnittstelle des Internet-PCs, z. B. ISDN-Karte oder Netzwerkkarte, hierfür verwendet wird. Je nach verwendeter Zugangstechnik werden unter Umständen spezielle Programme oder Hardware-Komponenten, z. B. DSL-Modem bzw. Router, benötigt.

Ergänzende Kontrollfragen:

- Wurde ein Nutzungskonzept für den Einsatz von Internet-PCs erstellt?
- Enthält das Nutzungskonzept auch die IT-Sicherheitsanforderungen an den Internet-Zugang?

M 2.235 Richtlinien für die Nutzung von Internet-PCs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsbeauftragter

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsbeauftragter

Für die sichere Nutzung von Internet-PCs ist es erforderlich, dass hierfür verbindliche Richtlinien festgelegt werden. Diese Richtlinien müssen allen beteiligten Mitarbeitern der Institution, d. h. mindestens den Benutzern des Internet-PCs und den zuständigen Administratoren, bekannt gemacht werden.

Es wird empfohlen, die Richtlinien für die Nutzung des Internet-PCs in einem Dokument zusammenzufassen und als Datei auf dem Internet-PC zur Verfügung zu stellen, z. B. auf dem Desktop. Dabei sollten mindestens folgende Teilaspekte berücksichtigt werden:

Benutzer über Risiken informieren

Die Benutzer sollten in kurzer, verständlicher Form über die Risiken informiert werden, die mit der Nutzung des Internet-PCs verbunden sind. Diese Information dient gleichzeitig als Motivation für die nachfolgenden Richtlinien.

fachkundige Administration

Auch der Internet-PC muss durch fachkundiges Personal administriert und gewartet werden. Dies kann entweder durch die vorhandene Administration, z. B. für IT-Systeme im Hausnetz, oder durch andere Mitarbeiter erfolgen, die dann entsprechend geschult werden müssen. Die Zuständigkeit sollte in den Richtlinien dokumentiert werden.

In einigen Fällen kann es zweckmäßig sein, dass Benutzer bestimmte Konfigurationseinstellungen selbst vornehmen dürfen. Dies sollte in den Richtlinien vermerkt, anderenfalls sollte es untersagt werden.

Wer, wann, wofür

In den Richtlinien sollte festgelegt werden, welche Personen den Internet-PC zu welchen Zeiten und für welche Zwecke benutzen dürfen. In diesem Zusammenhang ist insbesondere festzulegen, ob nur dienstliche oder auch private Nutzung - z. B. in der Mittagspause - zugelassen ist.

Weiterhin sollte dokumentiert werden, welche Programme für die Nutzung von Internet-Diensten verwendet werden dürfen und ob aktive Inhalte, wie z. B. Javascript, Java oder ActiveX, auf dem Internet-PC ausgeführt werden dürfen. Wichtig ist in diesem Zusammenhang auch, ob Benutzer selbständig Browser-Erweiterungen ("Plug-Ins") installieren und nutzen dürfen.

Falls das verwendete Betriebssystem eine Benutzertrennung unterstützt, sollten Client-Programme für die Nutzung von Internet-Diensten nicht unter dem Administrator-Benutzerkonto, z. B. *root* oder *Administrator*, gestartet werden. Auch von Administratoren sollten hierfür normale Benutzerkonten verwendet werden.

Weitergabe von Informationen

Es müssen Regelungen dafür festgelegt werden, welche persönlichen Daten und welche Informationen über die Behörde bzw. das Unternehmen, z. B. Postadressen, über den Internet-Zugang weitergegeben werden dürfen. Dazu gehört auch die Frage, ob Nachrichten mit einer dienstlichen Absenderadresse gesendet werden dürfen, falls der Internet-PC für E-Mail oder News genutzt wird.

Umgang mit Daten aus dem Internet

Außerdem sollte in den Richtlinien vorgegeben werden, welche Daten auf dem Internet-PC abgespeichert werden dürfen und welche Verzeichnisse hierfür vorgesehen sind. Es muss auch geregelt werden, unter welchen Bedingungen Daten vom Internet-PC in das Hausnetz oder umgekehrt transportiert werden dürfen.

In beiden Fällen ist mindestens eine Prüfung auf Computer-Viren durchzuführen. Für den Import von Daten und Programmen ins Hausnetz wird der Einsatz eines Schleusen-PCs empfohlen.

Falls eine lokale Datenhaltung auf dem Internet-PC vorgesehen ist, muss geregelt werden, ob die Benutzer für eine evtl. erforderliche Datensicherung selbst verantwortlich sind oder ob dies automatisch bzw. durch die Administration geschieht. Dies ist besonders wichtig, wenn der Internet-PC für E-Mail, Banking, elektronische Beschaffung oder ähnliche Aufgaben eingesetzt wird.

unerlaubte Inhalte

Die Benutzer müssen darüber belehrt werden, welche Angebote, z. B. illegale Inhalte, Pornographie oder Extremismus, auf keinen Fall genutzt werden dürfen. Außerdem müssen die Benutzer darüber belehrt werden, dass sie sich bei der Nutzung des Internets an geltende Rechtsvorschriften und die "Netiquette" halten müssen, da sie ja im Namen der Behörde bzw. des Unternehmens agieren.

Umgang mit Authentisierungsdaten

Für die Einwahl beim Internet Service Provider oder für die lokale Anmeldung am Internet-PC werden meist Passwörter benötigt. In den Richtlinien sollte vorgegeben werden, welches Format und welche (Mindest-)länge diese Passwörter haben und wie oft sie geändert werden müssen.

Falls eine Benutzer-Authentisierung im Einsatzkonzept vorgesehen ist, sind die Benutzer darüber zu belehren, dass sie mit den Authentisierungsgeheimnissen sorgfältig umgehen und sich vom System abmelden müssen, wenn sie den Internet-PC verlassen.

Schließlich sollte festgelegt werden, ob das für die Einwahl beim Internet Service Provider benötigte Passwort abgespeichert werden darf oder ob es bei jeder Einwahl erneut eingegeben werden muss. Diese Entscheidung sollte auf einer Einschätzung beruhen, wie groß die Gefahr einer missbräuchlichen Nutzung der Internet-Anbindung im vorliegenden Einsatzumfeld ist. Ein doppelter Zugangsschutz (erst Benutzeranmeldung, dann Eingabe des Einwahlpasswortes) wird von Benutzern oft nicht akzeptiert.

Je nach Anwendungsfall und Einsatzumgebung müssen unter Umständen weitere Richtlinien oder Regelungen für den Internet-PC getroffen werden.

Ergänzende Kontrollfragen:

- Wurden für die Nutzung des Internet-PCs alle erforderlichen Richtlinien festgelegt?
- Sind die Richtlinien allen Benutzern des Internet-PCs bekannt?

M 2.236 Planung des Einsatzes von Novell eDirectory

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Grundsätzlich gibt es zwei Einsatzszenarien für eDirectory:

- der Einsatz als Managementprodukt für Ressourcen in einem gegebenen Netz oder
- die Verwendung als (Meta-)Verzeichnisdienst (LDAP-Server).

Abstrakt gesehen bildet das eDirectory eine hierarchisch und baumartig organisierte, Objekt-basierte Datenbank. Es ist an den Verzeichnisdienst-Standard X.500 angelehnt, von dem es die interne Struktur und den internen Aufbau entliehen hat. Es ist jedoch kein X.500-kompatibler Verzeichnisdienst, da das Zugriffsprotokoll auf dem proprietären NDAP (Novell Directory Access Protocol) basiert.

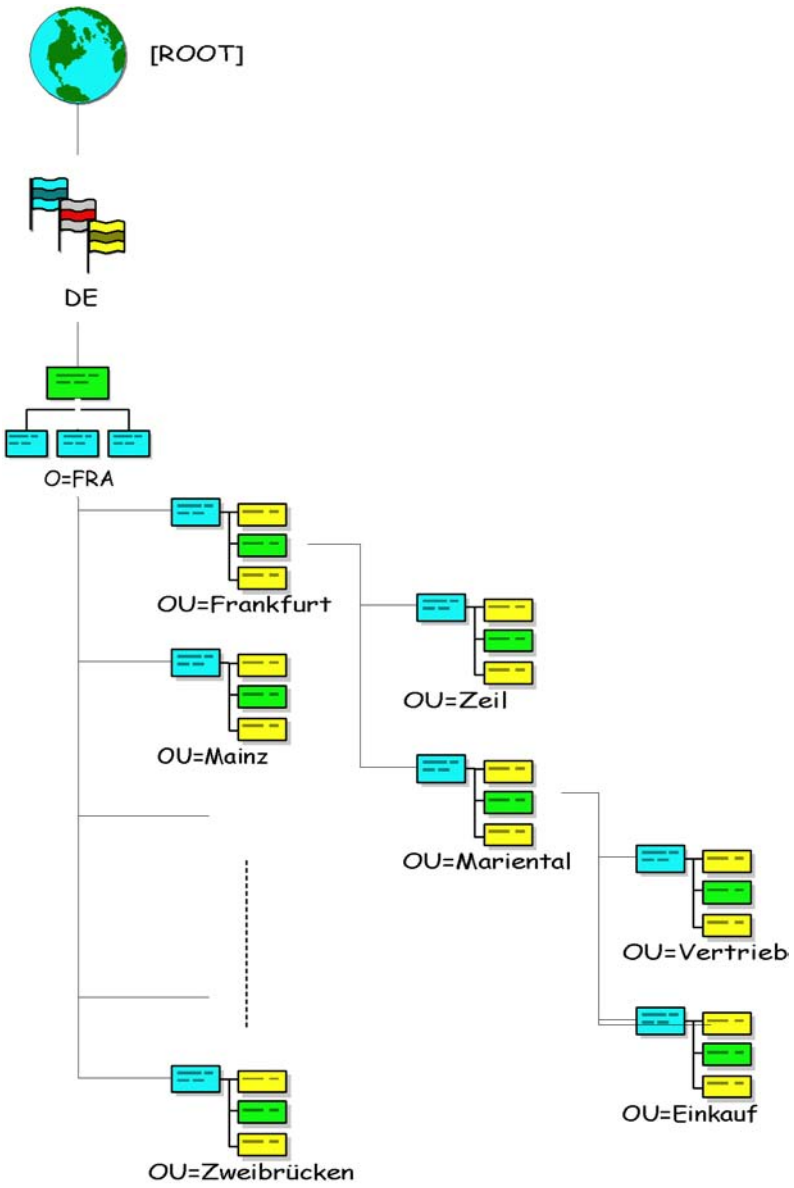
Baum-Konzept

Das Baum-Konzept von eDirectory stellt sich auf folgende Weise dar: in einem Baum (*Tree*) werden Server, Benutzer und weitere Ressourcen abgebildet und können durch den Baum-Administrator verwaltet werden. Ein Baum bildet grundsätzlich eine administrative Grenze und limitiert auch den Wirkungsbereich von Berechtigungen.

Schema

Ein eDirectory-Verzeichnisbaum besteht aus verschiedenen Objekten. Jedes Objekt gehört einer ausgezeichneten Klasse an, z. B. Benutzerobjekt oder Serverobjekt, und ist gemäß dieser Klasse aus verschiedenen Attributen bzw. Eigenschaften zusammengesetzt. Die verschiedenen Objektattribute können unterschiedliche Werte aufnehmen, z. B. Telefonnummer oder IP-Adresse. Die Informationen über die bestehenden Objektklassen inklusive der darin vorkommenden Attribute werden im Directory-Schema gehalten. Durch Änderungen der Schemadefinition können neue Objektklassen erzeugt oder bestehende Objektklassen mit veränderten Attributsätzen versehen werden. Bei Veränderung des Schemas spricht man dann vom *Extended Schema*. eDirectory kennt verschiedene vordefinierte Objekttypen:

- *Tree-Objekt*: Dieses Objekt ist die Wurzel aller eDirectory-Objekte eines Verzeichnisbaums und enthält Informationen über diesen, z. B. Name des Baums. Unterhalb des Tree-Objekts können weitere Objekte angeordnet sein.
- *Container-Objekte*: Diese Objekte dienen dazu, andere Objekte zu gruppieren. Standardmäßig stehen die Objekte Land (Country, C), Organisation (Organization, O) und Organisations-Einheit (Organizational Unit, OU) zur Verfügung. Unterhalb eines OU-Objektes können weitere OU-Objekte enthalten sein, sowie so genannte Leaf-Objekte (siehe unten).
- *Leaf-Objekte*: Dies sind Server-, Benutzer-, Benutzer-Gruppen-, Rollen-, Drucker-, Druckerwarteschlangen-, Profil- sowie Applikations-Objekte. Weiterhin können auch Alias-Objekte zum Verweis auf bestehende Objekte in anderen Teilbäumen definiert werden



Wurzel- und Zertifizierungsstelle

In einem eDirectory-Baum gibt es immer eine ausgezeichnete Wurzel, die eine gewisse Sonderstellung besitzt: sie wird bestimmt durch den ersten Server, der in einem Baum installiert wird. Auf diesem Server läuft die Zertifizierungsstelle (CA) des Baums, der Voraussetzung für die Einbindung weiterer eDirectory-Server in den Baum ist. Die CA kann später auch auf einen anderen eDirectory-Server verschoben werden. Sämtliche weiteren eDirectory-Installationen müssen sich bei dem gegebenen eDirectory-Baum anmelden. Dabei muss der genaue Kontext, in dem der eDirectory-Server in einen bestehenden Baum eingebunden wird, angegeben werden. Ein späteres Verschieben der eDirectory-Server ist nur sehr schwer möglich, so dass der Server-Kontext im Voraus geplant werden muss.

automatische Replizierung

Die ersten drei eDirectory-Server eines Baums erhalten automatisch eine vollständige Replica der Verzeichnisdaten, die weiteren nicht mehr - sofern dies nicht explizit so konfiguriert wird.

Baumstruktur sorgfältig planen

Nach einer Standardinstallation existiert eine zunächst einfache eDirectory-Struktur, die von eDirectory angelegt wird und dann entsprechend der Planung verändert werden kann. Da eDirectory primär der Verwaltung von IT-Ressourcen dient, sollte beim Aufbau der eDirectory-Baumstruktur darauf geachtet werden, dass die Struktur vornehmlich auf administrative Gegebenheiten abgestimmt wird. Wenn stattdessen zwanghaft die organisatorische Unternehmensstruktur bis ins Kleinste nachgebildet wird, kann dies zu Problemen in der Administration führen.

Baumstruktur nicht zu flach wählen

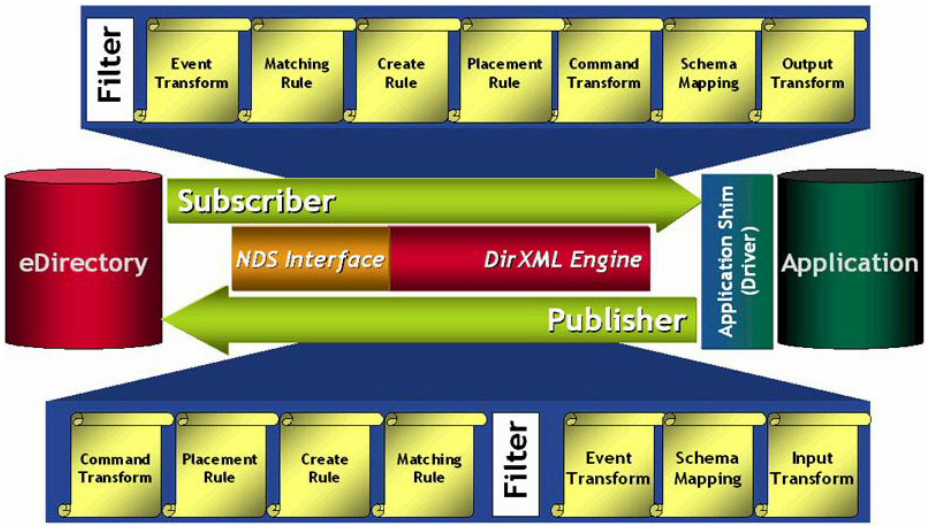
Es ist weiterhin darauf zu achten, dass die gewählte Baumstruktur nicht zu flach ist, damit sich die Replizierung zwischen den eDirectory-Servern nicht auf den gesamten Baum auswirkt. Der Ausfall eines einzelnen eDirectory-Servers oder der Verbindung dieses Servers zum Restsystem führt anderenfalls zu Fehlermeldungen sämtlicher in den Replizierungsring eingebundener Server.

Vorsicht bei Schemaänderungen

Die möglichen Anordnungen von eDirectory-Objekten, d. h. welches Objekt welche anderen Objekte enthalten darf, welche Attribute existieren und aus welchen Attributen Objekte zusammengesetzt werden, wird durch das so genannte eDirectory-Schema definiert. Das von eDirectory vorgegebene Schema kann verändert werden, dies stellt jedoch einen gravierenden Eingriff in die Verzeichnisstruktur dar, der nur nach sorgfältiger Planung durchgeführt werden darf.

DirXML-Schnittstelle

Der eDirectory-Verzeichnisdienst bietet die Möglichkeit, mit anderen Verzeichnisdiensten über einen Synchronisationsmechanismus Daten im XML-Format abzugleichen. Als XML-Schnittstelle steht dazu das Produkt *DirXML* zur Verfügung. Diese besteht aus einem Kern (*engine*) und verschiedenen Treibern für diverse unterstützte Zielsysteme, z. B. Lotus Notes, SAP R/3, Windows 2000 Active Directory, Netscape (iPlanet), etc. Es gibt dabei zwei Kommunikationskanäle: Zum einen den so genannten *Publisher Channel*, unter dem fremde Verzeichnisdienste Änderungen ihres Datenbestandes dem eDirectory mitteilen können. Zum anderen gibt es den *Subscriber Channel*, mit dessen Hilfe eingeschriebene fremde Verzeichnisdienste von Änderungen im eDirectory erfahren.



Der Einsatz der *DirXML*-Schnittstelle bedarf auf jeden Fall einer genauen Planung, um später unerwünschte Seiteneffekte zu vermeiden, z. B. Endlosschleifen.

Im Rahmen der eDirectory-Planung sind folgende Aspekte zu berücksichtigen:

- Welche Gliederung in Organisations-, Organisationseinheit- und weitere Container-Objekte soll gewählt werden?
- Welche Objektklassen werden benötigt und welche Attribute sollen diese haben?
- Welche Benutzer und Server sollen in welchen Organisationseinheiten zusammengefasst werden?

Für jede Organisation muss entschieden werden,

- welche Administratorgruppen benötigt werden,
- welches administrative Modell umgesetzt wird (zentrale oder dezentrale Verwaltung),
- welche administrativen Rollen innerhalb der Baumstruktur existieren sollen,
- ob und an wen administrative Aufgaben delegiert werden sollen,
- welche Sicherheitseinstellungen für verschiedene Typen von Servern und Benutzergruppen gelten sollen,
- auf welche Informationen über die verschiedenen eDirectory-Schnittstellen (z. B. eDirectory-Clients, LDAP) von wem zugegriffen werden darf.

Dokumentation der eDirectory-Struktur

Generell muss die geplante eDirectory-Struktur dokumentiert werden. Dies trägt maßgeblich zur Stabilität, konsistenten Administration und damit zur Systemsicherheit bei. Es empfiehlt sich insbesondere festzuhalten:

- Welche Schemaänderungen werden durchgeführt? Dabei sollen auch die Gründe für die Änderung dokumentiert sein.
- Welche Objektklassen werden in welcher Weise verwendet, speziell welche Attribute werden für welche Inhalte genutzt?

Dokumentation der eDirectory-Objekte

Für jedes eDirectory-Objekt sollte dokumentiert sein:

- Name und Position im eDirectory-Baum (z. B. "StandortBerlin", Vater-Objekt: OU "Filialen-Deutschland"),
- welchem Zweck das Objekt dient,
- welche administrativen Zugriffsrechte für das Objekt und dessen Attribute vergeben werden sollen (z. B. vollständig verwaltet von "Admin1"),
- wie die Vererbung von eDirectory-Rechten konfiguriert werden soll, z. B. blockieren oder filtern der Rechtevererbung,
- welche Sicherheitsäquivalenzen zwischen Objekten bestehen sollen.

Rollen-basierte Administration und Delegation

Die eDirectory-Administration und das benutzte administrative Modell muss auf jeden Fall geplant werden. Besonders auch die Einrichtung einer Rollen-basierten Administration und die Möglichkeit der Delegation von Administrationsaufgaben sind sicherheitskritisch. Bei sinnvoller, übersichtlicher und konsistenter Planung kann die Sicherheitsadministration durch diese Funktionalitäten transparenter und effizienter gestaltet werden.

Die Nutzung von eDirectory beinhaltet den Betrieb einer eigenen, eingebundenen Zertifizierungsstelle (CA). Auch hier muss sich die Planung nach den Anforderungen und besonders nach der zuvor aufgestellten Sicherheitsleitlinie richten.

Zusammengefasst ergeben sich folgende sicherheitsrelevante Kernaspekte bei der eDirectory-Planung:

- Bäume begrenzen die administrative Macht von Administratoren und den Verzeichnisdienst an sich.
- Standardmäßig ist bei der Erstinstallation von eDirectory der Benutzer *Admin* innerhalb des Organisationscontainers des eDirectory-Baums angelegt. Dieser besitzt das so genannte *Supervisor*-Recht auf den gesamten Baum.

möglichst einfache Berechtigungsstruktur wählen

- Administrative Delegation wird durch die Vergabe von Zugriffsrechten auf eDirectory-Objekte und deren Attribute erreicht. Die Verteilung der Zugriffsrechte muss gemäß dem administrativen Modell erfolgen. Die Mechanismen für Zugriffsrechte im eDirectory sind unter anderem Vererbung, Kontrolle der Vererbung, Wirkungsbereich von Zugriffseinstellungen und Sicherheits-Äquivalenz zwischen Objekten. Damit können sehr komplexe Berechtigungsstrukturen aufgebaut werden, die sehr schnell unübersichtlich und nicht mehr administrierbar werden, so dass sich durch Fehlkonfigurationen im eDirectory Sicherheitslücken ergeben können. Eine möglichst einfache Berechtigungsstruktur ist daher vorzuziehen.
- Schemaänderungen sind kritische Operationen und dürfen nur von autorisierten Administratoren nach sorgfältiger Planung durchgeführt werden.

Abschließend sei darauf hingewiesen, dass Fehler in der eDirectory-Planung und den zugrunde liegenden Konzepten nach erfolgter Installation nur mit beträchtlichem Aufwand zu berichtigen sind.

Ergänzende Kontrollfragen:

- Wurde eine eDirectory-Planung durchgeführt?
- Wurde für jeden geplanten eDirectory-Server sein genauer Kontext innerhalb des Verzeichnisbaums festgelegt?
- Sind alle Beteiligten in die Planung einbezogen worden?
- Ist ein bedarfsgerechtes eDirectory-Berechtigungskonzept entworfen worden?
- Wurde die Synchronisation der Verzeichnisdaten mit weiteren Verzeichnisdiensten geplant?
- Wurde das Konzept der Rollen-basierten Administration konsistent geplant?

M 2.237 Planung der Partitionierung und Replikation im Novell eDirectory

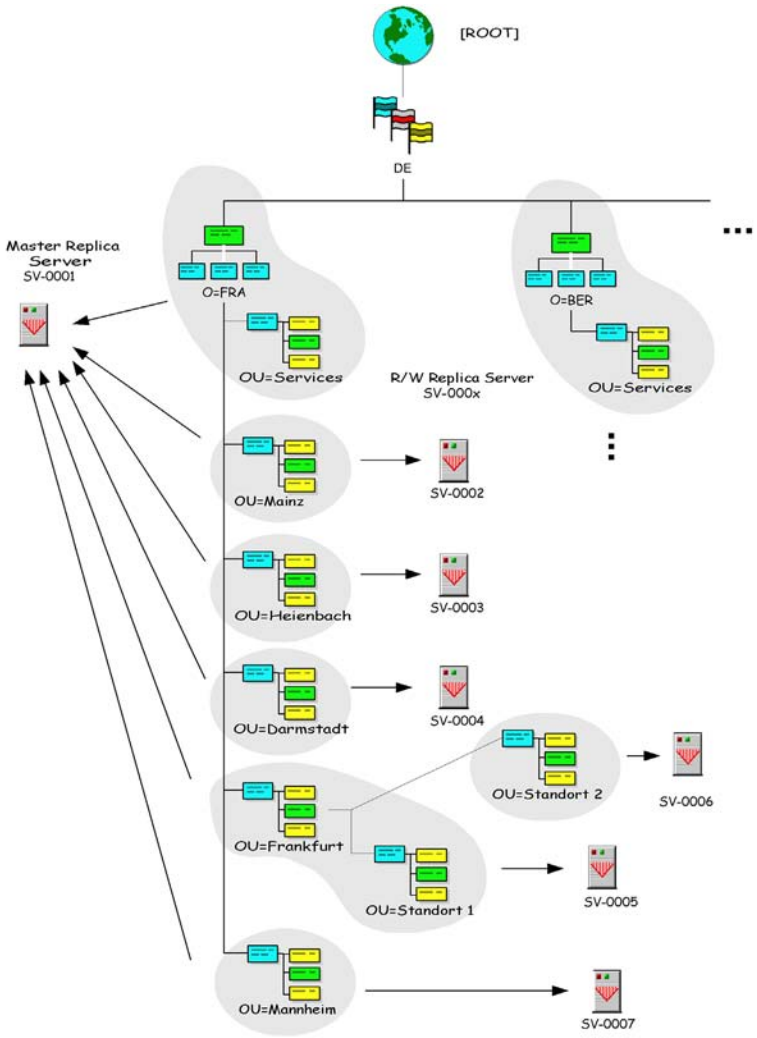
Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Partitionierung

Als skalierbarer Verzeichnisdienst bietet eDirectory die Möglichkeit, Teile der Verzeichnisdatenbank in Partitionen zu zerlegen und auf verschiedene eDirectory-Server zu verteilen. Dies verkürzt die mittleren Zugriffszeiten, da die Suche sich unter Umständen nur auf eine spezielle Partition und nicht den gesamten Verzeichnisbaum erstrecken muss. Außerdem erhöht es die Ausfallsicherheit, da bei einem Serverausfall nur die dort befindliche Partition und nicht die gesamte Verzeichnisdatenbank betroffen ist. Weiterhin erlaubt es die Partitionierung, die Daten gemäß einer zuvor vorgenommenen Klassifizierung auf entsprechend gesicherte Server zu verteilen.

Bei der Planung der Partitionierung sind die vom eDirectory definierten Regeln für Partitionen zu berücksichtigen.



Partitionen können wiederum Unterpartitionen enthalten, welche gemäß den festgelegten Regeln gebildet wurden. Auf Partitionen können verschiedene Operationen ausgeführt werden, z. B. Erzeugen, Zusammenführen, Bewegen oder Annullieren einer der genannten Operationen.

Replikation

Neben dem Mechanismus der Partitionierung des Verzeichnisbaums bietet eDirectory die Möglichkeit, Teile des Verzeichnisbaums auf andere eDirectory-Server zu replizieren. In der Terminologie von eDirectory wird dabei von *Replicas* gesprochen. In jeder Partition gibt es eine so genannte *Master-Replica.* Diese bildet den Mittelpunkt der jeweiligen Partition. Das Anlegen neuer Unterpartitionen oder neuer Replicas der aktuellen Partition ist von der Verfügbarkeit des *Master-Replica-Servers* abhängig. Es gibt verschiedene Möglichkeiten, die Verzeichnisdaten auf andere Server zu replizieren:

- *Read/Write Replica*: Auf Read/Write Replicas einer Partition kann genauso zugegriffen werden, wie auf die Master-Replica selbst. Insbesondere ist es in einer Read/Write Replica möglich, Modifikationen der Daten vorzunehmen. Die Informationen werden automatisch zwischen den einzelnen Replicas ausgetauscht. Sofern der Server, auf dem die Master-Replica gehalten wird, dauerhaft ausfällt, kann eine Read/Write Replica zur Master-Replica umkonfiguriert werden.
- *Read-Only Replica*: Diese Replicas empfangen lediglich Synchronisations-Updates von anderen Replicas. Clients können den Inhalt einer Read-Only Replica nicht ändern.
- *Filtered Read/Write Replica*: Auf diese Server wird lediglich ein Teil einer eDirectory-Partition repliziert. Die Auswahl des replizierten Inhaltes ist dabei sowohl auf der Ebene der Objektklassen als auch auf der Ebene einzelner Attribute möglich. Der Inhalt dieser Replica kann von Clients verändert werden. Bei einer Änderung des Informationsstandes wird der Inhalt automatisch mit den weiteren Replicas synchronisiert.
- *Filtered Read-Only Replica*: Dieser Typ einer Replica enthält nur eine Auswahl der gesamten Partition, die zudem nicht durch Clients verändert werden kann. Für die Auswahl des zu replizierenden Inhaltes bestehen die gleichen Möglichkeiten wie bei Filtered Read/Write Replicas.

Die oben beschriebenen Arten von Replicas werden manuell eingerichtet und konfiguriert. Die Replizierung selbst läuft automatisch ab. Ein weiterer Replikationstyp sind die *Subordinate-Reference-Replicas*. Diese werden vom eDirectory-System jedoch selbst angelegt und verwaltet. Sie enthalten lediglich Sprungadressen, um effizient Objektnamen über Partitionsgrenzen hinweg auflösen zu können (so genanntes *tree walking*).

Bei der Planung der Partitionen sollten folgende Punkte beachtet werden:

Schutzbedarf

- Berücksichtigung des Schutzbedarfs: Die Informationen, die im Verzeichnis gehalten werden, sollten gemäß ihrem Schutzbedarf klassifiziert werden. Anhand dieser Klassifizierung sollte die Verteilung der Objekte auf entsprechend geschützte Server erfolgen. Dabei ist darauf zu achten, dass besonders der Inhalt des Security-Containers auf einem ausreichend abgesicherten Server gelagert wird, da es sich hierbei um sensitive Informationen handelt. Im

Security-Container werden beispielsweise die *Key Management Objects* sowie die *Security Policies* gespeichert.

- geforderte Verfügbarkeit des Verzeichnisdienstes: Zur Verbesserung der Lastverteilung müssen hinreichend viele Repliken der Verzeichnisdaten auf eDirectory-Servern angelegt werden.
- Verteilung der Administrationsaufgaben: Damit eine Rollentrennung der Administrationsaufgaben mit der Trennung der Datenhaltung einhergeht, sollten die Administrationsaufgaben auf einzelne Partitionen verteilt werden.
- Einhaltung der eDirectory-Regeln zur Partitionierung. Die wesentlichen Regeln dabei sind:
  - Jede Partition beginnt hierarchisch mit einem einzelnen Container-Objekt.
  - Die Partition muss ein zusammenhängender Sub-Tree des eDirectory-Baums sein.
  - Verschiedene Partitionen dürfen sich nicht überschneiden.
  - Der Name der Partition muss der *Fully Qualified Distinguished Name* (*FQDN*) des Wurzelobjekts der Partition sein.
- Die genauen Kontexte der Server, welche Partitionen/Replicas halten. Ist die Struktur zu flach, so entsteht ein hoher interner Replizierungsaufwand. Darüber hinaus führen einzelne - momentan nicht verfügbare - Server zu entsprechenden Statusmeldungen bei sämtlichen weiteren in den Replizierungsring eingebundenen eDirectory-Servern.

Bei der Planung der Replicas sind folgende Punkte zu berücksichtigen:

- Aus den Anforderungen an Verfügbarkeit und Ausfallsicherheit des Verzeichnisdienstes müssen die Vorgaben für die Anzahl der anzulegenden Replicas abgeleitet werden.
- Die geforderte Systemperformance führt zur Planung der Lastverteilung.
- Es muss entschieden werden, ob durch die Definition von Filtern für Replicas ein Sicherheitsgewinn erzielt werden kann.

  Dieser liegt vor allem in der Möglichkeit einer getrennten Datenhaltung entsprechend einer zuvor vorgenommenen Klassifizierung der Daten. Es kann damit das Grundprinzip realisiert werden, dass jeder eDirectory-Server nur diejenigen Daten hält, welche er "benötigt" (bzw. welche die zugreifenden Nutzer oder Applikationen benötigen).

  Bei unbedachter Konfiguration kann dieser Sicherheitsgewinn allerdings wirkungslos bleiben. Ein möglicher Nachteil kann die Systemperformance sein. Sind gesuchte Daten auf einem eDirectory-Server nicht vorhanden bzw. nicht sichtbar, weil sie durch entsprechende Filterregeln ausgeblendet sind, so wird im Hintergrund weitergesucht (sofern dies zugelassen ist). Eine nicht bedarfsgerechte Konfiguration der Filterregeln kann also die Systemperformance negativ beeinflussen.

Beispiel: Ein eDirectory-Server steht im Intranet einer Organisation und eine Teilmenge der dort gehaltenen Verzeichnisdaten soll auch im Internet verfügbar sein. Eine mögliche Lösung ist, einen weiteren eDirectory-Server in der demilitarisierten Zone (DMZ) zwischen Intranet und Internet mit einer gefilterten Replica aufzustellen, welche nur die im Internet tatsächlich benötigten Verzeichnisdaten hält.

- Die Datenhaltung muss geplant werden. Hier geht es um eine möglichst detaillierte Planung, welche Daten von wem und von wo aus zugreifbar sein sollen. Für die Durchsetzung der Vorgaben können beispielsweise gefilterte Replicas eingesetzt werden.

Planung der Datenhaltung

M 2.238 Festlegung einer Sicherheitsrichtlinie für Novell eDirectory

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Als eine der organisatorischen Hauptaufgaben bei der Planung des eDirectory-Einsatzes muss zunächst eine Sicherheitsrichtlinie fixiert werden. Durch die Sicherheitsrichtlinie wird festgelegt, welche Sicherheitsbestimmungen in einem eDirectory-System gelten sollen und wie diese bei der Installation umgesetzt werden müssen.

Durch die eDirectory-Sicherheitsrichtlinie sollten sämtliche sicherheitsbezogenen Themenbereiche eines eDirectory-Verzeichnisdienstes geregelt werden. Die folgende Liste gibt einen groben Überblick über die Bereiche, die durch eine solche Richtlinie geregelt werden sollten. Die Liste muss je nach Einsatzszenarien in der Behörde bzw. im Unternehmen entsprechend angepasst, ausgestaltet und erweitert werden.

Allgemeines:

- Wie sollen eDirectory-Server physikalisch abgesichert werden?
- Welche eDirectory-Komponenten, z. B. ConsoleOne und iMonitor, sollen genutzt werden?
- Welche Baumstruktur soll gewählt werden?
- Wie wird diese Baumstruktur partitioniert?
- Werden Schemaänderungen vorgenommen?
- Welche Objektklassen mit welchen Attributsätzen werden eingesetzt?
- Welche Repliken welchen Typs sollen angelegt werden?
- Welche Rechner sind eDirectory-Server und welche Rechner halten eine Replica?

Rechtevergabe:

- Welcher Benutzer darf welche Rechte ausüben?
- Welcher Administrator darf welche Rechte ausüben?
- Welche Authentisierungsverfahren sollen gewählt werden?
- Wie wird die Vererbung von Rechten innerhalb der Baumstruktur definiert?
- Welche Sicherheitsäquivalenzen zwischen Objekten oder Objektklassen werden definiert?

Administration:

- Welche Administratorrollen werden definiert?
- Wer darf Schemaänderungen vornehmen?
- Welche Administrationsaufgaben dürfen bzw. sollen delegiert werden?

Datenkommunikation:

- Welche Datenkommunikation ist abgesichert abzuwickeln?
- Mit welchen Mechanismen werden ggf. Vertraulichkeit, Integrität und Authentizität der Daten geschützt?

Zertifikatsautorität:

- Welche Parameter für die CA sind zu verwenden?
- Wer darf Einstellungen der CA ändern?
- Welche Objekte sind mit Zertifikaten zu versehen?
- Welche Zertifikate sind für SSL-Verbindungen einzusetzen?

Dateisystem des unterliegenden Betriebssystems:

- Welche Berechtigungen auf Systemdateien gelten für die verschiedenen Administratoren und Benutzer?
- Soll Verschlüsselung auf Dateisystemebene eingesetzt werden?

LDAP:

- Welche Benutzer dürfen unter welchen Bedingungen über LDAP auf das eDirectory zugreifen?
- Soll anonymer Login unterstützt werden?
- Welche Netzapplikationen dürfen via LDAP auf das eDirectory zugreifen?
- Soll die LDAP-Kommunikation generell über SSL laufen?
- Dürfen die Benutzerpasswörter im Klartext übertragen werden?

Client-Zugriff auf den eDirectory-Verzeichnisdienst:

- Welche Authentisierungsverfahren sollen eingesetzt oder erlaubt werden?
- Auf welchen Verzeichnisbaum darf vom Netz aus zugegriffen werden?
- Welche Ressourcen sind aus dem Netz von welchen Benutzern zugreifbar?

Verschlüsselung von Attributen

- Soll der *Secret Store* Mechanismus (verfügbar über das Zusatzmodul *Secure Login*) zur Verschlüsselung von Attributen genutzt werden?

Fernzugriff zur Systemüberwachung und Administration:

- Darf das Tool *iMonitor* genutzt werden?
- Wer darf das Tool *iMonitor* nutzen?
- Wie wird das Protokoll HTTPS zu diesem Zweck konfiguriert?

Diese komponentenspezifische Auflistung von Themengebieten kann in folgende zeitliche Abfolge gebracht werden:

1. Definition der eDirectory-Baumstruktur

Im ersten Schritt ist die logische Struktur des eDirectory-Baumes, die Aufteilung in Organisation und Organisationseinheiten sowie insbesondere auch die Zuordnung der Server und der zu verwaltenden Netz-Ressourcen festzulegen (siehe M 2.236 *Planung des Einsatzes von Novell eDirectory*).

Anschließend muss über die im Verzeichnisdienst gehaltenen Objekte und deren Attribute entschieden werden. Bei Bedarf sind hierzu Schemaänderungen am eDirectory vorzunehmen. Weiterhin sollte an dieser Stelle über die Partitionierung der Verzeichnisdaten und über die Einrichtung von Repliken entschieden werden (siehe M 2.237 *Planung der Partitionierung und Replikation im Novell eDirectory*).

2. Regelung der Verantwortlichkeiten

Ein eDirectory-Verzeichnisdienst sollte von geschulten Netzadministratoren sicher betrieben werden. Dabei ist im Rahmen der Notfallvorsorge eine geeignete Stellvertreterregelung zu treffen. Generell sollte ein Konzept zur rollenbasierten Administration erstellt werden. Nur die berechtigten Sicherheits-Administratoren dürfen eDirectory-Sicherheitsparameter verändern.

Die Verantwortlichkeiten der einzelnen Benutzer des eDirectory-Verzeichnisses sind unter Schritt 10 dargestellt.

3. Festlegung von Namenskonventionen

Um die Verwaltung des eDirectory-Verzeichnisbaums zu erleichtern, sollten eindeutige Namen für die Server, Applikationen, Drucker, Benutzer, Benutzergruppen und die weiteren eDirectory-Objekte verwendet werden.

4. Festlegung der Regeln für Benutzerkonten

Vor der Einrichtung von Benutzerkonten sollten die Restriktionen, die für alle oder nur für bestimmte Konten gelten sollen, festgelegt werden. Dies betrifft insbesondere die Regelungen für Passwörter und für die Reaktion des Systems auf fehlerhafte Login-Vorgänge. Außerdem sollte das Erstellen der Login-Skripts geregelt werden.

5. Einrichtung von Gruppen (Organizational Roles)

Zur Vereinfachung der Administration sollten Benutzer-Objekte, für die die gleichen Anforderungen gelten, zu Gruppen zusammengefasst werden. Die korrespondierenden eDirectory-Objekte heißen *Organizational Roles*. Benutzerrechte sowie Zugriffsrechte auf Verzeichnisobjekte und gegebenenfalls weitere vordefinierte Funktionen werden dann den Gruppen (Organizational Roles) und nicht einzelnen Benutzer-Objekten zugeordnet. Die Benutzer-Objekte erben die Rechte und Berechtigungen der Gruppen (Organizational Roles), denen sie angehören. So ist es z. B. denkbar, alle Mitarbeiter einer Abteilung in einer Gruppe (Organizational Role) zusammenzufassen. Benutzerberechtigungen sollten nur dann einzelnen Benutzern zugewiesen werden, wenn dies ausnahmsweise unumgänglich ist.

6. Festlegung der Vorgaben für Protokollierung

Hierbei ist festzulegen, welche vom eDirectory generierten Ereignisse zu protokollieren sind und bei welcher Ereigniskombination eine Benachrichtigung an den Sicherheits- bzw. Systemadministrator zu erfolgen hat. Weiterhin muss entschieden werden, wie lange die gesammelten Ereignisdaten aufzubewahren sind.

7. Regelungen zur Datenspeicherung

Es ist festzulegen, wo Benutzerdaten gespeichert werden (siehe M 2.138 *Strukturierte Datenhaltung*). Bei eDirectory werden Benutzerdaten nur auf eDirectory-Servern abgelegt. Eine Datenspeicherung auf den lokalen Festplatten der einzelnen Clients findet nicht statt. Die Frage nach der Datenspeicherung ist jedoch auf der Ebene einzelner Partitionen zu klären. Datenbestände sollten in Bezug auf ihren Schutzbedarf klassifiziert werden, und entsprechend sollte die Partitionierung des Verzeichnisses auf vertrauenswürdige und gesicherte Hosts vorgenommen werden. Dabei sind besonders die hochsensiblen Daten des Security-Containers zu berücksichtigen.

8. Einrichtung von Projektverzeichnissen

Um eine saubere Trennung von benutzer- und projektspezifischen Daten (Objekten) untereinander durchzusetzen, sollte eine geeignete Verzeichnisstruktur festgelegt werden, die eine solche Objekthaltung unterstützt.

9. Vergabe der Zugriffsrechte

Für die Objekte des Verzeichnisdienstes ist festzulegen, welche Attribute für den Betrieb freizugeben und welche Zugriffsrechte ihnen zuzuweisen sind.

10. Verantwortlichkeiten der Administratoren und Benutzer im Client-Server-Netz

Neben der Wahrnehmung der Netzmanagement-Aufgaben (siehe Nr. 2) müssen weitere Verantwortlichkeiten festgelegt werden. Es ist festzulegen, welche Verantwortung die einzelnen Administratoren im eDirectory-Verzeichnissystem übernehmen müssen. Dies können zum Beispiel Verantwortlichkeiten sein für

- die Verwaltung des eDirectory-Baums oder einzelner Partitionen,
- die Verwaltung der Schemadefinition,
- die Verwaltung der CA und der Key Management Objekte (KMO),
- die Auswertung der Protokolldateien auf den einzelnen Servern oder Clients,
- die Vergabe von Zugriffsrechten,
- das Hinterlegen und den Wechsel von Passwörtern und die Durchführung von Datensicherungen.

Auch die Benutzer müssen in einem eDirectory-Verzeichnisdienst mit Client-Zugriff bestimmte Verantwortlichkeiten übernehmen, insbesondere wenn ihnen Rechte zur Ausführung administrativer Funktionen gegeben werden. In

der Regel beschränkt sich dies jedoch auf die Vergabe der eigenen Passwörter für das Login.

11. Schulung

Abschließend muss festgelegt werden, welche Benutzer zu welchen Teilaspekten geschult werden müssen. Erst nach ausreichender Schulung kann der Produktivbetrieb aufgenommen werden. Besonders die Administratoren sind hinsichtlich der Verwaltung und der Sicherheit von eDirectory gründlich zu schulen.

Die so entwickelten Sicherheitsrichtlinien sind zu dokumentieren und im erforderlichen Umfang den Benutzern des eDirectory-Verzeichnisdienstes mitzuteilen. Bei der Definition der Sicherheitsrichtlinie für eDirectory ist zu beachten, dass sie sich an den bisher geltenden Sicherheitsrichtlinien der Behörde bzw. des Unternehmens orientieren muss, diesen nicht widersprechen (Konsistenz) und auch nicht im Widerspruch zu geltendem Recht stehen darf. In der Regel wird eine eDirectory-Sicherheitsrichtlinie existierende Regelungen spezifisch anpassen oder aber sinngemäß erweitern, z. B. durch zusätzliche Anforderungen für Komponenten. Dabei sind unter Umständen neue Regelungen für eDirectory-spezifische Funktionalitäten, z. B. iMonitor, zu treffen. Generell gilt, dass sich die Planung des eDirectory-Verzeichnisdienstes an den jeweiligen Sicherheitsrichtlinien orientiert, dabei jedoch auch Einfluss auf die Sicherheitsrichtlinien besitzt (Feedback-Prozess).

Ergänzende Kontrollfragen:

- Sind alle für den geplanten Einsatz von eDirectory relevanten Bereiche durch die Sicherheitsrichtlinien abgedeckt?
- Wurden zeitliche Abhängigkeiten für die Umsetzung der Sicherheitsrichtlinien berücksichtigt?
- Sind alle Benutzer über die eDirectory-Sicherheitsrichtlinien informiert?

M 2.239 Planung des Einsatzes von Novell eDirectory im Intranet

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

eDirectory ist als Management-Produkt für IT-Ressourcen einer Organisation geeignet. Dazu wird die Organisationshierarchie auf einen eDirectory-Baum abgebildet und der Zugriff auf die im Verzeichnis gehaltenen Objekte entsprechend vergeben. Dabei können Automatismen, wie die Vererbung von Zugriffsberechtigungen auf Teilbäume und das Einrichten von Benutzergruppen (Organizational Roles), die Administration des Verzeichnissystems erleichtern.

eDirectory kann auf verschiedenen Serverplattformen betrieben werden: Netware, Windows NT/2000, Linux sowie Sun Solaris.

Neben dem prinzipiell für alle Applikationen möglichen LDAP-Zugang zum eDirectory bietet Novell spezielle Client-Software an, die für bestimmte Systeme das Ressourcen- und Benutzermanagement im eDirectory erlaubt. Dabei handelt es sich um

- den *Novell Client für Windows* (derzeit - Februar 2002 - in der Version 4.83 für Windows NT/2000/XP und Version 3.31 für Windows 95/98/ME),
- die *Novell User Account Management Software* für Solaris sowie Linux auf Intel-Plattform.

Dabei kann eDirectory auch zur Authentisierung von Netware-Servern und zur Zugriffskontrolle auf dort gehaltene Volumes genutzt werden.

Folgende Aspekte sind bei der Einrichtung eines eDirectory-Verzeichnisdienstes im Intranet zu planen:

- der Verzeichnisbaum und Abbildung der IT-Ressourcen darin,
- die einzusetzenden Objektklassen sowie deren Attributsätze,
- gegebenenfalls Planung einer Schemaänderung,
- die Einrichtung von Benutzern und Benutzergruppen (siehe M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*),
- die Anbindung von Benutzern an das eDirectory (siehe M 4.157 *Einrichten von Zugriffsberechtigungen auf Novell eDirectory*),
- die Zugriffsrechte von Benutzern auf das eDirectory (siehe M 4.157 *Einrichten von Zugriffsberechtigungen auf Novell eDirectory*),
- das Administrationskonzept für das eDirectory (siehe M 3.29 *Schulung zur Administration von Novell eDirectory*),
- die Partitionierung und die Replizierung (siehe M 2.237 *Planung der Partitionierung und Replikation im Novell eDirectory*),
- der Zertifikatsdienst (siehe M 4.155 *Sichere Konfiguration von Novell eDirectory*),

- die Client-Anbindung an das eDirectory (siehe M 4.156 *Sichere Konfiguration der Novell eDirectory Clientsoftware*),
- der LDAP-Zugriff auf das eDirectory durch Netzapplikationen (siehe M 4.158 *Einrichten des LDAP-Zugriffs auf Novell eDirectory*),
- die Verschlüsselung des Netzverkehrs,
- die Datensynchronisation mit fremden Verzeichnisdiensten mittels *DirXML*,
- der Einsatzes des *Service Location Protocols* (SLP),
- Audits (siehe M 4.160 *Überwachen von Novell eDirectory*),
- ein automatisiertes und protokolliertes periodisches Backup (siehe auch M 6.81 *Erstellen von Datensicherungen für Novell eDirectory*),
- die Notfallvorsorge für den Systemausfall (siehe auch M 6.80 *Erstellen eines Notfallplans für den Ausfall eines Novell eDirectory Verzeichnisdienstes*).

M 2.240 Planung des Einsatzes von Novell eDirectory im Extranet

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

eDirectory lässt sich auch als E-Business-Plattform im Internet betreiben. In diesem Zusammenhang fungiert das eDirectory oft als LDAP-Server, der Daten für seine Benutzer in seinem Verzeichnisdienst bereithält. Die Benutzeranbindung erfolgt dabei über das LDAP-Protokoll, welches auf TCP/IP aufsetzt.

Prinzipiell können sich Benutzer auf drei verschiedene Arten via LDAP mit eDirectory verbinden:

- als [Public] Objekt (*Anonymous Bind*),
- als Proxy User (*Proxy User Anonymous Bind*),
- als NDS User (*NDS User Bind*).

Hier ist bei der Planung speziell zu berücksichtigen, ob ein *Anonymous Bind* zugelassen wird oder nicht. Standardmäßig hat das [Public] Objekt uneingeschränktes *Browse*-Recht auf den eDirectory-Baum.

Strukturierung der Verzeichnisdaten

Die Planung sollte eine Aufteilung der Verzeichnisdaten in drei Kategorien vorsehen:

- Daten, auf die über anonymen Login zugegriffen werden kann,
- Daten, auf die nach erfolgreicher Authentisierung zugegriffen werden darf, sowie
- Daten, auf die von außen prinzipiell nicht zugegriffen werden darf.

getrennte Speicherung

Die Verzeichnisdaten sollten entsprechend dieser Aufteilung in getrennten Bereichen gespeichert werden. Dies erleichtert unter anderem die Durchführung von Datensicherungen und die Sicherstellung des korrekten Zugriffsschutzes. Ein eDirectory-Server mit direkter Internet-Anbindung sollte möglichst keine Daten halten, auf die von außen nicht zugegriffen werden braucht.

Weiterhin ist bei Bedarf der Einsatz von SSL für den LDAP-Zugriff auf das eDirectory zu planen. Es ist dann zu entscheiden, ob die Authentisierung über Passwörter oder Zertifikate erfolgen soll. Wird SSL nicht eingesetzt, so muss entschieden werden, ob Passwörter im Klartext übertragen werden können oder ob die Option *allowing cleartext passwords* ausgeschaltet wird.

eDirectory-Server durch Firewall absichern

Da der eDirectory-Server in diesem Einsatzszenario über eine direkte Internet-Anbindung verfügt, ist der Einsatz einer Firewall zu planen. Eine geeignete Vorgehensweise hierzu findet sich in Baustein B 3.301 *Sicherheitsgateway (Firewall)*.

Ergänzende Kontrollfragen:

- Welche Daten sollen von außen anonym erreichbar sein?
- Welche Daten sollen nach erfolgter Authentisierung erreichbar sein?
- Ist der Einsatz von SSL erforderlich, um die Vertraulichkeit bzw. Integrität der übertragenen Daten sicherzustellen?

M 2.241 Durchführung einer Anforderungsanalyse für den Telearbeitsplatz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Bevor ein Telearbeitsplatz eingerichtet wird, ist es sinnvoll, eine Anforderungsanalyse durchzuführen. Sinn dieser Anforderungsanalyse ist es, alle in Frage kommenden Einsatzszenarien zu bestimmen, um daraus die benötigten Hard- und Software-Komponenten für die Anbindung des häuslichen Arbeitsplatzes abzuleiten. Hierdurch können spezielle Anforderungen identifiziert werden, die den Einsatz bestimmter Systeme und/oder Software erforderlich machen (siehe hierzu z. B. Baustein B 4.4 *Remote Access* oder Baustein B 4.5 *LAN-Anbindung eines IT-Systems über ISDN*).

Dokumentation und Abstimmung

Die Ergebnisse einer solchen Anforderungsanalyse müssen dokumentiert und mit den IT-Verantwortlichen abgestimmt werden.

Im Rahmen dieser Anforderungsanalyse sind u. a. folgende Fragen zu klären:

- Bis zu welchem Vertraulichkeitsanspruch dürfen Daten im Rahmen der Telearbeit am Telearbeitsplatz, also außerhalb der "schützenden Mauern" der Behörde bzw. des Unternehmens, bearbeitet werden?
- Zu welchem Zweck wird der Zugang zur Institution genutzt (Abfragen von Informationen, Einstellen von Informationen, Programmnutzung)?
- Wie hoch ist der Datenverkehr zwischen dem häuslichen Arbeitsplatz und der Institution?
- Benötigt der Telearbeiter Zugriff auf das Intranet der Institution? Wenn ja, muss der Zugriff auf das gesamte Intranet, d. h. auf alle dort verfügbaren Daten und Dienste erfolgen oder nur auf Teilbereiche des Intranets?
- Ist für die Telearbeiter die Nutzung des Internets vorgesehen? Wenn ja, bekommt der Telearbeiter einen eigenen Internet-Zugang oder wird dieser Zugang über das Intranet der Institution realisiert?

Übertragungswege festlegen

Je nach dem Vertraulichkeitsanspruch der Daten kann es erforderlich sein, bestimmte Übertragungswege von der Organisation zum Telearbeitsplatz festzulegen. Dabei kann es sinnvoll sein, bestimmte Übertragungswege auszuschließen oder Mindestanforderungen dafür festzulegen. Beispielsweise könnte es vorgeschrieben sein, Papierdokumente mit vertraulichen Informationen nur auf direktem Weg von der Organisation zum Telearbeitsplatz in verschlossenen Transportbehältern zu transportieren. Ebenso könnten für verschiedene Vertraulichkeitsgrade unterschiedliche Verschlüsselungsverfahren für die Datenübertragung vorgesehen sein.

Ähnliche Überlegungen sollten angestellt werden, wenn die im Rahmen der Telearbeit zu verarbeitenden Informationen besonders vor Manipulation geschützt werden müssen.

Ergänzende Kontrollfragen:

- Wurde eine Anforderungsanalyse für den Telearbeitsplatz durchgeführt?
- Wurden die Anforderungen an den Telearbeitsplatz mit den IT-Verantwortlichen (Administratoren und anderem technischem Personal) abgestimmt?
- Ist der Schutzbedarf der Informationen, die im Rahmen der Telearbeit verarbeitet werden, festgestellt und dokumentiert?

M 2.242 Zielsetzung der elektronischen Archivierung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Um eine elektronische Archivierung in einer Institution einzuführen, sind die Ziele festzulegen, die damit erreicht werden sollen. Dabei muss das Management der betreffenden Organisation einbezogen werden. Gegebenenfalls ist eine Koordinierung mit übergeordneten Organisationseinheiten notwendig. Insbesondere ist festzulegen,

- in welchen Bereichen welche Daten archiviert werden sollen,
- welches Sicherheitsniveau es zu erreichen gilt,
- welcher Funktions- und Leistungsumfang angestrebt ist und
- wer die Verantwortung hierfür trägt.

Ziele im Archivierungskonzept dokumentieren

Die Ergebnisse sind im Archivierungskonzept (siehe Maßnahme M 2.243 *Entwicklung des Archivierungskonzepts*) zu fixieren.

Welche Daten sind zu archivieren?

Die Bestimmung der zu archivierenden Daten dient der Eingrenzung der technischen Anforderungen an das auszuwählende Archivsystem. Die Eingrenzung sollte aber so allgemein erfolgen, dass ausreichend Spielraum für die technische Ausgestaltung bleibt, wobei zu beachten ist, dass sich Anforderungen auch im Laufe der Zeit ändern können. Besonders auf Managementebene sind allgemeine Charakterisierungen sinnvoll wie:

- alle Daten/Dokumente der Abteilung ,
- alle Daten/Dokumente der Geschäftsprozesse,
- alle Geschäftsdaten,
- alle Buchhaltungsdaten,
- alle Kundendaten, sowie
- alle Daten der Klassifikationsstufe.

Schutzbedarf berücksichtigen

Wenn Daten mit unterschiedlichem Schutzbedarf archiviert werden sollen, wird empfohlen, die Ziele und Anforderungen an die Archivierung anhand der jeweiligen Schutzbedarfskategorie zu definieren. Ein Beispiel hierfür ist die Archivierung von Dokumenten, die als offen, intern, geheim o. ä. klassifiziert worden sind.

Welches Sicherheitsniveau soll erreicht werden?

Das zu erreichende Sicherheitsniveau bei der Archivierung lässt sich auf Managementebene typischerweise wie folgt charakterisieren:

- Erfüllung gesetzlicher sowie organisationsinterner Anforderungen an den Schutz der Daten bei der Archivierung sowie darüber hinaus (z. B. nach Entsorgung der Datenträger),
- Widerstandsfähigkeit des Archivierungsprozesses gegen Manipulation,
- Widerstandsfähigkeit des verwendeten Archivsystems gegen interne und externe Angriffe auf die gespeicherten Daten sowie das IT-System selbst.

Wenn Daten und Dokumente klassifiziert werden, kann das Sicherheitsniveau auch anhand dieser Klassifikation detaillierter differenziert werden.

Welcher Funktions- und Leistungsumfang soll erreicht werden?

Der angestrebte Funktions- und Leistungsumfang elektronischer Archivierung kann je nach Organisation unterschiedlich ausfallen. Üblicherweise werden auf Managementebene die folgenden Anforderungen definiert:

- Integrationsfähigkeit in die bestehende IT-Systemlandschaft, **Integrationsfähigkeit**
- Integrationsfähigkeit in bestehende IT- und Dokumentenmanagement-Prozesse,
- Einhaltung (gesetzlich sowie intern) vorgeschriebener Speicher- und Löschfristen für Daten,
- Aussonderungsmodalitäten und Beachtung der Anbietungspflicht.

Dies betrifft vor allem die öffentliche Verwaltung, da öffentliche Stellen unter Umständen dazu verpflichtet sind, Daten, die von besonderer Bedeutung sind, z. B. gesellschaftlicher, politischer oder historischer Art, einem dafür zuständigen Archiv nach Ablauf der Aufbewahrungsfrist anzubieten. Erst wenn dieses entscheidet, dass die entsprechenden Daten nicht archivwürdig sind, dürfen diese endgültig gelöscht werden. Über die Archivwürdigkeit von Daten kann in vielen Fällen erst nach Ablauf der Aufbewahrungsfrist entschieden werden, so dass die Daten am Ende der Aufbewahrungsfrist nicht immer automatisch bearbeitet werden können.

- Einhaltung des angestrebten Sicherheitsniveaus der Daten sowie
- Migrationsfähigkeit des Archivsystems, wenn sich Anforderungen und Einflussfaktoren ändern. **Migrationsfähigkeit**

Wer trägt die Verantwortung?

Mit dem Aufbau bzw. dem Betrieb der elektronischen Archivierung müssen Verantwortliche benannt werden. Üblicherweise wird von Seiten des Managements eine Fachabteilung bzw. deren Leiter mit der Umsetzung der Archivierung beauftragt. Hiermit müssen auch Zielvorgaben, Befugnisse, personelle und finanzielle Ressourcen verknüpft werden. Die Delegation der Umsetzung ist entsprechend den organisationsinternen Richtlinien durchzuführen und im Archivierungskonzept zu fixieren.

Ergänzende Kontrollfragen:

- Sind sämtliche zu archivierende Daten im Archivierungskonzept aufgeführt?
- Ist das angestrebte Sicherheitsniveau der zu archivierenden Daten festgelegt?
- Ist der angestrebte Funktions- und Leistungsumfang der elektronischen Archivierung festgelegt?
- Sind die Verantwortlichkeiten für die Archivierung festgelegt und dokumentiert?

M 2.243 Entwicklung des Archivierungskonzepts

Verantwortlich für Initiierung: IT-Sicherheitsmanagement,

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Archivverwalter

Der Aufbau eines Archivsystems sollte sorgfältig konzipiert werden. Dabei sind einerseits zahlreiche Einflussfaktoren (z. B. organisationsinterne oder rechtliche Vorgaben, technische und organisatorische Umgebungsbedingungen) zu beachten, andererseits bestehen vielfältige technische Möglichkeiten, um ein elektronisches Archiv aufzubauen. Daher sollte zunächst ein Konzept entwickelt werden, in dem alle Einflussgrößen und Entscheidungskriterien für die Wahl eines konkreten Archivierungssystems und der entsprechenden Produkte berücksichtigt werden und das gleichzeitig unter Kostengesichtspunkten wirtschaftlich vertretbar ist.

Grundlage für das Archivierungskonzept ist die in M 2.242 *Zielsetzung der elektronischen Archivierung* festgelegte Zielsetzung.

Im Archivierungskonzept ist der technische bzw. organisatorische Einsatz des Archivsystems festzulegen, also z. B.

- die Zuständigkeiten und Verantwortlichkeiten,
- die Definition von Benutzerrollen (z. B. Archivverwalter, Administratoren, Benutzer, technische Benutzer),
- Definition von Zugriffsrechten und Modalitäten zur Rechtevergabe,
- Abgrenzung der zu archivierenden Daten,
- Schutz der archivierten Daten, z. B. durch Verschlüsseln und Signieren,
- die angestrebte Systemanbindung bzw. die Einsatzbedingungen für Archivierungskomponenten,
- die technische Ausgestaltung des Archivsystems,
- der Betrieb des Archivsystems (z. B. Beschreibung von Service Level Agreements).

Konzept schriftlich dokumentieren

Die Ergebnisse sollten aktualisierbar und erweiterbar schriftlich dokumentiert werden. Das Archivierungskonzept selbst sollte in allen umgesetzten Fassungen aufbewahrt werden. Die Mitarbeiter sind über den sie betreffenden Teil des Konzepts zu unterrichten. Die Unterrichtung sollte nachprüfbar dokumentiert werden. Ein möglicher Aufbau eines Archivierungskonzepts ist im nachfolgenden Inhaltsverzeichnis beispielhaft aufgezeigt:

Inhaltsverzeichnis Archivierungskonzept

1. **Dokumentkontext**
   - Regelungsgegenstand
   - Regelmäßige Anpassung
   - Anordnung der Umsetzung
2. **Definitionen**
   - Archivierung, Dokumentenbegriff
   - Langzeitarchivierung, Archivierung zu Revisionszwecken
   - Beschreibung der Einsatzart und des Archivsystems

3. **Gefährdungslage zur Motivation**
   - Abhängigkeit der Institution vom Datenbestand
   - Typische Gefährdungen wie Datenverlust, Rekonstruktionsfehler, ...
   - Institutionsrelevante Schadensursachen
   - Beispiele zu Schadensfällen im eigenen Haus
4. **Festlegung einer organisationsinternen Sicherheitsleitlinie**
   - Festlegung von Verantwortlichkeiten
   - Zielsetzung, Sicherheitsniveau
5. **Beschreibung der Einflussfaktoren**
   - Identifikation der zu archivierenden Daten
   - Vertraulichkeitsbedarf der Daten
   - Integritätsbedarf der Daten
   - Authentizitätsbedarf der Daten
   - Verfügbarkeitsanforderungen an die Daten
   - Rechtliche Rahmenbedingungen
   - Archivierungsfristen (minimale, bei Bedarf auch maximale Speicherdauer)
   - Anforderungen an die Performance beim Einlesen bzw. Auslesen von Daten, Rekonstruktionsaufwand
   - Datenvolumen sowie Änderungsvolumen
   - Art der Daten (Formate)
   - Art der Zugriffe auf die archivierten Daten (lokal oder verteilt im LAN bzw. WAN)
   - Zu beachtende Normen und Standards
   - Erforderliche Funktionalität
   - Personalaufwand
   - Kosten inklusive Folgekosten (Wartung, Administration, Updates, etc.)
   - Kenntnisse und IT-spezifische Qualifikationen der Benutzer
6. **Festlegung des Einsatzes**
   - Art des Archivsystems
   - Einsatzbedingungen an das Archivsystem
   - Zeitraum des Einsatzes
   - Benennung der Verantwortlichen
   - Festlegung von Service Level Agreements
   - Durchführung der personellen Maßnahmen (Schulung, Vertretungsregelungen, Verpflichtungen, Rollenzuteilung)
   - Dokumentation der Einsatzbedingungen und der Konfiguration
   - Interoperabilität, Standardkonformität, Investitionsschutz
   - Regelmäßige Datensicherung
   - Virenschutz
   - Einsatz kryptographischer Verfahren
7. **Randbedingungen für die Archivierung**
   - Vertragsgestaltung
   - Refresh-Zyklen für die Speichermedien
   - Bestandsverzeichnis
   - Löschen von Daten
   - Vernichtung von unbrauchbaren Datenträgern
   - Vorhalten von arbeitsfähigen Lesegeräten

8. Sporadische Restaurierungsübungen

Einzelne Punkte dieses Konzepts werden in den Maßnahmen

- M 2.242 *Zielsetzung der elektronischen Archivierung*,
- M 2.244 *Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung*,
- M 2.245 *Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung*,
- M 2.246 *Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung*,

näher adressiert.

Archivierungskonzept regelmäßig anpassen

Bei der elektronischen Archivierung handelt es sich nicht um eine einmalige Aufgabe, sondern um einen dynamischen Prozess. Ein Archivierungskonzept muss daher regelmäßig den aktuellen Gegebenheiten angepasst werden.

Ergänzende Kontrollfragen:

- Ist das Archivierungskonzept verbindlich festgelegt?
- Ist das vorliegende Archivierungskonzept aktuell?
- Sind die Mitarbeiter über den sie betreffenden Teil des Konzepts nachweislich unterrichtet worden?
- Wird die Aktualität des Konzepts regelmäßig überprüft?
- Werden Änderungen der Einflussfaktoren zeitnah berücksichtigt?

M 2.244 Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Archivverwalter

Bevor eine Entscheidung getroffen werden kann, welche Verfahren und Produkte für die elektronische Archivierung eingesetzt werden sollen, müssen eine Reihe von technischen Einflussfaktoren ermittelt werden. Dazu sollten auch die Eigentümer der zu archivierenden Daten befragt werden, also beispielsweise die Verantwortlichen der einzelnen IT-Systeme bzw. IT-Anwendungen und die Systemadministratoren. Die Ergebnisse sind nachvollziehbar im Archivierungskonzept (siehe M 2.243 *Entwicklung des Archivierungskonzepts*) zu dokumentieren. Die für die elektronische Archivierung maßgeblichen technischen Einflussfaktoren sind unter anderem

- das zu erwartende Datenaufkommen,
- die Dateiformate der zu archivierenden Dokumente,
- das Änderungsvolumen und Versionierung,
- die Aufbewahrungsdauer der Dokumente,
- die Zahl und Art der Zugriffe,
- die vorhandene IT-Einsatzumgebung sowie
- zu beachtende Normen und Standards.

Die angegebenen Einflussfaktoren sind nachfolgend detaillierter dargestellt:

Zu erwartendes Datenaufkommen

Datenaufkommen abschätzen

Ein wesentliches Kriterium für die Auswahl elektronischer Archivsysteme ist die Größe der zu archivierenden Dateien und das in Zukunft zu erwartende Datenaufkommen. Dies kann typischerweise nur großzügig abgeschätzt werden.

Die Dateigröße von Dokumenten hängt dabei auch sehr stark von der Wahl des Dateiformates und dem Umfang der Rendition (siehe weiter unten) ab.

Dateiformate der zu speichernden Dokumente

Je nach Wahl des Archivsystems können in diesem grundsätzlich alle verwendeten Dateiformate abgelegt werden, z. B. die in Büroumgebungen üblichen Formate (DOC, PDF, RTF, ASCII, ZIP, etc.) oder auch Bild- und Tondateien (JPG, GIF, WAV, MPEG, etc). Besondere Bedeutung erhalten bei der Archivierung jedoch Dateiformate, die eine langfristige Stabilität hinsichtlich der Syntax und Semantik der Daten bieten (wie z. B. SGML, XML oder auch HTML) oder Bilddateien, die ein exaktes Abbild des ehemals vorhandenen Papierdokuments darstellen können (z. B. TIFF). Die einzelnen Datenformate sind in Maßnahme M 4.170 *Auswahl geeigneter Datenformate für die Archivierung von Dokumenten* detailliert beschrieben.

Dokumente in mehreren Formaten archivieren

Bei der elektronischen Archivierung haben sich in der Vergangenheit mehrere Dateiformate etabliert, die eine unterschiedliche Eignung für künftige Verwendungszwecke der Daten aufweisen. Häufig kann oder soll jedoch der

spätere Verwendungszweck nicht festgelegt werden. In so einem Fall ist aber nicht vorhersagbar, welches das beste Datenformat für die spätere Verwendung ist. Ebenso häufig bestehen bereits zum Zeitpunkt der Datenspeicherung konkurrierende Anforderungen an die Wahl des Dateiformates, die sich aus den unterschiedlichen Verwendungszwecken ergeben. Deshalb hat es sich, vor allem bei der Langzeitarchivierung, als vorteilhaft erwiesen, Dokumente in mehreren Dateiformaten gleichzeitig zu archivieren. Die Dokumente müssen dazu vorher konvertiert werden. Dieser Vorgang wird als Rendition bezeichnet. Bei der Rendition ist jedoch auf eine genaue Dokumentation der Verfahrensweise zu achten. Informationen über das Originalformat müssen mit archiviert werden.

Die Rendition von Dokumenten und anschließende Speicherung in mehreren Dateiformaten wirkt sich unmittelbar auf die für die Archivierung notwendige Speicherkapazität aus.

Änderungsvolumen und Versionstiefe

Bei der Archivierung von Dokumenten ist zu überlegen, welche Änderungen an den Dokumenten im Lauf der Zeit auftreten werden, wie häufig dies zu erwarten ist und wie damit zu verfahren ist. Wenn archivierte Dokumente geändert werden sollen, bestehen folgende Möglichkeiten:

- Das ursprüngliche Dokument wird durch die geänderte Version ersetzt.
- Die neue Version des Dokuments wird zusätzlich zur ursprünglichen Version archiviert (Versionierung), wobei unter Umständen nur eine maximale Anzahl von Versionen desselben Dokuments archiviert bleibt (Versionstiefe).

Versionierung

Durch organisationsinterne oder rechtliche Anforderungen kann eine Versionierung der Dokumente gefordert werden. Hier wird insbesondere auf die Maßnahmen M 2.245 *Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung* und M 2.246 *Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung* verwiesen.

Eine Versionierung kann auch durch die Wahl des Speichermediums (z. B. WORM - Write Once Read Multiple) erzwungen werden.

Sofern eine Versionierung von Dokumenten vorgenommen wird, muss dies bei der Berechnung der notwendigen Speicherkapazität des Archivsystems berücksichtigt werden.

Aufbewahrungsdauer der Dokumente

Für die Kalkulation der notwendigen Speicherkapazität des Archivsystems ist eine Abschätzung der Aufbewahrungsdauer der archivierten Dokumente unerlässlich. Für die Aufbewahrungsdauer ergeben sich aufgrund rechtlicher oder organisationsinterner Vorgaben minimale, jedoch teilweise auch maximale Speicherfristen, die zu beachten sind.

Die Aufbewahrungsdauer hat jedoch nicht nur Einfluss auf die Speicherkapazität des Archivsystems, sondern auch auf die Auswahl des Speichermediums sowie dessen Entsorgung nach Ablauf der Aufbewahrungsdauer.

Zahl und Art der Zugriffe

Zugriffszahlen sowie die Art der Zugriffe auf das Archivsystem haben Auswirkungen auf die Konfiguration des Archivservers und die Auswahl der Speicherkomponenten.

Als Einflussfaktoren sind daher zu ermitteln:

- Wie viele Zugriffe werden innerhalb eines vorgegebenen Zeitraums auf das Archivsystem erfolgen?
- Wie hoch ist der Anteil von Schreibzugriffen gegenüber Lesezugriffen?
- Welche Antwortzeiten werden verlangt?
- Erfolgen die Zugriffe direkt von Benutzer- bzw. Clientsystemen auf das Archivsystem oder durch ein übergeordnetes Dokumentenmanagementsystem?
- Muss das Archivsystem zwischen Zugriffen verschiedener Benutzer unterscheiden oder erfolgt dies durch übergeordnete Komponenten?
- Muss das Archivsystem mehrere, voneinander getrennte Archive verwalten (Mandantenfähigkeit)? **Mandantenfähigkeit**

IT-Einsatzumgebung

Archivsysteme sind typischerweise in komplexere IT-Landschaften eingebettet. Hierdurch ergeben sich technische Anforderungen, z. B. hinsichtlich

- der Netzanbindung,
- der verwendbaren Netzprotokolle (deren Definition z. B. bekannt sein muss, wenn die Kommunikationsverbindung über Firewalls geführt wird),
- Kompatibilität zu anderen Programmen oder IT-Systemen,
- der Einbindung in Systemmanagement-Umgebungen sowohl zur Administration als auch zur Überwachung des Archivsystems,
- der Administrations- und Nutzungsschnittstellen sowie
- der Antwortzeiten des Archivsystems.

Zu beachtende Normen und Standards

Die im Bereich der Archivierung bestehenden Standards konzentrieren sich auf die Bereiche

- Dateiformate und Kompressionsverfahren,
- Speichermedien und deren Aufzeichnungsverfahren sowie
- Dokumentenmanagement-Software.

Systemhersteller erhalten durch die Offenlegung von Schnittstellen, die im Rahmen der Standardisierung erfolgt, die Möglichkeit, eine Kompatibilität von Systemkomponenten, Schnittstellen und Datenformaten herzustellen. Deshalb kann durch die Berücksichtigung von Standards bei der Auswahl von Archivsystemen eine längerfristige Planungs- und Investitionssicherheit ge- **Planungs- und Investitionssicherheit**

währleistet werden. Bei den in diesem Baustein empfohlenen Maßnahmen wird auf die derzeit gültigen Standards Bezug genommen.

Für den Anwender bedeutet die Orientierung an Standards eine Verringerung der Abhängigkeit von einzelnen Herstellern, Systemlieferanten und Dienstleistern. Bei den langen Zeiträumen, über die Archivsysteme typischerweise eingesetzt werden, ist dies besonders wichtig, da nicht absehbar ist, wie sich Produktlinien langfristig entwickeln. So könnte sich z. B. bei Insolvenz eines Herstellers proprietärer Speicherkomponenten das Problem ergeben, dass das Archivierungssystem nicht mehr in der bisherigen Art durch Zukauf neuer Speichermedien und -komponenten erweitert werden kann. In Behörden und Unternehmen mit hohem Archivierungsbedarf führt dies typischerweise kurzfristig den Eintritt in die Migrationsphase herbei. Bei Einsatz standardisierter Komponenten kann dagegen einfach ein anderer Lieferant für die betroffene Teilkomponente gewählt werden.

Hinsichtlich Standards ist allerdings zu beachten, dass auch diese mit der Zeit aufgrund neuer technologischer Entwicklungen an Relevanz verlieren und bei Bedarf durch neue Standards ersetzt werden. Diese unterscheiden sich gelegentlich inhaltlich grundlegend, äußerlich aber nur in der Versionsnummer. Zudem besteht auch ein Wettbewerb zwischen unterschiedlichen Standardisierungsgremien und Herstellern, die naturgemäß auf der Suche nach wirtschaftlichem Einfluss am Markt sind, wodurch es auch konkurrierende Standards gibt.

Wartung und Systembetreuung sicherstellen

Prinzipiell ist die Archivierung jedoch auch ohne Beachtung von Standards unter Nutzung proprietärer Datei- und Speicherformate möglich, sofern über den Archivierungszeitraum eine ausreichende Wartung und Systembetreuung durch Hersteller und eine Anpassung der Schnittstellen an sich verändernde Anforderungen sichergestellt wird. Es wird jedoch aus obigen Gründen empfohlen, sich bei der Planung von Archivsystemen eng an geltenden Standards für Dateiformate und Schnittstellen zu orientieren.

Bereits bei der Planung eines Archivsystems sollte eine spätere Migration berücksichtigt werden, da sich bei der langfristigen Speicherung von Daten typischerweise zwischendurch die Technik oder die Anforderungen ändern. Besondere Sorgfalt sollte daher auf die Planung und Auswahl von Schnittstellen, Dateiformaten und Index-Datenbank verwendet und alle Entscheidungen nachvollziehbar dokumentiert werden.

M 2.245 Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Archivverwalter

Für die Aufbewahrung bestimmter Informationen bestehen verschiedene rechtliche Vorgaben, deren Nichteinhaltung zivil- oder strafrechtliche Konsequenzen haben kann. Daher sollten sich die Verantwortlichen informieren, welche rechtlichen Vorgaben in ihrem Fall anzuwenden sind. Hieraus ergeben sich Anforderungen für die Gestaltung des Archivierungskonzepts, die bei der Planung elektronischer Archivierung berücksichtigt werden müssen. Dies betrifft unter anderem

- die Mindestaufbewahrung aus steuerlichen, haushaltsrechtlichen oder sonstigen Gründen,
- Höchstaufbewahrungsdauer aus Datenschutzgründen,
- Zugriffsrechte für Externe, wie z. B. Steuerbehörden, sowie
- Qualität von digitalen Signaturen.

Die anzuwendenden rechtlichen Grundlagen sind im Einzelfall zu klären.

Im Folgenden werden einige Quellen genannt, die in Deutschland typischerweise zu berücksichtigen sind:

- Bürgerliches Gesetzbuch (BGB)

  Hier werden insbesondere Anforderungen an die Rechtsgültigkeit von Dokumenten im Zivilrecht gestellt. Das BGB definiert auch Verjährungsfristen, z. B. für Schadenersatz aus unerlaubter Handlung.

- Zivilprozessordnung (ZPO)

  Analog zum BGB wird durch die ZPO geregelt, welche Dokumente als Urkunde anerkannt werden müssen, beispielsweise aufgrund einer eigenhändigen Unterschrift oder einer qualifizierten digitalen Signatur.

- Handelsgesetzbuch (HGB)

  Hier werden Anforderungen an die Ordnungsmäßigkeit und Revisionsfähigkeit der Geschäftstätigkeit gestellt. Dies umfasst auch bestimmte Aufbewahrungsfristen für Geschäftsdokumente.

- Grundsätze ordnungsmäßiger Datenverarbeitung (GoDV)

  Die GoDV sind selbst keine gesetzliche Vorschrift, sondern hergeleitet aus den im HGB definierten Grundsätzen ordnungsmäßiger Buchführung. Sie sind als de facto-Standard für die DV-Revision in Unternehmen zu verstehen.

- Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)

  Das Bundesministerium der Finanzen hat die in den GoDV vorgesehenen Revisionsanforderungen im Rahmen der GDPdU präzisiert. Dies betrifft hauptsächlich alle steuerlich relevanten digital vorliegenden Dokumente.

Hierbei wird u. a. gefordert, dass alle zur Auswertung der Daten notwendigen Informationen wie Dateistruktur, Datenfelder, interne und externe Verknüpfungen in maschinell auswertbarer Form zur Verfügung stehen müssen.

- Gesetze und Vorschriften zum Schutz personenbezogener Daten

  Sofern personenbezogene Daten archiviert werden, müssen die hierfür geltenden Gesetze und Vorschriften eingehalten werden. Dazu gehören vor allem das Bundesdatenschutzgesetz (BDSG) und die entsprechenden Gesetze der Länder.

Weiterhin gibt es Gesetze und Vorschriften, die speziell für Behörden und in der Verwaltung zu beachten sind, beispielsweise:

- Bundesarchivgesetz und die entsprechen Landesarchivgesetze,
- Registraturrichtlinie für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien (RegR),
- Empfehlungen des Bundesarchivs zur Aussonderung elektronischer Akten im Konzept zur Aussonderung elektronischer Akten der Koordinierungs- und Beratungsstelle der Bundesregierung für Information in der Bundesverwaltung (Schriftenreihe der KBSt, Band 40).

Organisationsspezifisch gelten darüber hinaus zahlreiche weitere gesetzliche und organisationsinterne Regelungen (z. B. Vorschriften für Sozialversicherungsträger, Krankenhäuser, Pharmaindustrie, Militär oder Kreditwesen), die im Einzelfall ermittelt werden müssen. Wesentliche Regelungskriterien sind üblicherweise die Aufbewahrungsdauer sowie der Vertraulichkeits- und Integritätsbedarf, wobei bei letzteren neben der Stärke auch die Zeitdauer des Schutzbedarfs eingeht.

Für die öffentliche Verwaltung besteht darüber hinaus die gesetzliche Verpflichtung, auch in digitaler Form vorliegende Dokumente den zuständigen Archiven anzubieten (Anbietungspflicht).

M 2.246 Ermittlung der organisatorischen Einflussfaktoren für die elektronische Archivierung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Archivverwalter

Für die elektronische Archivierung gibt es eine Reihe von organisatorischen Einflussfaktoren, die bei der Konzeption des Archivsystems berücksichtigt werden müssen. Dazu gehören unter anderem

- der Zeitraum des Einsatzes des Archivsystems,
- die Archivierungsfristen,
- der Vertraulichkeitsbedarf der Daten,
- der Verfügbarkeitsbedarf der Daten,
- der Integritätsbedarf der Daten,
- der Authentizitätsbedarf der Daten,
- die Festlegung akzeptabler Antwortzeiten,
- der Rekonstruktionsaufwand,
- der Personalaufwand,
- die Kenntnisse und IT-spezifischen Qualifikationen der Benutzer,
- die Ergonomie und Bedienfreundlichkeit des Archivsystems,
- die Einhaltung von Standards und
- die finanziellen Randbedingungen.

Die angegebenen Einflussfaktoren sind nachfolgend detaillierter dargestellt.

Einsatzzeitraum des Archivsystems

Lebensdauer der Komponenten

Die Einsatzdauer eines Archivsystems ist getrennt von der Zeitdauer der Archivierung zu kalkulieren. Es ist eine Abschätzung vorzunehmen, über welchen Zeitraum das konkret auszuwählende System betriebsbereit sein soll. Dies wirkt sich auf die Auswahl der Komponenten, speziell auf die geforderte Lebensdauer der Komponenten, aus.

Ein langer Zeitraum impliziert die Auswahl langlebiger IT-Komponenten sowie die Gestaltung entsprechender Service- und Lieferverträge, die typischerweise mit höheren Kosten verbunden sind.

Ein kurzer Zeitraum impliziert eine frühere Migration des Archivs auf ein neues Archivsystem.

Archivierungsfristen

Für die Kalkulation der notwendigen Speicherkapazität des Archivsystems ist eine Abschätzung der Aufbewahrungsdauer der archivierten Dokumente unerlässlich. Für die Aufbewahrungsdauer ergeben sich aufgrund rechtlicher oder organisationsinterner Vorgaben minimale, jedoch teilweise auch maximale Speicherfristen, die zu beachten sind.

Die Aufbewahrungsdauer hat jedoch nicht nur Einfluss auf die Speicherkapazität des Archivsystems, sondern auch auf die Auswahl des Speichermediums sowie dessen Entsorgung nach Ablauf der Aufbewahrungsdauer.

Vertraulichkeitsbedarf der Daten

Bei der Bestimmung des Vertraulichkeitsbedarfs ist vor allem zu beachten, dass sich dieser Bedarf während der Archivierungsfrist ändern kann. Hierbei können wirtschaftliche und juristische Einflussfaktoren Geltung erlangen. Typischerweise ist davon auszugehen, dass der Vertraulichkeitsbedarf im Lauf der Zeit abnimmt.

Wenn ein langfristiger Schutz der Vertraulichkeit gefordert wird, so hat dies Einfluss auf die organisatorische Gestaltung des Archivierungskonzepts (siehe M 2.264 *Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung*) und die Auswahl technischer Komponenten.

Verfügbarkeitsbedarf der Daten

Die elektronische Archivierung wird typischerweise zur langfristigen Aufbewahrung von Daten und Dokumenten eingesetzt. Hierbei ist als wesentliche Anforderung in einem der vorigen Punkte bereits festgelegt worden, für welchen Zeitraum die betreffenden Dokumente zu archivieren sind.

Daneben ist festzulegen, welche weitergehenden Anforderungen an die Verfügbarkeit zu stellen sind, z. B. die Ausfallsicherheit des Archivsystems und die Stabilität der verwendeten Speichermedien.

Integritätsbedarf der Daten

Die Integrität elektronisch archivierter Dokumente muss typischerweise auch nach einer langen Aufbewahrungsdauer noch sichergestellt und prüfbar sein. Hierbei ist insbesondere davon auszugehen, dass Ursprungsdokumente und weitere Kontextinformationen zwischenzeitlich nicht mehr existieren, die Integritätsprüfung also unmittelbar vom Archivsystem bereitgestellt werden muss.

Es muss neben der Klassifizierung des Integritätsbedarfs (z. B. niedrig bis mittel, hoch oder sehr hoch) festgelegt werden, über welchen Zeitraum dies prüfbar sein soll.

Authentizitätsbedarf der Daten

Analog zur Integrität muss auch der Authentizitätsbedarf und der Zeitraum festgelegt werden, innerhalb dessen die Authentizität von Dokumenten prüfbar sein muss. Auch hier ist davon auszugehen, dass typischerweise nach einer längeren Archivierungsdauer die Ursprungsdokumente und Kontextinformationen nicht mehr beigebracht werden können. Die Authentizitätsprüfung muss also vom Archivierungsprozess bereitgestellt werden.

Bestimmung akzeptabler Antwortzeiten

Zwischen der Anfrage an ein Archivsystem und der Antwort ergibt sich eine Verzögerung (Antwortzeit). Die Anforderungen an diese Verzögerung werden typischerweise durch eine zu erzielende mittlere und eine maximal akzeptable Antwortzeit definiert.

Die Antwortzeit ist nach unterschiedlichen Faktoren zu charakterisieren, u. a.

- die Zeitdauer bis zur Reaktion des Archivsystems bei einer Anfrage,
- die Zeitdauer bis zur Speicherbestätigung des Archivsystems und
- die Zeitdauer bis zur vollständigen Übertragung des gewünschten Dokuments an das Clientsystem.

Die geforderte Antwortzeit hängt dabei sehr stark vom Einsatzszenario ab. So kann z. B. bei der Abfertigung von Passagieren auf Flughäfen eine Abfragezeit von wenigen Minuten eine sinnvolle Anforderung sein. Bei einer Recherche in Altdatenbeständen eines Grundbuchamtes können dagegen durchaus Reaktionszeiten im Stundenbereich innerhalb der Regelarbeitszeit akzeptabel sein.

subjektive Anforderungen

Typischerweise ergeben sich auch subjektive Anforderungen an die Antwortzeiten. So kann z. B. eine hohe Reaktionszeit auf Suchanfragen oder beim Öffnen archivierter Dokumente als störender empfunden werden als eine gleich lange Zeitdauer bis zur Speicherbestätigung bei der Ablage von Dokumenten im Archiv.

Die Anforderungen an die Antwortzeit sind zu ermitteln und zu dokumentieren.

Rekonstruktionsaufwand

Es ist zu bestimmen, welcher zeitliche und technische Aufwand für das Wiederfinden und Bereitstellen archivierter Dokumente akzeptabel ist. Dies ist abhängig von der Art und Struktur der archivierten Daten und daher vom konkreten Einsatzszenario.

Personalaufwand

Der Personalaufwand für den Betrieb des Archivsystems stellt einen wesentlichen Einflussfaktor bei der Auswahl des Systems dar. Organisationsspezifisch ist zu ermitteln, welcher zusätzliche Personalaufwand und welche zusätzliche individuelle Belastung des Personals durch die Archivierung als tragbar angesehen werden.

Dies hat Auswirkungen auf die künftige Personalplanung, da gegebenenfalls zusätzliches Personal erforderlich ist. Die Rollen Archivverwalter, Archivadministrator und (technischer) Benutzer sind mindestens zu besetzen. Wenn im laufenden Betrieb zu wenig Personal verfügbar ist, muss die fehlende Personalkapazität durch externe Wartungs- und Serviceverträge kompensiert werden.

Kenntnisse und IT-spezifische Qualifikationen der Benutzer

Die Auswahl geeigneter Bedienschnittstellen des Archivsystems wird unter anderem von den Vorkenntnissen der vorgesehenen Benutzer beeinflusst. Hier sollte ermittelt werden, welche IT-spezifischen Fachkenntnisse vorliegen.

Dies hat auch Einfluss auf die Gestaltung von Dienstleistungen im Umfeld der Archivierung, etwa die Organisation einer Benutzerunterstützung (Helpdesk).

Schulung der Benutzer

Alle Benutzer müssen in jedem Fall im Umgang mit dem Archivsystem geschult werden, damit Schäden durch Fehlbedienung möglichst vermieden werden. Die erforderliche Schulung muss in der Kalkulation der Gesamtkosten berücksichtigt werden.

Ergonomie und Bedienfreundlichkeit des Archivsystems

Die Bedienfreundlichkeit hat maßgeblichen Einfluss auf die Akzeptanz durch die Benutzer und dadurch auch auf die ordnungsgemäße Nutzung des Archivsystems.

Pilot- und Testinstallationen

Neben gesetzlichen Anforderungen zur Ergonomie an Arbeitsplätzen ist hierbei auch der subjektive Eindruck von Benutzern zu berücksichtigen. Die Ermittlung entsprechender Anforderungen kann z. B. über eine Befragung der künftigen Benutzer erfolgen, es sollten jedoch auch Erfahrungen aus Pilot- und Testinstallationen der vorgesehenen Archivsystem-Komponenten einfließen.

Einhaltung von Standards

Investitionsschutz

Für die Interoperabilität mit anderen Produkten und Organisationsprozessen sollte darauf geachtet werden, dass Archivsystem-Komponenten gewählt werden, die konform zu bestehenden Standards sind. Obwohl auch Standards nicht dauerhaft bestehen, sondern im Lauf der Zeit ebenfalls vom technischen Fortschritt überholt werden, wird die Einhaltung der maßgeblichen Standards typischerweise als Investitionsschutz angesehen.

Dies ist jedoch abhängig vom konkreten Einsatzzweck und der Einsatzumgebung. Es sollte daher individuell ermittelt werden, welche Standards maßgeblich sind. Einige relevante technische Standards sind in den Maßnahmen M 4.169 *Verwendung geeigneter Archivmedien* und M 4.170 *Auswahl geeigneter Datenformate für die Archivierung von Dokumenten* beschrieben.

Finanzielle Randbedingungen

Die Einführung von Archivsystemen und die Gestaltung eines entsprechenden organisatorischen Rahmens werden typischerweise von den anfallenden Kosten beeinflusst:

- einmalige Investitionen,
- laufenden Kosten, inklusive Personalkosten,
- Lizenzgebühren.

Die technische Planung des Betriebs von Archivsystemen wird daher typischerweise von einer Finanzplanung begleitet. Hierbei sind die

organisationsinternen Regelungen (Budgetplanung, Verteilung von Kostenstellen, etc.) zu berücksichtigen.

Die notwendigen Schulungen der Benutzer und Administratoren müssen in die Kalkulation der Gesamtkosten der Archivierung einbezogen werden.

M 2.247 Planung des Einsatzes von Exchange/Outlook 2000

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Bevor Exchange/Outlook 2000 eingeführt wird, muss entschieden werden, für welche Einsatzzwecke das System genutzt werden soll. Von der Nutzungsart hängt ab, welche Server-Variante beschafft werden muss, z. B. *Exchange 2000 Enterprise Server* oder *Exchange 2000 Conferencing Server*, und sie bestimmt Art und den Umfang der notwendigen Planungen. Insbesondere hängen auch die festzulegenden Sicherheitsrichtlinien stark vom geplanten Einsatzszenario ab.

Generell kann grob zwischen drei verschiedenen Einsatzvarianten von Exchange-Servern unterschieden werden:

- Einsatz als Intranet-Server und Zugriff über Outlook 2000 Clients. In diesem Szenario liegt das Hauptaugenmerk auf dem Einsatz als internes System zur Bürokommunikation (E-Mail, Terminvereinbarung, Koordination von Gruppenarbeit).
- Einsatz als Intranet-Server und Zugriff über Web-Clients. In diesem Szenario liegt der Schwerpunkt auf der Nutzung von Browsern zum Zugriff auf einen Exchange-Server. Da an der Web-Schnittstelle des Exchange-Servers gänzlich andere Sicherheitsmechanismen genutzt werden, wird die sichere Konfiguration der Web-Schnittstelle als eigenes Szenario betrachtet.
- Einsatz in der DMZ (Demilitarisierte Zone). Ein Exchange-Server kann auch als öffentlich zugänglicher Informations-Server in einer DMZ eingesetzt werden. Diese Nutzungsart erfordert aufgrund der exponierten Stellung des Servers besondere Aufmerksamkeit bei der Systemkonfiguration.

Innerhalb dieser Einzelszenarien kann weiter dahingehend unterschieden werden, welche Funktionen von Exchange genutzt werden sollen, z. B. interne E-Mail, Internet-Mail, Konferenz-Funktionen, Instant Messaging, LDAP-Server oder HTML-Server. Eine Unterscheidung auf dieser Ebene soll hier nicht erfolgen. Grundsätzlich gilt jedoch, dass für die Nutzung jeder Funktionalität eine eigene Planung erforderlich ist, bei der auch Sicherheitsaspekte zu berücksichtigen sind. Für einige Funktionen existieren passende, allgemeine Bausteine in den IT-Grundschutz-Katalogen, siehe beispielsweise Baustein B 5.3 *E-Mail*, die dann zur Anwendung kommen.

Grundsätzlich müssen bei der Einsatzplanung folgende Aspekte berücksichtigt werden:

- Exchange 2000 integriert sich in das Active Directory (AD) von Windows 2000. Daher sollte die Exchange 2000 Planung mit der Planung des Active Directory (siehe M 2.229 *Planung des Active Directory*) abgestimmt sein. Bei der Installation von Exchange 2000 wird eine Schema-Erweiterung des Active Directories durchgeführt. Damit beeinflusst eine Exchange-Installation das Active Directory nachhaltig, so dass der Schema-Administrator des Windows 2000 Systems unbedingt beteiligt werden muss. Außerdem müssen die an der Planung beteiligten Personen ausreichende Kenntnisse über den generellen Aufbau des Windows 2000/XP Systems haben, insbesondere über die Verteilung der Domänen-Controller und die Erreichbarkeit des sogenannten Global Catalog Servers.

Integration in das Active Directory

- Bei der Planung des Einsatzes von Exchange 2000 und Outlook 2000 ist über die Aufteilung in sogenannte *Routing Groups* zu entscheiden. Dies sind Verbände von Exchange-Servern, die über eine spezielle Hochgeschwindigkeitsverbindung miteinander kommunizieren. Dies löst das *Site-Konzept* (Standort-Konzept) von Exchange 5.5 ab. Weiterhin ist über die Aufteilung der Exchange-Server in administrative Gruppen zu entscheiden.

Aufteilung in Routing Groups

- Die E-Mail-Datenbanken können partitioniert und auf verschiedene Exchange-Server verteilt werden. Damit lassen sich E-Mail-Daten mit unterschiedlichem Schutzbedarf auf entsprechend physikalisch gesicherte Server aufteilen. Bei bedarfsgerechter Planung kann dies gleichzeitig die Performance und die Ausfallsicherheit erhöhen. Dies gilt auch für den Einsatz der Replikation der E-Mail-Datenbanken, die genutzt werden kann, um die Ausfallsicherheit zu erhöhen.

Partitionierung

- Begleitend zur Planung des gewünschten Einsatzszenarios und der Verteilung der Exchange-Server ist eine Sicherheitsrichtlinie zu entwerfen, in der die für Exchange spezifischen Aspekte behandelt werden. Die dabei zu berücksichtigenden Gesichtspunkte sind in der Maßnahme M 2.248 *Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000* zusammengefasst.

Sicherheitsrichtlinie erstellen

- Die Konfiguration des Exchange-Systems erfolgt über die Mechanismen der System- und Gruppenrichtlinien von Windows 2000/XP. Diese Einstellungen müssen mit den allgemeinen Richtlinieneinstellungen von Windows 2000/XP abgestimmt sein (siehe auch M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000* und M 2.326 *Planung der Windows XP Gruppenrichtlinien*).

- Für die Anbindung eines Exchange-Systems an fremde E-Mail/Messaging-Systeme, z. B. X.400 oder ccMail, stehen sogenannte *Connectoren* zur Verfügung, welche die Verbindung zwischen den verschiedenen E-Mail-Systemen herstellen. Der Einsatz dieser Connectoren ist sorgfältig zu planen, um einen reibungslosen Ablauf des E-Mail-Verkehrs zu gewährleisten.

Connectoren planen

- Um die Weiterleitung von E-Mails über die eingerichteten Routing Groups hinweg zu ermöglichen, muss der Einsatz sogenannter *Bridgehead Server* geplant werden. Da diese Server in der Regel mit fremden Netzen kommunizieren müssen, sollten sie in einer demilitarisierten Zone (DMZ) oder zumindest hinter einer Firewall (siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)*) platziert werden.

Bridgehead Server sicher betreiben

- Der Einsatz der Outlook 2000 Clients, deren Zugriffsmöglichkeiten auf das Exchange-System und die Absicherung dieser Zugriffe müssen geplant werden. Es ist ferner die Frage zu beantworten, ob eine Anbindung als MAPI-Client gewünscht ist oder nicht. In der Vergangenheit wurde die MAPI-Schnittstelle häufig zur Verbreitung von Programmen mit Schadfunktionen (z. B. Viren, Würmer, usw.) missbraucht.

Zugriffsmöglichkeiten der Clients festlegen

- Die Administration des Exchange/Outlook 2000 Systems muss geplant werden. Die Aufgaben reichen dabei von der Festlegung der Verantwortlichkeiten inklusive Stellvertreterregelung in der Organisation bis zur Definition geeigneter Administrationsrollen. In den entsprechenden Domänen müssen dann Benutzergruppen mit passenden Rechten eingerichtet werden.
- Die E-Mail-Konten und die verwendeten Newsgroups der Organisation müssen geplant werden.
- Der Einsatz eines integrierten Viren-Schutzprogramms im Exchange/Outlook 2000 System muss geplant werden. Dabei ist zu entscheiden, ob ein solches Programm Server- und/oder Client-seitig eingesetzt wird.

Virenschutz

- Die Behandlung aktiver Inhalte muss konsistent geplant werden. Dabei muss eine organisationsweit einheitliche Vorgehensweise festgelegt werden, nachdem die jeweiligen Vor- und Nachteile gegeneinander abgewogen wurden.

Behandlung aktiver Inhalte

- Die organisationsweite Verwendung von "Out-of-Office"-Nachrichten muss entschieden werden, da bei der Verwendung dieser Funktionalität interne, personenbezogene Information, wie z. B. die Abwesenheit einer konkreten Person, auch nach außen gelangen können.

Umgang mit Abwesenheiten

- Die Verwendung von E-Mail-Filtern zur Abwehr von Spam-Mail (unerwünschte Werbe-E-Mail) muss geplant werden.
- Für die Benutzung der Kalenderfunktion und der Aufgabenliste müssen ggf. die Zugriffsmöglichkeiten fremder Benutzer auf diese Funktionen festgelegt werden.
- In der Planung ist zu berücksichtigen, welche Outlook-Benutzer einen gemeinsamen Rechner verwenden. Entsprechend sind Profile auf diesen Rechnern anzulegen und gegenseitig abzusichern.
- Sollen Chat-, Instant Messaging-, Audio- oder Videokonferenz-Dienste in der Organisation genutzt werden, so muss deren Einsatz konzipiert werden.

Audit und Protokollierung

- Es muss ein Konzept für Audit und Protokollierung entworfen werden. Dazu ist festzulegen, wie die Audit- und Protokollierungsfunktion des Exchange-Systems genutzt wird. Wird bereits ein unternehmensweites Audit- oder Protokollierungssystem eingesetzt, so ist zu entscheiden, ob und wie die Exchange-Integration erfolgt. Es ist darauf zu achten, den Datenschutzbeauftragten und den Personal- bzw. Betriebsrat frühzeitig in die Planung einzubeziehen, da im Rahmen der Überwachung auch personenbezogene Daten anfallen können.
- Für das Exchange-System muss ein Backup-Konzept und ein Notfallvorsorge-Konzept erstellt werden. Dabei ist auf die Integration in existierende Konzepte zu achten.
- Erfolgt der Zugriff auf ein Exchange-System über HTTP (HyperText Transfer Protocol) so ergeben sich besondere Sicherheitsaspekte. Diese sogenannte OWA-Funktionalität (*Outlook Web Access)* war in der Vergangenheit (speziell bei Exchange 5.5) oftmals das Ziel von Angriffen. Die Absicherung und die Konfiguration muss deshalb besonders sorgfältig geplant und umgesetzt werden. In Anbetracht der Sicherheitsrisiken beim Einsatz der OWA-Funktionalität muss im Unternehmen bzw. in der Behörde zunächst prinzipiell die Frage geklärt werden, ob der Browser-Zugriff überhaupt genutzt werden soll. Wird die OWA-Funktionalität genutzt, so ist allgemein folgendes zu beachten:
- Es ist zu entscheiden, auf welche Inhalte zugegriffen werden darf, z. B. öffentliche Verzeichnisse (*public folders*), Newsgroups oder auch auf die eigene *Inbox*.

Aufstellung des Exchange-Servers

- Die Aufstellung des Exchange-Servers, auf den über das Internet zugegriffen werden kann, ist sorgfältig zu planen. Hierbei geht es sowohl um die geeignete Abschottung nach außen als auch nach innen. In den meisten Fällen sollte der von außen erreichbare Exchange-Server in einer sogenannten *Demilitarisierten Zone* (DMZ) aufgestellt werden. Weitere Hinweise hierzu finden sich im Baustein B 3.301 *Sicherheitsgateway (Firewall)*.
- Es ist zu beachten, dass ohne den Einsatz von Verschlüsselung, z. B. mit Hilfe von SSL, die zwischen Client und Server ausgetauschten Nachrichten unter Umständen von unberechtigten Dritten mitgelesen werden können. Der Einsatz von SSL muss genau geplant werden, damit eine sichere beidseitige Authentisierung von Client und Server erreicht werden kann.

Die Planung des Exchange/Outlook-Systems darf nur dann als abgeschlossen betrachtet werden, wenn auch das sogenannte *Roll-out* im Detail geplant worden ist. Dabei wird u. a. die Installationsreihenfolge der einzelnen Exchange-Server und aller Outlook-Clients festgelegt.

Ergänzende Kontrollfragen:

- Wurde das unterliegende Windows 2000/XP System bedarfsgerecht geplant?
- Wurde der Schema-Administrator in die Planung des Exchange-Systems einbezogen?
- Existiert ein Plan zur Verteilung der Exchange/Outlook-Software?

M 2.248 Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Wie für jedes in einer Behörde oder einem Unternehmen eingesetzte Client-Server-System muss auch für den Einsatz von Exchange 2000 Servern und Outlook 2000 Clients eine geeignete Sicherheitsrichtlinie festgelegt werden.

Da sich Exchange 2000 sehr stark in die Windows 2000 Umgebung integriert, speziell in das Windows 2000 Active Directory, muss die Windows 2000 Sicherheitsrichtlinie berücksichtigt werden (siehe hierzu M 2.228 *Festlegen einer Windows 2000 Sicherheitsrichtlinie* sowie M 2.229 *Planung des Active Directory*).

In der Sicherheitsrichtlinie für Exchange/Outlook 2000 ist festzulegen,

- welche Benutzer auf welche Server zugreifen dürfen und welche Benutzer auf welche Server *nicht* zugreifen sollen (Ausschlussliste),
- welche Benutzer mit welchen Rechten auf welche E-Mail-Datenbanken (*Mail Store*) zugreifen dürfen,
- welche anderen Server auf einen Exchange-Server zugreifen dürfen,
- wie E-Mail-Datenbanken repliziert werden,
- welche Bestandteile von E-Mail-Datenbanken repliziert werden und
- von wo aus auf einen Exchange-Server zugegriffen werden darf.

Wird die Sicherheitsrichtlinie festgelegt, so sind außerdem auch folgende Aspekte zu berücksichtigen:

- Die Sicherheitsrichtlinie für Exchange/Outlook muss konform zu den geltenden generellen Sicherheitsrichtlinien des Unternehmens bzw. der Behörde sein.
- Es muss festgelegt werden, wann eine Kommunikationsabsicherung, z. B. für Netz- oder E-Mail-Kommunikation, vorgenommen werden muss (z. B. beim Zugriff mittels Browser oder generell beim Zugriff über das Internet). Dabei ist auch festzulegen, welche Mechanismen dafür genutzt werden sollen.
- Die Gruppen für die Exchange-Administration, die *Routing Groups*, die Zugriffsberechtigungen zwischen diesen Gruppen (Benutzer- und Server-orientiert) und die Replikation von E-Mail-Datenbanken müssen geplant werden.
- Für die Kommunikationsbeziehungen nach außen müssen jeweils dedizierte Sicherheitsricht-linien festgelegt werden. Dabei ist auf Konsistenz mit anderen Richtlinien zu achten, die dem Schutz der physischen und logischen Grenzen der Organisation dienen.

Die Sicherheitsrichtlinie muss an alle mittel- und unmittelbar betroffenen Personen der Organisation verteilt und am besten in Form einer internen Schulung dargestellt werden.

Ergänzende Kontrollfragen:

- Können alle relevanten Sicherheitsvorschriften auf Exchange/Outlook 2000 abgebildet werden?
- Müssen existierende Sicherheitsvorschriften geändert werden?
- Werden alle Benutzer über neue oder veränderte Sicherheitsvorschriften informiert?

M 2.249 Planung der Migration von "Exchange 5.5-Servern" nach "Exchange 2000"

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

In der Praxis wird ein bereits bestehendes E-Mail-System häufig migriert, anstatt eine vollständige Neuinstallation durchzuführen. Exchange 5.5 ist ein weit verbreitetes E-Mail- und Messaging-System, so dass die Migration von Exchange 5.5 nach Exchange 2000 ein wichtiges Szenario darstellt.

weitreichender Design-Wechsel

Der Wechsel von Exchange 5.5 zu Exchange 2000 bedeutet einen gravierenden Sprung in nahezu sämtlichen Teilaspekten. Es handelt sich deshalb nicht um ein Software-Update, sondern um einen weitreichenden Designwechsel. Bei diesem Wechsel ist nicht nur die Exchange-Software betroffen, sondern auch das zugrundeliegende Betriebssystem Windows 2000. Ein installierter Windows 2000 Server ist Systemvoraussetzung für den Betrieb von Exchange 2000. Häufig fällt deshalb die Migration von Exchange 5.5 nach Exchange 2000 mit dem Wechsel des Betriebssystems von Windows NT 4 nach Windows 2000 und der Einführung des Active Directory zusammen.

Integration ins Active Directory

Exchange 2000 ist so konzipiert, dass es sich in das Windows 2000 Active Directory integriert. Bei der Installation von Exchange 2000 wird eine sogenannte Schema-Erweiterung des Active Directories vorgenommen. Eine Schema-Veränderung ist ein grundlegender Eingriff in das Active Directory, die nicht rückgängig gemacht werden kann. Es ist deshalb unerlässlich, den Windows-Systemadministrator und speziell den Active Directory-Schema-Administrator in die Migrationsplanung einzubeziehen.

Dass das Active Directory durch Exchange 2000 genutzt wird, hat folgende Auswirkungen:

Access Control Lists

- Access Control Lists (ACLs) sind auf jede einzelne Ressource anwendbar, so z. B. auf einzelne *Items* von öffentlichen Verzeichnissen sowie auch auf deren Eigenschaften (*Properties*).
- Anders als Exchange 5.5 verwendet Exchange 2000 keine Rollen mehr, da sich die Sicherheit nicht mehr aus dem *Information Store* selbst ableitet. Stattdessen wird die Berechtigung zur Administration des Exchange-Servers im Active Directory vergeben.

Security Identifiers

- Die *Security Identifiers* (*SID*s) für Benutzer- und Gruppenobjekte werden in der ACL der jeweiligen Exchange-Objekte verwendet. Anonyme Zugriffsberechtigungen werden einem speziellen anonymen *Logon-Konto* zugewiesen. Jede Gruppe erhält Standardeinstellungen für die Zugriffsberechtigungen.
- Berechtigungen auf Benutzer-, Objekt- und Property-Basis können explizit verboten werden. Verbotseinstellungen haben dabei Vorrang vor Erlaubniseinstellungen.

Kerberos

- Als Authentisierungsprotokoll im Netz wird Kerberos 5 verwendet. Details dazu finden sich beispielsweise in der Beschreibung des Bausteins 6.9 Windows 2000 Server.

Routing Groups

Die bei Exchange 5.5 noch übliche *Site*-Gruppierung von Exchange-Servern werden unter Exchange 2000 durch die sogenannten *Routing Groups* abgelöst. Die so im Verbund organisierten Exchange-Server erlauben den Datenaustausch mit hoher Bandbreite. Bei Exchange 2000 wird nun standardmäßig das *Simple Mail Transfer Protocol* (SMTP) eingesetzt, anstelle der vormals verwendeten *Remote Procedure Calls* (RPCs).

Auch hinsichtlich der Administration der Exchange-Server ergibt sich ein Unterschied: Sie beschränkte sich vormals auf eine NT-Domäne, nun ist die übergreifende Verwaltung über Domänen hinweg innerhalb eines *Forests* durch entsprechend autorisierte Administratoren möglich.

Partitionierung und Replizierung

Die Aufgaben der Partitionierung und der Replizierung von Inhalten der E-Mail-Datenbank übernimmt in vollem Umfang das Active Directory. Hier ist jedoch eine bedarfsgerechte Planung wesentlich, wenn eine Steigerung der Performance erreicht werden soll.

Fremde E-Mail-Systeme, z. B. X.400 oder ccMail, werden mittels sogenannter *Connectoren* an das Exchange-System angebunden. Speziell für die hier betrachtete Migration wird auch ein Connector zur Anbindung eines Exchange 5.5 Systems an das Active Directory angeboten.

Migration planen und dokumentieren

Die Migration muss in ihren einzelnen Schritten möglichst detailliert geplant, der angestrebte Migrationsprozess dokumentiert und allen Beteiligten zugänglich gemacht werden. Im Überblick sind folgende Schritte im Rahmen des Migrationprozesses durchzuführen:

- Backup des Exchange 5.5-Systems
- Probelauf der Exchange 2000 Software in einem Testszenario
- Windows 2000 Active Directory auf Domänen-Controller installieren
- Einrichten des Windows 2000 Netzes und der gewünschten Dienste (DNS, DHCP, etc.)
- Neue Rechner (für Exchange 2000 Server) mit Windows 2000 Server installieren
- Neue Rechner (für Exchange 2000 Server) Mitglied der gewünschten Domänen werden lassen
- Installation der Exchange 2000 Software auf den dafür vorgesehenen Windows 2000 Servern
- Verteilung der Outlook 2000 Clients
- Einrichten der Benutzerkonten inklusive der E-Mail-Funktionalität
- Einspielen der alten E-Mail-Daten. Dies kann dadurch geschehen, dass ein *Connector* zu einem Exchange 5.5 Server eingerichtet wird.

Folgende Aspekte sind aus Sicherheitssicht bei der Planung der Migration zu berücksichtigen:

- Welche E-Mail-Konten und öffentliche Verzeichnisse (*public folders*) sind zu migrieren?

- Wird die bestehende Sicherheitsrichtlinie übernommen oder geändert bzw. ergänzt?
- Ist das Active Directory-Konzept berücksichtigt und ggf. ergänzt worden?
- Welche fremden E-Mail-Systeme müssen angebunden werden?
- Welche Routing- und Administrations-Gruppen werden definiert?
- Die bestehende Installation von Exchange 5.5 sollte gesichert und zumindest so lange vorgehalten werden, bis das Exchange 2000 System zuverlässig in Betrieb genommen ist.
- Die neue Software sollte in einem separaten Testnetz getestet werden.

geänderte Terminologie

Allgemein ist zu beachten, dass sich die Terminologie der Objekte von Exchange 5.5 nach Exchange 2000 teilweise geändert hat. So wechseln beispielsweise die Begriffe *Mailbox* zu *Mail-Enabled User*, *Distribution List* zu *Distribution or Security Group*, *Custom Recipient* zu *Contact* und einiges weitere mehr.

Ergänzende Kontrollfragen:

- Wurde der Windows 2000 Systemadministrator an der Planung der Migration beteiligt?
- Wurden die vorzunehmenden Schema-Änderungen am Active Directory dokumentiert?
- Wurden für die Migration Backups des Systems und der Daten eingeplant?

M 2.250 Festlegung einer Outsourcing-Strategie

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung, IT-Verfahrensverantwortlicher

Die Bindung an einen Outsourcing-Dienstleister erfolgt auf lange Sicht, ist zunächst kostenintensiv und mit Risiken verbunden. Eine gute Planung des Outsourcing-Vorhabens ist daher wichtig. Dabei müssen neben den wirtschaftlichen, technischen und organisatorischen Randbedingungen auch die sicherheitsrelevanten Aspekte bedacht werden. Folgende Gesichtspunkte sollten betrachtet werden:

- Unternehmensstrategie (Flexibilität, Abhängigkeiten, zukünftige Planungen),
- Machbarkeitsstudie mit Zusammenstellung der Rahmenbedingungen,
- betriebswirtschaftliche Aspekte mit Kosten-Nutzen-Abschätzung.

Nach ersten strategischen Überlegungen muss zunächst geklärt werden, welche Aufgaben oder IT-Anwendungen generell für Outsourcing in Frage kommen.

rechtliche Rahmenbedingungen

Dabei darf die Bedeutung der rechtlichen Rahmenbedingungen nicht unterschätzt werden. Gesetze könnten beispielsweise das Auslagern bestimmter Kernaufgaben einer Institution generell verbieten oder zumindest weitreichende Auflagen enthalten und die Beteiligung von Aufsichtsbehörden vorschreiben. In der Regel bleibt der Auftraggeber weiterhin gegenüber seinen Kunden oder staatlichen Stellen voll verantwortlich für Dienstleistungen oder Produkte, unabhängig davon, ob einzelne Aufgabenbereiche ausgelagert wurden.

generelle Sicherheitsaspekte

Die IT-Sicherheit wird leider häufig zu Beginn der Planung vernachlässigt, obwohl ihr eine zentrale Bedeutung zukommt. Dies gilt sowohl für technische als auch organisatorische Sicherheitsaspekte, denen im Outsourcing-Szenario eine entscheidende Rolle zukommt. Generell ist nämlich zu bedenken:

- Die Entscheidung zum Outsourcing ist in der Regel nicht einfach zu revidieren. Die Bindung an den Dienstleister erfolgt unter Umständen sehr langfristig.
- Der Dienstleister hat Zugriff auf Daten und IT-Ressourcen des Auftraggebers. Der Outsourcing-Auftraggeber verliert dadurch die alleinige und vollständige Kontrolle über Daten und Ressourcen. Je nach Outsourcing-Vorhaben betrifft dies dann auch Daten mit hohem Schutzbedarf.

Datenübertragung

- Für die technische Umsetzung des Outsourcing-Vorhabens ist es notwendig, dass zwischen Auftraggeber und Dienstleister Daten übertragen werden. Dadurch ergibt sich automatisch ein erhöhtes Gefahrenpotential.
- In der Regel ist es erforderlich, dass Mitarbeiter oder Subunternehmer des Outsourcing-Dienstleisters (und damit Betriebsfremde) zeitweise in den Räumlichkeiten des Auftraggebers arbeiten müssen. Auch dadurch ergibt sich ein erhöhtes Gefahrenpotential.

- Im Rahmen eines Outsourcing-Vorhabens müssen neue Prozesse und Arbeitsabläufe entworfen, eingeführt und durchgeführt werden. Die Folgen der notwendigen Umstellungen müssen geklärt und abgeschätzt werden.
- Für jeden Outsourcing-Dienstleister besteht ein nicht zu unterschätzender Interessenskonflikt: Einerseits muss er die Dienstleistung möglichst kostengünstig erbringen, um seinen Gewinn zu maximieren, andererseits erwartet der Auftraggeber hohe Dienstleistungsqualität, Flexibilität und kundenfreundliches Verhalten. Dieser Punkt ist erfahrungsgemäß der am häufigsten unterschätzte. Während IT-Manager in der Regel sehr kritisch und kostenbewusst sind und Versprechungen von Herstellern und Beratern mit großer Skepsis begegnen, ist beim Outsourcing leider oft das Gegenteil zu beobachten. Allzu leicht verfällt hier der Auftraggeber den Werbeaussagen der Dienstleister in der frohen Erwartung, seine IT-Kosten signifikant senken zu können. Die Praxis lehrt jedoch, dass höchstens die Dienstleistungen in der Zukunft erbracht werden, die von Anfang an vertraglich fixiert worden sind. Stellt sich heraus, dass die Dienstleistungsqualität unzureichend ist, weil der Auftraggeber Leistungen erwartet, die er - im Gegensatz zum Outsourcing-Dienstleister - als selbstverständlich erachtet, sind Nachbesserungen in der Regel ohne hohe zusätzliche Kosten nicht zu erwarten. Jeder IT-Manager, der über Outsourcing nachdenkt, sollte sich die Mühe machen nachzurechnen, zu welchen Kosten ein Dienstleister die vereinbarte Leistung erbringen muss, damit Auftraggeber und Auftragnehmer beide von dem Vertragsverhältnis profitieren. Bei dieser Rechnung stellt sich vielleicht heraus, dass eine seriöse Leistungserbringung zu den versprochenen niedrigen Kosten höchst unwahrscheinlich ist.

Jeder Dienstleister muss Geld verdienen!

Um die Outsourcing-Strategie festzulegen, muss daher immer eine individuelle Sicherheitsanalyse durchgeführt werden. Nur so kann letztendlich festgestellt werden, wie bestehende IT-Systeme oder IT-Verbünde abgegrenzt und getrennt werden können, damit Teile davon ausgelagert werden können. In dieser frühen Projektphase wird das Sicherheitskonzept naturgemäß nur Rahmenbedingungen beschreiben und keine detaillierten Maßnahmen enthalten. Die IT-Sicherheitsanalyse sollte nach der in der IT-Grundschutz-Vorgehensweise beschriebenen Methodik durchgeführt werden:

individuelle Sicherheitsanalyse

- Es sollte eine IT-Strukturanalyse durchgeführt werden, sofern IT-Outsourcing geplant ist.
- Danach erfolgt eine Schutzbedarfsfeststellung.
- Im Einzelfall kann auch jetzt schon eine IT-Grundschutz-Analyse erfolgen, um den Handlungsbedarf sowie die Kosten für umzusetzende Maßnahmen zu identifizieren. Die Ergebnisse können dann insbesondere in die Betrachtung der Wirtschaftlichkeit des Outsourcing-Vorhabens mit einbezogen werden.

Wenn der Schutzbedarf wichtiger Systeme oder Anwendungen hoch ist oder die Modellierung des IT-Verbunds nach IT-Grundschutz nicht möglich ist, muss eine ergänzende Sicherheitsanalyse (z. B. Risikoanalyse) durchgeführt werden. Sind die sicherheitsrelevanten Gefährdungen analysiert worden, kann festgelegt werden, ob und wie diesen begegnet werden soll.

Schlussendlich wird dennoch ein gewisses Restrisiko durch den Outsourcing-Auftraggeber zu tragen sein. Die Ergebnisse der Sicherheitsanalyse gehen unmittelbar in die Kosten-Nutzen-Abschätzung ein.

strategische Überlegungen

Das Management darf bei der Entwicklung einer erfolgversprechenden, langfristigen Outsourcing-Strategie den Blick nicht nur auf die Einsparung von Kosten richten. Die Auswirkungen eines Outsourcing-Vorhabens auf die Aufgabenerfüllung, das Geschäftsmodell und das Dienstleistungs- oder Produktportfolio müssen ebenfalls berücksichtigt werden. Sollen Standardabläufe oder Kerngeschäftsprozesse ausgelagert werden? Wichtig ist in diesem Zusammenhang, dass die Fähigkeit, Anforderungen an die IT selbst zu bestimmen und zu kontrollieren in ausreichendem Maße erhalten werden. Insbesondere an die Weiterentwicklung und Pflege selbstentwickelter IT-Systeme und Anwendungen sollte gedacht werden.

Die nachfolgenden Hinweise beleuchten Vor- und Nachteile von Outsourcing mit Bezug zur IT-Sicherheit.

- Vorteil: Es besteht die Möglichkeit, neue Dienstleistungen (z. B. durch Diversifikation oder Ausweitung der Produktpalette) zu etablieren. In der Folge muss das festgelegte Sicherheitsniveau jedoch auch für das ausgeweitete Angebot sichergestellt werden.

höhere Flexibilität

- Vorteil: Es besteht mehr Flexibilität, beispielsweise können Systeme, Ressourcen oder der Personalbedarf schneller angepasst bzw. erweitert werden, da dies vom Outsourcing-Dienstleister unter Umständen auch kurzfristig eingekauft werden kann. Fixe Kosten können so in variable umgewandelt werden. In Folge können sich jedoch durch die Erweiterungen (z. B. von IT-Systemen) auch neue Sicherheitsprobleme ergeben.

höheres IT-Sicherheitsniveau durch externe Experten

- Vorteil: Im Idealfall kann durch das Outsourcing-Vorhaben ein besseres IT-Sicherheitsniveau erreicht werden, da der Dienstleister Spezialisten beschäftigt, so dass dadurch auch neue, sicherheitskritische Anwendungen betrieben werden können. Gerade in der IT-Sicherheit ist es sehr zeitaufwändig und benötigt viel technisches Wissen, regelmäßig die Flut an Sicherheitshinweisen, Security-Bulletins, Updatemeldungen und Bug-Reports auszuwerten, ihre Relevanz zu erkennen und bei Bedarf rasch die richtigen Schritte einzuleiten. Zunehmende Komplexität der angebotenen Hard- und Softwarelösungen, immer kürzere Produktzyklen, steigende Vernetzung und steigende Anforderungen der Nutzer machen es zudem außerordentlich schwierig, immer wieder die richtige Balance zwischen Sicherheit und "mehr Funktionalität" zu finden.
- Vorteil: Gerade in Unternehmen oder Behörden mit kleiner IT-Abteilung haben einzelne Mitarbeiter oft einen hohen Stellenwert. Stehen sie einmal nicht zur Verfügung (Krankheit, Urlaub) oder verlassen die Institution, können sich gravierende Sicherheitsprobleme ergeben, weil es keinen gleichwertigen Vertreter gibt. Dienstleister hingegen können in der Regel auf mehrere gleich qualifizierte Experten zurückgreifen, die sich gegenseitig vertreten können.
- Vorteil: Von einigen Institutionen wird Outsourcing häufig als vielleicht einzige Möglichkeit gesehen, eine Neugestaltung ihrer IT-Systeme und Anwendungen gegen interne Widerstände durchzusetzen. Im Zuge des

Outsourcings soll eine heterogene Systemlandschaft aufgeräumt und standardisiert werden.

- Nachteil: Wenn das Know-how der vom Outsourcing-Dienstleister eingesetzten Spezialisten nicht angemessen ist, so können dadurch gravierende IT-Sicherheitslücken entstehen. Ist zusätzlich intern nicht mehr das Fachwissen vorhanden, um das Sicherheitsniveau beim Outsourcing-Dienstleister zu kontrollieren, werden Sicherheitslücken womöglich nicht einmal entdeckt.
- Nachteil: Eine Ausweitung des Dienstleistungsangebots oder die Erweiterung von IT-Systemen ist nicht mehr allein eine Entscheidung des eigenen Managements. Der Outsourcing-Dienstleister muss immer an der Diskussion beteiligt werden. Dienstleister kompensieren nicht selten günstige Konditionen bei Vertragsabschluss durch hohe Forderungen bei späteren Sonderwünschen oder neuen Anforderungen des Auftraggebers. Der dann entstehende Kostendruck führt oftmals zu Einsparungen bei der IT-Sicherheit.
- Nachteil: Der Aufwand für die Kontrolle der Dienstleistungsqualität darf nicht unterschätzt werden. Sollten hierbei Defizite festgestellt werden, können diese schwierig und zeitaufwendig zu beheben sein, vor allem wenn es zu Meinungsverschiedenheiten zwischen Auftraggeber und Dienstleister kommt. Wenn Fragen der IT-Sicherheit dann nicht zeitnah gelöst werden, können sich Sicherheitslücken ergeben.

Kosten-Nutzen-Analyse

Eine umfassende Kosten-Nutzen-Analyse jedes Outsourcing-Vorhabens ist essentiell für den strategischen und wirtschaftlichen Erfolg. Es ist daher wichtig, alle Parameter zu kennen und auch richtig einzuschätzen.

Der strategische Wert der folgenden Ressourcen muss unter den Rahmenbedingungen des Outsourcing-Vorhabens eingeschätzt werden:

- Know-how
- Mitarbeiter
- IT-Systeme und Anwendungen

Bei der Kosten-Nutzen-Analyse können Studien und Erfahrungsberichte anderer Institutionen wertvolle Informationen liefern.

Dokumentation der gewählten Strategie

Abschließend ist die Outsourcing-Strategie zu dokumentieren. Die Ziele, Chancen und Risiken des Outsourcing-Vorhabens sollten eindeutig beschrieben werden. Es empfiehlt sich unter diesem Gesichtspunkt außerdem, die im Rahmen eines laufenden Outsourcing-Vorhabens gemachten Erfahrungen in die Dokumentation der Outsourcing-Strategie zu integrieren. Es sollte dabei auch auf Fehlentscheidungen und daraus abgeleitete Empfehlungen für die Zukunft hingewiesen werden.

Ergänzende Kontrollfragen:

- Sind alle betrieblichen und rechtlichen Rahmenbedingungen abgeklärt?
- Wurden IT-Sicherheitsgesichtspunkte ausreichend berücksichtigt?

M 2.251 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Leiter IT , Administrator,

Wenn eine Outsourcing-Strategie festgelegt wurde, müssen die IT-Sicherheitsanforderungen so konkret ausgearbeitet werden, dass auf ihrer Basis der geeignete Dienstleister ausgesucht werden kann. Dabei sind Sicherheitsanforderungen an den Outsourcing-Dienstleister selbst, die benutzte Technik (inklusive Kommunikationswege und -dienste), aber auch an die eigene Organisation zu stellen. Die Erstellung eines detaillierten Sicherheitskonzeptes, das auf den hier formulierten Anforderungen aufbaut und nach Auswahl des Dienstleisters ausgearbeitet wird, wird in M 2.254 *Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben* beschrieben.

Es ist zu bedenken, dass das Festlegen von IT-Sicherheitsanforderungen ein iterativer Prozess ist:

- Zunächst werden die gewünschten IT-Sicherheitsanforderungen durch den Auftraggeber spezifiziert.
- Danach wird in der Angebotsphase abgeglichen, wie und ob die gewünschten IT-Sicherheitsanforderungen durch die anbietenden Dienstleister geleistet werden können (siehe auch M 2.252 *Wahl eines geeigneten Outsourcing-Dienstleisters*).
- Ist ein Dienstleister ausgewählt, so muss mit diesem die weitere Verfeinerung der IT-Sicherheitsanforderungen (z. B. basierend auf den eingesetzten Betriebssystemen oder Sicherheitsmechanismen) erarbeitet werden. In der Endphase dieses Abstimmungsprozesses müssen dann auch die Sicherheitsanforderungen für die konkrete Umsetzung definiert werden.

Generell ergeben sich für Outsourcing-Szenarien folgende Mindestsicherheitsanforderungen:

Umsetzung von IT-Grundschutz

- Die Umsetzung des IT-Grundschutzes ist eine Minimalforderung an beide Outsourcing-Parteien. Zusätzlich müssen sowohl Outsourcing-Dienstleister als auch der Auftraggeber selbst ein IT-Sicherheitskonzept besitzen und dieses umgesetzt haben.
- Es ist wichtig, die relevanten IT-Verbünde genau abzugrenzen (z. B. nach Fachaufgabe, Geschäftsprozess, IT-Systemen), so dass alle Schnittstellen identifiziert werden können. An die Schnittstellen können dann entsprechende technische Sicherheitsanforderungen gestellt werden.
- Es muss eine Ist-Strukturanalyse von IT-Systemen und Anwendungen (siehe auch M 2.250 *Festlegung einer Outsourcing-Strategie*) erfolgen.
- Es muss eine Schutzbedarfsfeststellung (z. B. von Anwendungen, Systemen, Kommunikationsverbindungen, Räumen) bezüglich Vertraulichkeit, Integrität und Verfügbarkeit erfolgen (siehe auch M 2.250 *Festlegung einer Outsourcing-Strategie*).

Natürlich sind auch relevante Gesetze und Vorschriften zu beachten. Dies kann besonders in Fällen, in denen Auftraggeber oder Dienstleister länderübergreifend oder weltweit operieren, aufwendig sein.

Im Rahmen der IT-Sicherheitsanforderungen ist festzulegen, welche Rechte (z. B. Zutrittsrechte, Zugriffsrechte auf Daten und Systeme) dem Outsourcing-Dienstleister vom Auftraggeber eingeräumt werden.

Die Anforderungen an Infrastruktur, Organisation, Personal und Technik müssen beschrieben werden. Es genügt hier oftmals die Verpflichtung auf ein Sicherheitsniveau, das IT-Grundschutz entspricht. Sollten darüber hinausgehende Anforderungen bestehen, müssen diese detailliert beschrieben werden. Dies hängt entscheidend von der Sicherheitsstrategie und bereits vorhandenen Systemen und Anwendungen ab. Beispielsweise könnten folgende Punkte in Abhängigkeit vom Outsourcing-Vorhaben detailliert werden:

Organisatorische Regelungen und Prozesse

- Anforderungen an sicherheitskritische organisatorische Prozesse (z. B. Zeitrestriktionen für den Alarmierungsplan) können spezifiziert werden.
- Spezielle Anforderungen an bestimmte Rollen können festgelegt werden. Es kann beispielsweise gefordert werden, dass ein IT-Sicherheitsbeauftragter mit speziellen Kenntnissen (z. B. Host-Kenntnissen) beim Outsourcing-Dienstleister benannt werden muss.

Hard-/Software

- Der Einsatz zertifizierter Produkte (z. B. gemäß Common Criteria oder ITSEC) beim Outsourcing-Dienstleister kann gefordert werden.
- Anforderungen an die Verfügbarkeit von Diensten und IT-Systemen können gestellt werden. Beispielsweise kann in diesem Zusammenhang der Grad und die Methode der Lastverteilung (z. B. für Web-Server mit Kundenzugriff bei sehr vielen Kunden) vorgegeben werden.
- Vorgaben an die Mandantenfähigkeit sowie die diesbezügliche Trennung von Hard- und Software können formuliert werden. Beispielsweise kann festgelegt werden, dass keine IT-Systeme des Auftraggebers in Räumen untergebracht werden dürfen, in denen bereits Systeme anderer Mandanten des Dienstleisters stehen.

Kommunikation

- Spezielle Verfahren zur Absicherung der Kommunikation zwischen Dienstleister und Auftraggeber wie Einsatz von Verschlüsselungs- und Signaturverfahren (siehe auch Bausteine B 4.4 *Remote Access* und B 1.7 *Kryptokonzept*) können fest vorgegeben werden.

Kontrollen und QS

- Allgemeine Anforderungen bezüglich Kontrolle und Messung von Sicherheit, Qualität oder auch Abläufen und organisatorischen Regelungen können festgelegt werden, z. B. Zeitintervalle, Zuständigkeiten.

- Gewünschte Verfahren oder Mechanismen für die Kontrolle und Überwachung, wie unangekündigte Kontrollen vor Ort, Audits (unter Umständen durch unabhängige Dritte) können spezifiziert werden.
- Anforderungen an die Protokollierung und Auswertung von Protokolldateien können festgelegt werden.

Generell bilden die festgelegten IT-Sicherheitsanforderungen eine der Grundlagen für die Wahl eines geeigneten Outsourcing-Dienstleisters. Spezielle IT-Sicherheitsanforderungen müssen jedoch eventuell an das von Dienstleistern umsetzbare IT-Sicherheitsniveau angepasst werden.

Ergänzende Kontrollfragen:

- Ist IT-Grundschutz als Minimalanforderung in die Anforderungsliste aufgenommen worden?
- Sind alle IT-Sicherheitsanforderungen für das Outsourcing-Vorhaben ausreichend detailliert beschrieben?

M 2.252 Wahl eines geeigneten Outsourcing-Dienstleisters

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung, Leiter IT, IT-Sicherheitsmanagement

Bei der Wahl eines geeigneten Outsourcing-Dienstleisters sind ein möglichst detailliertes Anforderungsprofil und ein darauf basierendes Pflichtenheft entscheidende Erfolgsfaktoren. Nur so kann eine bedarfsgerechte Ausschreibung erfolgen, auf die sich auch geeignete Dienstleister bewerben.

Die Ausschreibung sollte die

allgemeine Beschreibung

- Beschreibung des Outsourcing-Vorhabens (Aufgabenbeschreibung und Aufgabenteilung) sowie
- Beschreibungen zum geforderten Qualitätsniveau, welches nicht zwangsläufig dem Niveau des Auftraggebers entsprechen muss, enthalten.

Sicherheitsanforderungen

Weiterhin müssen den potenziellen Dienstleistern auch möglichst detailliert

- die IT-Sicherheitsanforderungen und
- die Kriterien zur Messung von Servicequalität und Sicherheit

mitgeteilt werden (siehe M 2.251 *Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben*). In Einzelfällen kann es notwendig sein, die Detailanforderungen bezüglich Sicherheit nur gegen eine Vertraulichkeitsvereinbarung (Non-Disclosure-Agreement) an Dienstleister herauszugeben, da sich daraus Hinweise auf existierende oder geplante Sicherheitsmechanismen ableiten lassen.

Das Anforderungsprofil hängt stark von der Art des Outsourcing-Vorhabens ab. Als wichtige grundsätzliche Bewertungskriterien für Dienstleister und dessen Personal können gelten:

Anforderungen an Outsourcing-Dienstleister

Herkunft des Outsourcing-Dienstleisters

- Bei ausländischen Dienstleistern müssen besondere Aspekte bedacht werden. Dazu gehören beispielsweise: fremde Gesetzgebung, andere Haftungsregelungen, Spionagerisiko, andere Sicherheitskultur, im Partnerunternehmen bzw. durch die landesspezifische Gesetzgebung zugelassene und verwendbare Sicherheitsmechanismen.

Größe des Dienstleisters

- Die Größe des Dienstleisters kann bei der Auswahl ein Argument sein. Bei kleinen Unternehmen könnte das Insolvenzrisiko höher sein. Bei großen Unternehmen ist zu bedenken, dass diese sehr viele Auftraggeber und Projekte haben, so dass ein einzelner Auftraggeber nur einer unter vielen ist und keine bevorzugte Stellung einnimmt.

Referenzen

- Der Dienstleister sollte Referenzen für ähnliche Outsourcing-Vorhaben aufweisen können. Dabei ist auf Interessenskonflikte durch Geschäftsbeziehungen zu Konkurrenten des Auftraggebers und auf die Unabhängigkeit von bestimmten Herstellern (z. B. Zulieferer, die Konkurrenten des Auftraggebers sind) zu achten.

- Die Organisationsform eines Dienstleisters kann in Betracht gezogen werden, da dies z. B. die Haftungsgrenzen beeinflussen kann. Die Eigentümerstruktur sollte recherchiert werden, um mögliche Einflussfaktoren im Vorfeld abzuklären. **Eigentümerstruktur und Organisationsform**
- Die Kundenstruktur sollte beachtet werden, da dies darauf hinweist, in welchem Wirtschaftssektor der Anbieter seine Stärken hat. **Kundenstruktur**
- Ein Qualitätsnachweis bzw. eine Zertifizierung, z. B. nach ISO 27001 auf Basis von IT-Grundschutz oder ISO 9000, ist eine sinnvolle Forderung. **Zertifizierung**
- Auskünfte über die aktuelle wirtschaftliche Lage sowie Erwartungen an die zukünftige Geschäftsentwicklung der Dienstleister sollten eingeholt werden. **Solvenz**

Anforderungen an Mitarbeiter

Auch an die Mitarbeiter eines Dienstleisters sind diverse Anforderungen zu stellen (siehe auch M 2.226 *Regelungen für den Einsatz von* Fremdpersonal und M 3.33 *Sicherheitsüberprüfung von Mitarbeitern*).

- Die Qualifikation der Mitarbeiter muss in die Bewertung der Angebote einfließen. Es ist nach der Projektvergabe darauf zu achten, dass die im Angebot genannten Mitarbeiter auch später tatsächlich eingesetzt werden. **Qualifikationsprofil**
- Die Anzahl der verfügbaren Mitarbeiter muss bewertet werden. Dabei sollten auch die Vertretungsregelungen und die Arbeitszeiten hinterfragt werden. **Ressourcenplanung**
- Bei der Wahl ausländischer Partner muss eine gemeinsame Sprache für die Kommunikation zwischen den eigenen Mitarbeiter und denen des Dienstleisters festgelegt werden. Hierbei sollte auch hinterfragt werden, ob die vorhandenen Sprachkenntnisse für die Klärung von Detailproblemen ausreichen. Die Erfahrungen zeigen, dass viele Personen aus Angst, sich zu blamieren, lieber zu wichtigen Fragen schweigen, wenn sie ihre Sprachfähigkeiten als nicht perfekt einschätzen. **Kommunikationssprache**
- Entsprechend dem erforderlichen Sicherheitsniveau für das Outsourcing-Vorhaben sollte in die Bewertung der Angebote mit aufgenommen werden, ob eine Sicherheitsüberprüfung der Mitarbeiter vorliegt bzw. eine solche durchgeführt werden kann. **Sicherheitsüberprüfung**

Ergänzende Kontrollfragen:

- Ist ein Bewertungsmaßstab mit Bewertungskriterien für die Anbieterauswahl festgelegt worden?
- Sind die Sicherheitsanforderungen im Bewertungsmaßstab berücksichtigt?
- Ist der Bewertungsmaßstab auf das konkrete Outsourcing-Vorhaben zugeschnitten worden?

M 2.253 Vertragsgestaltung mit dem Outsourcing-Dienstleister

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement, Leiter IT

Nachdem ein Outsourcing-Dienstleister ausgewählt wurde, müssen alle Aspekte des Outsourcing-Vorhabens vertraglich in sogenannten Service Level Agreements (SLAs) festgehalten und geregelt werden. Die Aspekte, die im Folgenden beschrieben werden, sind als Hilfsmittel und Checkliste bei der Vertragsgestaltung zu sehen. Art, Umfang und Detaillierungsgrad der vertraglichen Regelungen hängen immer vom speziellen Outsourcing-Projekt ab. Je höher der Schutzbedarf der ausgelagerten IT-Systeme und Anwendungen ist, desto sorgfältiger und detaillierter muss der Vertrag zwischen Auftraggeber und Dienstleister ausgehandelt werden. Der Dienstleister sollte auf Einhaltung des IT-Grundschutzes und auf die vom Auftraggeber vorgegebenen Sicherheitsanforderungen verpflichtet werden (siehe M 2.251 *Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben*). Dazu gehört natürlich, dass der Outsourcing-Dienstleister sich verpflichtet, ein IT-Sicherheitskonzept inklusive eines Notfallvorsorgekonzepts zu erstellen und Sicherheitsmaßnahmen sowie Systeme und Anwendungen zu dokumentieren.

Zusätzlich zur allgemeinen Leistungsbeschreibung empfiehlt es sich jedoch immer, auch eine genaue quantitative Leistungsbeschreibung vertraglich zu fixieren, z. B. zu Verfügbarkeitsanforderungen, Reaktionszeiten, Rechenleistung, zur Verfügung stehendem Speicherplatz, Anzahl der Mitarbeiter, Supportzeiten.

Generell wäre eine allgemeine Verpflichtung auf die Einhaltung des IT-Grundschutzes zwar zufriedenstellend, es empfiehlt sich jedoch immer, alle vereinbarten Leistungen so genau und eindeutig wie möglich vertraglich festzuhalten. Dadurch lassen sich später Streitigkeiten zwischen den Parteien vermeiden. Nachträgliche Konkretisierungen und Ergänzungen des Vertrages, die aufgrund unterschiedlicher Interpretationen der beschriebenen Leistungen notwendig werden, sind oftmals mit deutlichen Kostenerhöhungen für den Auftraggeber verbunden. Auch die Erstellung des IT-Sicherheitskonzeptes selbst sollte Vertragsbestandteil sein. Insbesondere ist zu klären, wer für die fachlichen Inhalte verantwortlich ist und welche Mitwirkungspflichten dem Auftraggeber obliegen.

Im Folgenden findet sich eine Themenliste von Aspekten, die aus Sicherheitssicht geregelt werden sollten. Weitere Hinweise zu Details können den jeweiligen Maßnahmen der IT-Grundschutz-Kataloge entnommen werden:

Infrastruktur

- Absicherung der Infrastruktur des Dienstleisters (z. B. Zutrittskontrolle, Brandschutz, ...)

Organisatorische Regelungen/ Prozesse

- Festlegung von Kommunikationswegen und Ansprechpartnern

- Festlegung von Prozessen, Arbeitsabläufen und Zuständigkeiten
  - Verfahren zur Behebung von Problemen, Benennung von Ansprechpartnern mit den nötigen Befugnissen
  - regelmäßige Abstimmungsrunden
- Archivierung und Löschung von Datenbeständen (insbesondere bei Beendigung des Vertragsverhältnisses)
- Zugriffsmöglichkeiten des Dienstleisters auf IT-Ressourcen des Auftraggebers: Wer greift wie auf welches System zu? Wie sind die Zuständigkeiten und Rechte?
- Zutritts- und Zugriffsberechtigungen für Mitarbeiter des Dienstleisters zu den Räumlichkeiten und IT-Systemen des Auftraggebers
- Zutritts- und Zugriffsberechtigungen für Mitarbeiter des Auftraggebers zu den Räumlichkeiten und IT-Systemen des Dienstleisters

Personal

- Gestaltung der Arbeitsplätze von externen Mitarbeitern (Einhalten von Computerarbeitsplatzrichtlinien)
- Festlegung und Abstimmung von Vertretungsregelungen
- Verpflichtung zu Fortbildungsmaßnahmen

Notfallvorsorge

- Kategorien zur Einteilung von Fehlern und Störfällen nach Art, Schwere und Dringlichkeit
- erforderliche Handlungen beim Eintreten eines Störfalls
- Reaktionszeiten und Eskalationsstufen
- Mitwirkungspflicht des Auftraggebers bei der Behebung von Notfällen
- Art und zeitliche Abfolge von regelmäßigen und adäquaten Notfallübungen
- Art und Umfang der Datensicherung
- Vereinbarung, ob bzw. welche Systeme redundant ausgelegt sein müssen
- Von besonderer Bedeutung können Regelungen im Fall höherer Gewalt sein. Es sollte beispielsweise geklärt sein, wie bei einem Streik des Personals des Dienstleisters die Verfügbarkeit von Daten und Systemen sichergestellt werden kann. Besonders wenn Dienstleister und Auftraggeber unterschiedlichen Branchen angehören oder ihren Sitz in verschiedenen Ländern haben, kann der Auftraggeber von derartigen Vorkommnissen gänzlich überrascht werden.

Haftung, juristische Rahmenbedingungen

- Eine Verpflichtung auf die Einhaltung von geltenden Normen und Gesetzen sowie der vereinbarten Sicherheitsmaßnahmen und sonstigen Rahmenbedingungen ist vertraglich zu regeln. Ebenso sind Vertraulichkeitsvereinbarungen (Non-Disclosure-Agreements) vertraglich zu fixieren.

- Die Einbindung Dritter, Subunternehmer und Unterauftragnehmer des Dienstleisters ist zu regeln. In der Regel empfiehlt es sich nicht, diese grundsätzlich auszuschließen, sondern sinnvolle Regelungen festzulegen.
- Die Eigentums- und Urheberrechte an Systemen, Software und Schnittstellen sind festzulegen. Es ist auch zu klären, ob der Dienstleister bereits bestehende Verträge mit Dritten (Hardwareausstattung, Serviceverträge, Softwarelizenzen etc.) übernimmt.
- Die Weiterverwendung der vom Dienstleister eingesetzten Tools, Prozeduren, Skripte, Batchprogramme ist für den Fall der Beendigung des Dienstleistungsverhältnisses zu regeln.
- Regelungen für das Ende des Outsourcing-Vorhabens, z. B. für einen Wechsel oder bei Insolvenz des Dienstleisters, können spezifiziert werden. Auf ein ausreichend flexibles Kündigungsrecht ist zu achten.
- Der Auftragnehmer ist zu verpflichten, nach Beendigung des Auftrags alle Hard- und Software inklusive gespeicherter Daten, die dem Auftraggeber gehören, zurückzugeben. Alle vorhandenen Daten inklusive Datensicherungen sind ebenfalls zurückzugeben oder (je nach Vereinbarung) zu vernichten.
- Die Aufteilung von Risiken zwischen Auftraggeber und Dienstleister muss bedacht werden.
- Haftungsfragen im Schadensfall sind zu klären.
- Sanktionen oder Schadensersatz bei Nichteinhaltung der Dienstleistungsqualität müssen festgelegt werden. Die Bedeutung von Schadensersatzzahlungen und juristischen Konsequenzen sollte dabei nicht überschätzt werden. Zu bedenken sind nämlich die folgenden Punkte:

  1. Quantifizierbarkeit des Schadens

  - Wie wird beispielsweise ein Imageschaden gemessen?
  - Wie ist es zu bewerten, wenn gravierende Pflichtverletzungen aufgedeckt werden, die nur zufällig nicht zu einem größeren Schaden geführt haben?

  2. Insolvenz des Dienstleisters

  - Das Recht auf Schadensersatzzahlungen ist wertlos, wenn diese die Zahlungsfähigkeit des Dienstleisters übersteigen und dieser Insolvenz anmeldet. Nachfolgend fallen dann mindestens Kosten für den Umzug zu einem neuen Dienstleister an.

  3. Katastrophale Schäden

  - Eine Konventionalstrafe kommt zu spät, wenn der Auftraggeber durch das Ausmaß des Schadensereignisses seiner Geschäftsgrundlage beraubt wird und im schlimmsten Fall durch die Schadensfolgen die Zahlungsunfähigkeit eintritt.

4. Beweisbarkeit

- Kann ein Schaden nachgewiesen bzw. der Verursacher überführt werden (z. B. Nachweis von Spionage oder Manipulationen)?

Es ist immer zu bedenken, dass Schadensersatzzahlungen nur das allerletzte Mittel sind und nicht dazu führen dürfen, dass aus Kostengründen andere Sicherheitsmaßnahmen vernachlässigt werden. Sicherheit lässt sich nicht mit juristischen Mitteln erzielen.

Mandantenfähigkeit

- Die notwendige Trennung von IT-Systemen und Anwendungen verschiedener Kunden muss vereinbart werden.
  - Es ist sicherzustellen, dass Probleme bei anderen Kunden nicht die Abläufe und Systeme des Auftraggebers beeinträchtigen.
  - Es ist sicherzustellen, dass Daten des Auftraggebers unter keinen Umständen anderen Kunden des Outsourcing-Dienstleisters zugänglich werden.
- Falls notwendig, muss die physikalische Trennung (d. h. dezidierte Hardware) vereinbart werden.
- Falls notwendig, muss vereinbart werden, dass die vom Dienstleister eingesetzten Mitarbeiter nicht für andere Auftraggeber eingesetzt werden. Es kann auch sinnvoll sein, diese auf Verschwiegenheit zu verpflichten, so dass die eingesetzten Mitarbeiter nicht mit anderen Mitarbeitern des Dienstleisters auftraggeberbezogene Informationen austauschen dürfen.

Änderungsmanagement und Testverfahren

- Es müssen Regelungen gefunden werden, die es ermöglichen, dass der Auftraggeber immer in der Lage ist, sich neuen Anforderungen anzupassen. Dies gilt insbesondere, wenn beispielsweise gesetzliche Vorgaben geändert wurden. Es ist festzulegen, wie auf Systemerweiterungen, gestiegene Anforderungen oder knapp werdende Ressourcen reagiert wird.
- In diesem Zusammenhang ist auch die Betreuung und Weiterentwicklung bereits vorhandener Systeme zu regeln. Nicht selten übernimmt der Dienstleister selbstentwickelte Systeme oder Software vom Auftraggeber, der damit die Fähigkeit verliert, diese in seinem Sinne weiterzuentwickeln. Der Evolutionspfad von Systemen muss daher geregelt werden.
- Eine kontinuierliche Verbesserung der Dienstleistungsqualität und des IT-Sicherheitsniveaus sollte bereits in den SLAs festgeschrieben werden.
- Der Zeitrahmen für die Behebung von Fehlern ist festzulegen.
- Testverfahren für neue Soft- und Hardware sind zu vereinbaren. Dabei sind folgende Punkte einzubeziehen:
  - Regelungen für Updates und Systemanpassungen
  - Trennung von Test- und Produktionssystemen
  - Zuständigkeiten bei der Erstellung von Testkonzepten
  - Festlegen von zu benutzenden Testmodellen

- Zuständigkeiten bei Auftraggeber und Dienstleister bei der Durchführung von Tests (z. B. Mitarbeit oder Hilfestellung des Auftraggebers, Abnahme- und Freigabeprozeduren)
- Informationspflicht und Absprache vor wichtigen Eingriffen ins System (Negativbeispiel: Der Dienstleister spielt ein neues Betriebssystem auf dem Server ein. Durch unerwartete Fehler dabei werden wichtige Anwendungen gestört, ohne dass der Auftraggeber sich vorbereiten konnte.)
- Genehmigungsverfahren für die Durchführung von Tests
- Festlegung zumutbarer Qualitätseinbußen während der Testphase (z. B. Verfügbarkeit)

Kontrollen

- Dienstleistungsqualität und IT-Sicherheit müssen regelmäßig kontrolliert werden. Der Auftraggeber muss die dazu notwendigen Auskunfts-, Einsichts-, Zutritts- und Zugangsrechte besitzen. Wenn unabhängige Dritte Audits oder Benchmark-Tests durchführen sollen, muss dies bereits im Vertrag geregelt sein.
- Allen Institutionen, die beim Auftraggeber Prüfungen durchführen müssen (z. B. Aufsichtsbehörden) müssen auch beim Outsourcing-Dienstleister die entsprechenden Kontrollmöglichkeiten (z. B. Zutrittsrechte, Dateneinsicht) eingeräumt werden.

Ergänzende Kontrollfragen:

- Sind alle Vereinbarungen schriftlich fixiert?
- Enthält der Vertrag eindeutige und quantifizierbare Leistungsbeschreibungen?
- Sind genaue Regelungen für das Laufzeitende des Vertrages getroffen worden?

M 2.254 Erstellung eines IT-Sicherheitskonzepts für das Outsourcing-Vorhaben

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator, Leiter IT

Für jedes Outsourcing-Vorhaben muss ein IT-Sicherheitskonzept existieren. Dieses kann unter anderem auf Grundlage der IT-Grundschutz-Kataloge erstellt sein. Outsourcing-Projekte sind dadurch gekennzeichnet, dass sich viele technische und organisatorische Details erst im Laufe der Planung und bei Migration der Systeme ergeben. Das IT-Sicherheitskonzept, das nach Beauftragung eines Dienstleisters erarbeitet wird, wird daher in den wenigsten Fällen gleich vollständig und endgültig sein und muss während der Migrationsphase von allen Beteiligten stetig weiterentwickelt und konkretisiert werden. Die Migrationsphase ist daher von entscheidender Bedeutung für den Erfolg des Gesamtprojektes und wird in Maßnahme M 2.255 *Sichere Migration bei Outsourcing-Vorhaben* ausführlich beschrieben.

Generell unterscheiden sich IT-Sicherheitskonzepte für Outsourcing-Vorhaben nur wenig von IT-Sicherheitskonzepten für selbstbetriebene IT-Systeme. Es ergeben sich jedoch folgende Besonderheiten, die berücksichtigt werden müssen:

- Am Outsourcing-Vorhaben sind aus technischer Sicht in der Regel drei Parteien beteiligt:

  1. Outsourcing-Auftraggeber
  2. Outsourcing-Dienstleister
  3. Netzprovider

  Der Netzprovider stellt die Anbindung zwischen den Outsourcing-Parteien bereit. Die Zuständigkeit für die Netzanbindung fällt dabei in der Regel dem Outsourcing-Dienstleister zu.

- Jeder Beteiligte muss ein eigenes IT-Sicherheitskonzept erstellen und umsetzen, welches auch das spezielle Outsourcing-Vorhaben umfasst. Damit sind IT-Sicherheitskonzepte erforderlich:

  - für den Einflussbereich des Outsourcing-Dienstleisters,
  - für den Einflussbereich des Auftraggebers sowie
  - für die Schnittstellen und die Kommunikation zwischen diesen Bereichen.

- Zusätzlich zu den Einzelkonzepten ist ein IT-Sicherheitskonzept für das Gesamtsystem zu erstellen, welches die Sicherheit im Zusammenspiel der Einzelsysteme betrachtet.

- Die verschiedenen Teil-Konzepte müssen zwischen Auftraggeber und Dienstleistern abgestimmt werden. Dabei ist der Auftraggeber am IT-Sicherheitskonzept des Outsourcing-Dienstleisters nicht direkt beteiligt, sollte aber in einem Audit prüfen, ob es vorhanden und ausreichend ist. Für

das Audit kann der Auftraggeber dabei auch auf externe Dritte zurückgreifen.

Die in M 2.251 *Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben* und M 2.253 *Vertragsgestaltung mit dem Outsourcing-Dienstleister* genannten Sicherheitsanforderungen bilden dabei die Basis für das IT-Sicherheitskonzept. Aufbauend auf den dort beschriebenen grundlegenden Anforderungen muss im IT-Sicherheitskonzept die detaillierte Ausgestaltung erfolgen, wobei beispielsweise die Maßnahmen konkretisiert und Ansprechpartner namentlich festgelegt werden.

Sicherheitskonzept für Testphase

Erfahrungsgemäß ist der Übergang (Migration) von Aufgaben und IT-Systemen vom Auftraggeber zum Outsourcing-Dienstleister eine Projektphase, in der verstärkt mit Sicherheitsvorfällen zu rechnen ist. Aus diesem Grund müssen im Sicherheitskonzept Regelungen und Maßnahmen zur Migration behandelt werden, die in M 2.255 *Sichere Migration bei Outsourcing-Vorhaben* genauer behandelt werden.

Im Folgenden sind einige Aspekte und Themen aufgelistet, die im IT-Sicherheitskonzept im Detail beschrieben werden sollten. Da die Details eines IT-Sicherheitskonzeptes direkt vom Outsourcing-Vorhaben abhängen, ist die Liste als Anregung zu verstehen und erhebt keinen Anspruch auf Vollständigkeit. Neben einem Überblick über die Gefährdungslage, die der Motivation der Sicherheitsmaßnahmen dient, und den organisatorischen, infrastrukturellen und personellen Sicherheitsmaßnahmen können Maßnahmen aus folgenden Bereichen sinnvoll sein:

Organisation

- Umgang mit Daten und schützenswerten Betriebsmitteln wie Druckerpapier und Speichermedien, insbesondere Regelungen zum Anfertigen von Kopien und Löschen/Vernichten
- Festlegung von Aktionen, für die das "Vier-Augen-Prinzip" anzuwenden ist

Hard-/Software

- Einsatz gehärteter Betriebssysteme, um Angriffe möglichst zu erschweren
- Einsatz von Intrusion-Detection-Systemen (IDS), um Angriffe frühzeitig zu erkennen
- Einsatz von Datei-Integrität-Prüfungssystemen, um Veränderungen z. B. nach erfolgreichen Angriffen, zu erkennen
- Einsatz von Syslog- und Timeservern, um eine möglichst umfassende Protokollierung zu ermöglichen
- Einsatz kaskadierter Firewallsysteme zur Erhöhung des Perimeterschutzes auf Seiten des Dienstleisters
- sorgfältige Vergabe von Benutzer-Kennungen, Verbot von Gruppen-IDs für Personal des Dienstleisters

Kommunikation

- Absicherung der Kommunikation (z. B. durch Verschlüsselung, elektronische Signatur) zwischen Dienstleister und Auftraggeber, um sensitive Daten zu schützen
- Authentisierungsmechanismen

- Detailregelungen für weitere Netzanbindungen (siehe M 5.87 *Vereinbarung über die Anbindung an Netze Dritter*)
- Detailregelungen für den Datenaustausch (siehe M 5.88 *Vereinbarung über Datenaustausch mit Dritten*).

Kontrollen und QS

- Detailregelungen (z. B. unangekündigte Kontrollen vor Ort, Zeitintervalle, Zuständigkeiten, Detailgrad) für Kontrollen und Messung von Sicherheit, Dienstqualität, Abläufen und organisatorische Regelungen

Notfallvorsorge

- Das Notfallvorsorgekonzept ist in M 6.83 *Notfallvorsorge beim Outsourcing* beschrieben.

Ergänzende Kontrollfragen:

- Sind alle Teil-Sicherheitskonzepte (Auftraggeber, Dienstleister, Schnittstelle) erstellt worden?
- Wurde die IT-Sicherheitskonzeption des Dienstleisters durch den Auftraggeber oder unabhängige Dritte verifiziert?
- Sind alle IT-Sicherheitskonzepte gegeneinander abgestimmt und harmonieren miteinander?

M 2.255 Sichere Migration bei Outsourcing-Vorhaben

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Leiter IT, Administrator

Gefährdungslage

Nach Beauftragung des Outsourcing-Dienstleisters muss zunächst ein vorläufiges IT-Sicherheitskonzept entwickelt werden, in dem auch die Test- und Einführungsphase als Teilaspekt des Outsourcing-Vorhabens betrachtet wird. Zum einen sind in dieser Phase zahlreiche Betriebsfremde involviert, zum anderen müssen Abläufe etabliert, Aufgaben übertragen und Systeme neu eingerichtet bzw. angepasst werden. Einem sorgfältigen Testbetrieb kommt daher eine hohe Bedeutung zu. Besonders zu Testzwecken und in Phasen großer Arbeitsbelastung werden gerne "flexible" und "unkomplizierte" Lösungen gewählt, die selten sehr sicher sind. Es ist daher beispielsweise sicherzustellen, dass produktive Daten nicht ohne besonderen Schutz als Testdaten verwendet werden. Dies muss durch das IT-Sicherheitskonzept ausgeschlossen werden.

Vor der Erstellung eines Migrationskonzepts als Teil des Sicherheitskonzeptes für ein Outsourcing-Vorhaben muss ein IT-Sicherheitsmanagement-Team speziell für die Migrationsphase beim Auftraggeber eingerichtet worden sein. Dieses muss während der Migrationsphase auf Sicherheitsbelange achten und durch geeignete Maßnahmen auch schon im Vorfeld der Migration dafür sorgen, dass ein sicherer IT-Betrieb während der Migration gewährleistet ist. Die Größe des IT-Sicherheitsmanagement-Teams hängt dabei von Art und Größe des Outsourcing-Vorhabens ab, als Minimum kann es aus einem Sicherheitsexperten bestehen.

Aufgaben des IT-Sicherheitsmanagement-Teams

Dem IT-Sicherheitsmanagement-Team kommen dabei folgende Aufgaben zu, aus denen sich Regelungen und Vorgaben ableiten, die im Migrationskonzept zu erfassen sind:

- Es ist ein gemischtes Team aus Mitarbeitern des Auftraggebers und des Outsourcing-Dienstleisters zu bilden. Dieses kann auch durch externe Experten verstärkt werden, um spezielles Know-how verfügbar zu machen.
- Für die Migrationsphase muss eine IT-Sicherheitskonzeption erstellt werden.
- Die Verantwortlichkeiten und Hierarchien für die Migrationsphase sind festzulegen. Dabei ist es wichtig, dass klare Führungsstrukturen geschaffen und auf beiden Seiten eindeutige Ansprechpartner definiert werden. Zusätzlich ist darauf zu achten, dass auf beiden Seiten Verantwortlichkeiten auch auf hohen Ebenen definiert werden. Nur so kann sichergestellt werden, dass im Zweifelsfall mit entsprechendem Nachdruck gehandelt werden kann.
- Die erforderlichen Tests müssen geplant und durchgeführt werden, Abnahmeprozeduren erarbeitet und die Produktionseinführung geplant werden.
- Es sind geeignete interne Mitarbeiter für die Test-, Einführungsphase und den späteren Betrieb auszuwählen. Vertraglich kann sich ein Auftraggeber natürlich auch ein Mitspracherecht bei der Personalauswahl des Outsourcing-Dienstleisters einräumen lassen.

- Die Mitarbeiter des Auftraggebers sind zum Verhalten während und nach der Migrationsphase zu schulen. In der Regel sind die Mitarbeiter dabei mit neuen und unbekannten Ansprechpartnern konfrontiert. Dies birgt die Gefahr des Social Engineering (z. B. Anruf eines vermeintlichen Mitarbeiters des Sicherheitsteams des Dienstleisters).
- Der Dienstleister muss die relevanten Abläufe, Applikationen und IT-Systeme des Auftraggebers genau kennen lernen und dahingehend eingewiesen werden.
- Der störungsfreie Betrieb ist durch genaue Ressourcenplanung und Tests sicherzustellen. Die produktiven Systeme dürfen dabei nicht vernachlässigt werden. Dazu ist im Vorfeld zu überprüfen, ob die vorgesehenen Mitarbeiter zur Verfügung stehen. Zusätzlich müssen Störungen durch notwendige Tests einkalkuliert werden.
- Anwendungen und IT-Systeme, die der Dienstleister übernehmen soll, müssen ausreichend dokumentiert sein. Die Prüfung der Dokumentation auf Vollständigkeit muss dabei ebenso bedacht werden wie das Anpassen der vorhandenen Dokumentation auf die veränderten Randbedingungen durch das Outsourcing-Vorhaben. Die Dokumentation neuer Systeme oder Teilsysteme muss dabei ebenfalls sichergestellt sein.
- Während der Migration muss ständig überprüft werden, ob die SLAs oder die vorgesehenen IT-Sicherheitsmaßnahmen angepasst werden müssen.

Notfallvorsorgekonzept

In der Einführungsphase des Outsourcing-Vorhabens und der ersten Zeit des Betriebs muss dem Notfallkonzept besondere Aufmerksamkeit geschenkt werden. Bis sich bei allen Beteiligten die notwendige Routine, beispielsweise in der Behandlung von Fehlfunktionen und sicherheitsrelevanten Vorkommnissen eingestellt hat, sind verstärkt Mitarbeiter zu Bereitschaftsdiensten zu verpflichten.

Aktualisierung und Konkretisierung des Sicherheitskonzepts

Nach Abschluss der Migration muss sichergestellt werden, dass das IT-Sicherheitskonzept aktualisiert wird, da sich erfahrungsgemäß während der Migrationsphase immer Änderungen ergeben. Dies bedeutet insbesondere:

- Alle Sicherheitsmaßnahmen müssen konkretisiert werden.
- Ansprechpartner und Zuständigkeiten werden mit Namen und notwendigen Kontaktdaten (Telefon, Zeiten der Erreichbarkeit, eventuell erforderliche Zuordnungsbegriffe wie Kundennummern) dokumentiert.
- Die Systemkonfigurationen ist zu dokumentieren, wobei auch die eingestellten sicherheitsrelevanten Parameter zu erfassen sind.
- Das Personal ist durch Schulungsmaßnahmen auf den Regelbetrieb vorzubereiten.

Schulung

Als letzte Aufgabe muss das Outsourcing-Vorhaben nach der Migrationsphase in den sicheren Regelbetrieb (siehe M 2.256 *Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb*) überführt werden. Dabei ist vor allem darauf zu achten, dass alle Ausnahmeregelungen, die während

der Migrationsphase notwendig waren, wie z. B. erweiterte Zugriffsrechte, aufgehoben werden.

Ergänzende Kontrollfragen:

- Ist eine IT-Sicherheitskonzeption für die Migrationsphase erarbeitet worden?
- Enthält das Migrationskonzept alle notwendigen sicherheitsrelevanten Maßnahmen?
- Ist sichergestellt, dass alle Ausnahmeregelungen, die während der Migration notwendig sind, nach der Migration aufgehoben werden?
- Sind sowohl die Mitarbeiter des Auftraggebers als auch des Outsourcing-Dienstleisters ausreichend auf die Migration vorbereitet worden?

M 2.256 Planung und Aufrechterhaltung der IT-Sicherheit im laufenden Outsourcing-Betrieb

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Leiter IT, Administrator

Nachdem ein Outsourcing-Vorhaben umgesetzt wurde, muss die IT-Sicherheit auch im laufenden Betrieb gewährleistet werden. Dazu ist für das Outsourcing-Vorhaben ein Betriebskonzept zu planen, in dem auch die Sicherheitsaspekte berücksichtigt werden. Dabei unterscheiden sich die IT-bezogenen Einzelaufgaben generell nicht von denen, die zu planen und durchzuführen sind, wenn kein Outsourcing betrieben wird (siehe M 2.199 *Aufrechterhaltung der IT-Sicherheit*).

Besonderheiten ergeben sich jedoch dadurch, dass die Aufgaben auf mehrere Parteien verteilt sind und daher zusätzliche Aufgaben (z. B. Abstimmungen und Kontrollen) anfallen. Diese sind unter anderem:

- Dokumentationen und Richtlinien müssen regelmäßig aktualisiert werden.
- **Aktualität der Sicherheitskonzepte**
  Die geltenden Sicherheitskonzepte aller Beteiligten müssen daraufhin geprüft werden, ob sie noch aufeinander abgestimmt sind und das gewünschte Sicherheitsniveau gewährleisten. Insbesondere sollte der Outsourcing-Dienstleister den Auftraggeber über wichtige Änderungen in seinem Einflussbereich informieren.
- **Kontrollen**
  Regelmäßige Kontrollen zu folgenden Aspekten sind durchzuführen:
  - Durchführung der vereinbarten Audits
  - Umsetzungsstand der vereinbarten IT-Sicherheitsmaßnahmen
  - Wartungszustand von Systemen und Anwendungen
  - Rechtezuweisung durch den Dienstleister (Missbrauch von Rechten)
  - Einsatz von Mitarbeitern, die dem Auftraggeber nicht gemeldet wurden, z. B. bei Vertretungen
  - Performance, Verfügbarkeit, Qualitätsniveau
  - Datensicherung
- **Kommunikation**
  Regelmäßige Abstimmungsrunden zu folgenden Punkten sind abzuhalten:
  - Informationen müssen zwischen den Partnern ausgetauscht werden (z. B. Personalnachrichten, organisatorische Regelungen, Gesetzesänderungen, geplante Projekte, vorgesehene Tests und Systemänderungen, die zu Beeinträchtigungen der Dienstleistungsqualität führen können).
  - Probleme müssen identifiziert und analysiert werden.
  - Wichtig sind gegenseitiges Feedback und das Aufspüren von Verbesserungspotentialen. Zur Motivation der Mitarbeiter können besonders positive Beispiele einer gelungenen Kooperation dargestellt werden.
  - Änderungsmanagement: Änderungswünsche (Hardware, Software, Ausweitung des Dienstleistungsportfolios, gestiegener Ressourcenbedarf etc.) sollten frühzeitig besprochen werden.

- Es müssen regelmäßige Übungen und Tests zu folgenden Themen durchgeführt werden: **Tests und Übungen**
  - Reaktion auf Systemausfälle (Teilausfall, Totalausfall)
  - Wiedereinspielen von Datensicherungen
  - Beherrschung von Sicherheitsvorfällen

Ergänzende Kontrollfragen:

- Wurde ein Betriebskonzept für das Outsourcing-Vorhaben festgelegt?
- Enthält das Betriebskonzept Verfahren und Maßnahmen, die das gewünschte Sicherheitsniveau im laufenden Betrieb sicher stellen?
- Werden regelmäßig die notwendigen Kontrollen durchgeführt?
- Sind alle Sicherheitskonzepte noch aktuell?
- Gibt es eine regelmäßige Kommunikation zwischen den Vertragspartnern?

M 2.257 Überwachung der Speicherressourcen von Archivmedien

Verantwortlich für Initiierung: Leiter IT, Archivverwalter

Verantwortlich für Umsetzung: Leiter IT, Archivverwalter, Administrator

Benachrichtigung und Alarmierung

Die auf den Archivmedien vorhandene, freie Speicherkapazität ist kontinuierlich zu überwachen. Wenn die freie Speicherkapazität unter einen festzulegenden Schwellwert sinkt, sollte eine Benachrichtigung des Administrators sowie gegebenenfalls eine Signalisierung an eine Systemmanagement-Umgebung erfolgen. Sinkt die freie Speicherkapazität weiter unter einen kritischen Grenzwert, sollte eine Alarmierung ausgelöst werden.

Bei der Alarmierung ist besonders darauf zu achten, dass sie rollenbezogen erfolgt, das heißt unabhängig von konkreten Personen. Damit ist sichergestellt, dass auch im Krankheitsfall oder bei Urlaub Alarmierungen wahrgenommen werden.

Schwellwert und Grenzwert festlegen

Der Schwellwert, der kritische Grenzwert sowie die Eskalationsprozeduren und -wege sind organisationsspezifisch festzulegen.

Für die Festlegung der Grenzwerte müssen die verwendeten Archivmedien und das durchschnittliche Volumen der zu archivierenden Daten zugrunde gelegt werden. Nach Auslösen des kritischen Alarms muss gewährleistet sein, dass für eine hinreichende Zeit weiterhin das durchschnittliche Datenaufkommen archiviert werden kann. Typischerweise wird für den Schwellwert eine Restkapazität von 15% der Gesamtkapazität des Speichermediums und für den kritischen Grenzwert eine Restkapazität von 10% zugrunde gelegt.

leere Archivmedien vorhalten

Um etwaige Lieferengpässe bei Speichermedien zu überbrücken, sollte eine ausreichende Zahl leerer Archivmedien an einem bekannten Ort gelagert werden. Dabei müssen die klimatischen und physikalischen Lagerbedingungen eingehalten werden (siehe M 1.60 *Geeignete Lagerung von Archivmedien*).

Für den Fall der Alarmierung ist zu dokumentieren, in welcher Weise und in welchem Zeitraum eine Reaktion auf die Alarme erfolgen soll. Dies ist z. B. in *Service Level Agreements* (SLAs) festzulegen, falls der Betrieb des Archivsystems durch Dritte erfolgt.

Neben dem Speicherplatz müssen ggf. noch betriebssystem- oder anwendungsspezifische Restriktionen überwacht werden. Die entsprechenden Programmdokumentationen müssen daraufhin geprüft werden. In Zweifelsfällen oder bei fehlenden Angaben in der Dokumentation sollte der jeweilige Hersteller zu Rate gezogen werden. Beispielsweise können die Anzahl der maximal zugelassenen Dateien pro Verzeichnis oder die maximal erlaubten Datenbankeinträge überschritten werden, so dass keine weiteren Daten auf dem Speichermedium angelegt werden können.

Ergänzende Kontrollfragen:

- Ist eine kontinuierliche Überwachung des verbleibenden Speicherplatzes gewährleistet?
- Sind die Grenzwerte für eine Alarmierung festgelegt und dokumentiert?
- Sind leere Archivmedien in genügender Stückzahl an einem bekannten Ort gelagert?

M 2.258 Konsistente Indizierung von Dokumenten bei der Archivierung

Verantwortlich für Initiierung: Leiter IT, Archivverwalter

Verantwortlich für Umsetzung: Leiter IT, Archivverwalter, Administrator

Beim Betrieb eines Archivs ist es wichtig, alle abgelegten Dokumente und Datensätze eindeutig zu referenzieren, um sie bei späteren Archivanfragen korrekt wiederfinden zu können. Zusätzlich bieten Archivsysteme die Möglichkeit von Suchanfragen. Da eine Volltextsuche abhängig von Art und Umfang der archivierten Daten sehr lange dauern kann, speichern Archivsysteme zu jedem Dokument einen separaten Datensatz mit Indexangaben in einer eigenen Suchdatenbank. Struktur und Umfang der Indexangaben sind in der Regel konfigurierbar und sollten die folgenden Eigenschaften aufweisen:

- Eindeutigkeit: Die Dokumentenbezeichner müssen eindeutig sein.
- Unterstützung zu erwartender Suchanfragen: Durch die Kontextangaben sollen spätere Suchanfragen beschleunigt werden. Da der spätere Suchkontext nicht feststeht, kann im Vorfeld nur eine Abschätzung späterer Suchanfragen vorgenommen und versucht werden, die Kontextangaben so aussagekräftig wie möglich zu gestalten.
- Geringer Umfang: Ein geringer Umfang an Indexdaten beschleunigt spätere Suchanfragen, jedoch kann ein zu geringer Umfang der Indexdaten Suchanfragen behindern bzw. das Auffinden von Dokumenten erschweren. Der Umfang der Kontextangaben ist letztlich in Abhängigkeit vom erwarteten Datenvolumen festzulegen.

Diese Parameter müssen grundsätzlich vor der Inbetriebnahme des Archivs festgelegt werden. Trotzdem kann es im Laufe der Zeit notwendig werden, die Eigenschaften zu ändern. Je nach Umfang und Art der Änderung der Indexdaten kann dies eine sehr aufwändige Neuindizierung der Archivdatenbestände erforderlich machen.

Der konkrete Kontext für einzelne zu archivierende Dokumente kann auf unterschiedliche Art und Weise erzeugt werden. Drei Verfahren werden dabei unterschieden:

- **manuelle Erstellung:**

  Auf der Ebene des Dokumentenmanagementsystems werden Indexangaben zu jedem Dokument über eine Eingabemaske manuell erzeugt. Hierdurch besteht besonders bei großen Datenmengen die Gefahr, dass inkonsistente Indexangaben erfasst werden.

- **halbautomatische Erzeugung:**

  Diese Verfahren automatisieren die Vergabe von Indexdaten, gestatten jedoch eine manuelle Kontrolle und Korrektur.

- **vollautomatische Erzeugung:**

  Hierbei werden Dokumentindizes vollautomatisch ohne manuelle Eingriffsmöglichkeit vergeben.

Die Wahl des Verfahrens ist abhängig vom erwarteten Datenvolumen. Werden in unregelmäßigen Abständen einzelne Dokumente archiviert, ist ein manuelles Verfahren auf der Grundlage konkreter Vorgaben zur Erstellung eines Kontextes ausreichend.

Werden regelmäßig große Datenvolumen archiviert, sollte ein halbautomatisches Verfahren zur Erzeugung der Indexdaten gewählt werden. Hier besteht die Möglichkeit, diese Informationen manuell zu kontrollieren und zu korrigieren, bevor Dokument und Dokumentindex archiviert werden und dann gegebenenfalls nicht mehr nachträglich geändert werden können.

Bei der vollautomatischen Erzeugung der Indexdaten können Fehler nicht erkannt bzw. korrigiert werden. Eine eventuelle Fehlzuordnung von zu archivierenden Dokumenten, z. B. zu Geschäftsprozessen, kann dann nicht erkannt oder ausgeschlossen werden. Dieses Verfahren sollte deshalb nur dann angewandt werden, wenn alle Dokumente so strukturiert sind, dass alle Indexdaten in jedem Fall zweifelsfrei und zuverlässig extrahiert werden können.

Ergänzende Kontrollfragen:

- Wie groß ist der Benutzerkreis und wie hoch ist das Datenaufkommen, so dass eine manuelle Indizierung vertretbar ist?
- Sind Kontrollen der vergebenen Indizes möglich?
- Ist die Struktur der Indizierung dokumentiert und kommuniziert?

M 2.259 Einführung eines übergeordneten Dokumentenmanagements

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator

Bei der elektronischen Archivierung müssen alle archivierten Dokumente eindeutig identifiziert und reproduziert werden können. Da dabei in der Regel große Datenbestände zu verwalten sind, wird der Einsatz eines übergeordneten Dokumentenmanagement-Systems (DMS), auch für kleine und mittlere Behörden bzw. Unternehmen, empfohlen.

Dokumentenmanagement-System

Ein Dokumentenmanagement-System (DMS) bildet die Schnittstelle zwischen Benutzer (-programmen) und Archivsystem und sorgt für eine konsistente Verwaltung, Versionierung und Zuordnung von elektronischen Dokumenten.

Pflege der Index-Datenbank

Das DMS übernimmt regelmäßig auch die Pflege der Index-Datenbank, in der die zu den elektronischen Dokumenten archivierte Kontextinformation verwaltet und eventuell um DMS-Bestandteile ergänzt wird.

Unterschieden werden dabei zum einen Systeme, die neben den Indizes auch die Dokumente selbst in einer Datenbank ablegen, und zum anderen Systeme, die in ihrer Datenbank ausschließlich Referenzdaten auf die eigentlichen Dokumente im jeweiligen Speichersystem ablegen. Die erstgenannten Systeme sind allerdings durch die Kapazität der Datenbank eingeschränkt und eignen sich damit nicht für die Archivierung großer Datenmengen.

Zugriffsrechte und Klassifikation

Darüber hinaus muss ein Dokumentenmanagement-System die Festlegung von Zugriffsberechtigungen zu den archivierten Dokumenten sowie zur Index-Datenbank ermöglichen. Das DMS sollte auch eine Klassifikation von Dokumenten unterstützen. Es sollten Profile und Referenztabellen angelegt werden können, anhand derer Dokumente klassifiziert und verschlagwortet werden.

Die Eigenschaften des DMS müssen langfristig gewährleisten, dass die archivierten Dokumente eindeutig identifiziert, geschützt und reproduziert werden können.

Organisatorische Einbettung

Dokumentenmanagement-Systeme müssen in geeigneter Weise eingesetzt und in die Organisation eingebettet werden. Hierzu sind entsprechende Organisationsprozesse zu definieren, zu dokumentieren und in der Behörde bzw. im Unternehmen umzusetzen.

Regelungsbedarf besteht unter anderem hinsichtlich

- des Einstellens von Dokumenten ins DMS,
- der Nutzung des DMS beim Umgang mit Dokumenten,
- der Verantwortlichkeiten für Nutzung und Betrieb des DMS,
- der Rechtevergabe und der Zuständigkeit hierfür sowie
- der Anforderungen an den Betrieb des DMS (Service Level Agreements).

Letztlich soll durch die Organisationsprozesse sichergestellt werden, dass das Dokumentenmanagement auch in der vorgesehenen Weise benutzt und nicht etwa umgangen wird. Nur so ist eine vollständige und konsistente Archivierung der in der Organisation genutzten elektronischen Dokumente und Informationen möglich.

Standardisierung

Die am Markt angebotenen Dokumentenmanagement- und Archivsysteme sind nicht alle miteinander kompatibel. Dies ist sowohl durch die verwendete Technologie als auch durch die verwendeten Medien- und Speicherformate verursacht.

Um diese Probleme zu beheben, arbeiten die am Markt operierenden DMS-Hersteller in verschiedenen Gremien an der Vereinheitlichung der dem Dokumentenmanagement zugrundeliegenden Technologien zum Speichern und Wiedergewinnen von Dokumenten. Bei der Auswahl des DMS sollten die betreffenden Standards berücksichtigt werden, damit DMS- und Archivkomponenten langfristig verträglich sind.

Die wichtigsten Gruppen bzw. Standards sind:

- ODMA

  Schnittstelle zu Anwendungen

  Innerhalb der AIIM (Association for Information and Image Management) ist die ODMA-Gruppe (Open Document Management API) als Standardisierungsgremium tätig. ODMA bezeichnet eine standardisierte Schnittstelle zwischen dem Dokumentenmanagement-System und den Benutzeranwendungen. Es vereinfacht an dieser Stelle die Einbindung der Anwendungen.

  Die meisten Anbieter unterstützen diesen Standard.

- DMA

  Integration verschiedener DMS

  Die DMA (Document Management Alliance) ist als Projektgruppe innerhalb der AIIM gegründet worden. Sie ist aus einem Zusammenschluss von drei anderen Standardisierungsgremien, die ebenfalls im Umkreis der DMS gearbeitet haben, hervor gegangen:

  - ISO-Gruppe Document Filing and Retrieval - ISO 10166
  - Document Enabled Networking
  - Shamrock Document Management Coalition

  Die DMA etabliert einen Standard, mit dessen Hilfe Dokumentensammlungen und Dokumentenmanagement-Software über verschiedene Plattformen und Systeme hinweg einfach integriert werden können.

  Für den Benutzer ergibt sich so eine einheitliche Sicht auf alle Dokumenttypen, unabhängig vom Ort der Ablage oder der Erstellung.

  Nahezu alle führenden Hersteller halten diesen Standard ein. Im konkreten Einzelfall ist die Einhaltung der Standards allerdings zu prüfen.

- WfMC

  Die WfMC (Workflow Management Coalition, Belgien) arbeitet als Standardisierungsorgan im Bereich der Workflows.

Zusammenwirken von Workflow-Produkten

Das Ziel ist, Software-Spezifikationen zu erstellen, mit deren Hilfe einheitliche Voraussetzungen für das Zusammenwirken unterschiedlichster Workflow-Produkte und -Komponenten in unterschiedlichsten Umgebungen geschaffen werden.

Fast alle namhaften Hersteller arbeiten in diesem Gremium mit.

Ergänzende Kontrollfragen:

- Ist überprüft worden, ob der Einsatz eines Dokumentenmanagement-Systems sinnvoll ist?
- Ist die Verantwortung für Betrieb und Nutzung des DMS dokumentiert und bekannt?
- Ist die Nutzung des DMS in der Organisation verpflichtend geregelt und dokumentiert?
- Unterstützt das DMS die Vergabe und Kontrolle von Rollen und Zugriffsberechtigungen?
- Unterstützt das eingesetzte DMS die einschlägigen Standards?

M 2.260 Regelmäßige Revision des Archivierungsprozesses

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Revisor

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Revisor, Archivverwalter

Der Prozess der Archivierung ist regelmäßig einer Revision zu unterziehen, um seine Korrektheit und Ordnungsmäßigkeit zu prüfen und daraus die Korrektheit und Authentizität der im Archivsystem abgelegten Dokumente abzuleiten.

Hierzu ist eine geeignete Vorgehensweise für die Revision entsprechend des in M 2.243 *Entwicklung des Archivierungskonzepts* beschriebenen Konzeptes zu entwickeln und in Form einer Checkliste zu dokumentieren.

Diese Checkliste sollte mindestens die folgenden Punkte umfassen:

Fragen zu Verantwortlichkeiten

- Sind die verantwortlichen Personen benannt und in ihre Aufgaben eingewiesen worden? Ist dies dokumentiert?
- Bestehen Vertretungsregelungen für alle verantwortlichen Personen?

Fragen zum Organisationsprozess

- Bestehen organisationsweite Regelungen zum Einsatz elektronischer Archivierung?
- Ist organisationsweit geregelt und dokumentiert, welche Dokumente zu archivieren sind? Ist diese Regelung umfassend und vollständig?
- Sind die Sicherheitsanforderungen an die Dokumente dokumentiert?
- Werden die organisationsweiten Regelungen regelmäßig an aktuelle Entwicklungen angepasst?
- Werden alle Anpassungen der Regelungen ordnungsgemäß dokumentiert und archiviert?

Fragen zum Einsatz der Archivierung

- Bestehen eindeutige Regelungen, welche Dokumente zu archivieren sind?
- Bestehen dokumentierte Regelungen, welche Kontextangaben zu archivierten Dokumenten vergeben werden, etwa die Angabe von Dokumentkategorien?
- Werden die zu archivierenden Dokumente vollständig und reproduzierbar archiviert?
- Werden die Anforderungen an die Vertraulichkeit der zu archivierenden Dokumente eingehalten?
- Werden die Anforderungen an die Authentizität der zu archivierenden Dokumente eingehalten?
- Werden die Anforderungen an die Integrität der zu archivierenden Dokumente eingehalten?

- Werden die Anforderungen an die Verfügbarkeit der zu archivierenden Dokumente eingehalten?
- Werden die rechtlichen Vorgaben an die Archivierung eingehalten?
- Sind alle Benutzer und Administratoren entsprechend ihrer Rollen und Aufgaben geschult und eingewiesen? Ist dies dokumentiert?

Fragen zur Redundanz der Archivdaten

- Werden Archivdaten ausreichend redundant gespeichert und aufbewahrt, z. B. durch den Einsatz redundanter Archivsysteme oder alternativer Backup-Medien?
- Erfolgt eine regelmäßige Datensicherung der Archivsysteme sowie gegebenenfalls der Archivdaten?
- Sind die Datensicherungen den Vorgaben entsprechend durchgeführt worden?
- Sind die Datensicherungen der Archivdaten vollständig und lesbar?
- Gab es seit der letzten Revision Datenverluste?
  Wenn ja, wie häufig und wie schwer waren diese Vorfälle?
- Traten Fehler bei der Rekonstruktion archivierter Dokumente auf?
  Wenn ja, wie häufig waren diese Vorfälle und waren die Fehler behebbar?

Fragen zur Administration

- Wird der geforderte Refresh-Zyklus der Archivmedien eingehalten?
- Werden nicht mehr benötigte, beschriebene Archivmedien ordnungsgemäß vernichtet und entsorgt?
- Werden Lesegeräte und Speichermedien im geforderten Maße vorgehalten?

Technische Beurteilung des Archivsystems

Die Revision sollte auch eine technische Neubewertung der Archivsystem-Komponenten und der verwendeten Datenformate beinhalten. Hierdurch soll gewährleistet werden, dass technische Weiterentwicklungen frühzeitig erkannt werden und technische Änderungen am Archivsystem selbst durch den Hersteller im Vorfeld bekannt sind.

Bei dieser Prüfung kann sich herausstellen, dass technische Komponenten des Archivsystems geändert werden müssen. Dann muss sichergestellt werden, dass ausgetauschte Komponenten, z. B. Laufwerke, Speichermedien, Betriebssoftware, einwandfrei mit allen anderen Komponenten unter Beibehaltung der für den Betrieb notwendigen Funktionalität zusammenarbeiten.

Die Prüfergebnisse der Revisionen sind ebenfalls gemäß den Anforderungen an den Archivierungsprozess selbst zu archivieren.

Ergänzende Kontrollfragen:

- Findet eine regelmäßige Revision des Archivierungsprozesses statt?
- Ist die Vorgehensweise für Revisionen dokumentiert?
- Werden die Ergebnisse der Revision ebenfalls archiviert?

M 2.261 Regelmäßige Marktbeobachtung von Archivsystemen

Verantwortlich für Initiierung: Leiter IT, Archivverwalter

Verantwortlich für Umsetzung: Leiter IT, Archivverwalter

Die geforderten Aufbewahrungszeiten für Archivdaten liegen normalerweise um ein Vielfaches höher als die durchschnittliche Lebenserwartung einzelner Bestandteile eines elektronischen Archivs. Dies betrifft sowohl Hardware- als auch Software-Komponenten.

Um den vollen Funktionsumfang über den gesamten Zeitraum der Archivierung dennoch sicher zu stellen, ist davon auszugehen, dass einzelne Hardware-Komponenten, ganze Baugruppen oder auch Software-Komponenten unter Umständen mehrfach ausgetauscht werden müssen.

Eine wichtige Voraussetzung dazu ist eine regelmäßige Marktbeobachtung. Diese dient dazu, sich abzeichnende Veränderungen rechtzeitig zu registrieren. Solche Veränderungen können z. B. sein:

- Änderung eines alten Standards oder Verabschiedung eines neuen Standards bei Speicherformaten,
- Veränderungen beim Hersteller des genutzten Archivsystems oder seiner Speicherkomponenten (Wechsel auf neue Systemplattformen, Beendigung einer Produktreihe und Einstellung des Supports, Einstellung der Produktion von Speichermedien, Insolvenz eines Herstellers),
- Bekanntwerden von Sicherheitslücken oder Schwachstellen, z. B. bei eingesetzten Verschlüsselungsalgorithmen.

Kontakt zu Herstellern aufbauen

Es wird empfohlen, einen regelmäßigen Kontakt zu allen beteiligten Herstellern aufzubauen, beispielsweise durch die Teilnahme an Informationsforen, z. B. Newsgroups und Mailinglisten, in denen aktuelle Informationen über das eingesetzte Archivsystem regelmäßig versandt werden.

Informationen sammeln und auswerten

Es sollte mindestens eine Person dafür verantwortlich sein, die oben beschriebenen Informationen regelmäßig aufzunehmen, nach ihrer Bedeutung für das verwendete Archivsystem auszuwerten und gegebenenfalls notwendige Aktivitäten zu empfehlen. Hierzu muss festgelegt werden, wie eine eventuell erforderliche Migration des Systems eingeleitet wird. Die hier gewonnenen Informationen fließen in die regelmäßige Revision des Archivierungsprozesses (siehe M 2.260 *Regelmäßige Revision des Archivierungsprozesses*) ein.

Ergänzende Kontrollfragen:

- Ist eine verantwortliche Person für die Informationsbeschaffung benannt?
- Ist die regelmäßige Teilnahme an entsprechenden Informationsforen gesichert?
- Ist festgelegt, wie eine Migration des Archivsystems eingeleitet wird?

M 2.262 Regelung der Nutzung von Archivsystemen

Verantwortlich für Initiierung: Leiter IT, Archivverwalter

Verantwortlich für Umsetzung: Leiter IT, Archivverwalter, Administrator

Durch entsprechende Regelungen ist sicherzustellen, dass das Archivsystem in der im Archivierungskonzept (siehe Maßnahme M 2.243 *Entwicklung des Archivierungskonzepts*) vorgesehenen Weise genutzt wird. Hierzu sollten Richtlinien für die Benutzung und die Administration des Archivsystems erstellt werden. Die Richtlinien sind entsprechend den organisatorischen Gepflogenheiten in der jeweiligen Institution zu verankern und bekanntzugeben. Beim Einsatz externer Personen sind diese auf die Beachtung dieser Richtlinien zu verpflichten.

Richtlinien für die Administration

Die Administrationsrichtlinien sollten mindestens die folgenden Punkte umfassen:

- Festlegung der Verantwortung für Betrieb und Administration des Archivsystems,
- Vereinbarungen über Leistungsparameter (Service Level Agreements) beim Betrieb des Archivsystems, insbesondere wenn die Administration oder der Betrieb durch Externe erfolgen soll,
- Modalitäten der Vergabe von Zutritts- und Zugriffsrechten zu den Komponenten des Archivsystems und den Archivmedien,
- Modalitäten der Vergabe von Zugangsrechten zu den vom Archiv bereitgestellten Diensten,
- Regelungen zum Umgang mit archivierten Daten und Archivmedien,
- Überwachung des Archivsystems und der Umgebungsbedingungen für das Archivsystem und die verwendeten Archivmedien,
- Regelung zur Datensicherung der Software-Komponenten des Archivsystems selbst,
- Protokollierung der Aktivitäten am Archivsystem.

Richtlinien für Benutzer

Die Benutzerrichtlinien sollten mindestens umfassen:

- Erläuterung der Zielsetzung der elektronischen Archivierung und der Archivierungsfristen für Dokumente,
- Festlegung der Verantwortung für Arbeiten mit dem Archivsystem,
- Festlegung, in welchem Umfang die Nutzung des Archivsystems verpflichtend ist,
- Modalitäten der Vergabe von Zugangsrechten zu den vom Archiv bereitgestellten Diensten,
- Schulungsanforderungen an Benutzer, damit sie zur Nutzung des Archivsystems freigeschaltet werden dürfen,
- Regelung der Vergabe von Kontextinformationen zu den archivierten Dokumenten, siehe auch M 2.258 *Konsistente Indizierung von Dokumenten bei der Archivierung,*

- Verpflichtung zum sorgfältigen Umgang mit recherchierten Dokumenten unter Beachtung der eventuellen Zweckbindung der Informationen,
- Regelung zum Umgang mit Dokumenten nach Ablauf der festgelegten Archivierungsdauer,
- Regelung, dass Daten, deren Löschung nach einem festgelegten Zeitraum vorgesehen ist, nicht mehr verwendet werden dürfen, obwohl sie unter Umständen aus technischen Gründen noch vorhanden sind,
- Regelung zum Umgang mit personenbezogenen Daten,
- Nutzung der vom Archivsystem bereitgestellten Schutzmechanismen, um eine spätere Prüfung der Integrität und Authentizität der archivierten Dokumente zu ermöglichen, sowie zur Gewährleistung der erforderlichen Vertraulichkeit,
- Verpflichtung zur Überprüfung der Integrität und Authentizität recherchierter Dokumente vor der Weiterverwendung,
- Umgang mit Daten, deren Integrität sich nicht nachweisen lässt, z. B. bei fehlgeschlagener Signaturprüfung,
- Protokollierung der Benutzeraktivitäten am Archivsystem,
- Abrechnungsmodalitäten bei Nutzung des Archivsystems durch mehrere Organisationseinheiten.

Die Regelungen sowie deren Kenntnisnahme durch die Administratoren und Benutzer des Archivsystems sind zu dokumentieren.

Ergänzende Kontrollfragen:

- Sind Regelungen zur Nutzung des Archivsystems dokumentiert und in der Behörde bzw. im Unternehmen verpflichtend umgesetzt?

M 2.263 Regelmäßige Aufbereitung von archivierten Datenbeständen

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Archivverwalter

Für eine ordnungsgemäße Archivierung muss über den gesamten Archivierungszeitraum hinweg sichergestellt werden, dass

- das benutzte Datenformat dem Stand der Technik entspricht und von den verwendeten Anwendungen derzeit und zukünftig verarbeitet werden kann,
- die gespeicherten Daten auch zukünftig lesbar sind und unter Beibehaltung der Semantik und der Nachweiskraft reproduziert werden können,
- das benutzte Dateisystem auf dem Speichermedium von allen beteiligten Komponenten verarbeitet werden kann,
- die Speichermedien jederzeit physikalisch einwandfrei gelesen werden können,
- die verwendeten kryptographischen Verfahren zur Verschlüsselung und zur digitalen Signatur dem Stand der Technik entsprechen und
- für alle Komponenten der Speichereinheit (Speichermedien, Laufwerke, Jukeboxen sowie die Steuersoftware) Ersatz- und Wartungsmöglichkeiten bestehen.

Ist abzusehen, dass eine der geforderten Eigenschaften in naher Zukunft nicht mehr gegeben ist, müssen die betroffenen Systeme ausgetauscht werden. Dabei ist zu berücksichtigen, dass unter Umständen eine erhebliche Menge an archivierten Daten auf neue Datenträger kopiert werden muss.

Kompatibilität testen

Für die Aufbereitung verschlüsselter oder signierter Dokumente wird auf die Maßnahmen M 2.264 *Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung* und M 2.265 *Geeigneter Einsatz digitaler Signaturen bei der Archivierung* verwiesen.

Ergänzende Kontrollfragen:

- Gibt es Dokumentationen über die Haltbarkeit der Datenträger und daraus resultierende Arbeitsanweisen, wann Daten auf neue Datenträger umkopiert werden müssen?

M 2.264 Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement, Administrator

Kryptographische Verfahren unterliegen einem technologischen Alterungsprozess, da im Laufe der Zeit durch mathematische oder technische Weiterentwicklungen Schwächen aufgezeigt werden können, die bei deren Auswahl noch nicht bekannt oder relevant waren.

Bei Aufbewahrungsfristen von 10 Jahren und länger ist davon auszugehen, dass verschlüsselte oder signierte Daten wiederholt mit neuen Schlüsseln und gegebenenfalls auf Basis neuer Algorithmen umgeschlüsselt werden müssen, um die Vertraulichkeit bzw. Integrität der Daten weiterhin zu schützen.

kryptographische Entwicklung beobachten

Um beurteilen zu können, ob ein Algorithmus weiterhin zuverlässig und ausreichend sicher ist, sollten die Entwicklungen auf dem Gebiet der Kryptographie kontinuierlich beobachtet werden. Darüber hinaus sind einschlägige Informationsquellen laufend dahingehend auszuwerten, ob Möglichkeiten bekannt werden, bestehende Verfahren zu kompromittieren.

rechtzeitig neu verschlüsseln bzw. signieren

Wenn die verwendeten Kryptoverfahren nicht mehr zeitgemäß sind und daher die Vertraulichkeit oder Integrität der verschlüsselten Daten nicht mehr sichergestellt werden kann, müssen die Daten neu verschlüsselt bzw. signiert werden.

Folgende Aspekte sind bei der Neuverschlüsselung zu beachten (siehe auch Baustein B 1.7 *Kryptokonzept*):

- Es muss ein nach aktuellen Maßstäben sicherer Kryptoalgorithmus verwendet werden, von dem angenommen werden kann, dass er für einen langen Zeitraum sicher ist.
- Es muss ein Verfahren zur Verschlüsselung und Schlüsselverteilung gewählt werden, das den Anforderungen der Archivierungsanwendung gerecht wird.
- Die neu erzeugten Schlüssel müssen auf sicherem Weg an die Benutzer des Kryptoverfahrens verteilt werden.
- Eine Authentisierung der Kryptoschlüssel (z. B. durch ein elektronisches Zertifikat) ist vorzusehen.
- Die Ursprungsdatei muss nach erfolgreicher Verschlüsselung vernichtet werden, bei WORM-Medien der gesamte Datenträger.
- Wenn Datenträger im Rahmen der Neuverschlüsselung ausgesondert werden, sind auch diese sicher zu entsorgen.
- Neben den Haupt-Datenträgern sind auch Backup-Datenträger sicher zu entsorgen bzw. alte Dateien sicher zu löschen.

Die Verteilung der Schlüssel kann auf zwei unterschiedlichen Wegen erfolgen: Falls die Schlüsselerzeugung durch eine unabhängige, vertrauenswürdige Instanz erfolgen soll, ist sicherzustellen, dass die neuen Schlüssel ver-

traulich und unverfälscht an den ursprünglichen Eigentümer des Dokuments übertragen werden.

Bei der Nutzung asymmetrischer Verfahren zur Verschlüsselung kann der Dokumenteneigentümer alternativ auf Verlangen selbst ein neues Schlüsselpaar erzeugen und den öffentlichen Schlüssel der archivierenden Instanz mitteilen.

zeitlicher Vorlauf und Aufwand

In jedem Fall ist zu berücksichtigen, dass eine derartige Neuverschlüsselung einen gewissen Vorlauf braucht: Die Eigentümer der Daten bzw. der Schlüssel müssen benachrichtigt, die notwendigen Schlüssel generiert und verteilt werden. Bei einer großen Anzahl verschiedener Eigentümer und großen Datenmengen ist ein entsprechender Aufwand einzukalkulieren.

Bei der Auswahl eines möglichst langfristig zuverlässigen neuen Kryptoverfahrens sollte ein aktueller und anerkannter sicherer Algorithmus ausgewählt werden. Ist zum derzeit verwendeten Algorithmus keine wirklich gute Alternative verfügbar, sollte geprüft werden, ob eine Erhöhung der Schlüssellänge als Übergangslösung infrage kommt.

Backup-Medien nicht vergessen!

Nach der Neuverschlüsselung und erneuter Archivierung sind die alten Datenbestände zuverlässig zu vernichten. Falls die Ursprungsdaten auf WORM-Medien archiviert wurden, sind die Datenträger, auf denen die Daten in der bisherigen Verschlüsselung gespeichert wurden, sicher zu entsorgen. Auf wiederbeschreibbaren Medien müssen die Daten zuverlässig gelöscht werden (vergleiche dazu M 2.167 *Sicheres Löschen von Datenträgern*). Es ist zu beachten, dass auch die auf Backup-Medien vorgehaltenen Daten neuverschlüsselt und alte Backup-Medien selektiv gelöscht oder vernichtet werden müssen (siehe hierzu M 6.84 *Regelmäßige Datensicherung der System- und Archivdaten*).

Ergänzende Kontrollfragen:

- Werden die Entwicklungen auf dem Gebiet der Kryptographie beobachtet?
- Sind die Zuständigkeiten für die Neuverschlüsselung klar definiert?
- Werden alte Datenträger sicher vernichtet?
- Werden in die Neuverschlüsselung auch die Backup-Daten einbezogen?

M 2.265 Geeigneter Einsatz digitaler Signaturen bei der Archivierung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement, Archivverwalter, Administrator

Digitale Signaturen sind für die elektronische Archivierung eine Herausforderung, da sie technisch bedingt eine begrenzte Lebensdauer haben, die vorher nicht immer bekannt ist. Andererseits sind sie aber auch erforderlich, wenn elektronische Dokumente wirklich beweissicher archiviert werden müssen. Die Aussagekraft digitaler Signaturen hängt sehr stark von deren Interpretation zum Zeitpunkt der Prüfung und damit vom so genannten Gültigkeitsmodell ab. Es bestehen derzeit auch noch keine langfristigen praktischen Erfahrungen mit der Archivierung digital signierter Dokumente, da digitale Signaturen erst seit wenigen Jahren praktisch eingesetzt werden.

Gültigkeit und Beweiskraft

Diese beiden Eigenschaften einer digitalen Signatur werden üblicherweise wie folgt definiert: Eine digitale Signatur ist genau dann **gültig**,

- wenn sie mathematisch richtig ist und
- wenn zum *Zeitpunkt der Signaturausübung* der zugehörige Signaturschlüssel gültig war.

Eine digitale Signatur ist genau dann **beweiskräftig**,

- wenn sie zum *Zeitpunkt der Prüfung* entsprechend dem verwendeten Gültigkeitsmodell als gültig anerkannt wird und
- wenn der zugehörige Signaturschlüssel nicht kompromittiert ist.

Aussagekraft digitaler Signaturen

Digitale Signaturen können zu unterschiedlichen Zwecken eingesetzt werden, unter anderem

- zum Nachweis der Integrität von Dateien,
- zur Beglaubigung der Authentizität von kryptographischen Schlüsseln oder elektronischen Dokumenten sowie
- zur Authentisierung.

Der Einsatz und die Aussagekraft digitaler Signaturen sind anwendungsspezifisch im Rahmen einer Sicherheitsrichtlinie (Policy) vorzugeben. In dieser Policy sollte unter anderem festgelegt werden,

- unter welchen Voraussetzungen digitale Signaturen erzeugt werden,
- von welcher Stelle digitale Signaturen erzeugt werden (bei Zertifikats-Signaturen z. B. in einem neutralen Trust Center),
- welches Gültigkeitsmodell für die Anwendung herangezogen wird,
- ob und wie digitale Signaturen gegebenenfalls widerrufen werden können sowie

- welche Aussage damit verbunden sein soll, d. h. was damit beglaubigt wird (bei einem Zeitstempel beispielsweise das Vorliegen eines Dokuments zu einem bestimmten Zeitpunkt).

Die Policy muss schriftlich dokumentiert und archiviert werden, damit bei einer späteren Prüfung der digitalen Signatur klar ist, was die Signatur aussagt (d. h. beweisen soll) und was nicht. Außerdem sollte sie auch in geeigneter Form veröffentlicht werden, damit alle, die auf die Signaturen vertrauen müssen bzw. wollen, sich darauf beziehen können.

Lebensdauer digitaler Signaturen

Die Lebensdauer digitaler Signaturen wird durch die technische Entwicklung von Hard- und Software sowie Fortschritte der Kryptographie beschränkt (siehe G 2.79 *Unzulängliche Erneuerung von digitalen Signaturen bei der Archivierung* und G 4.47 *Veralten von Kryptoverfahren*). Es muss davon ausgegangen werden, dass digitale Signaturen nach einem Zeitablauf von ca. 5 Jahren als veraltet gelten, da ihre Aussagekraft nachlässt. Schlüsselzertifikate und Zeitstempel sollten von einem Trust Center daher in der Regel für maximal 5 Jahre ausgestellt werden. Sie können aber auch kurzfristig für ungültig erklärt werden, wenn dies notwendig sein sollte. Dies wird als Sperrung bezeichnet.

Sperrung von Schlüsselzertifikaten

Wenn Schlüsselzertifikate durch die Zertifizierungsinstanz gesperrt werden, weil z. B. die Signaturschlüssel kompromittiert sind, muss schnell gehandelt werden. Alle ab diesem Zeitpunkt mit dem betreffenden Schlüssel erfolgten Signaturen haben ihre faktische Aussagekraft (z. B. Beweiskraft) verloren. Die Gültigkeit der Signaturen hängt jedoch auch vom Gültigkeitsmodell ab. Im Gegensatz zum Schalenmodell sind beim Kettenmodell im Grunde zunächst keine weiteren Aktionen bei der Kompromittierung von Schlüsseln erforderlich.

Dies kann unmittelbare Folgen für die Aussagekraft archivierter Dokumente haben. Wenn die betroffenen archivierten Dokumente nur mit dem nun ungültigen Schlüssel signiert sind, so ist diese Signatur je nach verwendetem Gültigkeitsmodell nicht mehr beweiskräftig.

Empfehlung

Für die Archivierung digital signierter Dokumente gibt es derzeit keine erprobten Standards, durch deren Anwendung eine langfristige Gültigkeit und Beweiskraft der Signaturen sichergestellt werden kann. Bis sich entsprechende Standards etablieren, sollten daher unter Berücksichtigung der bei der Langfristarchivierung auftretenden Gefährdungen folgende Empfehlungen beachtet werden:

- Die Aussagekraft der Signaturen und Zertifikate ist in einer Policy zu dokumentieren. Die Policy muss ebenfalls archiviert werden.
- Es sollte ein unabhängiges Trust Center zur Generierung von Schlüsselzertifikaten und Zeitstempeln eingebunden werden.
- Alle zu einem Dokument gehörenden Signaturen, Zeitstempel, Zertifikate und die für die Signatur- bzw. Zertifikatsprüfung benötigten Schlüssel

müssen ebenfalls archiviert werden. Dies kann entweder lokal oder zentral durch das Trust Center erfolgen.

- Je nach Anforderungen an die Aussagekraft der Signaturen müssen u. U. weitere Kontextinformationen archiviert werden. Bei qualifizierten Signaturen gemäß Signaturgesetz gehören hierzu z. B. Verzeichnisdienstauskünfte des Zertifizierungsdiensteanbieters.
- Nach spätestens 5 Jahren, mindestens vor Ablauf der regulären Gültigkeit der Schlüsselzertifikate sollten die digitalen Signaturen und Zertifikate erneuert werden. Solange der Verzeichnisdienst integer verfügbar bleibt, ist dies eigentlich nur dann erforderlich, wenn die Eignung der Algorithmen nicht mehr gegeben ist. Da bei der Archivierung die Daten für einen längeren Zeitraum unbearbeitet vorgehalten werden, ist es sinnvoll, diese trotzdem vorsichtshalber alle 5 Jahre erneut zu signieren.
- Die Überprüfung einer digitalen Signatur schlägt fehl, sobald auch nur ein Bit im Dokument oder dessen Signatur geändert wird. Eine bitgenaue Archivierung ist deshalb unbedingt erforderlich, um die Gültigkeit der Signatur zu erhalten. Aus diesem Grund sollten entsprechende Fehlerkorrekturmaßnahmen bei der Speicherung der signierten Dokumente getroffen werden.
- Die Verantwortlichen für die elektronische Archivierung sollten sich regelmäßig über die Entwicklungen auf dem Gebiet der digitalen Signaturen informieren.

Archivierungsmodelle

Im Folgenden werden verschiedene Modelle für die Archivierung digital signierter Dokumente beschrieben. Dabei bleibt zunächst die Archivierung von Schlüsselverwaltungsinformationen, wie Zertifikaten oder Sperrlisten, unberücksichtigt.

Solange es bei den beschriebenen Modellen unwesentlich ist, ob das Originaldokument nur eine oder mehrere Signaturen enthält, wird von einer Originalsignatur gesprochen. Mehrere Originalsignaturen werden nur dann erwähnt, wenn die Funktionsweise der Archivierung sich dadurch ändert.

Die Beschreibungen der Modelle sind nach folgenden Punkten strukturiert:

- Notwendige Infrastruktur
- Ablauf der Archivierung eines signierten Dokuments
- Ablauf der Abfrage eines Dokuments aus dem Archiv
- Semantik der durch die Archivierung erfolgten zusätzlichen Signaturen, d. h. was wird durch diese Signaturen bestätigt?
- Vorgehensweise bei der Prüfung der Beweiskraft der Originalsignatur
- Notwendiges Vertrauen in die Instanzen, die an der Archivierung beteiligt sind

An die Beschreibung schließt sich eine kurze Diskussion der unterschiedlichen Modelle an.

Modell 1: Archivierungsstelle mit Eingangsstempelung

- Infrastruktur

  Vertrauenswürdige Archivierungsstelle, die auch Zertifizierungsdienste anbietet (Trust Center)

- Ablauf der Archivierung

  Das Dokument wird zusammen mit der Angabe des Zeitpunktes seines Eingangs bei der Archivierungsstelle archiviert.

- Ablauf der Abfrage

  Das Dokument zusammen mit der Zeitangabe seines Eingangs in die Archivierungsstelle wird durch die Archivierungsstelle zum Zeitpunkt der Abfrage digital signiert. Durch die Signatur der Archivierungsstelle wird die Authentizität des Dokuments nachgewiesen und dessen Integrität geschützt.

- Semantik der Signatur der Archivierungsstelle

  Durch die Signatur bei der Dokumentenabfrage bestätigt die Archivierungsstelle, dass das betreffende Dokument bei ihr zum angegebenen Zeitpunkt eingegangen und archiviert worden ist.

- Prüfung der Beweiskraft der Originalsignatur

  Um die Authentizität und Integrität des Dokuments zu verifizieren, wird zunächst die Signatur der Archivierungsstelle geprüft. Die Originalsignatur gilt genau dann als beweiskräftig, wenn sie zum angegebenen Zeitpunkt des Dokumenteneingangs bei der Archivierungsstelle beweiskräftig war. Diese Prüfung bleibt dem Benutzer überlassen. Die hierzu erforderlichen Zertifikate können ihm entweder von derselben Archivierungsstelle zusammen mit dem Dokument bereitgestellt werden oder müssen von ihm bei einer anderen geeigneten Stelle angefordert werden.

- Vertrauensmodell

  Der Archivierungsstelle wird Vertrauen für die integere Speicherung der signierten Dokumente und für die Korrektheit des Zeitpunkts des Dokumenteneingangs entgegengebracht.

  Gelingt es einem Angreifer, den Zeitpunkt des Dokumenteneingangs zu manipulieren, so kann er die Beweiskraft der Dokumente ändern. Durch Angabe eines späteren Zeitpunkts lässt sich die Beweiskraft eines Dokuments ausschalten. Andererseits kann bei einem archivierten Dokument mit gültiger, aber nicht beweiskräftiger Signatur die Beweiskraft durch Angabe eines früheren Eingangszeitpunkts vorgetäuscht werden.

  Die Korrektheit des gespeicherten Zeitpunkts des Dokumenteneingangs ist durch geeignete Schutzmaßnahmen sicherzustellen. Hierzu können digitale Signaturen verwendet werden, wie bei den Modellen 3 und 4.

Modell 2: Archivierungsstelle mit Bestätigungsstempelung

- Infrastruktur

  Vertrauenswürdige Archivierungsstelle, die auch Zertifizierungsdienste anbietet (Trust Center)

- Ablauf der Archivierung

  Beim Eingang des Dokuments bei der Archivierungsstelle wird die Beweiskraft der Originalsignatur des Dokuments geprüft. Das Dokument wird nur dann archiviert, falls die Beweiskraft zum aktuellen Zeitpunkt verifiziert werden kann. Bei mehreren Originalsignaturen wird deren Beweiskraft einzeln festgestellt. Das Dokument wird zusammen mit den Angaben über die Beweiskraft der einzelnen Signaturen archiviert, falls mindestens eine der Originalsignaturen beweiskräftig ist.

- Ablauf der Abfrage

  Zum Zeitpunkt der Abfrage wird das Dokument durch die Archivierungsstelle digital signiert, gegebenenfalls zusammen mit den Angaben über die Beweiskraft der Originalsignaturen. Durch die Signatur der Archivierungsstelle wird die Authentizität des Dokuments nachgewiesen und dessen Integrität geschützt.

- Semantik der Signatur der Archivierungsstelle

  Durch die Signatur der Archivierungsstelle wird die Beweiskraft der Originalsignatur bestätigt. Bei mehreren Originalsignaturen werden die mitgelieferten Angaben über deren Beweiskraft einzeln bestätigt.

- Prüfung der Beweiskraft der Originalsignatur

  Um die Authentizität und Integrität der Archivantwort zu verifizieren, wird die Signatur der Archivierungsstelle geprüft. Die Beweiskraft der Originalsignatur ergibt sich aus den mitgelieferten Angaben bzw. aus der Archivierung an sich.

- Vertrauensmodell

  Der Archivierungsstelle wird Vertrauen für die integere Speicherung der signierten Dokumente und für die Prüfung der Beweiskraft der Dokumente vor der Archivierung entgegengebracht.

  Wenn es einem Angreifer unbemerkt gelingt, einen ehemals gültigen Signaturschlüssel zu brechen und Dokumente mit gefälschten Signaturen ins Archiv einzubringen, gelten diese als beweiskräftig. Durch geeignete Maßnahmen ist daher sicherzustellen, dass die Beweiskraft signierter Dokumente vor der Aufnahme ins Archiv geprüft und der Datenbestand vor unberechtigtem Hinzufügen von Daten geschützt wird.

Modell 3: Trust Center mit Zeitstempeldienst

- Infrastruktur

  Rollentrennung zwischen einer Archivierungsstelle und einem vertrauenswürdigen Zeitstempeldienst (Trust Center), die miteinander kommunizieren.

- Ablauf der Archivierung

  Beim Eingang des Dokuments bei der Archivierungsstelle wird die Beweiskraft der Originalsignatur durch einen Zeitstempel des Trust Centers für die Dauer der Beweiskraft dieses Stempels bestätigt.

  Regelmäßig vor dem Ablauf der Beweiskraft des letzten Zeitstempels wird das Gesamtdokument, d. h. das Dokument inklusive aller Signaturen, mit einem neuen Zeitstempel des Trust Centers versehen.

- Struktur eines archivierten Dokuments

  Ein archiviertes Dokument enthält mindestens das signierte Originaldokument und einen Zeitstempel über dieses Dokument. Im Laufe der Zeit verlängert es sich durch zusätzliche Zeitstempel, die jeweils über das signierte Originaldokument inklusive aller bisherigen Zeitstempel ausgeführt werden.

- Ablauf der Abfrage

  Das Dokument inklusive aller Zeitstempel wird im aktuellen Zustand ausgeliefert.

- Semantik eines Zeitstempels

  Bei einer Zeitstempelung wird durch eine speziell für diesen Zweck vorgesehene Signatur des Trust Centers bestätigt, dass das Dokument zu dem im Zeitstempel angegebenen Zeitpunkt vorlag.

- Prüfung der Beweiskraft der Originalsignatur

  Die Beweiskraft des letzten Zeitstempels wird direkt verifiziert. Jeder andere Zeitstempel wird geprüft, indem seine Beweiskraft zum Zeitpunkt des jeweils nachfolgenden Zeitstempels verifiziert wird (rekursive Verifikation). Die Prüfung der Beweiskraft der Originalsignatur erfolgt zu dem Zeitpunkt, der im ersten Zeitstempel angegeben ist.

- Vertrauensmodell

  Der Archivierungsstelle wird Vertrauen für die integere Speicherung der Dokumente entgegengebracht. Beim Trust Center wird dem Zeitstempeldienst vertraut.

  Anhand der Kette von Zeitstempeln ist die Beweiskraft der Originalsignatur lückenlos nachweisbar.

Modell 4: Trust Center mit Archivstempeldienst

- Infrastruktur

  Rollentrennung zwischen einer Archivierungsstelle und einem vertrauenswürdigen Archivstempeldienst (Trust Center), die miteinander kommunizieren.

- Funktionsweise einer Archivstempelung

  Wird ein Dokument zum ersten Mal einer Archivstempelung unterzogen, entspricht dieser Vorgang der Zeitstempelung: Das Dokument wird mit einem Zeitstempel versehen.

Falls ein Dokument bereits genau einmal den Archivstempeldienst durchlief und somit schon einen Zeitstempel enthält, wird bei der erneuten Archivstempelung zunächst dieser Zeitstempel geprüft. Nur falls der Zeitstempel beweiskräftig ist, wird das Dokument inklusive Zeitstempel mit einer speziellen Archivsignatur signiert.

Enthält ein Dokument bereits eine Archivsignatur, wird bei einer erneuten Archivstempelung zunächst die Archivsignatur geprüft. Nur falls die bisherige Archivsignatur beweiskräftig ist, wird sie durch eine aktuelle Archivsignatur ersetzt.

- Ablauf der Archivierung

  Beim Eingang des Dokuments bei der Archivierungsstelle wird die Beweiskraft der Originalsignatur durch die Archivstempelung des Trust Centers für die Dauer der Beweiskraft des hinzugefügten Zeitstempels bestätigt.

  Regelmäßig vor dem Ablauf der Beweiskraft des Zeitstempels oder der letzten Archivsignatur muss eine Archivstempelung durch das Trust Center erfolgen.

- Struktur eines archivierten Dokuments

  Ein archiviertes Dokument besteht mindestens aus dem signierten Originaldokument und einem Zeitstempel darüber. Nach Ablauf der Beweiskraft des Zeitstempels enthält es zusätzlich genau eine Archivsignatur. Diese Signatur ist über das signierte Originaldokument und den Zeitstempel gebildet.

- Ablauf der Abfrage

  Das Dokument inklusive aller Signaturen wird im aktuellen Zustand ausgeliefert.

- Semantik der Archivsignatur

  Die Archivsignatur bestätigt die Beweiskraft des Zeitstempels. Der Zeitstempel wiederum bestätigt das Vorliegen des Originaldokuments zum angegebenen Zeitpunkt.

- Prüfung der Beweiskraft der Originalsignatur

  Zunächst wird die Beweiskraft der Archivsignatur und anschließend die Beweiskraft der Originalsignatur zum im Zeitstempel angegebenen Zeitpunkt verifiziert.

- Vertrauensmodell

  Der Archivierungsstelle wird Vertrauen für die integere Speicherung der Dokumente entgegengebracht. Beim Trust Center ist ein vertrauenswürdiger Archivstempeldienst notwendig.

- Der Archivstempeldienst muss die Beweiskraft einer vorhergehenden Signatur prüfen. Gelingt es einem Angreifer, diese Prüfung zu unterdrücken und gefälschte, signierte Dokumente mit einer Archivsignatur zu versehen, gelten diese als beweiskräftig. Durch geeignete Maßnahmen muss daher sichergestellt werden, dass die Beweiskraft der bisherigen

Signatur vor der Erneuerung oder dem Hinzufügen einer Archivsignatur geprüft wird.

Diskussion der Modelle

Je geringer das Vertrauen der Benutzer in die Archivierungsstelle ist, desto höher ist der Aufwand für die beweiskräftige Archivierung digital signierter Dokumente.

Bei vollem Vertrauen in die Archivierungsstelle ist Modell 2 anwendbar. Es ist für einen Benutzer das "bequemste" Modell, da dieser bei der Abfrage des archivierten Dokuments über die Beweiskraft der Originalsignatur informiert wird. Der Benutzer vertraut darauf, dass die Angaben der Archivierungsstelle stimmen. Über diese hinaus hat er keine Kontrollmöglichkeit. Will er einen Dritten von der Beweiskraft der Originalsignatur überzeugen, kann er lediglich auf die Antwort der Archivierungsstelle verweisen und auf deren durch Archivierungsrichtlinien belegte Vertrauenswürdigkeit.

In Modell 1 muss der Benutzer selbst die Beweiskraft der Originalsignatur des abgefragten Dokuments prüfen. Die Archivierungsstelle liefert ihm lediglich den Zeitpunkt, an dem das Dokument bei ihr einging. Ein Dritter kann ebenso wie der Benutzer die Prüfung der Beweiskraft durchführen, muss allerdings der Zeitangabe der Archivierungsstelle vertrauen.

Beide Modelle haben den Vorteil, dass der organisatorische Aufwand der Archivierungsstelle minimal ist: Nach der Archivierung ist keine weitere Behandlung des Dokuments erforderlich. Die Archivierung selbst dient als Versiegelung der Originalsignatur für die gesamte Archivierungsdauer. Entsprechend kritisch ist die Integrität des Datenbestandes des Archivs. Unberechtigtes Hinzufügen von Daten kann dazu führen, dass gefälschte Signaturen als beweiskräftig anerkannt werden.

In den Modellen 3 und 4 sind archivierte Daten selbst wiederum durch digitale Signaturen integritätsgeschützt. Dadurch wird verhindert, dass gefälschte signierte Dokumente als beweiskräftig anerkannt werden, wenn sie unberechtigt in das Archiv eingebracht werden.

Eine weitere vertrauensfördernde Maßnahme in den Modellen 3 und 4 ist die Möglichkeit, die Zuständigkeiten für die Dokumentenspeicherung einerseits und die Signaturversiegelung andererseits auf unterschiedliche Stellen zu verteilen: Archivierungsstelle und Trust Center.

Das notwendige Vertrauen in die Archivierungsstelle beschränkt sich dabei, wie es üblicherweise bei der Archivierung der Fall ist, auf die Speicherung von Dokumenten. Darüber hinaus erfordert die erfolgreiche Archivierung digital signierter Dokumente die regelmäßige Kommunikation mit dem Trust Center. Zunächst muss jedes eingehende Dokument durch das Trust Center zeitgestempelt werden, da der Zeitpunkt des Dokumenteneingangs bei der Archivierungsstelle für die nachträgliche Prüfung der Beweiskraft entscheidend ist.

In Modell 4 bestätigt das Trust Center regelmäßig die ordnungsgemäße Archivierung bis zum aktuellen Zeitpunkt, indem es die Beweiskraft der bisherigen Archivsignatur des Dokuments verifiziert und diese Signatur durch eine neue Archivsignatur ersetzt. Der zeitliche Abstand zwischen dem Ende

der Beweiskraft des Zeitstempels und dem Zeitpunkt der letzten Archivstempelung vergrößert sich dadurch laufend. Die Archivsignatur bestätigt daher die Beweiskraft des Zeitstempels nur, solange die Archivstempelung im Trust Center ordnungsgemäß verläuft. Insbesondere betrifft dies die Überprüfung der Beweiskraft der bisherigen Archivsignatur. Ohne diese Prüfung kann die Archivierungsstelle gefälschte signierte Dokumente zur Archivstempelung vorlegen, die dann Beweiskraft erhalten. Der Benutzer muss also der ordnungsgemäßen Ausführung der Archivstempelung durch das Trust Center vertrauen.

Bei Modell 3 kann der Benutzer den zeitlich lückenlosen Ablauf der regelmäßigen Signaturversiegelung kontrollieren. Als Dienstleistung des Trust Centers ist lediglich eine Zeitstempelung erforderlich. Diese Zeitstempelung ist nicht spezifisch für die Archivierung und umfasst keine Überprüfungen. Ein vorliegendes Dokument wird ohne vorhergehende Betrachtung, sozusagen "blind" mit der aktuellen Zeit versehen und signiert. Eine vertrauenswürdige Realisierung einer Zeitstempelung ist daher im Allgemeinen einfacher als eine vergleichbar vertrauenswürdige Realisierung einer Archivstempelung.

Die Modelle 3 und 4 bieten zwar im Vergleich zu den Modellen 1 und 2 eine höhere Vertrauenswürdigkeit, hierbei ist es jedoch für die Benutzer komplizierter, die Beweiskraft der Originalsignatur zu überprüfen. Zusätzlich zur Beweiskraft der Originalsignatur zum Zeitpunkt des ersten Zeitstempels ist in Modell 3 eine ganze Kette von Zeitstempeln auf Beweiskraft zu prüfen, in Modell 4 hingegen nur die Beweiskraft der Archivsignatur.

Für die Langzeitarchivierung digitaler Signaturen gibt es noch keine erprobten Standards. Hier müssen sich noch einheitliche Konzepte und Standards durchsetzen, daher sollten sich die Verantwortlichen für die elektronische Archivierung regelmäßig über die Entwicklungen auf diesem Bereich informieren. Die zuvor beschriebenen Modelle sind somit als Beispiele zu verstehen, zur Archivierung digital signierter Dokumente sind durchaus auch andere Verfahren denkbar.

Ergänzende Kontrollfragen:

- Gibt es ein Konzept sowie eine Sicherheitsrichtlinie für den Einsatz digitaler Signaturen bei der Archivierung?
- Sind das vorliegende Konzept sowie die Sicherheitsrichtlinie aktuell?
- Sind die Mitarbeiter über den sie betreffenden Teil des Konzepts nachweislich unterrichtet worden?
- Wird die Aktualität des Konzepts regelmäßig überprüft?

M 2.266 Regelmäßige Erneuerung technischer Archivsystem-Komponenten

Verantwortlich für Initiierung: Leiter IT, Archivverwalter

Verantwortlich für Umsetzung: Leiter IT, Archivverwalter, Administrator

technischer Fortschritt

Archivsysteme müssen über lange Zeiträume auf aktuellem technologischen Stand gehalten werden. In der Informationstechnik haben Standards für Hard- und Software sowie Datenformate zur digitalen Speicherung in der Vergangenheit im Vergleich zu den avisierten Zeiträumen einer Archivierung nur kurzzeitigen Bestand gehabt. Es ist davon auszugehen, dass dies auch künftig so bleibt, da die Standards in hohem Maße vom technischen Fortschritt geprägt werden.

Verschleißerscheinungen

Hardware-Komponenten unterliegen zudem Verschleißerscheinungen und müssen daher regelmäßig gewartet sowie gegebenenfalls ausgetauscht werden. Zusätzlich ist damit zu rechnen, dass Hersteller unvorhergesehen die Unterstützung bestehender Systeme einstellen oder, z. B. aufgrund von Insolvenz, nicht mehr in der Lage sind, langfristige Unterstützung zu gewährleisten.

Es ist daher damit zu rechnen, dass die Komponenten des Archivs regelmäßig erneuert werden müssen und unter Umständen eine Migration des kompletten Datenbestands auf ein neues Archivsystem notwendig ist.

Dieser Prozess ist eng mit der Maßnahme M 2.261 *Regelmäßige Marktbeobachtung von Archivsystemen* verknüpft.

Kompatibilität testen

Neue Hard- und Software ist vor der Installation in ein laufendes Archivsystem grundsätzlich ausführlich zu testen, um die Stabilität des bestehenden Systems nicht zu gefährden (siehe auch M 4.65 *Test neuer Hard- und Software*). Bei der Installation neuer Datenträger und Laufwerke muss auf Kompatibilität mit bestehenden Systemen und Datenträgern geachtet werden. Vor der Inbetriebnahme neuer Komponenten oder der Einführung neuer Datenformate ist ein Migrationskonzept zu erstellen, in dem alle Änderungen und Tests beschrieben werden. Das Archivierungskonzept (siehe M 2.243 *Entwicklung des Archivierungskonzepts*) ist unter Umständen anzupassen. Bei größeren Änderungen muss die in der Bausteinbeschreibung beschriebene Planungsphase erneut durchlaufen werden.

Bei der Änderung von Formaten muss geprüft werden, ob bei der Konvertierung von Altdaten in die neuen Formate aufgrund rechtlicher Anforderungen zusätzlich die Daten in ihren ursprünglichen Formaten archiviert werden müssen.

Ergänzende Kontrollfragen:

- Besteht für alle Komponenten (Software, Hardware und Speichermedien) des Archivs Unterstützung durch den Hersteller oder vergleichbare Unterstützung?
- Sind Kompatibilitätstests vor Installation neuer Komponenten verbindlich vorgeschrieben?

M 2.267 Planen des IIS-Einsatzes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT Administrator

Ein IIS bietet vielfältige Einsatzmöglichkeiten im Intranet und Internet. Er kann als einfacher Informations-Server oder auch als Basis für komplexe Web-Anwendungen genutzt werden. Soll ein IIS eingesetzt werden, so ist ein Betriebskonzept zu entwerfen. Bei der Planung eines IIS ist Folgendes aus Sicherheitssicht zu beachten:

- Die umzusetzenden Sicherheitsvorschriften müssen ausgearbeitet werden (siehe M 2.268 *Festlegung einer IIS-Sicherheitsrichtlinie*).

sichere Aufstellung der Server

- Der Standort der IT-Systeme, auf denen der IIS betrieben wird, ist festzulegen. Alle Systeme mit IIS sollten in Serverräumen oder in einem Rechenzentrum aufgestellt werden. Hierbei zu realisierende Maßnahmen sind in Baustein B 2.4 *Serverraum* bzw. B 2.9 *Rechenzentrum* beschrieben. Wenn kein Serverraum zur Verfügung steht, kann ein IIS alternativ in einem Serverschrank aufgestellt werden (vergleiche B 2.7 *Schutzschränke*).

sichere Anbindung an das Internet

- Ein Webserver, auf den aus dem Internet zugegriffen wird, muss in einem separaten Netz (einer so genannten Demilitarisierten Zone, DMZ) angesiedelt sein. Der Zugriff auf den Server muss durch eine Firewall abgesichert werden (siehe auch M 2.77 *Integration von Servern in das Sicherheitsgateway*).
- Bei Installation in der DMZ sollte der IIS ebenso wie andere existierende Systeme in der DMZ überwacht werden (siehe auch M 4.182 *Überwachen des IIS-Systems*).
- Der Webserver ist als Standalone-Server (nicht Mitglied einer Domäne) zu installieren.

Performance und Lastverteilung

- Ggf. ist die Installation von Systemen zur Erhöhung der Verfügbarkeit und Performance (Standby-Systeme, Lastverteilung) zu planen (siehe auch M 4.183 *Sicherstellen der Verfügbarkeit und Performance des IIS*).
- Ggf. ist die Anbindung an Datenbanken für komplexe Web-Anwendungen zu planen.

Rechtekonzept für Server

- Für die Server und die Verzeichnisse sind die Zugangs- und Zugriffsbeschränkungen zu planen. Dabei sollten nur die Berechtigungen vergeben werden, die auch wirklich benötigt werden (siehe auch M 4.185 *Absichern von virtuellen Verzeichnissen und Web-Anwendungen beim IIS-Einsatz*).
- Für die Web-Sites sind Zugriffsberechtigungen und die Authentisierungsmethode zu planen (siehe auch M 4.180 *Konfiguration der Authentisierungsmechanismen für den Zugriff auf den IIS*).

nicht benötigte Komponenten und Dienste deaktivieren

- Für jeden Server ist festzulegen, welche Komponenten und Dienste aktiviert werden. Nicht benötigte Komponenten und Dienste sind zu deaktivieren (siehe auch M 4.184 *Deaktivieren nicht benötigter Dienste beim IIS-Einsatz*). Bei der Planung sollte eine Funktionstrennung von

unterschiedlichen Servertypen berücksichtigt werden, beispielsweise FTP-Server und WWW-Server.

Die Sicherheit des Webservers hängt von vielen Faktoren ab, die wichtigsten sind jedoch

- die sichere Konfiguration des Betriebssystems,
- die sichere Konfiguration des IIS und
- die sichere Einbindung in die Systemumgebung.

Detaillierte Maßnahmen zur Absicherung dieser Hauptkomponenten finden sich in den IIS-spezifischen Maßnahmen der Maßnahmenkataloge 4 *Hardware/Software* und 5 *Kommunikation*.

Ergänzende Kontrollfragen:

- Ist der Server vom Internet aus erreichbar?
- Erfolgt der Zugriff durch anonyme oder authentisierte Benutzer?
- Ist der Server durch einen Proxy, eine Firewall oder ähnliches geschützt?

M 2.268 Festlegung einer IIS-Sicherheitsrichtlinie

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, IT-Sicherheitsmanagement

Für den Einsatz von IIS ist eine geeignete Sicherheitsrichtlinie zu definieren. In der Sicherheitsrichtlinie muss festgelegt werden, was zu unternehmen ist, um ein System effektiv abzusichern.

Zugriffsregeln

In der Sicherheitsrichtlinie müssen folgende Zugriffsregeln festgelegt werden:

- Welcher Benutzer darf auf welchen Server zugreifen und welche Benutzer sollen auf welchen Server nicht zugreifen (Ausschlussliste)?
- Welcher Benutzer darf auf welche Verzeichnisse und Web-Seiten zugreifen bzw. nicht zugreifen (Ausschlussliste)?
- Welche Authentisierung ist zum Zugriff auf Verzeichnisse und Web-Seiten erforderlich?
- Welche Anwendungen und Scripts werden mit welchen Rechten ausgeführt?
- Wie und mit welchen Rechten darf auf angeschlossene Datenbanken zugegriffen werden?
- Von wo aus darf auf den IIS zugegriffen werden?

Im Rahmen der Sicherheitsrichtlinie sind außerdem folgende Aspekte zu berücksichtigen:

- Die Sicherheitsrichtlinie für den IIS muss konform zu den geltenden generellen Sicherheitsrichtlinien sein (siehe M 2.192 *Erstellung einer IT-Sicherheitsleitlinie*).

Verschlüsselung und Signatur

- Außerdem muss festgelegt werden, ob eine Kommunikationsabsicherung, z. B. SSL, eingesetzt werden soll, welcher Mechanismus genutzt wird und welche Kommunikationsverbindungen geschützt werden sollen.

Audit und Protokollierung

- Es muss ein Auditing- und Protokollierungskonzept entworfen werden. Es ist darauf zu achten, dass der Datenschutzbeauftragte in die Planung mit einbezogen wird, da im Rahmen der Überwachung auch personenbezogene Daten anfallen können.

Alle Beteiligte müssen die Vorgaben kennen.

Die Sicherheitsrichtlinie für den IIS muss organisationsweit abgestimmt sein und allen Beteiligten, u. a. den zuständigen Administratoren, bekannt gegeben worden sein. Wenn sich Sicherheitsvorgaben verändern, müssen alle Beteiligten hierüber informiert werden.

Ergänzende Kontrollfragen:

- Existiert eine aktuelle Sicherheitsrichtlinie für den IIS?
- Können alle relevanten Sicherheitsvorschriften der organisationsweiten Sicherheitsrichtlinie auf den IIS abgebildet werden?
- Werden alle Beteiligten über neue oder veränderte Sicherheitsvorschriften informiert?

M 2.269 Planung des Einsatzes eines Apache Webservers

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Detailplanung für den Einsatz eines Apache-Webservers baut auf der allgemeinen Planung für den Aufbau eines Webangebots (siehe M 2.172 *Entwicklung eines Konzeptes für die WWW-Nutzung*) auf. Aus den festgelegten Zielen des Webangebots und weiteren Rahmenbedingungen (beispielsweise Zugriff auf Datenbanken) ergeben sich Anforderungen, die in der konkreten Planung für den Apache-Webserver berücksichtigt werden müssen. Die folgenden Themen, die auch untereinander Abhängigkeiten aufweisen, sollten bei der Planung berücksichtigt werden:

Auswahl der Hardware- und Betriebssystemplattform und der Apache-Version

Hardware auswählen

Die Hardware, auf der der Apache-Webserver eingesetzt wird, kann einen entscheidenden Einfluss auf die Gesamtleistung des entstehenden Systems haben. Dabei spielen bei einem Webserver, der vor allem statische Seiten ausliefert, Anzahl und Takt der eingesetzten Prozessoren praktisch keine Rolle mehr. Wichtiger ist in diesem Fall die Geschwindigkeit der eingesetzten Festplatten und des Speicherzugriffs.

Je mehr dynamische Seiten in einem Webangebot enthalten sind, desto wichtiger werden Prozessorgeschwindigkeit und Hauptspeicherausbau. Bei der Auswahl des Plattensubsystems sollte darauf geachtet werden, dass das System hohe Datenübertragungsraten beim "zufälligen" Lesen verschiedener Dateien bietet. Es sollte überlegt werden, die Partition, auf der die WWW-Daten abgelegt werden sollen, auf einem externen RAID-System zu installieren. Das RAID-System sollte das Austauschen von Festplatten im laufenden Betrieb (*hot-swap*) unterstützen und als RAID 5 organisiert werden. Dies erlaubt es, defekte Platten ohne Betriebsunterbrechung des Servers auszutauschen.

Betriebssystem auswählen

Der Apache-Webserver kann unter sehr vielen Betriebssystemen eingesetzt werden. Bei der Auswahl der Apache Version und des Betriebssystems, unter welchem der Apache-Webserver eingesetzt werden soll, sollten die folgenden Punkte berücksichtigt werden:

- Erst seit der Version 2 wird Windows als Betriebssystem "voll" unterstützt. Zwar existiert auch eine Portierung der Version 1.3 auf Windows, diese wird jedoch nicht als so stabil angesehen, wie die Unix-Versionen.
- Nicht alle Erweiterungsmodule, die es für den Apache-Webserver gibt, sind für alle Betriebssysteme verfügbar. Daher muss geprüft werden, welche Erweiterungsmodule für den geplanten Einsatz benötigt werden und für welche Plattformen diese verfügbar sind.
- Für die gewählte Plattform muss entsprechender interner oder externer Support zur Verfügung stehen. Die Administratoren müssen über die notwendigen Kenntnisse in dem Betriebssystem verfügen oder entsprechend geschult werden.

Binärversion oder eigenes Kompilieren

Der Apache-Webserver kann entweder aus dem Quellcode selbst kompiliert werden, oder es kann eine Binärversion installiert werden. Der Quellcode kann vom Server der Apache Foundation (*http://www.apache.org*) heruntergeladen werden. Binärversionen werden von verschiedenen Betriebssystemherstellern und Distributoren angeboten. Auch die Apache Foundation bietet vorkompilierte Versionen für verschiedene Betriebssysteme an.

Bei der Entscheidung, ob eine Binärversion eingesetzt oder der Apache-Webserver selbst kompiliert wird, sollten die folgenden Punkte berücksichtigt werden:

- Binärversionen sind meist auf eine bestimmte Standardkonfiguration zugeschnitten. Dies bedeutet, dass weniger Einfluss auf Installationspfade und die Zusammenstellung von Erweiterungsmodulen möglich ist.
- Binärversionen von Betriebssystemherstellern oder Distributoren sind oft nicht auf dem neuesten Versionsstand bzw. es vergeht einige Zeit, bevor eine neue Version verfügbar ist. Dies kann zu Problemen führen, wenn beispielsweise beim Auftauchen von Sicherheitslücken schnell eine neue Version benötigt wird. Andererseits bieten Binärversionen den Vorteil, dass sie vom Hersteller bzw. Distributor getestet sind, mit den vorhandenen Installationsmechanismen (Paketverwaltung oder ähnliches) installiert werden können und meist auch auf dem "Standard-Support-Weg" unterstützt werden. Die Binärversionen von der Apache Foundation sind meist relativ schnell verfügbar, es gibt jedoch keinen Standard-Support.

Binärversionen sind bequem, aber nicht so flexibel

- Das Kompilieren des Apache-Webservers aus dem Quellcode bietet die größtmögliche Flexibilität bei der Auswahl von Modulen und anderen Optionen. Zusätzlich sind Patches und neue Versionen immer zuerst als Quellcode verfügbar. Der Nachteil ist, dass ein Administrator mit entsprechenden Kenntnissen sowie ein entsprechend ausgerüsteter Entwicklungsrechner vorhanden sein müssen. Aus Sicherheitsgründen sollte auf dem Webserver-Rechner selbst kein Compiler installiert sein.

Kompilieren ist flexibel, aber aufwendiger

- Manche Module können nur verwendet werden, wenn der Apache-Webserver selbst übersetzt wird.

Festlegen benötigter Funktionalität

Die weiteren Anforderungen, die bei der allgemeinen Planung für das Webangebot aufgestellt wurden, müssen in konkrete Anforderungen an den Apache-Webserver übertragen werden.

Falls das Webangebot dynamische Seiten enthalten soll, sollte spätestens an dieser Stelle entscheiden werden, mit welcher Technik diese realisiert werden sollen. Ist der Zugriff auf Datenbanken, Verzeichnisdienste oder sonstige externe Resourcen erforderlich, so muss auch dafür festgelegt werden, wie der Zugriff realisiert werden soll.

Es sollte eine Liste der Module erstellt werden, die im Apache-Webserver eingesetzt werden müssen, um die Anforderungen zu erfüllen. Module, die in der Standardkonfiguration aktiv sind, für die jedoch kein konkreter Bedarf besteht, sollten nach Möglichkeit entfernt werden.

M 2.270 Planung des SSL-Einsatzes beim Apache Webserver (zusätzlich)

Verantwortlich für Initiierung: Leiter IT IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement Administrator

SSL (Secure Sockets Layer) bzw. TLS (Transport Layer Security) ist ein Transportprotokoll, das kryptographische Mechanismen zur Gewährleistung von Integrität, Vertraulichkeit und Authentizität übertragener Daten nutzt (siehe M 5.66 *Verwendung von SSL*).

Einsatzmöglichkeiten von SSL beim Apache-Webserver

Es gibt zwei Szenarien, in denen SSL zum Einsatz kommen kann:

Serverzertifikat und Verbindungsverschlüsselung

Im ersten Szenario verfügt nur der WWW-Server über ein Zertifikat. Der WWW-Client kann dann aufgrund dieses Zertifikates den WWW-Server authentisieren. Im Rahmen des SSL-Protokolles wird dann ein verschlüsselter und integritätsgeschützter Kanal etabliert, über den im folgenden die Daten zwischen WWW-Server und WWW-Client ausgetauscht werden können.

Client-Authentisierung

Im zweiten Szenario verfügt auch der Benutzer des WWW-Servers über ein eigenes Zertifikat, so dass im Rahmen des SSL-Protokolles eine gegenseitige Authentisierung erfolgen kann.

Der Einsatz von SSL in Verbindung mit einem WWW-Server erfordert eine sorgfältige Planung, bei der eine ganze Reihe von Aspekten berücksichtigt werden müssen. Beim Einsatz von SSL im ersten Szenario etwa kommen die folgenden Aspekte zum Tragen:

- Der WWW-Server benötigt ein SSL-Zertifikat, das für ihn von einer Zertifizierungsstelle ausgestellt wurde.
- Bei der Auswahl dieser Zertifizierungsstelle muss berücksichtigt werden, dass die WWW-Clients, die auf den WWW-Server zugreifen sollen, über das entsprechende Wurzelzertifikat dieser Zertifizierungsstelle verfügen müssen.
- Das SSL-Zertifikat eines Servers muss regelmäßig erneuert werden. Neben der Laufzeit des Zertifikates selbst muss hier auch die Laufzeit des Wurzelzertifikates berücksichtigt werden.
- Ein SSL-Zertifikat kann auch selbst erzeugt werden, beispielsweise mit dem OpenSSL Paket. Da solche Eigen-Zertifikate nicht von einer der Zertifizierungsstellen stammen, die normalerweise den Browsern bekannt sind, bekommen die Besucher in diesem Fall jedoch meist beim Zugriff eine Warnung angezeigt. Dies kann dadurch behoben werden, dass das zum Ausstellen des Server-Zertifikats benutzte Zertifikat manuell auf den Browsern installiert wird. Bei einer Nutzung eines SSL-gesicherten Webservers im Intranet kann dies eine berücksichtigenswerte Option sein.

SSL-Benutzerzertifikate müssen verwaltet werden

Wird SSL im zweiten Szenario auch zur Client-Authentisierung genutzt, so muss im Prinzip eine vollständige Public-Key-Infrastruktur geplant werden. Folgende Aspekte müssen dabei berücksichtigt werden:

- Für die einzelnen Benutzer müssen SSL-Zertifikate erstellt und verteilt werden.

- Die Gültigkeitsdauer der Benutzer-Zertifikate muss ebenso berücksichtigt werden, wie das Szenario eines Schlüsselwechsels der eingesetzten Zertifizierungsstelle.
- Die Richtlinien der für die Benutzer-Zertifikate genutzten Zertifizierungsstelle müssen konform zu den Anforderungen an die Authentisierung der Benutzer sein.
- Es muss in Betracht gezogen werden, dass der private SSL-Schlüssels eines Benutzers kompromittiert sein könnte. Daher sollte es auch Möglichkeiten geben, diese zu sperren. Dies kann durch Prüfen gegen eine Positivliste (noch gültige Zertifikate) oder durch Verwendung einer Negativliste (gesperrte Zertifikate) geschehen.

Prinzipiell besteht die Möglichkeit, SSL-Benutzerzertifikate nicht nur zur Authentisierung zu nutzen, sondern darüber hinaus auch Zugriffsrechte in Abhängigkeit von einzelnen Einträgen des Zertifikates zu vergeben (z. B. der Zugehörigkeit zu einer bestimmten Abteilung). Soll diese Möglichkeit genutzt werden, so muss darauf geachtet werden, dass

- die relevanten Einträge bei der Zertifizierung von Benutzern korrekt vorgenommen werden und
- die Zertifikate gesperrt werden, sobald die relevanten Einträge ungültig werden (z. B. wenn Mitarbeiter die Institution verlassen oder die Abteilung wechseln).

Können diese Voraussetzungen nicht gewährleistet werden, so ist im Rahmen der Definition einer Sicherheitsrichtlinie für den Webserver festzuhalten, dass Zugriffsrechte nicht auf der Basis von Zertifikatsfeldern eingerichtet werden dürfen.

Im Rahmen der Planung müssen schließlich die notwendigen Abläufe und Zuständigkeiten definiert werden. Die Planung ist zu dokumentieren. Die Dokumentation der Planung sollte getroffene Entscheidungen und die Beweggründe, die für diese Entscheidungen ausschlaggebend waren, klar herausstellen.

Verfügbare Implementierungen von SSL beim Apache-Webserver

Ab der Version 2.0 des Apache-Webservers wird SSL mit dem Modul *mod_ssl* vom Apache-Webserver direkt unterstützt. In der Version 1.3 ist keine Implementierung von SSL enthalten, sondern es ist eine Erweiterung des Apache-Webservers notwendig. Es existieren gibt zwei verschiedene Open-Source-Implementierungen von SSL: Apache-SSL (*http://www.apache-ssl.org*) und mod_ssl (*http://www.modssl.org*). Beide verwenden für die kryptographischen Algorithmen und die Realisierung des SSL-Protokolles selbst das Open-Source Paket OpenSSL (*http://www.openssl.org*). Die prinzipiellen Unterschiede zwischen den beiden Implementierungen bestehen in der Art der Integration von OpenSSL in den Apache-Webserver sowie in den verfügbaren Konfigurationsmöglichkeiten.

Vor der Verwendung von SSL muss daher im Rahmen der Planung (siehe M 2.269 *Planung des Einsatzes eines Apache Webservers*) entschieden werden, welche Implementierung genutzt werden soll. Diese Entscheidung

kann unter Berücksichtigung funktionaler Gesichtspunkte getroffen werden.

Bei der Planung des Einsatzes von SSL muss auch berücksichtigt werden, dass es in diesem Fall in der Regel notwendig sein wird, den Apache-Webserver aus den Quelltexten selbst zu kompilieren, da SSL in den meisten Binärdistributionen nicht enthalten ist.

Serverzertifikat

Der private Schlüssel des Server-Zertifikats sollte aus Sicherheitsgründen durch eine Passphrase geschützt sein. Dies bedeutet, dass die Passphrase beim Neustart des Servers eingegeben werden muss. Ein automatischer unbeaufsichtigter Neustart des Servers ist somit nicht möglich. Dieser Aspekt muss bei der Planung des Betriebs berücksichtigt werden.

Ergänzende Kontrollfragen:

- Ist geklärt, welche Art von Zertifikat für den WWW-Server benötigt wird?
- Wird SSL auch zur Benutzer-Authentisierung verwendet? Falls ja, sind die entsprechenden Rahmenbedingungen erfüllt?
- Ist festgelegt, welche Implementierung von SSL eingesetzt werden soll?

M 2.271 Festlegung einer Sicherheitsstrategie für den WWW-Zugang

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Wird der Zugang zum WWW nicht über eigenständige Internet-PCs (siehe Baustein B 3.210 *Internet-PC*) abgewickelt, sondern direkt über die Arbeitsplatz-Rechner, so muss für diesen Bereich eine eigene Sicherheitsstrategie festgelegt werden.

In der Sicherheitsstrategie für die WWW-Nutzung sollten die folgenden Fragen beantwortet werden:

- Wer erhält WWW-Zugang?
- Unter welchen Bedingungen bzw. zu welchem Zweck darf auf das WWW zugegriffen werden?
- Ist eine Benutzerschulung erforderlich und falls ja, wie wird sie durchgeführt?
- Wie wird technische Hilfestellung für die Benutzer gewährleistet?

Durch organisatorische Regelungen oder durch die technische Umsetzung sind dabei insbesondere die folgenden Punkte zu gewährleisten:

- Die Browser der Benutzer müssen durch den Administrator so vorkonfiguriert sein, dass ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht werden kann (siehe auch M 5.45 *Sicherheit von WWW-Browsern*).
- Dateien, deren Inhalt Anstoß erregen könnte, dürfen weder auf WWW-Servern eingestellt noch nachgefragt werden. Es muss festgelegt werden, welche Inhalte als anstößig gelten.
- Nach dem Download von Dateien sind diese explizit auf Computer-Viren zu überprüfen.

Alle Regelungen und Bedienungshinweise zur WWW-Nutzung sind schriftlich zu fixieren und sollten den Mitarbeitern jederzeit zur Verfügung stehen. Ein entsprechendes Muster findet sich unter den Hilfsmitteln zum IT-Grundschutz.

Die Benutzer müssen vor der WWW-Nutzung geschult werden, sowohl in der Nutzung ihrer WWW-Browser als auch des Internets, um Fehlbedienungen zu vermeiden und die Einhaltung der organisationsinternen Richtlinien zu gewährleisten. Insbesondere müssen sie hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen sensibilisiert werden.

Ergänzende Kontrollfragen:

- Existiert eine Sicherheitsstrategie für den Betrieb eines WWW-Servers?
- Existiert eine Sicherheitsstrategie für die Nutzung von WWW-Diensten?
- Sind die getroffenen Regelungen ausreichend?

M 2.272 Einrichtung eines WWW-Redaktionsteams

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Leiter IT, Fachverantwortliche

Ein Webangebot benötigt regelmäßige Pflege. Vor allem dann, wenn Inhalte oder Dienste angeboten werden, die sich häufiger ändern, wird der Pflegeaufwand relativ schnell anwachsen.

Im Konzept für das Webangebot (siehe M 2.172 *Entwicklung eines Konzeptes für die WWW-Nutzung*) werden Verantwortliche für verschiedene Aspekte der Pflege des Webangebots benannt. Überschreitet der Umfang des Angebots und der damit verbundene Pflegeaufwand ein bestimmtes Maß, so kann es sinnvoll sein, zur besseren Koordination eine eigenständige WWW-Redaktion einzurichten. Auf diese Weise werden die Verantwortlichkeiten noch einmal betont und sichtbar in der Organisationsstruktur abgebildet.

zentraler Anlaufpunkt

Die Einrichtung einer WWW-Redaktion bietet den Vorteil, dass ein zentraler Kontakt für alle Fragen, die das Webangebot betreffen, zur Verfügung steht. Innerhalb einer solchen Redaktion können meist einfacher effiziente Prozesse zur Sicherstellung der Aktualität und Korrektheit der Informationen im Webangebot (beispielsweise bestimmte Freigabeprozesse oder ein Vieraugenprinzip) etabliert werden, als wenn dies über verschiedene Organisationseinheiten hinweg geschehen müsste.

Die Redaktion sollte mindestens diejenigen Personen umfassen, die im WWW-Konzept als Verantwortliche genannt wurden. Oft ist es sinnvoll, weitere Personen in die Redaktion einzubinden. Eine WWW-Redaktion sollte folgende Mitglieder umfassen:

- einen Chefredakteur, der die Gesamtverantwortung für die Inhalte und Dienste im Webangebot übernimmt,
- für die verschiedenen inhaltlichen Bereiche jeweils einen Fachredakteur,
- einen Verantwortlichen für das optische Erscheinungsbild (Webdesign) des Webangebots,
- einen "technischen Webmaster", der für die technischen Aspekte des Betriebs des Webservers zuständig ist.

Falls auf dem Webserver umfangreichere Webanwendungen eingesetzt werden, so sollte auch für diese Anwendungen ein Ansprechpartner in der WWW-Redaktion vertreten sein. Die Fachredakteure, der Webdesigner und der technische Webmaster dienen jeweils als Ansprechpartner (Schnittstelle) zu den jeweiligen Fachbereichen.

Innerhalb der WWW-Redaktion müssen neben den normalen Redaktionsprozessen auch Vorgehensweisen und Zuständigkeiten für den Fall von Problemen festgelegt werden, damit eine schnelle und effiziente Reaktion auf Sicherheitsvorfälle gewährleistet ist (siehe auch M 2.173 *Festlegung einer WWW-Sicherheitsstrategie*).

M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Häufig werden Fehler in Software-Produkten bekannt, die dazu führen können, dass die Sicherheit der IT-Systeme, auf denen diese Produkte installiert sind, beeinträchtigt wird. Diese Schwachstellen müssen so schnell wie möglich behoben werden, damit sie nicht durch interne oder externe Angreifer ausgenutzt werden können. Dies ist ganz besonders wichtig, wenn die betreffenden Systeme mit dem Internet verbunden sind. Die Hersteller von Betriebssystem- oder Software-Komponenten veröffentlichen in der Regel Patches oder Updates, die auf dem jeweiligen IT-System installiert werden müssen, um den oder die Fehler zu beheben.

Auf dem Laufenden bleiben

Die Systemadministratoren sollten sich daher regelmäßig über bekannt gewordene Software-Schwachstellen informieren (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*).

Bezugsquellen kennen, Integrität und Authentizität überprüfen

Wichtig ist, dass Patches und Updates, wie jede andere Software, nur aus vertrauenswürdigen Quellen bezogen werden dürfen. Für jedes eingesetzte System oder Softwareprodukt muss bekannt sein, wo Sicherheitsupdates und Patches erhältlich sind. Außerdem ist es wichtig, dass Integrität und Authentizität der bereits installierten Produkte oder der einzuspielenden Sicherheitsupdates und Patches überprüft werden (siehe M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*), bevor ein Update oder Patch installiert wird. Vor der Installation sollten sie außerdem mit Hilfe eines Computer-Virenschutzprogramms geprüft werden. Dies sollte auch bei solchen Paketen gemacht werden, deren Integrität und Authentizität verifiziert wurde.

Auch Updates und Patches Testen

Sicherheitsupdates oder Patches dürfen jedoch nicht voreilig eingespielt werden, sondern müssen vor dem Einspielen getestet werden. Falls sich ein Konflikt mit anderen kritischen Komponenten oder Programmen herausstellt, kann ein solches Update sonst zu einem Ausfall des Systems führen. Nötigenfalls muss ein betroffenes System so lange durch andere Maßnahmen geschützt werden, bis die Tests abgeschlossen sind.

Backup

Vor der Installation eines Updates oder Patches sollte stets eine Datensicherung des Systems erstellt werden, das es ermöglicht, den Originalzustand wieder herzustellen, falls Probleme auftreten. Dies gilt insbesondere dann, wenn ausführliche Tests aus Zeitgründen oder mangels eines geeigneten Testsystems nicht durchgeführt werden können.

Dokumentation

In jedem Fall muss dokumentiert werden, wann, von wem und aus welchem Anlass Patches und Updates eingespielt wurden (siehe auch M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*). Aus der Dokumentation muss sich der aktuelle Patchlevel des Systems jederzeit schnell ermitteln lassen, um beim Bekanntwerden von Schwachstellen schnell Klarheit darüber zu erhalten, ob das System dadurch gefährdet ist.

Falls festgestellt wird, dass ein Sicherheitsupdate oder Patch mit einer anderen wichtigen Komponente oder einem Programm inkompatibel ist oder Probleme verursacht, so muss sorgfältig überlegt werden, wie weiter vorgegangen wird. Wird entschieden, dass auf Grund der aufgetretenen Probleme ein Patch nicht installiert wird, so ist diese Entscheidung auf jeden Fall zu dokumentieren. Außerdem muss in diesem Fall klar beschrieben sein, welche Maßnahmen ersatzweise ergriffen wurden, um ein Ausnutzen der Schwachstelle zu verhindern. Eine solche Entscheidung darf nicht von den Administratoren alleine getroffen werden, sondern sie muss mit den Vorgesetzten und dem IT-Sicherheitsbeauftragten abgestimmt sein.

Ergänzende Kontrollfragen:

- Wissen die Administratoren, von wo sie sicherheitsrelevante Patches und Updates beziehen können?
- Werden Sicherheitsupdates und Patches vor dem Einspielen überprüft und getestet?
- Wie werden die Veränderungen durch Updates und Patches dokumentiert?

M 2.274 Vertretungsregelungen bei E-Mail-Nutzung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Benutzer, Administrator

Für die Bearbeitung von E-Mail ist - ebenso wie bei jeder anderen Aufgabe - für jeden Mitarbeiter ein Vertreter zu benennen. Bei geplanter Abwesenheit sollten die Benutzer dann für den Vertreter eine E-Mail-Weiterleitung einrichten oder den Zugriff auf ihr Postfach freigeben. Bei spontaner Abwesenheit, z. B. wegen Krankheit, können andere Regelungen die zeitnahe E-Mail-Bearbeitung sicherstellen. Beispielsweise kann das Vorzimmer der betroffenen Abteilung die IT-Verantwortlichen informieren, die dann wiederum am E-Mail-Server eine Weiterleitung schalten. Dies ist allerdings nur dann zulässig, wenn klar geregelt ist, dass E-Mail nur dienstlich genutzt werden darf. Die Benutzer sollten außerdem per E-Mail über die Weiterleitung informiert werden. Sobald sie wieder im Haus sind, sollten sie den IT-Verantwortlichen mitteilen, dass die Weiterleitung aufgehoben werden kann.

Alternativ können grundsätzlich auch aufgabenbezogene E-Mail-Adressen eingerichtet werden. Auch hier muss natürlich sichergestellt sein, dass eingehende E-Mail jederzeit zeitnah bearbeitet wird.

Autoreply / Abwesenheitsassistent

Viele E-Mail-Clients bieten die Möglichkeit, vor einer längeren Abwesenheit einen Dienst zu aktivieren (*Autoreply*, unter Outlook *Abwesenheitsassistent*), der dafür sorgt, dass jeder Absender einer E-Mail während der vorgegebenen Abwesenheitszeiten eine Nachricht erhält, dass dieser Empfänger vorübergehend nicht zu erreichen ist. Dies hat oft Vorteile, führt aber häufig dazu, dass zu viele Informationen über den Benutzer und die Organisation breit gestreut nach außen gegeben werden.

Andererseits wird der Absender trotz einer solchen Benachrichtigung über die Abwesenheit meistens im unklaren darüber gelassen, wie mit seiner E-Mail weiter umgegangen wird. Es stellt sich dann die Frage, ob die E-Mail also bis auf weiteres unbearbeitet bleibt oder an einen Vertreter weitergeleitet wurde.

Daher sollten alle Benutzer darauf achten, dass weder die genaue Zeit der Abwesenheit noch Informationen über Interna weitergegeben werden, wie Telefonnummern oder Organisationseinheiten. Diese lassen sich für Angriffe über Social Engineering weiterbenutzen (siehe G 5.42 *Social Engineering*).

Auf jeden Fall sollten aber Vertreter für alle längeren Abwesenheitsphasen benannt werden. Dies kann auch Externen über solche Mechanismen wie den Abwesenheitsassistent mitgeteilt werden, so dass sie wissen, dass die E-Mail angekommen ist und bearbeitet wird.

Hinweis: Die meisten E-Mail-Programme mit Autoreply-Funktion bieten auch die Möglichkeit, die Benachrichtigung nach Kriterien, die die Benutzer selbst festlegen können, zu steuern. Damit kann dann beispielsweise voreingestellt werden, dass interne E-Mail-Absender andere Antworten erhalten als externe. Hierfür werden in der Regel aber tiefere Kenntnisse des E-Mail-Clients benötigt. Wenn daher Regeln zur Steuerung von Autoreply-Funktionen eingesetzt werden sollen, sollten die Administratoren dies entsprechend für die Benutzer vorbereiten.

Ergänzende Kontrollfragen:

- Ist geregelt, wie Vertretungsregelungen bei E-Mail umgesetzt werden?
- Wissen alle Benutzer, wie sie Vertretungsregelungen bei den E-Mail-Clients aktivieren können?

M 2.275 Einrichtung funktionsbezogener E-Mailadressen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Benutzer, Administrator

In vielen Organisationen werden Geschäftsprozesse inzwischen ganz oder teilweise per E-Mail abgewickelt. Dabei ist es wichtig, dass Nachrichten rechtzeitig den richtigen Empfänger erreichen. Durch Urlaub, Dienstreisen, Krankheit oder personelle Veränderungen können zu unterschiedlichen Zeitpunkten aber ganz verschiedene Personen für die Bearbeitung einer E-Mail zuständig sein.

Daher sollten für bestimmte Funktionen organisations- bzw. funktionsbezogene E-Mail-Adressen eingerichtet werden, um unabhängig von Personen die Zustellung zur richtigen Organisationseinheit zu garantieren. Dies ist insbesondere bei zentralen Anlaufstellen wichtig. Dieser Ansatz hat u. a. folgende Vorteile:

- E-Mails an funktionsbezogene Adressen können gegebenenfalls direkt an Stellvertreter verteilt werden. Dadurch kann auch bei Abwesenheit des Hauptansprechpartners eine zügige Bearbeitung erreicht werden. Werden E-Mails an funktionsbezogene Adressen nicht direkt an den jeweiligen Ansprechpartner weitergeleitet, sondern in eigenen Postfächern abgelegt, so hat dies einen zusätzlichen Vorteil im Bezug auf Datenschutz. In diesem Fall braucht nämlich im Fall einer ungeplanten Abwesenheit (beispielsweise Unfall, Krankheit) des eigentlichen Empfängers nicht dessen persönliches Postfach "geöffnet" zu werden.
- Bei einem Wechsel der Zuständigkeit müssen nicht alle Kommunikationspartner informiert werden. In diesem Fall müssen lediglich alle E-Mails, die an die funktionsbezogene E-Mail-Adresse gerichtet sind, an die neuen Ansprechpartner weitergeleitet werden.
- Funktionsbezogene E-Mail-Adressen können aussagekräftig benannt werden, z. B. *beratung@..., webmaster@..., vertrieb@...*, und lassen sich dadurch oft leichter merken als personenbezogene Adressen.
- Durch die Adressierung an die funktionsbezogene E-Mail-Adresse können die Empfänger auch unabhängig vom Betreff (*Subject*) erkennen, um welches Thema es in der E-Mail wahrscheinlich geht.

Für verschiedene Funktionen, die direkt mit dem Betrieb einer Internet-Domain zusammen hängen, wird darüber hinaus die Existenz gewisser funktionsbezogener E-Mailadressen (beispielsweise *postmaster*) in den relevanten De-Facto-Standards (IETF RFCs, hier insbesondere die RFC 822 und RFC 2142) explizit gefordert (siehe auch M 2.120 *Einrichtung einer Poststelle*).

Schema für E-Mailadressen festlegen

Werden organisations- oder funktionsbezogene E-Mailadressen eingeführt, so sollte ein geeignetes, nachvollziehbares Schema festgelegt werden, nach dem diese Adressen gebildet werden. Dies ist vor allem bei organisationsbezogenen Adressen wichtig, da solche Adressen eventuell nicht so "intuitiv" sind, wie funktionsbezogene Adressen.

Konfiguration dokumentieren

Je nachdem, welche Softwareprodukte (Mailserver und -clients, eventuell Verzeichnisserver etc.) verwendet werden, wird die Einrichtung organisations- und funktionsbezogener E-Mailadressen auf unterschiedliche Art und Weise erfolgen müssen. Dabei sollte die Konfiguration so dokumentiert werden, dass es im Falle eines Totalausfalls des Mailsystems möglich ist, die Konfiguration auf einem Ersatzsystem so "nachzubauen", dass keine Nachrichten verloren gehen. Zumindest muss dokumentiert sein, welche organisations- und funktionsbezogenen Adressen existieren und zu welchem Zweck sie dienen.

Ergänzende Kontrollfragen:

- Existieren die in RFC 822 geforderten technischen Funktionsadressen?
- Existieren Vertretungsregelungen für alle funktions- und organisationsbezogenen E-Mailadressen?
- Ist ein Schema festgelegt, nach dem funktions- und organisationsbezogene E-Mailadressen gebildet werden?

M 2.276 Funktionsweise eines Routers

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator

In großen Netzen kann kaum auf den Einsatz von Routern verzichtet werden. Router werden sowohl in lokalen Netzen als auch in Weitverkehrsnetzen eingesetzt (siehe auch Baustein B 4.4 *Remote Access*). Ohne den Einsatz von Routern wäre das Internet nicht funktionsfähig.

Router können gleichzeitig unterschiedliche Protokolle (z. B. IP, IPX) und Topologien (z. B. Ethernet, Token Ring, FDDI, ATM, Frame Relay, ISDN) unterstützen. Dadurch sind Router in der Lage, lokale Netze nahtlos mit Weitverkehrsnetzen zu verbinden. Nicht zuletzt diese Funktion von Routern hat mit dazu beigetragen, dass sich das Internet in der Vergangenheit so rasch entwickeln konnte.

Ein Router übernimmt im wesentlichen zwei Aufgaben. Zum einen wird eine geeignete Verbindung zwischen dem Quellsystem beziehungsweise Quellnetz und dem Zielsystem beziehungsweise Zielnetz ermittelt und zum anderen werden Datenpakete entlang dieser Verbindung transportiert. Wenn das Zielsystem (Zielnetz) direkt an dem Router angeschlossen ist - d. h. Router und Zielsystem befinden sich im selben Subnetz - wird das vom Quellsystem gesendete Datenpaket direkt an das Zielsystem gesendet.

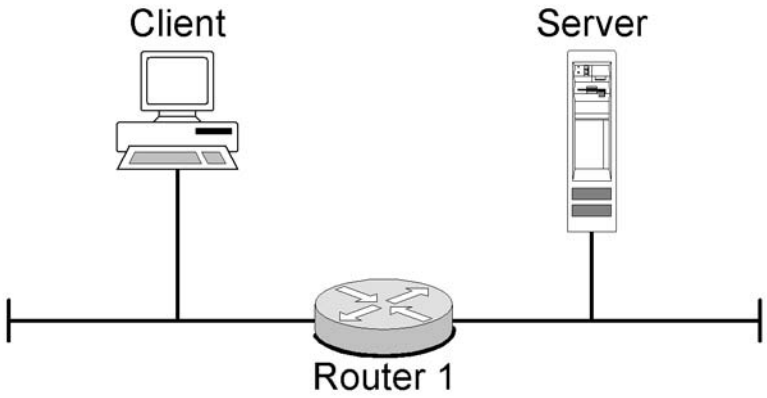


Abbildung: Routing

Next Hop

Wenn das Zielsystem (Zielnetz) nicht direkt am Router angeschlossen ist, sendet der Router das Datenpaket an einen benachbarten Router, der näher am Zielsystem (Zielnetz) angeschlossen ist, den sogenannten Next Hop. Der letzte Router in dieser Verbindungskette ist immer direkt am Zielnetz angeschlossen und sendet das Datenpaket zum Zielsystem.

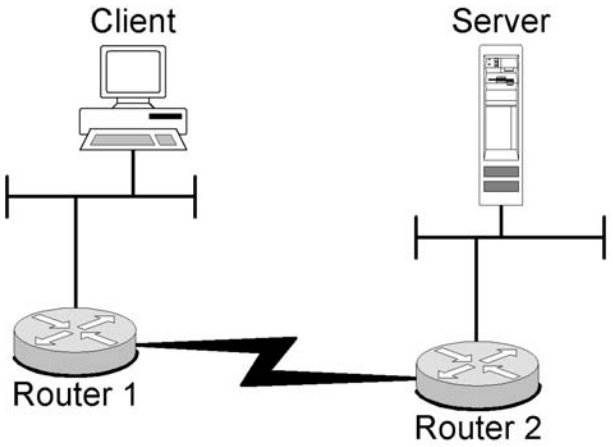


Abbildung: Routing

Die Aufgabe eines Routers ist es, eintreffende Datenpakete entweder direkt an den adressierten Empfänger zu übergeben, oder in das nächste Netz weiterzuleiten. In welches Netz das Datenpaket weitergeleitet wird, wenn es nicht direkt zugestellt werden kann, entscheidet die sogenannte Routing-Metrik. Die Metrik ist ein Maß für die Qualität der Verbindung zwischen dem Sender bzw. dem Router und dem Ziel des Paketes. Mit ihrer Hilfe entscheidet der Router, an welchen Next Hop er das Paket weitergibt. Routing-Metriken beziehen sich nicht ausschließlich auf die Länge des Weges zwischen Sender und Empfänger, sondern können auch andere Merkmale, wie beispielsweise die Qualität der Leitungen, die Bandbreite oder die Auslastung in die Entscheidung mit einbeziehen. Welche Kriterien verwendet werden, ist von dem verwendeten Routing-Protokoll abhängig.

Routing-Tabellen

Die Routing-Informationen werden in sogenannten Routing-Tabellen verwaltet. Routing-Tabellen enthalten Informationen darüber, über welche benachbarten Router als Next Hop für bestimmte Zielnetze dienen können. Router treffen die Entscheidung, an welchen Next Hop ein empfangenes Datenpaket weitergegeben wird, ausschließlich auf Basis dieser Routing-Tabellen. Deswegen ist es besonders wichtig, diese Tabellen vor Manipulationen zu schützen. Es sind eine Reihe von Angriffen bekannt, welche die Manipulierbarkeit von Routing-Tabellen ausnutzen. In der folgenden Abbildung ist der Inhalt einer Routing-Tabelle beispielhaft dargestellt.

Ziel	Next Hop	Hop Count
210.23.125.98	210.23.122.4	3
	127.200.45.123	5
	203.2.67.187	8
...	...	...

Tabelle: Beispielhafter Ausschnitt aus einer Routing-Tabelle

In diesem Beispiel würde der Router ein Paket mit der Zieladresse 210.23.125.98 an den Next Hop 210.23.122.4 weiterleiten. Der sogenannte

Hop Count gibt an, wie viele Zwischenstationen das Paket noch passieren muss, um sein Ziel über den betreffenden Next Hop zu erreichen. Sind für ein bestimmtes Ziel mehrere benachbarte Router als Next Hops verfügbar, so kann der Hop Count als eine Routing-Metrik verwendet werden, um den "günstigsten" Next Hop zu bestimmen. Auch beim Routing Protokoll RIP wird der Hop Count als Routing-Metrik verwendet.

Statisches und dynamisches Routing

Es wird in bezug auf das Routing zwischen statischem und dynamischem Routing unterschieden. Diese beiden Methoden unterscheiden sich hinsichtlich der Verwaltung der Routing-Tabellen.

Beim statischen Routing werden diese Tabellen manuell mit Hilfe von Systembefehlen gepflegt.

Beim dynamischen Routing erfolgt die Pflege der Routing-Tabellen automatisiert. Dies geschieht mit Hilfe von Routing-Protokollen. Hier wird noch einmal zwischen den Interior Gateway Protokollen (IGP) und den Exterior Gateway Protokollen (EGP) unterschieden. IGP wird innerhalb von Netzen verwendet, die unter eigener Administrationsverantwortung stehen. Die Zusammenfassung der unter eigener Verantwortung betriebenen Netze wird auch als Routing-Domäne bezeichnet. Mit Hilfe von EGP werden Routing-Informationen zwischen unterschiedlichen Routing-Domänen ausgetauscht.

Die folgende Abbildung stellt diesen Zusammenhang dar.

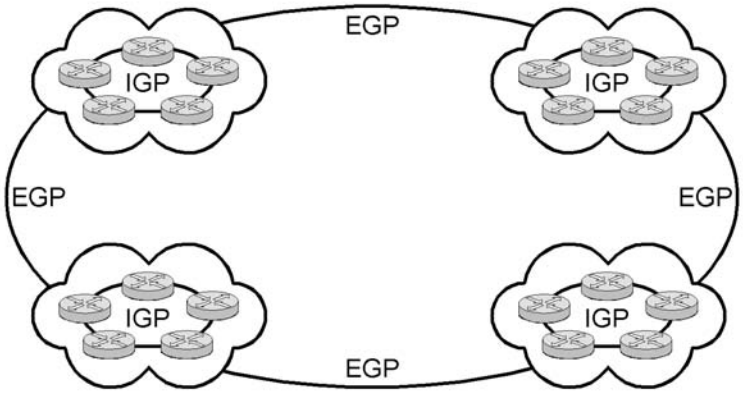


Abbildung: Austausch von Routing-Informationen

Routing-Protokolle

Die bekanntesten und standardisierten Routing-Protokolle sind das Routing Information Protocol (RIP), Open Shortest Path First (OSPF) und das Border Gateway Protocol (BGP), wobei es sich beim Border Gateway Protocol um ein Exterior Gateway Protokoll handelt. Erweitert werden diese Protokolle durch proprietäre Routing-Protokolle von unterschiedlichen Herstellern. Die bekanntesten Protokolle sind das Interior Gateway Routing Protocol (IGRP) und das Enhanced Interior Gateway Routing Protocol (EIGRP) des Herstellers Cisco.

Da Routing-Protokolle die Verwaltung von Routing-Tabellen automatisieren, haben Angreifer längst erkannt, Sicherheitslücken dieser Protokolle

auszunutzen, um die Routing-Tabellen zu modifizieren und so Datenpakete umzuleiten oder ganze Netze außer Betrieb zu setzen (siehe G 5.51 *Missbrauch von Routing-Protokollen*).

Bei der Implementierung eines dynamischen Routings zwischen Netzen ist in erster Linie auf die Sicherheitsfunktionen der verwendeten Routing-Protokolle zu achten (siehe M 5.112 *Sicherheitsaspekte von Routing-Protokollen*). Der Administrator muss besonderen Wert auf die sichere Authentisierung der benachbarten Router beim Austausch von Routing-Tabellen legen. Es sollten nur Routing-Protokolle verwendet werden, die eine verschlüsselte Authentisierung beim Austausch von Routing-Tabellen unterstützen.

Der Aufwand der manuellen Pflege von Routing-Tabellen ist zu groß, um in komplexen Netzen auf dynamisches Routing verzichten zu können. Der Einsatz von dynamischem Routing ist vor der Inbetriebnahme unter dem Gesichtspunkt der Sicherheit zu bewerten.

Kein dynamisches Routing bei hohem Schutzbedarf

Allgemein sollte in Netzen mit hohem Schutzbedarf nach Möglichkeit kein dynamisches Routing verwendet werden. Kann auf dynamisches Routing aus wichtigen Gründen nicht verzichtet werden, so sollten zumindest nur solche Routing-Protokolle verwendet werden, die eine sichere Authentisierung der beteiligten Geräte und eine gesicherte Übertragung der Routing-Informationen bieten.

In M 2.278 *Typische Einsatzszenarien von Routern und Switches* ist ein weiteres Szenario beschrieben, in dem vom Einsatz von Routing-Protokollen abgeraten wird.

Router als Paketfilter

Viele Router können auch für die Filterung von Datenpaketen verwendet werden, d. h. der Router wird als Paketfilter eingesetzt (siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)*).

Broadcast-Pakete werden von einem Router normalerweise nicht zwischen verschiedenen angeschlossenen Netzen transportiert. Hierdurch teilt der Router die angeschlossenen Netze in unterschiedliche Broadcast-Domänen auf.

Router verfügen allerdings meist noch über weitergehende Filterfunktionen. Beispielsweise können sogenannte Access Control Lists (ACL) konfiguriert werden. Der Router regelt anhand dieser Listen den Datenverkehr zwischen den beteiligten Netzen. Weitergehende Sicherheitsaspekte bei Access Control Lists sind in M 5.111 *Einrichtung von Access Control Lists auf Routern* zu finden.

Der Einsatz von Paketfiltern ist als alleinige Methode zur Kontrolle des Datenverkehrs zwischen Netzen mit einem unterschiedlichen Schutzbedarf meist nicht ausreichend. Mehr Informationen finden sich im Baustein B 3.301 *Sicherheitsgateway (Firewall)* beispielsweise in M 2.73 *Auswahl geeigneter Grundstrukturen für Sicherheitsgateways* und M 2.74 *Geeignete Auswahl eines Paketfilters*.

Router als VPN-Gateway

Einige am Markt verfügbare Router unterstützen die Funktion Virtual Private Network (VPN). Diese Router werden insbesondere dann eingesetzt, wenn sensitive Daten über ein Netz übertragen werden. Der Einsatz von Routern mit VPN-Funktionalität hat den Vorteil, dass anwendungsseitig keine Verschlüsselungsmechanismen vorhanden sein müssen. Die Verschlüsselung ist transparent für die Kommunikationspartner. Allerdings findet die Kommunikation auf der Strecke bis zum ersten verschlüsselnden Netzkoppelelement unverschlüsselt statt und birgt damit ein Restrisiko. Authentisierung ist hier nur zwischen den Koppelelementen möglich. Die eigentlichen Kommunikationspartner werden nicht authentisiert (M 5.68 *Einsatz von Verschlüsselungsverfahren zur Netzkommunikation*).

M 2.277 Funktionsweise eines Switches

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT,

Verantwortlich für Umsetzung: Administrator

Einführung

Ursprünglich arbeiteten Switches auf der OSI-Schicht 2, mittlerweile sind Switches mit unterschiedlichen Funktionen erhältlich. Hersteller kennzeichnen Switches meist mit dem OSI-Layer, der unterstützt wird. Dadurch entstanden die Begriffe Layer-2-, Layer-3- und Layer-4-Switch, wobei es sich bei Layer-3- und Layer-4-Switches eigentlich funktional bereits um Router handelt. Die ursprünglich unterschiedlichen Funktionen von Switches und Routern werden auf einem Gerät vereint. Dadurch wird die Abgrenzung der Gerätetypen (Switch oder Router) erschwert. Die wesentlichen Unterschiede dieser Geräte sind in der Einleitung zum Baustein B 3.302 *Router und Switches* aufgeführt.

Die ersten Switches entstanden aus den Bridges, die wie die modernen Switches heutzutage zur Auftrennung großer LAN-Segmente in mehrere kleine Segmente (Kollisionsdomänen) dienten. Bridges arbeiten in der Regel mit der Store-and-Forward-Technologie. Dabei wird jeder empfangene Ethernet-Frame eingelesen und dann anhand der Zieladresse entschieden, ob er an ein anderes LAN-Segment weitergegeben wird. Handelt es sich um lokalen Datenverkehr, erfolgt keine Weitergabe und der Frame gelangt nur zu den Stationen im lokalen Netz. Damit wird der lokale Verkehr auf einzelne Segmente begrenzt, was bei geeigneter Auslegung die Netzlast deutlich reduzieren kann. Bei kleineren Segmenten sinkt zudem der Anteil an Kollisionen und die Performance verbessert sich. Ist ein Frame an ein anderes Segment weiterzuleiten, wird er im Zwischenspeicher der Bridge abgelegt und anschließend an den Zielport übergeben. Zusätzlich kann beim Store-And-Forward die Integrität eines empfangenen Frames mit Hilfe von CRC-Prüfsummen überprüft werden. Korrupte Frames werden verworfen, was zu einer weiteren Verringerung der Netzlast beitragen kann.

Switches verfügen neben dem Store-and-Forward-Switching auch über den Mechanismus des Cut-Through-Forward-Switching, bei dem nur die Zieladresse - die ersten sechs Bytes eines Frames - gelesen wird. Hierdurch reduziert sich die Verzögerung zwischen dem Empfänger- und Sendeport erheblich. Allerdings ist es dabei nicht möglich, korrupte Frames auszufiltern. Durch das unnötige Weiterleiten fehlerhafter Frames kann eventuell ein Engpass entstehen. Abhilfe schafft ein adaptives Verhalten des Switches, bei dem der Frame während des Weiterreichens geprüft wird. Damit werden zwar korrupte Frames nicht ausgefiltert, aber der Switch kann die Qualität der Frames überwachen. Übersteigt der Prozentsatz der korrupten Frames einen vorher festgelegten Wert, so schaltet der Switch für diesen Port auf Store-and-Forward um, um in Zukunft zu filtern.

Switching-Tabellen

In der folgenden Abbildung ist beispielhaft eine sogenannte Switching-Tabelle dargestellt. In dieser Tabelle wird gespeichert, an welchem Port die Station mit der entsprechenden MAC-Adresse angeschlossen ist. Der Switch lernt diese Zuordnung dynamisch. Im Gegensatz zu einem Hub sendet der Switch einen Ethernet-Frame immer nur an den Port, an dem der Zielrechner angeschlossen ist. Dadurch wird die Bandbreite, die einem Gerät zur

Verfügung steht, nicht von der Kommunikation zwischen anderen angeschlossenen Stationen beeinflusst. Ein weiterer Effekt ist, dass die Kommunikation zwischen zwei Stationen von keiner der anderen Stationen mitgelesen werden kann. Davon ausgenommen sind Broadcasts und Multicasts, die an alle angeschlossenen Stationen gesandt werden. Ebenso werden Frames, deren Ziel-MAC-Adresse noch unbekannt ist, an alle Ports weitergeleitet.

Ziel MAC Adresse	Ziel Switch Port
0001.02c4.fdca	Fast Ethernet0/4
0001.026d.d412	Fast Ethernet0/8
0008.a345.12f3	Fast Ethernet0/12
0060.97ac.de59	Fast Ethernet0/16
...	...

Tabelle: Switching-Tabelle

Ein Frame, der an die Station mit der MAC-Adresse 0001.02c4.fdca gerichtet ist, wird vom Switch nur an den Port 01 weitergeleitet.

Da die Switching-Tabelle zur Steuerung des Datenflusses verwendet wird, muss sie vor Manipulationen geschützt werden. Es sind einige Angriffsmethoden bekannt, die die Integrität und Verfügbarkeit dieser Tabellen bedrohen (siehe G 5.112 *Manipulation von ARP-Tabellen*).

Layer-3- und Layer-4-Switches arbeiten analog auf einer entsprechend höheren OSI-Schicht.

Spanning Tree

Sind in einem lokalen Netz mit einer komplizierten Topographie mehrere Switches vorhanden, so kann es vorkommen, dass für die Verbindung zwischen zwei Geräten mehrere mögliche Wege existieren. Switching funktioniert aber nur dann, wenn zu jedem Zeitpunkt klar ist, an welchen Port ein Paket weitergeleitet werden muss. Andernfalls besteht die Gefahr, dass im Netz Schleifen (*Loops*) entstehen, auf denen Pakete immer im Kreis geschickt werden und niemals ihr eigentliches Ziel erreichen. Deswegen bieten Switches die Möglichkeit, automatisch untereinander eine logische Netzstruktur (einen sogenannten *Spanning Tree* des Netzes) "auszuhandeln", die eine reibungslose Funktion erlaubt. Zu diesem Zweck wird das sogenannte Spanning Tree Protocol (STP, IEEE 802.1d) verwendet. Überflüssige Verbindungen im Netz werden automatisch deaktiviert und nur dann wieder aktiviert, wenn die per STP ermittelte primäre Verbindung nicht verfügbar ist.

Hierzu muss jedem Switch eine Prioritätsinformation und eine eindeutige MAC-Adresse zugewiesen sein, es muss eine Multicast-Adresse für alle Switches existieren und jeder Port über eine ID eindeutig identifizierbar sein.

VLAN

Um den Broadcast-Verkehr in einem "geswitchten" Netz einzuschränken, lassen sich virtuelle Netze (VLANs) bilden. Hierbei wird innerhalb eines physikalischen Netzes eine logische Netzstruktur abgebildet, in dem funktionell zusammengehörende Arbeitsstationen und Server zu einem virtuellen Netz verbunden werden. Die Gründe für den Zusammenschluss zu einem VLAN können organisatorischer oder technischer Art sein. Unter dem

Aspekt der Unternehmensorganisation ist es beispielsweise möglich, alle Mitarbeiter einer Abteilung in eine Netzgruppe zusammenzufassen, auch wenn sie auf verschiedenen Etagen verteilt sind. Unter dem Aspekt der Arbeitsorganisation können Mitarbeiter, die gemeinsam an einem Projekt arbeiten, zu einer Netzgruppe zusammengefasst werden, auch wenn sie zu verschiedenen Abteilungen gehören.

Jedes VLAN bildet eine separate Broadcast-Domäne. Ein VLAN braucht nicht auf einen einzelnen Switch beschränkt zu sein, sondern es kann sich über ein ganzes geswitchtes Netz erstrecken. Die Netzbenutzer bilden dann nicht mehr aufgrund ihres Standortes ein Netzsegment, sondern sie können innerhalb des Intranets standortunabhängig mit anderen Nutzern zu einer Gruppe zusammengefasst werden.

Es wird zwischen port- und hostbasierten VLANs unterschieden. Bei portbasierten VLANs werden einzelne Anschlüsse (Ports) an einem Switch direkt einem VLAN zugeordnet. Das bedeutet, dass der zugeordnete Anschluss unabhängig von der angeschlossenen Station fest einem bestimmtem VLAN zugeordnet ist. Bei hostbasierten VLANs wird die Zugehörigkeit eines VLANs beispielsweise über die MAC-Adresse oder IP-Adresse der angeschlossenen Station gesteuert. Bei hostbasierten VLANs hat der Anwender die Möglichkeit, sein Endgerät an jedem beliebigen Ort innerhalb des Netzes anzuschließen, ohne dass er die Zugehörigkeit zu seinem VLAN verliert.

Trunking

Die Möglichkeit, VLANs über mehrere Switches auszudehnen, wird als Trunking bezeichnet. Hierbei wird pro Switch ein physischer Port für die Inter-Switch-Kommunikation reserviert, die logische Verbindung zwischen den Switches wird als Trunk bezeichnet. Trunking wird durch unterschiedliche, teils proprietäre Trunking-Protokolle realisiert. Der Ethernet-Rahmen wird beim Informationsaustausch zwischen den Switches in das Trunking-Protokoll gekapselt. Dadurch ist der Ziel-Switch in der Lage, die Information dem entsprechenden VLAN zuzuordnen. Als Standards werden IEEE 802.1q und beispielsweise die proprietären Protokolle ISL (Inter Switch Link) und VTP (VLAN Trunking Protokoll) des Herstellers Cisco verwendet.

Vorsicht Begriffsverwirrung

Manchmal wird auch die Bündelung (Zusammenfassung) mehrerer physikalischer Verbindungen zwischen Switches zur Erzielung entsprechend höherer Durchsatzraten als Trunking bezeichnet. Diese Funktionalität wird andererseits auch als "Channel Bonding" oder "Channeling" bezeichnet. Wenn in einem Dokument der Begriff Trunking auftaucht, so muss deswegen stets darauf geachtet werden, in welcher Bedeutung der Begriff gerade verwendet wird. Hier wird unter Trunking stets die Möglichkeit verstanden, VLANs über mehrere Switches zu verteilen.

Die folgende Abbildung zeigt eine Konfiguration mit zwei Switches, die über einen Trunk-Port verbunden sind. Der Rechner, der am linken Switch ebenfalls an einem Trunk-Port angeschlossen ist, stellt ein potentielles Sicherheitsrisiko dar, da er Zugriff auf die Daten aus allen VLANs hat, die auf dem Switch konfiguriert sind.

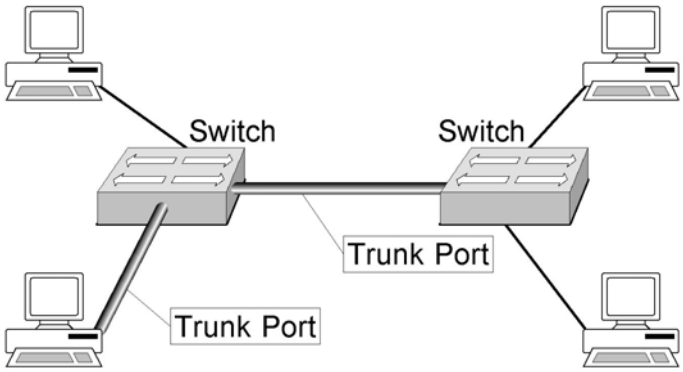


Abbildung: Trunking

Erstreckt sich ein VLAN über mehrere Switches, so steigt in der Praxis der Datenverkehr zwischen diesen Komponenten um den Anteil der mit Hilfe des Trunking- Protokolls übertragenen Informationen. Die Kommunikation zwischen Teilnehmern unterschiedlicher VLANs erfolgt über OSI-Schicht 3, das heißt die Pakete werden VLAN übergreifend geroutet. Das Routing kann auf einem Switch durchgeführt werden, der Routing-Funktionen unterstützt (siehe auch den Abschnitt zu Layer-3-Switches in der Einleitung zum Baustein B 3.302 *Router und Switches*), oder auf einem angeschlossenen Router erfolgen, der die VLANs auf der OSI-Schicht 3 verbindet.

Die folgenden Abbildungen zeigen Beispiele für ein (port-basiertes) VLAN, das sich über drei verschiedene Etagen eines Gebäudes erstreckt und für eine Konfiguration mit zwei verschiedenen VLANs auf einem Switch.

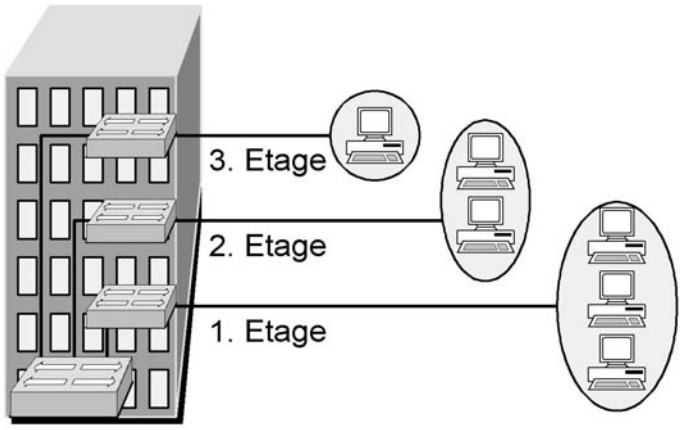


Abbildung: Beispiel für ein VLAN

Entgegen den Aussagen einiger Hersteller muss berücksichtigt werden, dass VLANs nicht entwickelt wurden, um Sicherheitsanforderungen bei der Trennung von Netzen zu erfüllen. VLANs bieten eine Vielzahl von Angriffspunkten, so dass insbesondere für die Trennung von schutzbedürftigen Netzen immer zusätzliche Maßnahmen umzusetzen sind. In der folgenden Beispiel-Abbildung kann nicht von einer sicheren Trennung zwischen dem VLAN 1 und VLAN 2 ausgegangen werden, da die beiden VLANs auf dem selben Switch realisiert sind.

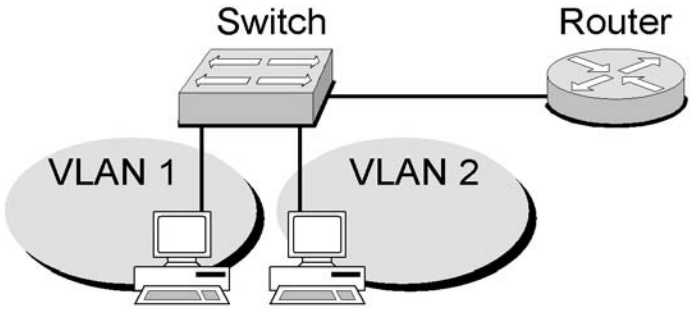


Abbildung: Zwei VLANs auf einem Switch

Auf einem Switch sollten keine VLANs mit unterschiedlichem Schutzbedarf konfiguriert sein. Soll dies aus wichtigen Gründen trotzdem geschehen, so müssen in jedem Fall zusätzliche Sicherungsmaßnahmen ergriffen werden, um ein angemessenes Sicherheitsniveau zu gewährleisten. Keinesfalls darf das Netz einer DMZ, die zwischen dem internen Netz und dem Internet steht, als VLAN auf dem selben Switch wie das interne Netz konfiguriert sein.

In der folgenden Abbildung wurde eine sichere Trennung von zwei VLANs mit unterscheidlichem Schutzbedarf realisiert, indem pro Switch lediglich ein VLAN konfiguriert wurde. Die Kopplung der Netze wird von einem Router übernommen, der als Paketfilter fungiert.

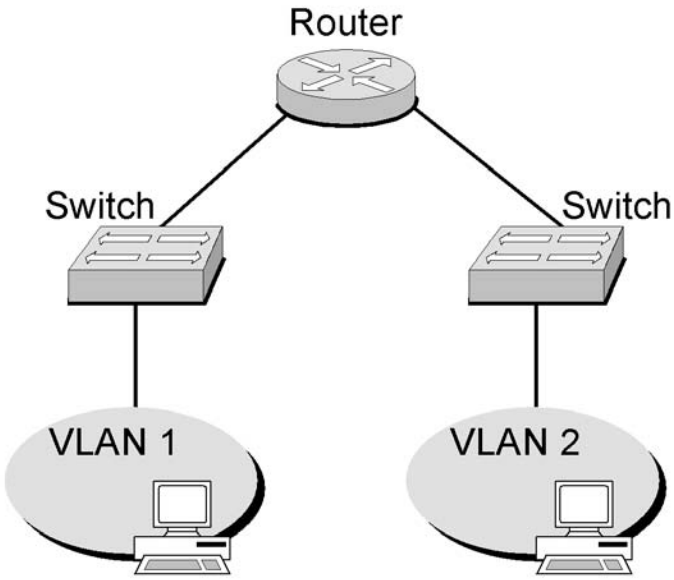


Abbildung: Sichere Trennung von VLANs

Ergänzende Kontrollfragen:

- Existieren VLANs mit unterschiedlichem Schutzbedarf? Falls ja: Wie ist die Trennung der VLANs realisiert?

M 2.278 Typische Einsatzszenarien von Routern und Switches

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Der Einsatzzweck von Routern bestimmt maßgeblich die Konfiguration der Systeme. Zudem bestimmt die Verwendung auch die zusätzlichen Funktionen, die von einem Router bereit gestellt werden müssen.

Router im internen Netz

Router sind in vielen Installationen als reine LAN-to-LAN-Router im Einsatz, um Subnetze zu verbinden und die Nebeneffekte von rein "geswitchten" Netzen, beispielsweise sogenannte Broadcast-Stürme, zu verhindern. In dieser Funktion werden heute allerdings vermehrt Switches mit integrierter Routing-Funktion (Layer-3- oder Layer-4-Switches, siehe auch M 2.277 *Funktionsweise eines Switches*) eingesetzt. Bei diesem Einsatzszenario hängen die Sicherheitsanforderungen an den Router stark vom Schutzbedarf der Teilnetze ab, die über den Router verbunden sind.

Router zur Anbindung an externe Netze

Wird ein Router zur Anbindung des eigenen Netzes einer Organisation an externe Netze eingesetzt, so spricht man von einem Border-Router. Oft sind Border-Router auch in ein Sicherheits-Gateway integriert und übernehmen in diesem die Funktion des externen Paketfilters (siehe unten). Bei Routern, die an fremde Netze angeschlossen sind, spielt die Sicherheit des Gerätes eine besonders wichtige Rolle, da sie Angriffen von außen direkt ausgesetzt sind.

Router als Paketfilter

Router werden oft als Bestandteil von Sicherheits-Gateways zum Anschluss an öffentliche Netze (beispielsweise das Internet) verwendet. Im folgenden Beispiel besteht das Sicherheits-Gateway aus einem internen Paketfilter, einem externen Paketfilter und einem Applikations-Gateway. Statt Applikations-Gateways werden oft auch Stateful-Inspection-Systeme als zentrale Teile von Sicherheits-Gateways eingesetzt. Die festgelegten Filterregeln werden sowohl auf dem zentralen System als auch auf den Routern (intern und extern) konfiguriert. Auf den Routern wird das Regelwerk durch die Einrichtung von Access Control Lists (ACLs) etabliert.

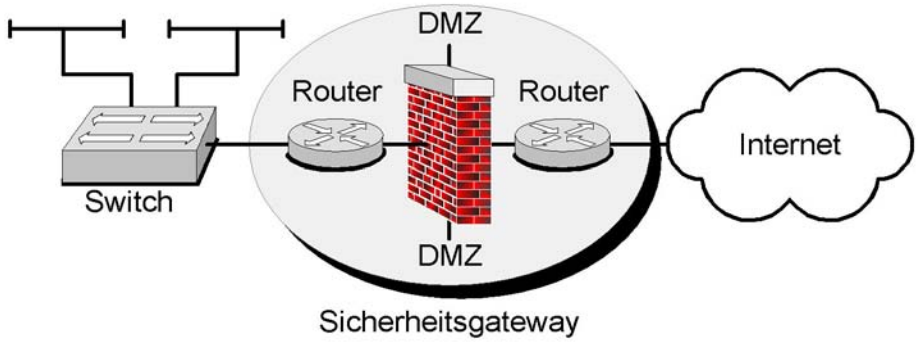


Abbildung 1: Router als Paketfilter

Die Funktion der Paketfilterung ist bei den meisten Routern bereits im Betriebssystem integriert. Es gibt auch Router, die bereits eine integrierte Stateful-Inspection-Firewall bereitstellen.

Es ist empfehlenswert, das Management der beteiligten Systeme (speziell die Einrichtung von Filterregeln) mit Hilfe einer einheitlichen Benutzeroberfläche durchzuführen. Dies hilft Konfigurationsfehler zu vermeiden, die beispielsweise Sicherheitslöcher im Sicherheits-Gateway öffnen oder zu Störungen des Netzbetriebs führen können.

Anforderungen an einen Router für diesen Einsatzzweck sind in M 2.73 *Auswahl eines geeigneten Firewall-Typs* zu finden.

Weiterhin sind bei der Konfiguration Vorgaben aus M 4.203 *Konfigurations-Checkliste für Router und Switches* als Mindestvoraussetzung zu berücksichtigen. Der äußere Paketfilter im aufgeführten Beispiel ist direkt an ein öffentliches Netz angeschlossen und damit einem erhöhten Risiko ausgesetzt. Deshalb muss dieser Router besonders restriktiv konfiguriert sein.

Anbindung von Außenstellen

Router können zur Anbindung von Außenstellen genutzt werden. In der nachfolgenden Abbildung dienen die dargestellten Router zur Kopplung von lokalen Netzen (LAN), die einen einheitlichen Schutzbedarf haben und unter einer einheitlichen Administrationsverantwortung stehen. In diesen Fällen werden zumeist keine oder nur schwache Filterregeln auf den Routern konfiguriert. In kleinen Netzen können statische Routen verwendet werden, während in mittleren oder großen Umgebungen Interior Gateway Protokolle als Routing-Protokolle eingesetzt werden. Die beteiligten Router sind somit Bestandteil einer abgeschlossenen Routing-Domäne. Als Verbindungstechnologien können ATM, Frame Relay, ISDN, DSL oder Standardfestverbindungen genutzt werden.

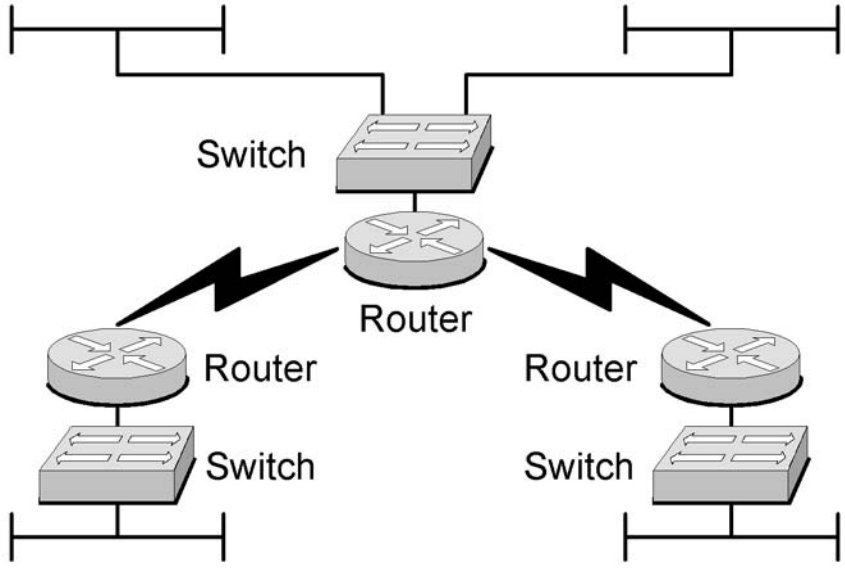


Abbildung 2: Anbindung von Außenstellen

Remote Access

In kleinen und mittleren Netzen werden Router oftmals auch zur Einwahl in lokale Netze (LAN) verwendet. Einwahlmöglichkeiten sollten jedoch nicht direkt in ein LAN integriert werden, sondern es sollte zumindest ein Einwahl-Router eingesetzt werden, der entsprechende Sicherheitsfunktionalität bietet, um das LAN vor Angriffen über die Einwahlzugänge zu schützen.

Ein möglicher Weg zur Absicherung einer Einwahl mit Hilfe eines Routers ist in der folgenden Abbildung dargestellt. Der Router wird in der DMZ eines Sicherheits-Gateways betrieben. Zusätzliche Sicherheit wird durch die Authentisierung mit Hilfe eines RADIUS-Servers erreicht. Der Router fungiert in diesem Fall als RADIUS-Client. Remote-User authentisieren sich nicht direkt am Router, sondern am RADIUS-Server. Dadurch können Benutzer zentral am RADIUS-Server verwaltet werden.

Durch die Verwendung eines One-Time-Passwort-Verfahrens (OTP) in Kombination mit einem Hardware-Token oder einer Smart-Card, wird eine starke Authentisierung erreicht. RADIUS-Server unterstützen in der Regel die Erweiterung von OTP-basierenden Verfahren durch die Installation von Plug-Ins oder durch die Kommunikation mit einem OTP-Server. Eine weitere Möglichkeit zur Erreichung einer starken Authentisierung ist die Einbindung der Remote-Access-Lösung in eine bestehende Public Key Infrastructure (PKI). Der RADIUS-Server muss in diesem Fall für den Zugriff auf einen Verzeichnisdienst konfiguriert sein. Dadurch lässt sich in Kombination mit einer Smart-Card eine zertifikatsbasierende starke Verschlüsselung erreichen. Weiterführende Maßnahmen sind im Baustein B 4.4 *Remote Access* und B 4.5 *LAN-Anbindung eines IT-Systems über ISDN* beschrieben.

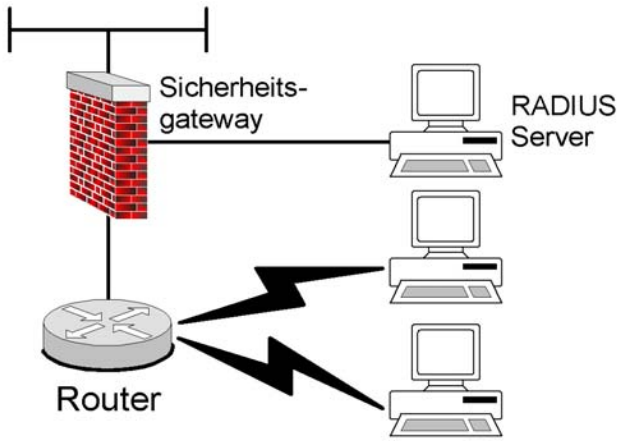


Abbildung 3: Remote Access

VPN

Eine weitere Möglichkeit Standorte sicher miteinander zu verbinden, ist die Nutzung von virtuellen privaten Netzen (VPN). Ein VPN ist ein gesicherter Tunnel, der über bestehende Netzinfrastrukturen geführt wird. Somit ermöglicht der Einsatz von VPNs eine sichere Übertragung von vertraulichen Informationen über unsichere Netze (z.B. das Internet). Der Datenverkehr zwischen zwei Endpunkten innerhalb eines VPN wird verschlüsselt. VPN-

fähige Router sollten eine starke Verschlüsselung (z.B. 3DES, AES) unterstützen. Viele am Markt verfügbare Router unterstützen die VPN-Funktionalität.

IPSec ist ein Standard, der über eine Reihen von RFCs und Internet-Drafts der IEEE definiert wird. Auf der Basis von IPSec lassen sich VPNs zwischen Geräten unterschiedlicher Hersteller konfigurieren. IPSec stellt die Datenvertraulichkeit, Datenintegrität und die Authentisierung zwischen den Endpunkten des VPN sicher. IPSec basiert auf der Netzschicht des OSI-Referenzmodells. Es nutzt das Internet Key Exchange (IKE) zur Ausführung der Protokoll-Algorithmusvereinbarung entsprechend der lokalen Konfiguration und zur Erzeugung der Verschlüsselungs- und Authentisierungsschlüssel. Eine weitere VPN-Technologie, die auf einem Standard beruht, ist das sogenannte "SSL-VPN", bei dem der Datenverkehr über eine mit SSL/TLS gesicherte Verbindung geleitet wird.

Neben VPNs auf der Basis von IPSec und SSL existieren verschiedene andere, sowohl proprietäre, als auch Open Source Technologien. Dabei muss beachtet werden, dass diese meist untereinander nicht kompatibel und teilweise nur für bestimmte Plattformen verfügbar sind.

Falls die beteiligten Komponenten die Einbindung in eine bestehende PKI ermöglichen, kann dadurch die Verwaltung von VPNs (speziell das Schlüsselmanagement) wesentlich erleichtert und die Skalierbarkeit verbessert werden.

Site-to-Site und Client-to-Site VPN

Es wird zwischen einem Site-to-Site-VPN und einem Client-to-Site-VPN unterschieden. Ein Site-to-Site-VPN dient zur Verbindung von Netzen. Dabei wird das VPN auf beiden Seiten durch entsprechend konfigurierte, VPN-fähige Router begrenzt. Diese Art von VPNs ist eine Alternative zur Verbindung von lokalen Netzen über Weitverkehrsstrecken.

Bei einem Client-to-Site-VPN wird ein VPN zwischen einem Client und einem VPN-fähigen Router aufgebaut. Dazu muss auf dem Client meist eine herstellerspezifische VPN-Client-Software installiert werden. Ein Client-to-Site-VPN ist als eine weitere Alternative des Remote-Zugangs zu lokalen Netzen anzusehen.

In der folgenden Abbildung ist beispielhaft eine VPN-Architektur dargestellt.

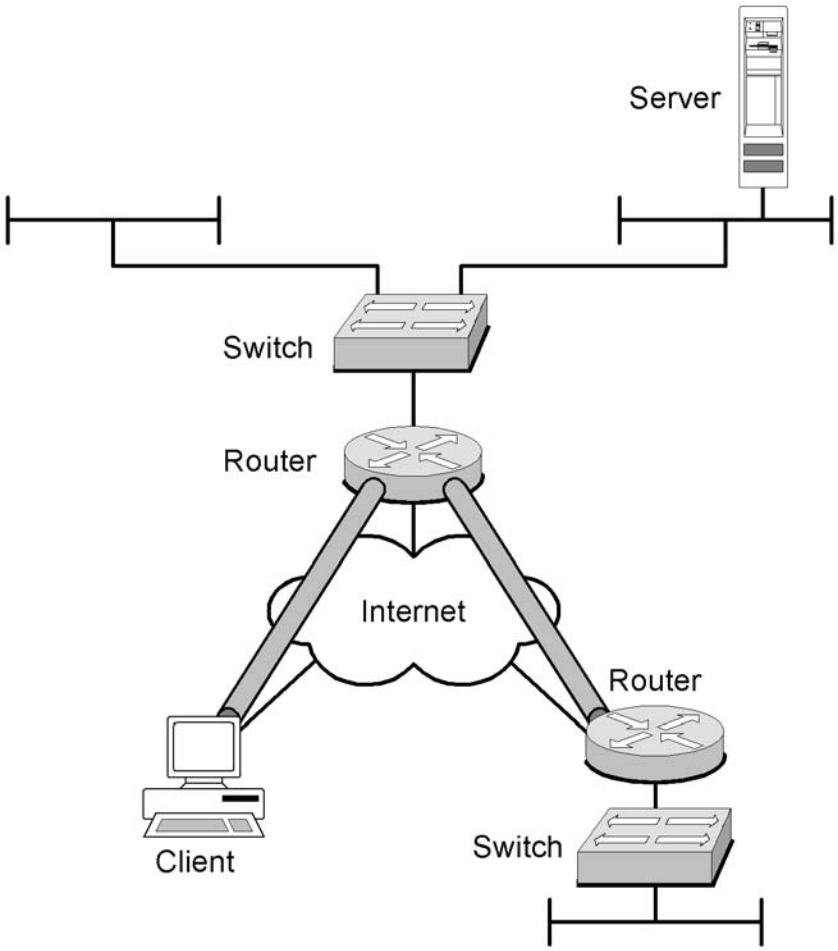


Abbildung 4: Beispiel für eine VPN-Architektur

Switches

Der Einsatzzweck eines Switches zur Bildung von VLANs ist in der Maßnahme M 2.277 *Funktionsweise eines Switches* beschrieben. Die folgende Abbildung zeigt ein typisches geswitchtes Netz.

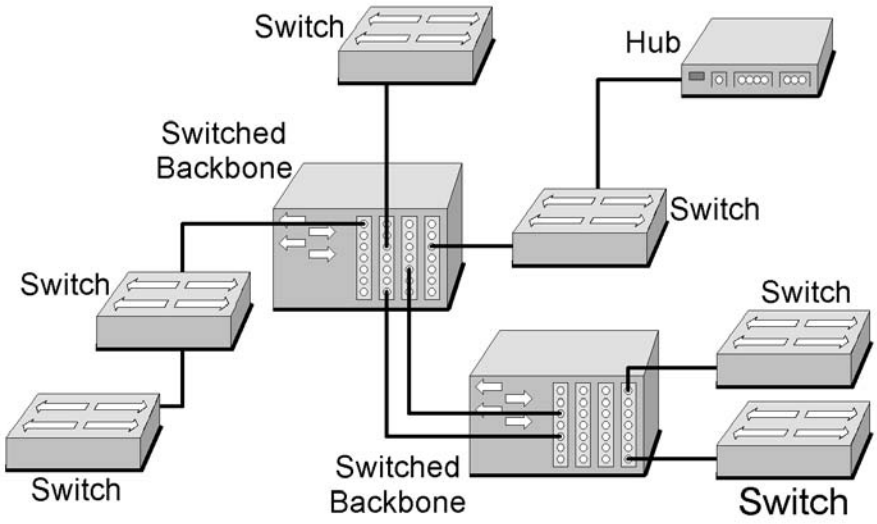


Abbildung 5: Geswitchtes Netz mit Backbone- und Access-Switches

In der Abbildung sind zwei Arten von Switches zu unterscheiden. Die Access-Switches, die sich durch eine hohe Anzahl von Anschlüssen (Ports) auszeichnen, stellen den unmittelbaren Anschluss der Endgeräte sicher. Die Access-Switches sind wiederum an zentrale Backbone-Switches angeschlossen.

Die Backbone-Switches bilden das so genannte Switched-Backbone. Ein Switched-Backbone bündelt die Bandbreite der angeschlossenen Switches, um eine hohe Durchsatzrate zwischen den Endgeräten sicherzustellen. Ein Switched-Backbone zeichnet sich also durch eine hohe Durchsatzrate aus. Der Durchsatz eines Switched-Backbones hängt von einigen Faktoren ab, die bei der Anschaffung von Geräten zu berücksichtigen sind. Die wichtigsten Faktoren sind der maximale Adresscache zur Vorhaltung der dynamisch erlernten MAC-Adressen, der Durchsatz der Backplane eines Backbone-Switches sowie die Leitungsgeschwindigkeit des Switched-Backbone.

Die beteiligten Switches müssen in einer Architektur ähnlich der Abbildung dynamisch erlernte Switching-Tabellen austauschen, um die Verbindung zwischen Endgeräten, die an unterschiedlichen Switches angeschlossen sind, effizient herstellen zu können. Dies geschieht mit zumeist herstellerabhängigen (proprietären) Protokollen (z. B. Cisco Discovery Protocol CDP).

In großen geswitchten Netzen werden Switches typischerweise kaskadiert. Dies wird in der Praxis mit Hilfe des sogenannten Uplink-Ports erreicht.

Ergänzende Kontrollfragen:

- Ist der Einsatzzweck der zu beschaffenden Netzkomponente definiert?
- Wo soll der Router eingesetzt werden?

- Welche Funktionen (VPN, Remote Access, Paketfilterung) soll der Router unterstützen?
- Wurden Anforderungen für den Einsatz der Router definiert?

M 2.279 Erstellung einer Sicherheitsrichtlinie für Router und Switches

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Da Router und Switches zentrale Elemente eines Netzes sind, ist der sichere und ordnungsgemäße Betrieb besonders wichtig. Dieser kann nur sichergestellt werden, wenn das Vorgehen in die bestehenden sicherheitstechnischen Vorgaben integriert ist.

Die zentralen sicherheitstechnischen Anforderungen (das zu erreichende Sicherheitsniveau) ergeben sich aus der organisationsweiten Sicherheitsleitlinie und sollten in einer spezifischen Sicherheitsrichtlinie für Router und Switches formuliert werden, um die übergeordnet und allgemein formulierte Sicherheitsleitlinie im gegebenen Kontext zu konkretisieren und umzusetzen.

In diesem Zusammenhang ist zu prüfen, ob neben der organisationsweiten Sicherheitsleitlinie weitere übergeordnete Vorgaben wie bspw. IT-Richtlinien, Passwortrichtlinien oder Vorgaben zur Internetnutzung zu berücksichtigen sind.

Die Sicherheitsrichtlinie muss allen Personen und Gruppen, die an der Beschaffung und dem Betrieb von Routern und Switches beteiligt sind, bekannt sein und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die Sicherheitsrichtlinie sollte zunächst das generell zu erreichende Sicherheitsniveau spezifizieren und grundlegende Aussagen zum Betrieb von Routern und Switches treffen. Nachfolgend sind einige Punkte aufgeführt, die berücksichtigt werden sollten:

- Allgemeine Konfigurationsstrategie ("Liberal" oder "Restriktiv")
- Regelungen für die Arbeit der Administratoren und Revisoren:
  - Über welche Zugangswege dürfen Administratoren und Revisoren auf die Syteme zugreifen (beispielsweise nur lokal an der Konsole, über ein eigenes Administrationsnetz oder über verschlüsselte Verbindungen)?
  - Welche Vorgänge werden müssen dokumentiert werden? In welcher Form wird die Dokumentation erstellt und gepflegt?
  - Gilt für bestimmte Änderungen ein Vieraugenprinzip?
  - Nach welchem Schema werden Administrationsrechte vergeben?
- Vorgaben für Beschaffung von Geräten anhand eines Anforderungsprofils
- Vorgaben für die Installation und Konfiguration
  - Vorgehen bei der Erstinstallation

  - Überprüfung der Default-Einstellungen hinsichtlich Sicherheitsgefährdungen
  - Regelungen zur physikalischen Zugriffskontrolle
  - Verwendung und Konfiguration von Konsole und sonstigen Zugriffsarten
  - Regelungen zur Benutzer- und Rollenverwaltung, Berechtigungsstrukturen (Ablauf und Methoden der Authentisierung und Autorisierung, Berechtigung zu Installation, Update, Konfigurationsänderungen etc.). Nach Möglichkeit sollte ein Rollenkonzept für die Administration erarbeitet werden.
  - Regelungen zur Einrichtung und Nutzung von VLANs und VPNs (beispielsweise: keine VLANs mit unterschiedlichem Schutzbedarf auf einem Switch)
  - Regelungen zu Erstellung und Pflege von Dokumentation, Form der Dokumentation: Verfahrensanweisungen, Betriebshandbücher
  - Falls allgemeine Vorgaben existieren: Zugelassene und nicht zugelassene Dienste, Protokolle und Netze
- Vorgaben für den sicheren Betrieb
  - Absicherung der Administration (beispielsweise: Zugriff nur über abgesicherte Verbindungen)
  - Einsatz von Verschlüsselung (Standards, Schlüsselstärken, Einsatzbereiche)
  - Vorgaben zu Passwortnutzung (Passwortregeln, durch Passwörter zu schützende Bereiche, Regeln und Situationen für Passwortänderungen, gegebenenfalls Hinterlegung von Passwörtern)
  - Werkzeuge für Betrieb und Wartung, Integration in ein bestehendes Netzmanagement
  - Berechtigungen und Vorgehensweisen bei Softwareupdates und Konfigurationsänderungen
- Protokollierung
  - Welche Ereignisse werden protokolliert?
  - Wo werden die Protokolldateien gespeichert?
  - Wie und in welchen Abständen werden die Protokolle ausgewertet?
- Datensicherung und Recovery (siehe auch M 6.91 *Datensicherung und Recovery bei Routern und Switches*)
  - Einbindung in das organisationsweite Datensicherungskonzept
- Störungs- und Fehlerbehandlung, Incident Handling
  - Regelungen für die Reaktion auf Betriebsstörungen und technische Fehler (lokaler Support, Fernwartung)
  - Regelungen für Sicherheitsvorfälle

  - Notfallvorsorge (siehe auch M 6.92 *Notfallvorsorge bei Routern und Switches*)
  - Einbindung in das organisationsweite Notfallvorsorgekonzept
- Revision und Audit (Verantwortlichkeiten, Vorgehen, Integration in ein übergreifendes Revisionskonzept)

Die Verantwortung für die Sicherheitsrichtlinie liegt beim IT-Sicherheitsmanagement, Änderungen und Abweichungen hiervon dürfen nur in Abstimmung mit dem IT-Sicherheitsmanagement erfolgen.

Bei der Erstellung einer Sicherheitsrichtlinie ist es empfehlenswert, so vorzugehen, dass zunächst ein Maximum an Forderungen und Vorgaben für die Sicherheit der Systeme aufgestellt wird. Diese können anschließend den tatsächlichen Gegebenheiten angepasst werden. Idealerweise wird so erreicht, dass alle notwendigen Aspekte berücksichtigt werden. Für jede im zweiten Schritt verworfene oder abgeschwächte Vorgabe sollte der Grund für die Nicht-Berücksichtigung dokumentiert werden.

Ergänzende Kontrollfragen:

- Wurde eine Sicherheitsrichtlinie für den Betrieb von Routern und Switches erstellt?
- Wann wurde die Sicherheitsrichtlinie zum letzten Mal aktualisiert?
- Wurde ein Sicherheitsniveau in der Sicherheitsrichtlinie definiert?
- Wurden in der Sicherheitsrichtlinie Vorgaben zur Einrichtung, zum Betrieb und zur Störungsbehandlung von Routern und Switches beschrieben?
- Wurden in der Sicherheitsrichtlinie unterschiedliche Einsatzzwecke der Komponenten berücksichtigt?

M 2.280 Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Aktive Netzkomponenten unterscheiden sich in ihrem Leistungsumfang, den angebotenen Sicherheitsmechanismen, Bedienkomfort und Wirtschaftlichkeit. Werden bei der Beschaffung Fehler gemacht, so kann dies schwerwiegende Folgen auf den sicheren Betrieb eines Netzes haben, da mit ungeeigneten Geräten das angestrebte Sicherheitsniveau unter Umständen nur schwer erreichbar ist.

Bevor Router und Switches beschafft werden, muss daher eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Aufgrund der Bewertung kann dann eine fundierte Kaufentscheidung erfolgen, die sicherstellt, dass das zu beschaffende Produkt im praktischen Betrieb den Anforderungen genügt.

Zentrale Sicherheitsanforderungen

Aus dem Blickwinkel der IT-Sicherheit sind zentrale Anforderungen an aktive Netzkomponenten, dass diese die Administration über sichere Protokolle erlauben und dass die Benutzerverwaltung des Geräts es erlaubt, das organisationsweite Rollenkonzept entsprechend umzusetzen. Die Anforderung, dass Passwörter nur verschlüsselt im Gerät gespeichert werden dürfen, sollte eigentlich eine Selbstverständlichkeit sein, jedoch gibt es immer noch Geräte, bei denen Passwörter im Klartext in Konfigurationsdateien gespeichert werden müssen. Bei Neubeschaffungen sollten keine Geräte mehr berücksichtigt werden, die keine sichere Administrationsmöglichkeit bieten und bei denen es nicht möglich ist, Passwörter verschlüsselt abzuspeichern.

Auch rein funktionale Merkmale aktiver Netzkomponenten können Auswirkungen auf die IT-Sicherheit haben. Meist ist dann der Grundwert Verfügbarkeit betroffen, beispielsweise wenn ein Gerät wegen unzureichender Speicherausstattung nicht die erforderlichen Durchsatzraten erreicht. Außerdem spielt die Unterstützung durch den Hersteller eine nicht zu vernachlässigende Rolle, wenn es beispielsweise darum geht, dass zeitnah Patches für Sicherheitslücken zur Verfügung gestellt werden.

Nachfolgend werden einige grundsätzliche Anforderungen bei der Beschaffung von Routern und Switches aufgelistet. Anschließend werden noch einige spezielle Anforderungen getrennt für Router und Switches beschrieben.

Allgemeine Kriterien für Router und Switches

1. Grundlegende funktionale Anforderungen

- Unterstützt das Gerät alle benötigten Protokolle und Verkabelungstypen?

2. Sicherheit

- Unterstützt das System sichere Protokolle zur Administration?

  Wenn Router und Switches nicht über ein eigenes Administrationsnetz administriert werden, müssen diese Geräte mit Hilfe von sicheren Netzprotokollen (beispielsweise SSH2) konfigurierbar sein.

- Unterstützt das System die verschlüsselte Speicherung von Passwörtern?

  Geräte, bei denen Passwörter unverschlüsselt gespeichert werden, sollten nicht mehr beschafft werden.

3. Wartbarkeit

- Bietet der Hersteller regelmäßige Updates und schnell verfügbare Sicherheitspatches an?

  Es ist insbesondere wichtig, dass der Hersteller zeitnah auf bekannt gewordene Sicherheitsmängel reagiert.

- Wird für das Produkt die Möglichkeit des Abschlusses von Wartungsverträgen angeboten?

  Oft ist der Zugriff auf Updates und Unterstützungsleistungen vom Hersteller nur in Verbindung mit einem gültigen Wartungsvertrag möglich.

- Können im Rahmen der Wartungsverträge maximale Reaktionszeiten für die Problembehebung festgelegt werden?

  Ein Wartungsvertrag ist nur dann geeignet, wenn mit den garantierten Reaktions- und Wiederinbetriebnahmezeiten die festgelegten Ansprüche an die Verfügbarkeit der Geräte abgedeckt werden können.

- Bietet der Hersteller einen technischen Kundendienst (Hotline) an, der in der Lage ist, sofort bei Problemen zu helfen?

  Dieser Punkt sollte Bestandteil des abgeschlossenen Wartungsvertrags sein. Beim Abschluss des Vertrags ist auf die Sprache der zur Verfügung gestellten Hotline des Herstellers zu achten.

4. Zuverlässigkeit/Ausfallsicherheit

- Wie zuverlässig und ausfallsicher ist das Produkt?

  Der Hersteller sollte Erfahrungswerte bezüglich der Zuverlässigkeit liefern können, beispielsweise Mean Time Between Failures (MTBF), Mean Time To Repair (MTTR).

- Bietet der Hersteller Hochverfügbarkeitslösungen an?

  Wenn durch den Abschluss von Wartungsverträgen die Verfügbarkeitsanforderungen nicht abgedeckt werden können, muss das System Hochverfügbarkeitslösungen unterstützen.

5. Benutzerfreundlichkeit

- Lässt sich das Produkt einfach installieren, konfigurieren, und administrieren?

  Es sollten darüber hinaus Schulungen für das Produkt angeboten werden.

6. Kosten

- Wie hoch sind die Anschaffungskosten der Geräte?

- Wie hoch sind die voraussichtlichen laufenden Kosten (Wartung, Betrieb, Support)?

Diese Kosten sollten bereits in der Beschaffungsphase mit berücksichtigt werden. Der Inhalt der Wartungs- und Supportverträge sollte geprüft werden (Reaktionszeiten, Hotline, Qualifikation des Personals, etc.).

- Wie hoch sind die voraussichtlichen laufenden Kosten für das Personal?
- Müssen zusätzliche Soft- oder Hardware-Komponenten angeschafft werden (z. B. RADIUS-Server, Netz-Management-System)?

  Diese Frage sollte bereits in der Planungsphase beantwortet werden. Wenn beispielsweise bereits ein Netz-Management-System im Einsatz ist, sollte die Kompatibilität mit den zu beschaffenden Geräten geprüft werden.

  Zudem sollte der Aufwand zur Integration der Geräte in eine bestehende Infrastruktur beachtet werden.
- Wie hoch sind die Kosten für die Schulung von Administratoren?

7. Funktionalität

- Kann das System sicher in die bestehende Netz-Management-Architektur eingefügt werden?

  Der Aufwand zur Integration sollte berücksichtigt werden. Der Hersteller sollte MIB-Tables und Angaben zu den unterstützten NMS-Protokollen liefern.
- Unterstützt das System NTP?

  NTP ist besonders im Hinblick auf die Protokollierung von Bedeutung, siehe auch M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation.*
- Unterstützt das System die Einbindung von Authentisierungsservern (beispielsweise RADIUS oder TACACS+)?

  Ist bereits ein Authentisierungsserver im Einsatz, so sollte das System diesen nutzen können.

8. Protokollierung

- Welche Möglichkeiten der Protokollierung sind vorhanden?

  Die angebotenen Möglichkeiten zur Protokollierung müssen mindestens die in der Sicherheitsrichtlinie festgelegten Anforderungen erfüllen. Insbesondere sind die folgenden Punkte relevant:

  - Ist der Detailgrad der Protokollierung konfigurierbar?
  - Werden durch die Protokollierung alle relevanten Daten erfasst?
  - Unterstützt das System zentrale Protokollierung (z. B. syslog)?

    Router und Switches sollten eine zentrale Protokollierung unterstützen, um eine gezielte Auswertung der Log-Dateien sicherstellen zu können.
- Kann die Protokollierung so erfolgen, dass die Bestimmungen des Datenschutzes erfüllt werden können?
- Werden Alarmierungsfunktionen unterstützt?

Angriffe auf Router und Switches sollten durch Alarmierungsfunktionen der Geräte zentral und zeitnah gemeldet werden. Dies kann beispielsweise auf Basis eines Netz-Management-Systems geschehen.

9. Infrastruktur

- Abmessungen und Kompatibilität mit Schutzschränken

  Auch der Platzbedarf von Routern und Switches ist bei der Beschaffung zu berücksichtigen. Kann das Gerät in die vorgesehenen Schutzschränke eingebaut werden (Formfaktor, Gewicht, Befestigungselemente)?

- Stromversorgung und Abwärme

  Vom Hersteller sollten Angaben zum Stromverbrauch und zu den Anforderungen an die Umgebungstemperatur verfügbar sein. Reicht die vorhandene Kapazität der Stromversorgung und der USV aus? Reicht die vorhandene Kühlleistung zur Abfuhr der Abwärme des Geräts aus?

Besondere Kriterien für Switches

1. Performance und Skalierbarkeit

- Kann das System den Ansprüchen an die Performance gerecht werden?

  Vom Hersteller sollten Angaben zum Datendurchsatz verfügbar sein, insbesondere sollte der Maximal-Durchsatz der Switch-Backplane beachtet werden. Weitere Größen, die Einfluss auf die Performance haben können, sind die Größe des Adress-Cache und des Speichers.

- Wie groß ist die Anzahl der bereitgestellten Ports?

  Ein Access-Switch sollte über eine ausreichende Anzahl von Ports zum Anschluss von Endgeräten verfügen. Oft lassen sich die Anschaffungskosten von unterschiedlichen Switches anhand der Kosten pro Port vergleichen.

- Ist das System "stackable" oder (beispielsweise durch zusätzliche Einschubkarten) modular erweiterbar?

  Zusätzlich erforderliche Funktionen oder der Bedarf an einer höheren Portdichte sollten nicht dazu führen, dass Geräte vorzeitig ausgetauscht werden müssen.

2. Funktionalität

- Unterstützt der Switch Layer-3-Switching (Routing)?

  In lokalen Netzen kann diese Funktion im Hinblick auf die Performance (Datendurchsatz) vorteilhaft sein.

- Unterstützt der Switch VLANs?

  Bei der Nutzung von VLANs sollte der Hersteller Angaben zum verwendeten Standard machen.

- Unterstützt der Switch Cut Through oder/und Store and Forward?

Besondere Kriterien für Router

1. Performance und Skalierbarkeit

- Kann das System den Ansprüchen an die Performance gerecht werden?

  Vom Hersteller sollten Angaben zum Datendurchsatz verfügbar sein. Falls der Router als VPN-Endpunkt eingesetzt werden soll, sind auch die unterstützten Verschlüsselungsverfahren und die Performance beim Ver- und Entschlüsseln der Daten wichtige Performance-Kriterien.

- Ist das Gerät modular erweiterbar?

  Die Anzahl der im Standardumfang bereitgestellten Interfaces, insbesondere die maximale Anzahl von unterstützten Interfaces sollte berücksichtigt werden.

2. Funktionalität

- Unterstützt der Router VPN-Funktionalität?

  Ein Router mit VPN-Funktionalität sollte den IPSec-Standard und starke Verschlüsselungsalgorithmen (3DES, AES) unterstützen.

- Unterstützt der Router die Nutzung von ACLs?

  Die Filterfunktionen der zu beschaffenden Router sind zu berücksichtigen (siehe auch M 5.111 *Einrichtung von Access Control Lists auf Routern*,).

- Welche Routing-Protokolle werden unterstützt?

  Der Router sollte sichere Routing-Protokolle unterstützen (siehe auch M 5.112 *Sicherheitsaspekte von Routing-Protokollen*).

Ergänzende Kontrollfragen:

- Wurden Anforderungen zur Beschaffung von Routern und Switches definiert?
- Wurde dabei auf unterschiedliche Einsatzzwecke der Geräte geachtet?
- Wurden die Anforderungen schriftlich hinterlegt?

M 2.281 Dokumentation der Systemkonfiguration von Routern und Switches

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Konfiguration von Routern und Switches wird meist mittels Konfigurationsdateien vorgenommen, die auf dem Gerät gespeichert sind. Router und Switches besitzen eine Reihe von Konfigurationsoptionen, die für den sicheren Betrieb wichtig sind. Bei der Erstinstallation beziehungsweise im Auslieferungszustand sind diese Einstellungen mit Default-Werten belegt.

Grundkonfiguration dokumentieren

Die Konfiguration, die bei der Inbetriebnahme des Geräts vorgenommen wird, muss so dokumentiert werden, dass sie jederzeit vom Administrator oder seinem Vertreter nachvollzogen werden kann. Insbesondere dann, wenn eine Konfiguration von einem Default-Wert abweicht, sollte in einem Kommentar in der Konfigurationsdatei festgehalten werden, warum die Einstellung so gewählt wurde.

Änderungen dokumentieren

Jede Änderung der Konfiguration sollte vom Administrator nachvollzogen werden können. Es wird empfohlen, mindestens folgende Punkte zu dokumentieren:

- Welche Änderung wurde durchgeführt?
- Warum wurde die Änderung durchgeführt (Anlass)?
- Wann wurde diese Änderung durchgeführt (Uhrzeit, Datum)?
- Wer hat die Änderung durchgeführt?

Die Dokumentation der Änderungen kann ebenfalls durch Kommentare in der Konfigurationsdatei erfolgen. Dabei ist es jedoch in der Regel sinnvoll, zu jeder Option nur die jeweils letzte Änderung in der Datei selbst zu speichern.

Vollständiges Protokoll der sicherheitsrelevanten Änderungen

Zusätzlich dazu sollten zumindest alle sicherheitsrelevanten Konfigurationsänderungen in einem Protokoll gespeichert werden, anhand dessen sich jederzeit nachvollziehen lässt, wie das Gerät zu einem bestimmten Zeitpunkt konfiguriert war. Dieses Protokoll sollte nicht auf dem Gerät selbst gespeichert werden.

Zur Erleichterung der Dokumentation und Protokollierung kann ein Revisions- und Versionskontrollsystem wie beispielsweise CVS eingesetzt werden. Ein solches System bietet den zusätzlichen Vorteil, dass notfalls eine frühere Konfiguration einfach wieder hergestellt werden kann. Netzmanagement-Systeme zur zentralen Administration bieten in der Regel ebenfalls eine integrierte Dokumentations- und Protokollfunktion.

Es ist empfehlenswert, die Dokumentation so zu gestalten, dass sie auch von einem Fachmann, der mit den konkreten Gegebenheiten der Systemlandschaft nicht vertraut ist, nachvollzogen werden kann.

Die Konfigurationsdateien sollten zur Notfallvorsorge zusätzlich zentral auf einem dafür vorgesehenen Server gespeichert werden. Für die zentrale Verwaltung von Konfigurationsdateien werden oft TFTP-Server verwendet. TFTP-Server sollten jedoch nur in einem abgesicherten Administrationsnetz betrieben werden, weil der Dienst TFTP eine Reihe von Schwachstellen

beinhaltet (siehe auch G 2.87 *Verwendung unsicherer Protokolle in öffentlichen Netzen*). Eine Alternative dazu ist die Übertragung per SCP (siehe auch M 5.64 *Secure Shell*).

Ergänzende Kontrollfragen:

- Werden Konfigurationsdateien zentral verwaltet?
- Werden Konfigurationsdateien hinsichtlich der oben genannten Punkte dokumentiert?
- Wird ein Versionskontrollsystem eingesetzt?

M 2.282 Regelmäßige Kontrolle von Routern und Switches

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Zur Sicherstellung des ordnungsgemäßen Betriebs der aktiven Netzkomponenten und der Korrektheit aller Konfigurationsparameter ist ein regelmäßiger, möglichst automatisierter, Kontrollprozess zu etablieren. Hierzu gehören beispielsweiseregelmäßige Funktionstests, Veranlassen von Änderungen und Prüfung der Umsetzung sowie die Überprüfung der Logfiles und Alarme.

Um die im laufenden Betrieb entstehende große Menge an relevanten Daten effektiv verarbeiten zu können, ist meist der Einsatz geeigneter Werkzeuge für eine möglichst weit automatisierte Kontrolle erforderlich. Dies kann beispielsweise durch die Einbindung in ein Netzmanagementsystem (NMS) geschehen.

Checkliste für die Kontrolle

Für die Kontrolle kann die Checkliste in M 4.203 *Konfigurations-Checkliste für Router und Switches* verwendet werden. Als Basis sollte die erstellte Sicherheitsrichtlinie für Router und Switches dienen (siehe M 2.279 *Erstellung einer Sicherheitsrichtlinie für Router und Switches*). Zusätzlich sollten folgende Punkte im Rahmen des Kontrollprozesses berücksichtigt werden:

Was wird getestet bzw. kontrolliert?

- Die generelle Funktionsfähigkeit von Geräten wird im Normalfall regelmäßig durch den Administrator im laufenden Betrieb geprüft.
- Die Integrität von Konfigurationsdateien sollte in regelmäßigen Abständen geprüft werden. Die Sicherheitsrichtlinie für Router und Switches sollte eine regelmäßige Überprüfung mit Festlegung von Verantwortlichkeiten vorschreiben.
- Der Stand der Datensicherung (zentral gespeicherte Konfigurationsdateien) sollte regelmäßig vom Administrator geprüft werden.
- Die Systemdokumentation sollte laufend vom Administrator aktualisiert werden. Die Aktualität kann im Rahmen von Audits geprüft werden.

Hierzu sind auch M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile* und M 2.64 *Kontrolle der Protokolldateien* zu berücksichtigen.

Wie wird getestet?

- Durch die Einbindung der Komponenten in ein Netzmanagement-System kann eine regelmäßige Kontrolle sichergestellt werden. Sicherheitsverletzungen, Ausfälle und Fehlfunktionen können mit Hilfe von Alarmierungsfunktionen des NMS zeitnah erkannt werden.
- Im Rahmen von Audits erfolgt meist eine stichprobenartige Kontrolle von Komponenten. Als Basis für ein Audit dient die erstellte Sicherheitsrichtlinie für Router und Switches. Wichtiger Bestandteil einer

solchen Untersuchung ist die Aktualität der Systemdokumentation, Stand der Datensicherung, Passwortwechsel, etc. Unter Zuhilfenahme der Checkliste aus M 4.203 *Konfigurations-Checkliste für Router und Switches* kann ein Großteil der sicherheitsrelevanten Einstellungen abgefragt werden.

- Es existiert eine Reihe frei verfügbarer Sicherheits-Tools (z. B. Nessus), welche die Sicherheitseinstellungen auf Routern und Switches prüfen können. Solche Tools können auf einem Rechner im Netz installiert sein. Es sollte nach Möglichkeit die aktuellste Version verwendet werden. Als Betriebssystem ist oft Unix bzw. Linux notwendig. Von diesem System aus kann der Administrator entsprechende Router und Switches scannen, um somit eine Vielzahl von Einstellungen dieser Geräte zu prüfen. Kommerzielle Tools bieten teilweise recht komfortable Auswertungen und Möglichkeiten zur Historienverfolgung der durchgeführten Scans.
- Eine Vielzahl von Sicherheitsunternehmen bieten regelmäßige Überprüfungen von Routern und Switches an. Durch turnusmäßige Berichte und Auswertungen erhält der Betreiber einen Überblick über den Zustand der Komponenten.

Wann wird getestet?

- Der Administrator prüft laufend und meist automatisiert die Funktion der Geräte mit Hilfe eines NMS-Systems. Die Systemdokumentation ist vom Administrator laufend aktuell zu halten.
- Der Stand der Datensicherung, die Integrität der Konfigurationsdateien und weitere Daten zur Konfiguration sollten vom Administrator regelmäßig (wöchentlich) geprüft werden.
- Scans mit der Hilfe von Sicherheits-Tools sollten nach Installation regelmäßig (monatlich) durch den Administrator vorgenommen werden. Die Ergebnisse sind zu prüfen und zu archivieren.
- Die Prüfung der Einhaltung von Sicherheitsrichtlinien muss regelmäßig erfolgen (z. B. jährlich im Rahmen von Sicherheits- oder Grundschutzaudits).

Wer testet?

- Der Administrator sollte laufend Prüfungen durchführen (Funktion der Komponenten, Stand der Datensicherung, Integrität der Konfigurationsdateien, Scans, etc.).
- Die Einhaltung von Sicherheitsrichtlinien bzw. von Sicherheitsmaßnahmen im Rahmen von Sicherheits- bzw. Grundschutzaudits darf nicht durch den Administrator geprüft werden, sondern hat abhängig vom etablierten Sicherheitsmanagementprozess durch einen Auditor, IT-Sicherheitsbeauftragten oder Revisor zu erfolgen.

Welche Informationen bilden die Grundlage der Kontrolle?

- Sicherheitsrichtlinie für Router und Switches
- Protokolldateien von Routern und Switches

- Systemdokumentation (siehe M 2.281 *Dokumentation der Systemkonfiguration von Routern und Switches*)
- IT-Sicherheitskonzept
- IT-Grundschutz-Kataloge
- Ergebnisse von durchgeführten Scans

Überprüfung der Konfiguration

Bei der Einrichtung der Router und Switches sind alle Default-Einstellungen zu prüfen und falls notwendig zu modifizieren. Hierbei werden beispielsweise nicht benötigte Dienste deaktiviert und Voreinstellungen den betrieblichen und sicherheitstechnischen Anforderungen angepasst. Eine Erläuterung der hierfür notwendigen Schritte findet sich in M 4.201 *Sichere lokale Grundkonfiguration von Routern und Switches* und M 4.202 *Sichere Netz-Grundkonfiguration von Routern und Switches*.

Die Umsetzung der Vorgaben zum Umgang mit Default-Einstellungen sind im Rahmen von regelmäßigen Audits zu überprüfen. Hierdurch können versehentliche oder vorsätzliche Veränderungen festgestellt und die Umsetzung von aktuellen Empfehlungen der Hersteller verifiziert werden. Dies kann ausgehend von der für jeden Gerätetyp beziehungsweise für jede Betriebssystemversion zu erstellenden Installationsanleitung erfolgen und sollte am jeweiligen Gerät verifiziert werden. Hierbei ist jedoch zu beachten, dass Betriebssystem-Kommandos bei manchen Herstellern nicht alle Default-Einstellungen anzeigen. Aus diesem Grund empfiehlt es sich, separate Software-Tools einzusetzen, um eine vollständige Analyse durchzuführen.

Für einen umfassenden Test aller Geräte können Softwareprodukte eingesetzt werden, die einen automatisierten Test mit konfigurierbaren Parametern ermöglichen.

Mirror Port

Zur Analyse des Datenverkehrs gibt es die Möglichkeit, einen Port des Routers oder des Switches als "Mirror Port" zu konfigurieren. Dabei wird der gesamte Datenverkehr eines beliebigen Ports auf den Mirror Port repliziert und kann mit entsprechenden Analyseprogrammen ausgewertet werden. Im Gegensatz zu anderen Analysemethoden wird der Datenverkehr dabei nicht unterbrochen oder beeinträchtigt.

Der Mechanismus bietet zwei Analysemethoden: Spiegelung des gesamten Datenverkehrs für einen definierten Port oder Spiegelung des Datenverkehrs für eine MAC-Adresse. Im zweiten Fall wird das gesamte Datenvolumen, welches mit einer definierten Quell- und/oder Ziel-MAC-Adresse über das Gerät läuft, auf den Mirror Port gespiegelt.

Der Mirror Port darf keinem produktiven VLAN und keiner Spanning Tree Group (STG) angehören. Standardmäßig muss "Port Mirroring" ausgeschaltet sein. Der Zugriff auf die Konfiguration des "Port Mirroring" ist zu schützen. Nach der Verwendung des Mirror Ports ist dieser wieder zu deaktivieren. Es ist regelmäßig zu prüfen, ob die Funktion Port Mirroring im Regelbetrieb deaktiviert ist.

Ergänzende Kontrollfragen:

- Ist die regelmäßige Kontrolle von Routern und Switches Bestandteil der Sicherheitsrichtlinie?
- Welches Prüfintervall wurde festgelegt?
- Wann und von wem wurden Router und Switches das letzte Mal geprüft?
- Wurde die Prüfung dokumentiert?
- Wurden entsprechende Aktionen aus der Prüfung abgeleitet und Verantwortlichkeiten festgelegt?

M 2.283 Software-Pflege auf Routern und Switches

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Jeglicher Betrieb von Software macht es notwendig, Betriebssystem und Konfiguration regelmäßig zu überprüfen und zu pflegen. Router und Switches können hiervon nicht ausgenommen werden, um beispielsweise funktionale Erweiterungen zu ermöglichen, Softwarefehler zu beheben und Performance und Sicherheit zu verbessern.

Dabei ist zu beachten, dass in der Praxis zur Pflege des Betriebssystems bei Router und Switches oftmals ein kompletter Austausch der Betriebssystemsoftware erforderlich ist. Das Einspielen von Updates oder Patches ist in vielen Fällen nicht möglich. Wie bei allen Konfigurationsänderungen ist mit angemessener Sorgfalt vorzugehen, da eine unsachgemäße Durchführung Beeinträchtigungen der Funktion und der Sicherheit der Geräte zur Folge haben kann. Insofern gehört zur sorgfältigen Planung einer Änderung immer auch eine Fallback-Strategie.

Einspielen neuer Software

Bei der Vorbereitung von Updates sind folgende Punkte zu beachten:

- Es muss ein geeignetes Zeitfenster vorgesehen werden. Der benötigte Aufwand sollte nicht unterschätzt werden und vorsichtshalber eine ausreichende Down-Time eingeplant werden.
- Die vom Hersteller beigefügten Hinweistexte (Release Notes) des neuen Release sind sorgfältig zu lesen.
- Bei neuen Softwareversionen sind eventuell einzelne Features nicht mehr enthalten oder funktionieren nicht korrekt. Manchmal ändern sich auch Defaulteinstellungen.
- Neue Versionen eines Programmes und insbesondere eines Betriebssystems müssen vor der Inbetriebnahme sorgfältig getestet werden, um die volle Funktionalität sicher zu stellen.
- Neue Programme oder Betriebssysteme sind unter Umständen weniger performant, beispielsweise wegen zusätzlicher Features oder höherem Speicherbedarf. Dies kann zu Problemen führen, wenn ein Router oder Switch bereits vor dem Upgrade an der Auslastungsgrenze betrieben wurde.

Viele Hersteller bieten zur Planung der Erweiterung Konfigurationswerkzeuge an. Diese ermöglichen es, ausgehend vom benutzen Gerät eine Konfiguration zu planen und die benötigten Hardwarebestandteile wie Interfaces und Speicher auszuwählen.

Bei der Durchführung von Updates sollten folgende Schritte durchgeführt werden:

- Beschaffung des Updates aus vertrauenswürdiger Quelle. Normalerweise sollten Updates nur vom Hersteller bezogen werden. Falls der Hersteller für die Updates Prüfsummen zur Verfügung stellt oder die Update-Pakete digital signiert, so sollten die Prüfsummen oder Signaturen überprüft

werden (siehe auch M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates* und M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*).

- Überprüfung der Integrität und Funktion des Updates
- Trennung des Gerätes vom produktiven Netz oder Deaktivierung aller Schnittstellen
- Nach Möglichkeit Sicherung der bestehenden Konfiguration und des Betriebssystems
- Einspielen des Updates
- Test
- Re-Aktivierung des Gerätes im Netz

Änderung der Konfiguration

Konfigurationsänderungen können sowohl direkt am Gerät an der System-Konsole (online) als auch auf einem eigenen Management-Rechner mit einem entsprechenden Konfigurationsprogramm oder einem Texteditor (offline) vorgenommen werden. Beide Vorgehen haben Vor- und Nachteile, generell ist jedoch die Offline-Konfiguration zu bevorzugen.

Die Online-Konfiguration kann in der Regel nur wenig komfortabel und ohne Zuhilfenahme von Tools erfolgen, beispielsweise ist das Einfügen von Kommentaren nicht immer möglich. Dafür wird die Syntax zeitnah überprüft.

Wenn die Erstellung von Konfigurationsdateien offline durchgeführt wird, stehen in der Regel komfortablere Werkzeuge zur Verfügung und es können Kommentare eingefügt werden. Nachteil bei dieser Vorgehensweise ist, dass oftmals Passworte im Klartext in die Konfigurationsdateien eingetragen werden müssen. Da die Passworte in der Konfigurationsdatei - und damit auch der bei Übertragung über das Netz auf das Gerät, sofern keine verschlüsselte Verbindung verwendet wird - lesbar sind, sollten diese sofort nach dem Einspielen der Konfigurationsdatei geändert werden. Eine andere Möglichkeit besteht darin, Passworte online zu setzen und die Konfiguration anschließend inklusive der verschlüsselten Passworte auszulesen.

Um sicher zu stellen, dass bei einem Boot-Vorgang aus dem Speicher die aktuelle Konfiguration eingelesen wird, muss die geänderte Konfiguration gespeichert werden, nachdem sie in das Gerät geladen wurde.

Bei manchen Geräten können Konfigurationsdateien für eine zentrale Administration auch auf separaten Servern gehalten und von dort geladen werden. Dies kann sowohl manuell als auch automatisiert - beispielsweise beim Bootvorgang - geschehen. Änderungen können somit automatisiert an die Geräte verteilt werden. Das Laden beim Bootvorgang ist jedoch wegen der Möglichkeit zur mutwilligen Störung, seiner Fehleranfälligkeit und der entstehenden Netzlast nicht empfehlenswert und wird nur selten genutzt. Die Sicherung und Verwaltung der Konfigurationsdateien hingegen sollte über einen derartigen zentralen Server erfolgen.

In jedem Fall muss der Administrationsrechner, auf dem die Offline-Konfiguration vorgenommen wird beziehungsweise auf dem die

Konfigurationsdaten gehalten werden, vor unbefugtem Zugriff besonders geschützt werden.

Ergänzende Kontrollfragen:

- Sind Sicherheitslücken eingesetzter Betriebssystemversionsstände bekannt?
- Werden veraltete Versionen verwendet?
- Wann wurde die letzte Aktualisierung durchgeführt?
- Wie findet die Informationsbeschaffung über Sicherheitslücken der eingesetzten Systeme statt?
- Wird vor der Konfigurationsänderung eine Sicherung durchgeführt?

M 2.284 Sichere Außerbetriebnahme von Routern und Switches

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Auf aktiven Netzkomponenten gespeicherte Konfigurations- oder Log-Dateien enthalten eine Vielzahl von Informationen über das Netz, die Infrastruktur, die Organisation und eventuell auch über Personen im Unternehmen. Wenn ein Gerät an Externe weitergegeben wird (etwa an den Hersteller oder den Service bei einem Garantieaustausch oder an einen etwaigen Käufer), dann können diese Informationen ausgewertet werden.

Beispielsweise können folgende Informationen aus Konfigurationsdateien gewonnen werden:

- Verwendete Protokolle (insbesondere Routing-Protokolle), IP-Adressen und Subnetze
- VLAN-Konfiguration
- Access Control Lists
- Passwörter und SNMP Community Strings
- Name und Kontaktdaten des Administrators (Banner)

Wegen der Sensibilität dieser Informationen ist darauf zu achten, dass die Dateien vor der Außerbetriebnahme oder dem Austausch defekter oder veralteter Geräte gelöscht beziehungsweise unlesbar gemacht werden. Die Vorgehensweise hängt dabei stark vom Hersteller des Gerätes ab. In der Sicherheitsrichtlinie für Router und Switches sollten hierfür entsprechende Verantwortlichkeiten definiert werden.

Viele Geräte unterstützen die Funktion des "Factory-Resets". Durch einen Befehl oder durch das Betätigen eines Schalters werden die Komponenten auf die werksmäßigen Default-Einstellungen zurück gesetzt. Dabei ist allerdings zu beachten, dass dieser Reset nicht zwangsläufig alle gespeicherten Einstellungen auf den ursprünglichen Zustand zurücksetzt. Eine anschließende Kontrolle ist daher zwingend erforderlich. Auf anderen Geräten können Konfigurationsdateien durch entsprechende Befehle komplett gelöscht oder durch andere Dateien ersetzt werden. Sollten die eingesetzten Geräte über keine der erwähnten Funktionen verfügen, ist eine individuelle Umkonfiguration oder die physikalische Zerstörung des Speichers erforderlich.

Gespeicherte Protokolldateien können auf einigen Geräten ebenfalls mit Hilfe des "Factory-Resets" gelöscht oder überschrieben werden. Dies ist allerdings als Ausnahme zu betrachten. Häufig kann eine Protokolldatei mit einem entsprechenden Befehl gelöscht werden. Vor der Außerbetriebnahme eines Gerätes sollte daher besonders darauf geachtet werden, dass keine Log-Dateien mehr vorhanden sind. Sollten die eingesetzten Geräte über keine der erwähnten Funktionen verfügen, ist eventuell die physikalische Zerstörung des Speichers erforderlich.

Oft sind Router und Switches von außen mit IP-Adressen, Hostnamen oder sonstigen technischen Informationen beschriftet. Auch diese Beschriftung sollte vor der Entsorgung entfernt werden.

Ergänzende Kontrollfragen:

- Ist die sichere Entsorgung von Geräten in der Sicherheitsrichtlinie für Router und Switches berücksichtigt?
- Werden Konfigurationsdateien und Log-Dateien vor der Entsorgung sicher gelöscht bzw. unlesbar gemacht?
- Wird die Beschriftung von den Geräten vor der Entsorgung entfernt?

M 2.285 Festlegung von Standards für z/OS-Systemdefinitionen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator

Die Festlegung von Standards für die z/OS-Systemdefinitionen ist eine der Voraussetzungen für ein funktionierendes System-Management. Standards unterstützen aber auch die Umsetzung von Sicherheitsregeln und deren Überwachung. Die folgenden Empfehlungen sollten dabei beachtet werden:

Vereinbarte z/OS-System-Standards müssen nachvollziehbar dokumentiert sein. Die Dokumentation muss für die Administratoren verfügbar sein.

Die Einhaltung der z/OS-System-Standards sollte regelmäßig überprüft werden.

Es sollte überlegt werden, eine Standardisierung für die folgenden Objekte zu vereinbaren:

- Account-Nummer
  in Jobs und für USER oder STCs
- ACS-Routinen
- Allokierungs-Regeln
- Application-ID (IMS)
- Assembler-Standards
- Benutzergruppen-Kennzeichen
  z. B. Netzadministration, Entwicklung, Test, Produktion und DB-Administration
- COBOL-Compiler-Optionen
- Command-Character (Console)
- Command-Character (Terminal)
- Coupling-Facility-Namen
- Dateien
  anzulegende Dateien sollten katalogisiert sein
- Datei-Namen
  evtl. mit Unterscheidungsmerkmalen für System, Entwicklung und Produktion. Der letzte Qualifier legt in der Regel die Dateiart fest. Kennzeichnung von Target- und DLIB-Dateien
- Datenbank-Namen
- DFSMS
  DATA-CLASS, STORAGE-CLASS, MANGEMENT-CLASS, STORAGE-GROUP, LLQ-Zuordnungen
- IMS-ID
- IMS-Start-Prozeduren
- Initiator-Klassen
- ISMF-Schutz-Festlegungen
- JES2
  Job-Klassen, Initiator, Parameter
- JOBCAT und STEPCAT sollten nicht verwendet werden (IBM hat im August 2004 angekündigt, den Support zu JOBCAT und STEPCAT ab z/OS 1.7 einzustellen.)

- Job-Namen
  evtl. mit Unterscheidungsmerkmalen für Entwicklung und Produktion
- Katalog-Namen
- LOGON-Prozeduren-Namen
- Member-Namen
  evtl. mit Unterscheidungsmerkmalen für Entwicklung und Produktion
- Output-Klassen
- PAGE-Datasets
- Parmlib-Member für JESx
- Prozeduren-Namen
- RACF-Resource-Klassen
- SMF-Belegung (System Management Facility)
- SMP/E-Datei-Namen
- SMP/E-Umgebungen für verschiedene Subsysteme
- SMP/E-Zonen-Datasets
- SMP/E-Zonen-Namen
- SMS-Datei-Namen
- SSID (Sub-System ID)
- Vermeidung von Standortkennzeichen
  Standortkennzeichen haben sich im Rahmen von Umstrukturierungen und Anwendungsverlagerungen nicht unbedingt als vorteilhaft erwiesen
- STC-Namen (Started Tasks)
- STEPCAT sollte nicht verwendet werden
- SVC-Belegung
- Sysplex-ID
- Systemdateien-Namen
- System-ID (mit Sysplex-Kennung)
- Table-Space-Namen
- TSO-LOGON-Prozeduren
- UNIT-Klassen
- USER-ID
- USERMODs
- Volume-Namen (System-Volumes, Anwendungs-Volumes)

In Abhängigkeit von den eingesetzten Subsystemen, Datenbanksystemen, Software-Produkten und Anwendungen kann diese Liste noch durch weitere Objekte ergänzt werden.

Ergänzende Kontrollfragen:

- Sind die vereinbarten Standards dokumentiert?
- Haben die Administratoren Zugang zu der Dokumentation der Standards?

M 2.286 Planung und Einsatz von zSeries-Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Leiter IT

Planung

Vor der Anschaffung und Inbetriebnahme von zSeries-Systemen müssen verschiedene planerische Tätigkeiten durchgeführt werden. Für die Planung des Einsatzes der zSeries-Systeme sind folgende Empfehlungen bezüglich der Sicherheit zu beachten:

Infrastruktur

Der Standort der zSeries-Hardware muss in einem zutrittsgeschützten Rechenzentrum geplant werden. Empfehlungen für die Infrastruktursicherheit von Rechenzentren finden sich in Baustein B 2.9 *Rechenzentrum*.

Hardware

Die Hardware-Ressourcen, die für den Betrieb benötigt werden, müssen geplant und in ihrer Kapazität entsprechend den Anforderungen dimensioniert werden. Dies betrifft die gesamte Hardware-Ausstattung, von der Anzahl der Prozessoren, über Kanäle, Festplatten und Bandstationen bis hin zu Netz-Komponenten (inklusive Netzanschlüsse).

Betriebssysteme

Es ist zu klären, welches der möglichen Betriebssysteme (z/OS, zLinux ohne Trägersystem, zLinux unter dem Trägersystem z/VM, etc.) für die Anforderungen der Anwendung zum Einsatz kommen muss.

Anforderung der Anwendungen

Die Anforderungen der Anwendungen an die Hardware und das Betriebssystem müssen bei der Planung berücksichtigt werden:

- Wie viele Anwender werden auf die Anwendung gleichzeitig zugreifen?
- Wird ein *Single-System* oder ein *Parallel-Sysplex System* benötigt? (u. a. eine Frage der Verfügbarkeit)
- Welches Datenvolumen wird durch den Betrieb der Anwendung anfallen? (Festplatten, Magnetbandstationen)
- Welchen Schutzbedarf hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit hat die Anwendung bzw. ihre Daten?
- Welche Netzanschlüsse werden benötigt bzw. von wo erfolgen Zugriffe (aus dem Internet, Intranet, eigene Netzumgebung)?

Prozesse

Es ist zu überprüfen, wie das neue System in die bestehenden Prozesse eingebunden werden kann. Dies betrifft z. B. das Change Management, Eskalations- und Meldeverfahren, Sicherheits-Audits und weitere Management-Disziplinen. Die Einhaltung der Sicherheitsvorgaben und -richtlinien der

Behörde oder des Unternehmens muss bei der Planung mit berücksichtigt werden.

Personal

Es ist zu überprüfen, wie viele Mitarbeiter mit welcher Ausbildung für den Betrieb des zSeries-Systems benötigt werden. Stehen nicht genügend ausgebildete Mitarbeiter mit Mainframe-Wissen zur Verfügung, müssen die Schulungsmaßnahmen rechtzeitig initiiert werden.

Einsatzszenarien

Im Folgenden werden exemplarisch einige typische Einsatzszenarien von zSeries-Systemen vorgestellt und Empfehlungen zur Trennung von Systemen mit unterschiedlichen Sicherheitsanforderungen beschrieben.

Batch-Systeme

Bei Batch-Systemen steht die Stapelverarbeitung im Vordergrund. Stapelverarbeitung bedeutet, dass vorgegebene Programme (*Batch-Jobs*) an Hand von durch JCL (*Job Control Language*) definierten Abläufen ohne Interaktion mit den Benutzern - in der Regel große - Datenbestände bearbeiten. Batch-Systeme können sowohl als Einzelsysteme als auch im Rahmen von *Parallel-Sysplex-Clustern* betrieben werden. Für Batch-Systeme ist zu überlegen, ob eine Scheduling-Funktion zur Kontrolle der Stapelverarbeitung eingesetzt werden soll (siehe M 2.287 *Batch-Job-Planung für z/OS-Systeme*). Die Verwaltung der Zugriffsrechte sollte durch RACF (*Resource Access Control Facility*) abgedeckt werden. Anhand der Anforderungen an die Skalierbarkeit ist außerdem zu prüfen, ob ein *Parallel-Sysplex-Cluster* eingesetzt werden sollte.

Online-Systeme

Online-Systeme verarbeiten Transaktionen, die durch interaktive Arbeiten der Benutzer am Bildschirm ausgelöst werden. Hierbei kommen häufig sogenannte Transaktionsmonitore wie CICS (*Customer Information Control System*) oder IMS (*Information Management System*) zum Einsatz. Wie bei Batch-Systemen sollte RACF zur Verwaltung und Durchsetzung der Zugriffsrechte verwendet werden. Bei hohen Anforderungen an die Verfügbarkeit des Online-Systems sollte geprüft werden, ob diesen Anforderungen durch den Einsatz eines *Parallel-Sysplex-Clusters* Rechnung getragen werden kann. Weitere Empfehlungen finden sich in der Maßnahme M 2.296 *Grundsätzliche Überlegungen zu z/OS-Transaktionsmonitoren*.

Web-Server

zSeries-Systeme werden auch als Web-Server für Internet- oder Intranet-Angebote eingesetzt. Als Betriebssystem kommt dabei z/OS oder auch zLinux (separat oder als Gast unter z/VM) zum Einsatz. Sicherheitsempfehlungen für den Betrieb von Linux auf zSeries-Systemen finden sich in der Maßnahme M 4.212 *Absicherung von Linux für zSeries*.

Datenbank-Server

z/OS-Systeme können auch als Datenbank-Server eingesetzt werden. Das System stellt dazu, häufig mit Hilfe der Datenbank-Software DB2, Services zur Verfügung, die es erlauben, Datenbankinformationen abzufragen oder deren Inhalte zu verändern. Datenbank-Server werden oft in Verbindung mit Transaktionsmonitoren (z. B. CICS) oder mit Webservern eingesetzt und liefern diesen den notwendigen Datenbank-Zugriff. Die Konzentration auf den reinen Datenbank-Service reduziert die Komplexität und verbessert die Performance des Systems gerade bei sehr großen Datenbanken. Wie bei den vorher beschriebenen Szenarien sollte RACF auch bei Datenbank-Servern zur Verwaltung und Durchsetzung der Zugriffsrechte verwendet werden. Weitere Empfehlungen zum Einsatz von DB2 finden sich in der Maßnahme M 2.296 *Grundsätzliche Überlegungen zu z/OS-Transaktionsmonitoren*.

Universelle Systeme

Universelle Systeme sind Mainframes, die mehrere der oben beschriebenen Dienste erbringen. Sie verarbeiten sowohl Batch-Jobs als auch Online-Transaktionen und enthalten einen (oder mehrere) Datenbank-Server. Gegebenenfalls werden sie zusätzlich auch noch als Webserver im Internet oder Intranet eingesetzt. In allen Bereichen sollte RACF als Sicherheitssystem eingesetzt werden.

System-Trennung

Da für Produktions-Systeme unter z/OS in der Regel höhere Sicherheitsanforderungen gelten als für Test- und Entwicklungssysteme, muss zwischen beiden Systemumgebungen eine Trennung erfolgen. Um diese Trennung zu realisieren, sind folgende Empfehlungen zu berücksichtigen:

Gemeinsame Festplatten-Zugriffe

Die Festplatten sind den Test- und Produktions-Systemen so zuzuordnen, dass unberechtigte Zugriffe auf Produktions-Daten verhindert werden können. Dabei erfolgt die Definition der Adressen im HCD (*Host Configuration Definition*). Es muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass Festplatten aus Test-Systemen an Produktions-Systemen (und umgekehrt) nicht *Online* gesetzt werden können und dass auf die gleichen Festplatten nicht gleichzeitig von Test- und Produktions-Systemen aus zugegriffen werden kann (*Shared DASD*).

Einsatz von FTP

Der Datenaustausch zwischen Produktions- und Test-Systemen sollte über FTP (*File Transfer Program*) erfolgen.

Shared Sysplex

Produktions- und Test-Systeme sollten nicht im selben *Parallel Sysplex*-Verbund betrieben werden. Ist eine solche Konstellation notwendig, muss eine logische Trennung über entsprechende Standards und RACF-Definitionen (*Resource Access Control Facility*) sicherstellen, dass kein Missbrauch von Dateizugriffen entstehen kann.

Shared RACF-Datenbanken

Es sollte überlegt werden, für Produktions- und Test-Systeme keine *Shared-RACF*-Datenbanken zu verwenden.

Ergänzende Kontrollfragen:

- Sind die Transaktionsmonitore über RACF gesichert?
- Ist sichergestellt, dass es keine *Shared-Dasd*-Verbindung zwischen Test- und Produktions-Systemen unter Produktionsbedingungen gibt?
- Ist sichergestellt, dass Test- und Produktions-Systeme nicht im gleichen *Parallel-Sysplex*-Verbund laufen?

M 2.287 Batch-Job-Planung für z/OS-Systeme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Beim Einsatz eines z/OS-Systems als Stapelverarbeitungs-Systems ist es bei einer größeren Anzahl von Batch-Jobs unabdingbar, dass der Ablauf dieser Jobs geplant, überwacht und bearbeitet werden muss. Da diese Tätigkeit manuell ohne Fehler kaum noch realisierbar ist, sollte Automations-Software, sogenannte *Job-Scheduler*, zur Ablaufsteuerung der Batch-Jobs eingesetzt werden.

Aufgaben der Job-Scheduler

Die Aufgabe der Job-Scheduler besteht im wesentlichen aus den Funktionen

- Starten der Batch-Jobs
- Überwachen des Betriebszustandes der Batch-Jobs (darüber hinaus sicherstellen, dass Ressourcen bereitstehen)
- Prüfen der Ergebnisse (über Returncodes) der Batch-Jobs
- Verfolgen der Abhängigkeiten von Batch-Jobs
- Verwalten des Status der Batch Jobs
- Korrektive Maßnahmen im Fehlerfall

Die Sicherheitsmechanismen, um den Job-Scheduler vor Missbrauch zu schützen, sollten durch ein Sicherheitssystem wie RACF (*Resource Access Control Facility*) realisiert werden.

Für den Einsatz des Job-Schedulers sind mindestens die folgenden Hinweise zu beachten:

Attribut OPERATIONS

Der Einsatz des RACF-Attributes *OPERATIONS* für die Kennung der *Started Task* des *Job Schedulers* sollte vermieden werden. Anderenfalls besteht die Gefahr, dass Batch-Jobs, die unter dieser Kennung gestartet werden, Zugriff zu nahezu allen Produktionsdateien haben (siehe M 2.289 *Einsatz restriktiver z/OS-Kennungen* und M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*). Falls der Hersteller für den Betrieb des Job-Schedulers das Attribut *OPERATIONS* fordert, sollte mit dem Hersteller geklärt werden, ob es hierzu Alternativen gibt.

Einsatz von RACF-SURROGAT-Kennungen

Um zu verhindern, dass die Batch-Jobs aus dem Job-Scheduler heraus unter der eventuell hoch autorisierten Kennung des Job-Scheduler laufen, sollte überlegt werden, ob RACF-SURROGAT-Kennungen als Verfahrenskennungen eingesetzt werden können. Dabei sind die Nachteile dieser Funktion zu berücksichtigen (siehe M 2.289 *Einsatz restriktiver z/OS-Kennungen*).

Prozedurdateien

Die Prozedurdateien des Job-Schedulers müssen so über RACF geschützt werden, dass der Zugriff auf die Prozedurdateien nur Mitarbeitern möglich ist, die diesen Zugriff für ihre Tätigkeit auch benötigen. Dabei ist die Anzahl auf ein Minimum zu beschränken. Eine Stellvertreter-Regelung muss in jedem Fall vorgesehen sein.

Die Kennung des Job-Schedulers muss lesenden Zugriff auf alle Prozedurdateien besitzen, um die Batch-Jobs entsprechend starten zu können.

Tool-Zugriff

Der Job-Scheduler wird meist über einen ISPF-Dialog (*Interactive System Productivity Facility*) gesteuert. Der Zugang zum Job-Scheduler sollte nur Mitarbeitern zur Verfügung stehen, die ihn für ihre Arbeit benötigen, sowie deren Vertretern. Der Zugangs- und Zugriffsschutz sollte über RACF erfolgen. Falls dies nicht möglich ist, müssen interne Sicherheitsmechanismen des Schedulers genutzt werden.

Systemadministration

Die Verwaltung der Batch-Jobs im Job-Scheduler sollte, wenn immer möglich, so über RACF geschützt werden, dass jede Anwender-Gruppe, wie Systembetreuer, Space-Management oder RACF-Administration, nur ihre Batch-Jobs einsehen und bearbeiten kann.

Ergänzende Kontrollfragen:

- Ist sichergestellt, dass die Kennung des Job-Schedulers ohne das RACF-Attribut *OPERATIONS* auskommt?
- Ist der Zugang zum Job-Scheduler-Programm über RACF geschützt?

M 2.288 Erstellung von Sicherheitsrichtlinien für z/OS-Systeme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Vor dem Einsatz von z/OS-Systemen müssen Sicherheitsrichtlinien für das z/OS-System und besonders auch für das Sicherheitssystem RACF (*Resource Access Control Facility*) geplant und festgelegt werden. Es sind folgende Empfehlungen zu berücksichtigen:

- Die z/OS-Systeme müssen in das unternehmens- bzw. behördenweite IT-Sicherheitsmanagement eingebunden werden. **IT-Sicherheits-management**
- Wie in Maßnahme M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen* beschrieben, ist ein Verfahren zur Verwaltung der Benutzer des z/OS-Systems und deren Kennungen zu erstellen. **Benutzerverwaltung**
- Es muss eine Richtlinie zum Gebrauch des Notusers erstellt werden (siehe Maßnahme M 6.93 *Notfallvorsorge für z/OS-Systeme)*. **Notuser-Verfahren**
- Eine Richtlinie zur Wiederherstellung der RACF-Datenbank unter z/OS muss erstellt werden (siehe Maßnahme M 6.93 *Notfallvorsorge für z/OS-Systeme)*. **RACF-Datenbank-Wiederherstellung**
- Ein Berechtigungsprozess für den Zugriff auf sicherheitskritische System-Ressourcen, wie z. B. APF-Dateien (*Authorized Programming Facility*), SVCs (*SuperVisor Calls*) usw., muss beschrieben und eingeführt sein.
- Ein Audit-Verfahren, wie in Maßnahme M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS* beschrieben, bzw. ein Monitoring-Verfahren, wie in Maßnahme M 2.292 *Überwachung von z/OS-Systemen* beschrieben, müssen etabliert sein. **Sicherheits-Audit / Monitoring**
- Ein Eskalations- und Meldeverfahren muss aufgebaut sein. In ihm muss festgelegt sein, wer Sicherheits-Verstöße erkennt, weitermeldet und welche Abwehrmaßnahmen zu ergreifen sind. **Eskalations-/ Melde-Verfahren**
- Eine Dokumentation zu Aufbau und Funktion eines Notsystems, wie in Maßnahme M 6.93 *Notfallvorsorge für z/OS-Systeme* beschrieben, muss erstellt sein (gilt nur für Einzel-Systeme). **Not-System**
- Es sollte eine Prüfliste mit Kontrollfragen erstellt werden, die alle wichtigen sicherheitsrelevanten Einstellungen des z/OS-Systems erfasst und deren Soll-Werte festlegt. Anhand dieser Prüfliste werden die Arbeitsanweisungen für die System- und RACF-Administratoren erstellt. Die Prüfliste dient dem Auditor als Basis für die Überprüfung der Systemsicherheit. In regelmäßigen Abständen muss die Prüfliste überarbeitet werden. Als Basis für eine solche Prüfliste können die Maßnahmen M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF* und M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen* dienen. **Prüfliste für Sicherheits-einstellungen**

Ergänzende Kontrollfragen:

- Ist eine Prüfliste für Sicherheitseinstellungen vorhanden?

- Ist ein Verfahren für Audit und/oder Monitoring eingeführt?
- Ist das Eskalations- und Meldeverfahren beschrieben und in die Praxis umgesetzt?

M 2.289 Einsatz restriktiver z/OS-Kennungen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Kennungen mit hoher Autorisierung

Für die Verwaltung des Sicherheitssystems RACF (*Resource Access Control Facility*) werden u. a. Kennungen mit hoher Autorisierung benötigt. Zur Minimierung des Missbrauchsrisikos sind die folgenden Regeln zu beachten:

SPECIAL, OPERATIONS, AUDITOR

Attribute mit hoher Autorisierung im RACF, wie *SPECIAL*, *OPERATIONS* und *AUDITOR*, gelten systemweit und dürfen nur an Anwender vergeben werden, die für ihre Tätigkeit diese Rechte benötigen. Kennungen mit diesen besonders hohen Rechten sind auf ein Minimum zu begrenzen, und deren Vergabe ist zu dokumentieren.

GROUP-SPECIAL, GROUP-OPERATIONS, GROUP-AUDITOR

Sind hohe Rechte erforderlich, so ist zu überlegen, ob diese Rechte nicht auf Gruppenebene (*GROUP-SPECIAL*, *GROUP-OPERATIONS* und *GROUP-AUDITOR*) für die jeweilige Kennung eingeschränkt werden können. Auch die Vergabe der auf Gruppenebene eingeschränkten Rechte ist auf ein Minimum zu begrenzen und zu dokumentieren.

Superuser (UID 0)

Im optionalen Unix-Segment der User-Kennung (*OMVS Segment*) wird eine für *Unix System Services* (USS) gültige Userid (*UID*) vergeben, unter der die z/OS-Kennung im USS geführt wird. Die UID 0 (*Superuser*) oder die Berechtigung, das *su*-Kommando ausführen zu dürfen, darf nur an die Anwender vergeben werden, die diese Berechtigung für ihre Arbeit benötigen.

SPECIAL und UID 0

Hoch autorisierte Kennungen mit Attribut *SPECIAL* dürfen aus Sicherheitsgründen nicht gleichzeitig mit UID 0 als *Superuser* unter USS laufen. Es ist weiterhin zu überlegen, ob die Attribute *SPECIAL* und *OPERATIONS* an die gleiche Kennung vergeben werden sollten.

Vergabe von UIDs

UIDs sollten nicht doppelt vergeben werden (gleiche UID für verschiedene User). Viele Tätigkeiten, für die in bestimmten Unix-Betriebssystemen unbedingt *Superuser*-Rechte benötigt werden, können im RACF einzeln über spezielle RACF-Profile der Klasse *UNIXPRIV* autorisiert werden. Eine solche Autorisierung über RACF-Profile ist in jedem Fall sicherer als die Vergabe der *Superuser*-Rechte oder su-Kommando-Berechtigung (siehe auch Maßnahme M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).

Audit-Verfahren

Um die Tätigkeit der Anwender mit hohen Berechtigungen auditieren zu können, muss ein entsprechendes Audit-Verfahren etabliert sein (siehe auch Maßnahme M 2.288 *Erstellung von Sicherheitsrichtlinien für z/OS-Systeme*) .

IBMUSER bei Neuinstallationen

Erfolgt eine Neuinstallation, so sind mit dem *IBMUSER* mindestens zwei Kennungen mit dem Attribut *SPECIAL* neu anzulegen. Ist dies erfolgt, so muss der *IBMUSER* gesperrt (*REVOKED*) werden und gesperrt bleiben. RACF-Definitionen sollten nicht mit der Kennung *IBMUSER* angelegt werden (siehe auch Maßnahme M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).

Notuser-Verfahren

Für den Fall, dass z. B. alle Kennungen mit dem Attribut *SPECIAL* gesperrt wurden, oder kein Anwender mit dieser Berechtigung im Notfall verfügbar ist, ist ein Notuser-Verfahren zu etablieren (siehe auch Maßnahme M 6.93 *Notfallvorsorge für z/OS-Systeme*).

Ergänzende Kontrollfragen:

- Ist der *IBMUSER* gesperrt?
- Gibt es ein Notuser-Verfahren?
- Gibt es eine Liste der Kennungen mit den Attributen *SPECIAL*, *OPERATIONS* oder *AUDITOR* bzw. der entsprechenden Gruppen-Attribute, und ist ihre Zahl auf ein Minimum beschränkt?

M 2.290 Einsatz von RACF-Exits

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Neben den Anpassungsmöglichkeiten von RACF (*Resource Access Control Facility*) durch Kommandos und Parameter ist es darüber hinaus möglich, zusätzliche Sicherheitsregeln durch den Einsatz von RACF-*Exits* zu implementieren. *Exits* werden an verschiedenen Stellen der RACF-Funktionen durchlaufen und erlauben dort individuelle Eingriffe. Ihr Einsatz erfordert ein hohes Maß an Wissen und Erfahrung in der Assembler-Programmierung.

Die folgenden Empfehlungen sollten beim Einsatz von *Exits* beachtet werden:

Wartung der Exits

Wenn *Exits* zur Erweiterung der RACF-Funktionalität notwendig sind, müssen diese per SMP/E (*System Management Program/Enhanced*) als *Usermod* eingebaut werden (siehe M 2.293 *Wartung von zSeries-Systemen*).

DES-Algorithmus zur Authentisierung

RACF verschlüsselt die Kennung mit Hilfe des DES-Algorithmus (*Data Encryption Standard*), wobei als Schlüssel das eingegebene Passwort benutzt wird (das Passwort selbst wird dabei nicht gespeichert). Um sicherzustellen, dass der DES-Algorithmus (und nicht der schwächere *Masking*-Algorithmus) benutzt wird, darf der in der *SYS1.LINKLIB* mitgelieferte *Exit ICHDEX01* nicht in der *Link Pack Area* eingesetzt werden. Es wird daher empfohlen, dieses Lade-Modul zu entfernen und den entsprechenden Eintrag in SMP/E zu deaktivieren (*Usermod*), damit zukünftige Wartungsaktivitäten dieses Lade-Modul nicht eventuell wieder installieren. Der DES-Algorithmus ist normalerweise die Standardeinstellung bei der Auslieferung von RACF unter z/OS.

Änderungen von Exits

Es ist zu beachten, dass bei Änderungen von *Exits* ein IPL (*Initial Program Load*) notwendig ist. Eine Ausnahme hiervon stellt *IRREVX01* dar; er lässt sich dynamisch nachladen.

Erweiterte Passwortregeln

Es sollte überlegt werden, ob die über die SETROPTS-Funktion von RACF zur Verfügung gestellten Mechanismen der Passwortregeln ausreichen oder ob über den *New Password Exit ICHPWX01* erweiterte Passwortregeln eingeführt werden sollen.

Verwendung von Tools

Beim Einsatz von Tools zur Passwort-Synchronsierung oder von Produkten zum Tape-Management ist zu überprüfen, ob RACF-*Exits* mit dem Produkt geliefert werden oder sogar Voraussetzung für das Funktionieren des jeweiligen Produktes sind.

Exit-Kontrolle

Der Einsatz von *Exits* kann über die Funktion *DSMON* kontrolliert werden. Eine solche Kontrolle sollte regelmäßig im Rahmen von Audits erfolgen (siehe auch M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS*). Eine

Ausnahme stellt *IRREVX01* dar. Dieser *Exit* sollte jedoch ebenfalls kontrolliert werden, wenn er verwendet wird.

Ergänzende Kontrollfragen:

- Ist der *Exit ICHDEX01* und damit der *Masking*-Algorithmus ausgeschaltet?
- Wurden alle verwendeten RACF-*Exits* per SMP/E als *Usermod* eingebaut?
- Steht die *Exit*-Auswertung über *DSMON* zur Verfügung?

M 2.291 Sicherheits-Berichtswesen und -Audits unter z/OS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator, Revisor

Zur Überwachung aller sicherheitsrelevanten Tätigkeiten muss ein Prozess eingerichtet werden. In diesem muss festgelegt sein, welche Sicherheitsreports regelmäßig erstellt werden und wie mit Abweichungen von den Vorgaben umgegangen wird. Diese Sicherheitsreports sollten als Information für den Auditor verwendet werden.

Darüber hinaus müssen zur Erhöhung der Betriebssicherheit eines z/OS-Systems regelmäßig IT-Sicherheits-Audits durchgeführt werden. Durch solche Audits wird überprüft, ob die geforderten Sicherheitseinstellungen und Abläufe eingehalten werden. Vorgaben hierfür finden sich in M 2.288 *Erstellung von Sicherheitsrichtlinien für z/OS-Systeme*.

Sicherheits-Berichtswesen

SMF-Sätze (System Management Facility) als Quelle des Berichtswesens

Für die Überwachung der IT-Sicherheit von z/OS-Systemen sind die SMF-Sätze des Typs 80 von Bedeutung. Sie protokollieren alle Zugriffe auf Ressourcen, die durch RACF-Profile geschützt werden. In diesen Profilen kann durch RACF-Definitionen festgelegt werden, ob nur unerlaubte oder auch erlaubte Zugriffe protokolliert werden. Unerlaubte Zugriffe müssen in jedem Fall protokolliert werden. Bei systemkritischen Dateien sollten in einem Produktionssystem auch die erlaubten Zugriffe über SMF erfasst werden, wenn die Datei dabei geändert wird. Beim Protokollieren über SMF-Sätze sollte immer darauf geachtet werden, dass durch das Aktivieren von SMF-Funktionen nicht zu viele Logdaten entstehen. Die Kapazität und die Performance des Systems darf nicht zu stark beeinträchtigt werden.

Es muss sichergestellt werden, dass der SMF-Satz Typ 80 auch wirklich geschrieben wird. Dies wird im Member *SMFPRM00* in der *Parmlib* definiert. Der Schutz der *Parmlib* ist in Maßnahme M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen* näher beschrieben.

Einsatz von Tools

- Einsatz des RACFICE-Tools

  Es ist zu überlegen, IBMs ICE-Tool (*RACFICE*) basierend auf IBMs *DFSORT* einzusetzen und dabei vorgefertigte Reports zu verwenden, vorhandene anzupassen oder neue zu erstellen.

  Bei den SMF-Sätzen können beispielsweise fehlgeschlagene Zugriffsversuche auf Ressourcen, erlaubte Zugriffe infolge besonderer Berechtigungen (*OPERATIONS*) und fehlgeschlagene Zugriffsversuche mit falschem Passwort als Reports erzeugt werden.

  Aus der RACF-Datenbank können zum Beispiel die Dateiprofile selektiert nach UACC (*Universal Access*), gesperrte Benutzerkennungen und Profile, die in den letzten 90 Tagen verändert wurden, als Reports erzeugt werden.

- Einsatz des RACF-Programms *DSMON*

  Es ist zu überlegen, das RACF-Programm *DSMON* als Basis für weitere Berichte zu benutzen. Dies ist in jedem Fall zu empfehlen, wenn kein *Real-Time-Monitor* eingesetzt werden soll, um Veränderungen an vitalen z/OS-Definitionen kontrollieren zu können.

- Einsatz von Independent Vendor Tools

  Die Auswertung der in den SMF-Sätzen protokollierten Informationen erfordert besondere Systemkenntnisse, wie z. B. der SMF-Programmfunktion. Es ist deshalb zu überlegen, separate Tools zur Auswertung dieser Datensätze einzusetzen. Entsprechende Programme sind von verschiedenen ISVs (*Independent Software Vendors*) erhältlich.

- Einsatz eines Real-Time-Monitors

  Bei besonderen Sicherheitsanforderungen ist zu überlegen, ob ein Berichtswesen auf Stapelverarbeitungsbasis aktuell genug ist oder ob ein *Real-Time-Monitor* zur Erkennung bestimmter Sicherheitsverstöße nicht sinnvoller ist. Dabei werden die SMF-Sätze über *SMF-Exits* (IEF083, IEF084, IEF085) direkt abgefangen und zu einem Monitor-Programm geleitet, das die Analyse und Darstellung übernehmen kann (siehe auch Maßnahme M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen*).

  Wichtige Informationen für eine Echtzeit-Überwachung sind z. B.:

  - Änderungen an APF-Dateien
  - Benutzung von Kennungen mit dem Attribut *SPECIAL* oder *OPERATIONS*
  - Erlaubte Zugriffe auf Grund des Attributes *OPERATIONS*
  - Mehrfache Zugriffsversuche mit falschem Passwort
  - Benutzung des Notusers

z/OS-Sicherheits-Audits

Unabhängigkeit der Auditoren

Die Durchführung der Audits muss durch unabhängige Auditoren erfolgen, d. h. das durchführende Personal darf sich und seine Arbeit nicht selbst auditieren.

Die Auditoren müssen z/OS-System- und RACF-Kenntnisse zur Durchführung ihrer Tätigkeit haben. Diese Kenntnisse sind durch regelmäßige Schulungen zu erwerben bzw. zu aktualisieren.

Autorisierung der Auditoren

Die Auditoren müssen Zugangsberechtigung zum System mit dem RACF-Attribut *AUDITOR* haben. Auch für die Files in HFS-Dateien muss dieses Attribut im jeweiligen FSP (*File Security Packet*) aktiviert sein.

Kontrolle über SMF-Sätze

Grundlage für das Audit sind die SMF-Sätze des Recordtyps 80. Die Informationen in der RACF-Datenbank legen dabei fest, welche Ereignisse in den

SMF-Sätzen protokolliert werden. Es muss deshalb sichergestellt werden, dass diese SMF-Sätze geschrieben werden und für Auswertungen zur Verfügung stehen.

Überprüfung von RACF-Profilen

Die Auditoren sollten überprüfen, ob bei Neueinrichtungen und Veränderungen von RACF-Profilen

- Genehmigungen vorliegen,
- die Funktionen bzw. Attribute (*SPECIAL, OPERATIONS*) in ihrem Befugnisumfang begründet sind (gilt auch für *GROUP-SPECIAL* und *GROUP-OPERATIONS*).

Gegenstand des Sicherheits-Audits

Ein vollständiges Sicherheits-Audit ist sehr komplex und muss eine große Anzahl von sicherheitsrelevanten Funktionen überwachen. Die folgenden Funktionen sollten mindestens überwacht werden:

- Kritische System-Einstellungen:
  - Program Properties Table (PPT)
  - Kontrolle der APF-Dateien (Authorized Programming Facility)
  - Kontrolle der Dateien aus der Linklist
  - SVC-Einsatz (SuperVisor Call)
  - Tabelle ICHRIN03 (Started Task Table)
- Kritische RACF-Funktionen:
  - RACF Authorized Caller
  - Einsatz von RACF Exits
  - RACF Started Procedures (hier besonders die Attribute Privileged und Trusted)
  - RACF Global Access Table
- Kritische Aktionen:
  - Aktivitäten von Kennungen mit SPECIAL, OPERATIONS (gilt auch für GROUP-SPECIAL und GROUP-OPERATIONS) oder Notuser, IBMUSER
  - Veränderung von sensitiven RACF-Parametern durch den Einsatz des SETROPTS-Kommandos
  - Alle Aufrufe des RACDEF-SVC (SVC 133) und alle Veränderungen an RACF-Profilen, die durch diesen RACF-Befehl entstanden sind
- Hinweise auf potentielle Sicherheitsverstöße:
  - Ballung von fehlgeschlagenen Anmelde- oder Zugriffsversuchen
  - Veränderung von Audit-Attributen
  - Behauptete bzw. identifizierte Benutzeridentität

- Art des versuchten Zugriffs (Erfolg oder Scheitern)

Einsatz von Audit-Tools

Zur Kontrolle der zu überwachenden Definitionen sollte mindestens der *DSMON* von RACF und das *RACFICE*-Paket eingesetzt werden. Es ist zu prüfen, ob ein zusätzliches Programm-Paket beschafft werden sollte, das die Auditoren bei ihrer Arbeit unterstützt.

Wichtig ist, dass ein Audit nur zur Feststellung von Tatsachen und nicht zur Ermittlung von Schuldigen dient, siehe auch M 2.182 *Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen*.

Ergänzende Kontrollfragen:

- Werden regelmäßig Sicherheitsberichte erstellt?
- Werden die RACF-Reporting-Tools *RACFICE* und *DSMON* benutzt?
- Ist ein *Real-Time-Monitor* im Einsatz?
- Werden SMF-Sätze des Typs 80 erstellt und können diese ausgewertet werden?
- Findet eine regelmäßige Überprüfung statt?
- Haben die Auditoren das Ihnen zugeordnete Attribut?

M 2.292 Überwachung von z/OS-Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um Fehlersituationen und Sicherheitsprobleme zeitnah erkennen und beheben zu können, ist es notwendig, den laufenden Betrieb von z/OS-Systemen zu überwachen. Dazu stehen verschiedene Datenquellen des Betriebssystems zur Verfügung. Diese können entweder manuell durch das *Operating* oder automatisiert durch Programme analysiert werden.

Die folgenden Empfehlungen sind bei der Überwachung von z/OS-Systemen zu berücksichtigen:

MCS-Konsole

Die MCS-Konsole (*Multiple Console Support*) stellt wichtige System-Meldungen (Fehler, Sicherheitsverstöße usw.) dar, auf die der Operator auch sofort reagieren kann. Um aus der Flut der Nachrichten die wichtigen herauszufiltern, ist der Einsatz der MPF-Funktion (*Message Processing Facility*) unbedingt erforderlich. Dabei ist es empfehlenswert, die wichtigen Nachrichten auf eine spezielle Konsole zu leiten, während die Kommunikation mit dem Betriebssystem auf anderen Konsolen stattfinden sollte. Es sollte überlegt werden, Farben zum Herausheben von kritischen Nachrichten einzusetzen.

SMF-Auswertung

Nahezu alle Aktivitäten des Betriebssystems werden über SMF-Sätze (*System Management Facility*) protokolliert. Diese Sätze sind in jedem Fall zur Analyse nach Sicherheitsverstößen heranzuziehen (siehe auch Maßnahme M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS*). Um auch Ereignisse der Vergangenheit analysieren zu können, muss ein entsprechendes Archivierungsverfahren für die SMF-Daten vorhanden sein. Da die SMF-Daten ebenso für Abrechnung und Performance-Analysen des z/OS-Systems herangezogen werden können, ist ferner zu überlegen, ob ein entsprechendes Berichtswesen aufgebaut werden soll.

SYSLOG-Auswertung

Alle wesentlichen Ereignisse werden darüber hinaus vom Betriebssystem im sogenannten SYSLOG (*System Log*) mitgeschrieben, das über SDSF (*System Display and Search Facility*) für JES2 oder über *Flasher* für JES3 für manuelle Analysen zur Verfügung steht. Es ist zu überlegen, ob Auswertungsprogramme erstellt und eingesetzt werden sollen, die das SYSLOG nach kritischen Nachrichten durchsuchen und entsprechende Reports erstellen.

Automation

Es ist zu überlegen, ob Automations-Programme eingesetzt werden sollen, die vordefinierte SYSLOG-Meldungen erkennen und entsprechende Reaktionen im System auslösen können. Hierzu gibt es eine Reihe von Produkten am Markt, auch MPF inklusive *Exit*-Programmierung kann benutzt werden.

Anwendungs-Logs

Viele Anwendungen schreiben eigene Protokolldaten, so zum Beispiel auch das USS-Subsystem (*Unix System Services*). Diese Protokolle sind ebenfalls

auf Sicherheitsverstöße zu analysieren, wichtige Nachrichten sind den Operatoren zur Verfügung zu stellen.

Zentrale Kontrolle

In größeren Installationen mit verschiedenen Standorten sollte eine zentrale Stelle existieren (*Focal Point*), an die alle für den Betrieb wichtigen Informationen gemeldet werden. Der Einsatz von Programmen, die das Geschehen übersichtlich - eventuell grafisch - darstellen können, ist zu überlegen.

Ergänzende Kontrollfragen:

- Gibt es eine zentrale Stelle, an die Informationen unterschiedlicher Systeme gemeldet werden (*Focal Point*)?
- Werden die SMF-Sätze analysiert, um Sicherheitsverstöße zu entdecken?
- Sind Nachrichten-Filter im Einsatz, um die wesentlichen Nachrichten herauszufiltern und besser darzustellen?

M 2.293 Wartung von zSeries-Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Maintenance-Konzeption umfasst die Wartung der zSeries-Hardware, des z/OS-Betriebssystems, der verschiedenen Programm-Produkte und die Wartung des zSeries-Microcode (*Firmware*). Wartung betrifft den kompletten Lebenszyklus eines Produktes, von der Neuinstallation über die permanente Pflege bis hin zum Abbau.

Wartung des zSeries-Hardware

Es ist zu empfehlen, für die Wartung der zSeries-Hardware einen Wartungsvertrag mit dem Hersteller bzw. mit vom Hersteller autorisierten Partnerunternehmen abzuschließen. Wartung kann entweder auf regelmäßiger Basis erfolgen oder wird notwendig, wenn interne Prüfprogramme Fehler entdecken und über RSF (*Remote Support Facility*) den Hersteller oder seinen Vertreter informieren. Zur Sicherstellung der Funktionsfähigkeit der Hardware (und auch der Basis-Software) ist eine regelmäßige Überprüfung der EREP-Reports (*Environmental Record Editing and Printing Program*) zu empfehlen. Die im EREP-Report dargestellten Informationen über Hard- und Software-Probleme werden von der Hardware und dem z/OS-Betriebssystem geliefert.

Wartung des z/OS-Betriebssystems

Die Wartung eines z/OS-Systems inklusive aller Subsysteme ist äußerst komplex und bedarf deswegen einer sorgfältigen Planung. Unter den Begriff Wartung fällt:

- Inbetriebnahme eines neuen Systems
- Änderungen als Funktionserweiterung oder Nachrüstung von Funktionen
- Behebung von gemeldeten Fehlern durch sogenannte PTFs (*Program Temporary Fixes*)
- Einbau von PTFs als präventive Maßnahme (besonders wichtig sind hier PTFs gegen gemeldete Sicherheitslücken) auf Grund von Herstellerinformationen
- Abbau von Systemen

Die Wartung von z/OS-Betriebssystemen kann normalerweise nicht ohne Unterbrechung des Betriebs durchgeführt werden.

Bei der Wartung des z/OS-Betriebssystems sind die folgenden Empfehlungen zu berücksichtigen:

Wartungspläne

Es müssen Wartungspläne erstellt werden, in denen festgelegt wird, wann Änderungen am System durchgeführt werden dürfen. Es müssen IPL-Termine (*Initial Program Load*) festgelegt und Testszenarien erarbeitet werden. Dies muss mit allen Beteiligten abgesprochen werden. Um fehlgeschlagene Änderungen notfalls wieder rückgängig machen zu können, muss ein Rückfall-Konzept erstellt werden.

Change Management

Alle Änderungen an Definitionen des z/OS-Betriebssystems (auch dynamische Änderungen während des produktiven Betriebs) müssen über das Change Management geplant und kontrolliert werden. Dies gilt auch für Neuinstallationen.

Neuinstallation

CustomPacs

Eine Neuinstallation wird notwendig, wenn ein z/OS-Betriebssystem erstmalig in Betrieb gehen soll oder wenn eine neue Version (bzw. neues Release) die vorhandene Version ablösen soll. Der Hersteller bietet hier unter dem Begriff *CustomPac* verschiedene, weitgehend vorbereitete Produkt- und Systemlieferungen an, die teils kostenlos, teils im Rahmen von Wartungsverträgen zur Verfügung stehen.

SystemPac ist ein Teil des *CustomPac*-Angebotes und erlaubt es, eine weitgehend vorbereitete Lieferung des z/OS-Betriebssystems - gegebenenfalls einschließlich einiger Zusatzprodukte - zu installieren. Zur Neuinstallation ist eine separate Systemumgebung (siehe unten) erforderlich. Durch die Nutzung von *SystemPac* kann der Aufwand und dadurch auch die Wahrscheinlichkeit von Bedienungsfehlern bei der Neuinstallation erheblich reduziert werden. Es sollte deshalb überlegt werden, bei Neuinstallationen von z/OS auf den *SystemPac*-Mechanismen zurückzugreifen. Dabei sind auch die Zusatzkosten zu berücksichtigen, die dadurch eventuell anfallen.

Permanente Pflege der Komponenten

Das z/OS-Betriebssystem und seine Programm-Produkte müssen permanent gepflegt werden. Fast alle Hersteller stellen für ihre Programme *Patches* (im Mainframe-System als PTFs bekannt) zur Verfügung, die Fehler beheben sollen. IBM stellt diese PTFs für das z/OS-Betriebssystem über verschiedene Kanäle zur Verfügung:

- als Einzellieferung auf Anforderung des Kunden (z. B. auf Grund einer Fehlersituation): hier muss der Anwender die Rahmenbedingungen selbst überprüfen, z. B. die Abhängigkeiten
- als *RefreshPac* im Rahmen präventiver Wartung, angepasst an das Kundensystem (von IBM vorgeprüft) oder
- als OMIS-Lieferung (*Online Maintenance Information System*). OMIS basiert auf den Daten des Kundensystems und ist ebenfalls von IBM vorgeprüft.

Es ist zu überlegen, ob präventive Wartung zur Erhöhung der Betriebssicherheit notwendig ist, oder ob PTFs nur bei aktuellen Fehlern eingespielt werden sollen. Sicherheitsrelevante Patches sollten in jedem Fall präventiv und zeitnah nach dem Erscheinen eingespielt werden. Dies gilt besonders für Systeme mit Internetzugang. Informationen über sicherheitsrelevante Patches können von IBM angefordert werden.

SMP/E-Wartung

Einsatz von SMP/E

Als zentrales Wartungs-Tool ist SMP/E einzusetzen, das *System Modifikation Program/Extended*. Durch die Bestandsführung der Software-Stände im CSI (*Consolidated Software Inventory*) wird sichergestellt, dass alle Informationen über Module, Versionen und Zusammenhänge des z/OS-Betriebssystems zur Verfügung stehen und damit Fehler bei der Installation der Patches möglichst vermieden werden.

Independent Software Vendors

Software-Produkte von ISVs (*Independent Software Vendors*) sollten möglichst ebenfalls über SMP/E installiert und gepflegt werden. Es ist zu überlegen, ob ISV-Produkte separat oder im Rahmen des *SystemPac*-Mechanismus installiert werden sollen.

Consolidated Software Inventory

Es sollte ein CSI für das z/OS-Betriebssystem existieren, bzw. im Falle einer *SystemPac*-Installation gemäß der Lieferung durch IBM sollte das (die) CSI(s), wie im Ablauf vorgesehen, angelegt werden. Pro Hersteller wird ein separates CSI empfohlen, um Problemen mit Namensgleichheit bei PTFs vorzubeugen.

USERMODS

Eigene Änderungen durch Anwender sollten nur mittels SMP/E installiert werden (als *USERMODS*). Dies stellt sicher, dass die eigenen Änderungen nicht durch Herstelleränderungen überspielt werden, ohne dass eine Information darüber vorliegt. Sie müssen nach jedem Releasewechsel des Systems bzw. der Module, auf denen die Änderungen aufsetzen, neu installiert und eventuell auch angepasst werden. *USERMODS* sollten auf ein Minimum begrenzt werden, da sie permanenten Pflegeaufwand nach sich ziehen.

ACCEPT-Läufe

Durch einen *ACCEPT*-Lauf wird ein PTF permanent im System abgelegt, d. h. es ist nicht mehr entfernbar. Ein *ACCEPT*-Lauf sollte daher erst stattfinden, wenn sichergestellt ist, dass die PTFs die festgestellten Probleme beseitigen und keine neuen erkennbaren Fehler hervorrufen.

APPLY CHECK

Es ist zu empfehlen, dass vor dem Einbau von PTFs über einen *APPLY CHECK SMP/E*-Lauf sichergestellt wird, dass die PTFs auch zur aktuell installierten Betriebssystem-Umgebung passen und keine zusätzlichen PTFs erforderlich sind (sogenannte *Prerequisites* oder *Corequisites*).

Test vor Produktion

Die betriebliche Zuverlässigkeit der gelieferten PTFs sollte erst auf einem Testsystem überprüft werden, bevor die PTFs in ein Produktionssystem eingebaut werden. Bei größeren Wartungsarbeiten (z. B. ein sogenannter *Refresh* mit hunderten von PTFs) muss dieser Ablauf in jedem Fall vorgesehen werden.

Kumulative Betriebssystemdateien

Es sollten keine Betriebssystemdateien an SMP/E vorbei kopiert werden, da hierdurch die Sicherheit der Wartung beeinträchtigt werden kann. Kumulierte Dateien sind solche, die aus mehreren Dateien zusammengesetzt worden sind. Sollen kumulierte Dateien verwendet werden, muss entweder die Bestandsführung in SMP/E angepasst oder ein separates Verfahren eingesetzt werden, um die Bestandskontrolle gewährleisten zu können. Es ist daher zu überlegen, ob der Mehraufwand gerechtfertigt ist.

Alternative Systemumgebung

Zum Einbau von PTFs sollte eine zweite (alternative) Systemumgebung benutzt werden. Hierfür sollten separate Festplatten mit einer Kopie des Originalsystems verwendet werden. Dies ermöglicht ein problemloses Einbauen während der Betriebszeiten und erlaubt ein schnelles IPL (*Initial Program Load*) von der veränderten *System Residence* (der Festplatte, von der der Boot-Vorgang eingeleitet wird). Darüber hinaus unterstützt diese Vorgehensweise (Flip-Flop-Verfahren) den schnellen Fallback, da die Festplatten der vorher aktiven Betriebssystemkomponenten noch zur Verfügung stehen.

System-Cloning

Unter *System-Cloning* versteht man das Kopieren der Betriebssystem-Komponenten auf einen neuen Festplatten-Satz unter Berücksichtigung der zu ändernden Definitionen. Es ist zu überlegen, ob ein Verfahren zum *System-Cloning* etabliert wird, um alternative System-Umgebungen schnell und sicher aufbauen zu können.

Ein solches Verfahren muss eigenständig erstellt werden, z. B. in Form eines Batch-Jobs mit mehreren Schritten. Die Benutzung von System-Variablen hilft hier wesentlich.

Einsatz symbolischer System-Variablen

Bei den z/OS-Parameter-Dateien sollte, soweit möglich, mit symbolischen Variablen gearbeitet werden. Dies vereinfacht das *System-Cloning* erheblich und vermeidet vielfach auch Fehldefinitionen. Ab dem z/OS-Betriebssystem V1R4 stehen bis zu 800 Variablen zur Verfügung.

Dokumentation

Es ist zu überlegen, ob ein Berichtswesen, basierend auf SMP/E, aufgebaut werden sollte, um jederzeit den aktuellen Stand der gesamten Software des Betriebssystems darstellen zu können.

Wartung des zSeries-Microcode (Firmware)

Zur Behebung von Code-Fehlern in der Firmware, zum Firmware-Update auf neue Versionen und zur Aktivierung oder Deaktivierung von Hardware-Komponenten (z. B. Prozessoren, Krypto-Hardware) werden von den Herstellern Microcode-Updates durchgeführt. Hierfür müssen folgende Hinweise beachtet werden:

Betreiberkontrolle

Updates durch den Hersteller dürfen nur nach Absprache mit dem Betreiber der zSeries-Systeme und nur unter Kontrolle von Mitarbeitern des Betreibers durchgeführt werden.

Hersteller-Erklärung

Der Hersteller der Betriebssystem-Software sollte eine Vertraulichkeits-Erklärung ausstellen.

Remote Wartung

Einsatz des Remote Support Facilities

Der externe Zugang (*Remote Access*) ist, wie in Baustein B 4.4 *Remote Access* und speziell in Maßnahme M 4.207 *Einsatz und Sicherung systemnaher z/OS-Terminals* beschrieben, zu schützen. Es muss sichergestellt werden, dass Änderungen an Firmware-Komponenten nur nach Abstimmung mit dem zSeries-Systembetreiber erfolgen.

Abbau des z/OS-Betriebssystems

Weiterführende Informationen zu dem Abbau eines z/OS-Betriebssystems sind unter M 2.297 *Deinstallation von z/OS-Systemen* zu finden.

Ergänzende Kontrollfragen:

- Wird SMP/E zur Installation und zu Wartungsarbeiten eingesetzt?
- Werden alle Anwender-spezifische Modifikationen über SMP/E installiert?
- Gibt es eine alternative System-Umgebung?
- Werden symbolische Variablen eingesetzt?
- Ist ein Verfahren zum System-Cloning etabliert?

M 2.294 Synchronisierung von z/OS-Passwörtern und RACF-Kommandos

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

In großen Mainframe-Verbünden kommunizieren oft viele z/OS-Betriebssysteme und ihre RACF-Datenbanken (*Resource Access Control Facility*) miteinander. Es besteht oftmals der Bedarf, Passwortänderungen oder RACF-Kommandos über mehrere z/OS-Systeme des Verbundes zu synchronisieren.

Bei der *Passwort-Synchronisation* werden die Passwörter der Anwender auf mehreren z/OS-Systemen automatisiert synchronisiert, so dass der Anwender nur ein Passwort verwenden muss.

Bei der *RACF-Kommando-Synchronisation* können RACF-Kommandos auf mehreren z/OS-Systemen parallel ausgeführt werden. Das entsprechende RACF-Kommando wird an einem System eingegeben und durch die zentrale RACF-Administration an alle anderen Systeme weitergeleitet. RACF unterstützt dies durch das Feature RRSF (*RACF Remote Sharing Facility*).

Solche Verbünde werden auch *Synchronisierungs-Verbund* genannt. Für einen *Synchronisierungs-Verbund* sind die folgenden Empfehlungen zu beachten.

Standardisierung

Es muss sichergestellt werden, dass der Aufbau und die verwendeten Regeln der RACF-Datenbanken auf allen Systemen des *Synchronisierungs-Verbunds* möglichst identisch sind. Vor der Einrichtung eines Synchronisierungs-Verbunds sollte eine möglichst weitgehende Standardisierung durchgeführt werden (siehe M 2.285 *Festlegung von Standards für z/OS-Systemdefinitionen*).

Sperren einer Benutzerkennung

Bei der Passwort-Synchronisation muss verhindert werden, dass das Sperren (*Revoke*) einer Benutzerkennung nach mehrmaliger Falscheingabe des Passwortes an alle anderen Systeme des Synchronisations-Verbundes weitergeleitet wird. Der Benutzer wäre sonst auf allen Systemen ausgesperrt. Ein Entsperren (*Resume*) kann beliebig oft übertragen werden.

Weiterleiten von RACF-Kommandos

Bei der *RACF-Kommando-Synchronisation* muss mit äußerster Sorgfalt vorgegangen werden. Denn fehlerhafte RACF-Kommandos, die zu ungewollten Änderungen führen, werden sofort auf allen Systemen des Synchronisations-Verbundes ausgeführt. Es sollte deshalb überlegt werden, besonders sicherheitskritische RACF-Kommandos, welche die Stabilität der angebundenen Systeme beeinflussen können, von der Synchronisation auszuschließen.

Absichern der Verwaltungsfunktion

Die Schnittstelle zu der Verwaltungs-Funktion des Synchronisations-Programmes (oft eine ISPF-Oberfläche - *Interactive System Productivity Facility*) darf nur autorisierten Mitarbeitern im Rahmen ihrer Tätigkeit zur Verfügung stehen.

Schadensbegrenzung durch Aufteilen des Verbundes

Zur Schadensbegrenzung bei der RACF-Kommando-Synchronisierung ist zu überlegen, einen großen Synchronisierungs-Verbund in zwei oder mehrere kleine Teilverbünde zu zerlegen.

Die Ausführung von fehlerhaften, sicherheitskritischen RACF-Kommandos kann dadurch auf den jeweiligen Teilverbund beschränkt werden. Ein Totalausfall aller Systeme, der auf fehlerhafte RACF-Kommandos zurückzuführen ist, kann auf diese Weise unter Umständen vermieden werden.

Die für den Betrieb notwendigen Festplatten der Systeme eines Teilverbundes müssen an die Systeme eines anderen Teilverbundes angeschlossen werden können. Dadurch können betriebswichtige Daten eines ausgefallenen Teilverbundes, wie die RACF-Datenbank, zumindest teilweise wieder hergestellt werden.

Die Aufteilung eines großen Synchronisierungs-Verbundes in mehrere kleinere Teilverbünde führt zu einem erhöhten Administrationsaufwand. Denn jeder Teilverbund muss separat administriert werden.

Ergänzende Kontrollfragen:

- Wird verhindert, dass das Sperren einer Benutzerkennung automatisiert weitergeleitet wird?
- Haben nur autorisierte Mitarbeiter Zugang zur Verwaltungs-Funktion des Synchronisations-Programms?

M 2.295 Systemverwaltung von z/OS-Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Systemverwaltung eines z/OS-Systems ist in verschiedene Bereiche aufgeteilt. Für viele Aufgaben gibt es in den Rechenzentren Spezialisten, die oft nur ganz bestimmte Tätigkeiten auf den z/OS-Systemen ausführen. Bei der Systemverwaltung sind nachfolgende Empfehlungen zu beachten:

Unterteilung in Rollen

Es sollte ein Rollenkonzept eingeführt werden. Dies ermöglicht die Zuordnung von System-Berechtigungen zu den Rollen und erleichtert hiermit die Arbeit der RACF-Administration.

Um die Vergabe von hohen Berechtigungs-Attributen im RACF zu reduzieren, sollte überlegt werden, die Administration in mindestens folgende Rollen zu unterteilen:

- Systemadministration

  Die Systemadministration (kein besonderes RACF-Attribut) ist für die Installation und Wartung der z/OS-Systeme verantwortlich. Ihre Berechtigungen dürfen nur die zu dieser Tätigkeit nötigen Arbeiten am System erlauben. Zugriffe auf Kundendaten sollten nur in Ausnahmefällen genehmigt werden (z. B. bei der Fehlersuche). Solche Zugriffe müssen mit dem jeweiligen Informationseigentümer abgestimmt werden.

- RACF-Administration

  Die RACF-Administration (RACF-Attribut *SPECIAL*) hat die folgende Aufgabe: Administration des Sicherheitsprogramms RACF sowie Anlegen und Löschen von Kennungen und Autorisierungen. Der RACF-Administrator vergibt und entzieht die Rechte auf Ressourcen im z/OS-System. Hieraus ergibt sich eine besondere Vertrauensstellung. Aus Sicherheitsgründen sollte die Zahl der Mitarbeiter, die dieser Rolle zugeordnet sind, auf ein Minimum begrenzt sein.

- Space-Management

  Das Space-Management (RACF-Attribut *OPERATIONS*) ist für die Verwaltung der Datenträger in z/OS-Systemen verantwortlich. Das Attribut *OPERATIONS* erlaubt den Zugriff auf alle Daten des Systems. Es sollte überlegt werden, Kennungen mit dem Attribut *OPERATIONS* in die ACCESS-Liste eines RACF-Profiles mit NONE aufzunehmen. Hierdurch wird der Zugriff über die *OPERATIONS*-Berechtigung verhindert. Allerdings können diese Dateien dann auch nur bedingt vom Space-Management verwaltet (z. B. Plattenverlagerung) werden.

- Operating

  Das Operating (kein besonderes RACF-Attribut) ist für den Betrieb der z/OS-Systeme verantwortlich. Da die Operatoren Zugang zu den Konsolen haben, muss das Operating in zutrittsgeschützten Räumen durchgeführt werden. Aus Gründen der Nachvollziehbarkeit sollten die Schichtpläne des Operating archiviert werden.

- Audits

  Der Auditor (RACF Attribut *AUDITOR*) kann alle sicherheitsrelevanten Systemeinstellungen einsehen, aber nicht ändern. Der Auditor gleicht die aktuellen Systemeinstellungen mit den vorgegebenen Systemeinstellungen ab.

Stellvertreter-Regelungen

Für alle wichtigen Rollen der Systemverwaltung müssen Stellvertreter-Regelungen vorhanden sein. Keinesfalls darf eine wichtige Rolle nur mit einer Person besetzt sein. Weitere Hinweise hierzu sind in M 3.10 *Auswahl eines vertrauenswürdigen Administrators und Vertreters* aufgeführt.

Ergänzende Kontrollfragen:

- Gibt es ein Rollenkonzept für z/OS-Systeme?
- Gibt es Stellvertreter-Regelungen für die wichtigen Rollen der Systemverwaltung?

M 2.296 Grundsätzliche Überlegungen zu z/OS-Transaktionsmonitoren

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der Einsatz von Transaktionsmonitoren muss detailliert geplant und durch geeignete Mechanismen abgesichert werden. Als Hilfestellung werden in dieser Maßnahme einige Empfehlungen im Überblick beschrieben, die sich aus Sicht der IT-Sicherheit beim Betrieb von Transaktionsmonitoren bewährt haben. Je nach Einsatzszenario sind in der Regel weitere spezifische Planungen und Sicherheitsmechanismen erforderlich, die hier nicht dargestellt werden können. Insbesondere wird in dieser Maßnahme nicht der Datenbankteil von IMS betrachtet.

Transaktionsmonitore werden auf Mainframe-Systemen für den Online-Betrieb eingesetzt. Sie ermöglichen den Anwendern, im Dialogbetrieb auf die gewünschten Daten über nachgeschaltete Datenbanksysteme zuzugreifen. Dabei gehört es zu den Kernaufgaben des Transaktionsmonitors sicherzustellen, dass die folgenden Bedingungen erfüllt werden:

- Eine Transaktion muss immer komplett durchgeführt werden. Ist das nicht realisierbar, muss das System auf den vorherigen Stand zurückgesetzt werden (Roll-Back).
- Das System sollte sich vor und nach der Transaktion in einem konsistenten Zustand befinden, ansonsten muss das System zurückgesetzt werden.
- Jeder Anwender soll nur Zugriff auf seine Daten erhalten und sollte isoliert sein von allen anderen Daten.
- Nach Durchführung der Transaktion muss sichergestellt werden, dass der veränderte Zustand gespeichert wird und später in der gleichen Form zur Verfügung steht. Im Falle eines Systemausfalls müssen die noch nicht gespeicherten Transaktionen notfalls automatisch wiederholt werden.

Diese Bedingungen gelten sowohl für den Online-Betrieb, als auch für Transaktionen, die im Batch-Betrieb durchgeführt werden.

Transaktionsmonitore werden heute üblicherweise in einer sogenannten Drei-Tier-Konfiguration (Tier = Stufen) eingesetzt (Präsentation, Anwendungslogik, Datenhaltung) und decken normalerweise die folgenden Kernfunktionen ab:

- Message Queuing (Verwalten des Nachrichten-Flusses)
- Lock-Verwaltung (Verwaltung der Zugriffe und gegenseitige Absicherung)
- Logging (Verwaltung der Log-Funktionen)
- Roll-Back Funktionen (Zurückspringen auf den vorherigen Zustand)
- Laststeuerung (Load Balancing)

- Two-Phase Commit-Synchronisation (stellt sicher, dass eine Transaktion komplett durchgeführt wird oder ein Roll-Back erfolgt)

Als Transaktionsmonitor wird u. a. IMS TM (*Information Management System Transaction Monitor*) oder CICS (*Customer Information Control System*) eingesetzt. Als Datenbanksystem steht für IMS der IMS-eigene DB-Teil, VSAM-Datenbanken (*Virtual System Access Method*) oder DB2 (*Database 2*) zur Verfügung. Für CICS können VSAM, IMS DB oder DB2 als Datenbanksysteme eingesetzt werden.

Auch wenn die Transaktionsmonitore und Datenbanksysteme aus historischen Gründen eigene interne Schutzsysteme zum Teil noch anbieten, wird in der heutigen Zeit meistens ergänzend ein Sicherheitssystem wie RACF (*Resource Access Control Facility*) eingesetzt. Mit RACF können die Authentisierung des Benutzers, der Schutz der Transaktionen und der Zugriffsschutz auf Datenelemente realisiert werden.

Allgemeine Überlegungen

Die Transaktionsmonitore IMS TM und CICS sind von der historischen Entwicklung her reine VTAM-Applikationen. Sie waren zu Beginn der Entwicklung für interne Netze konzipiert. Im Laufe der letzten Jahre sind jedoch durch die steigende Bedeutung des Internets erweiterte Schnittstellen bereitgestellt worden. Diese ermöglichen es, Zugriffe auf Anwendungen dieser Transaktionsmonitore auch vom Internet aus zu erlauben.

Die folgenden Empfehlungen gelten für den gesamten Bereich der Transaktionsmonitore und schließen die Datenbanken mit ein:

- Alle Sicherheitsmechanismen sollten möglichst durch RACF gesteuert werden. Die internen Sicherheitsmechanismen sind nur dort zu benutzen, wo es keine adäquaten RACF-Funktionen gibt.

Standards

- Es sollten vor Inbetriebnahme eines Transaktionsmonitors, wie IMS oder CICS, oder eines Datenbanksystems, wie DB2, Standards für alle relevanten Definitionen entwickelt werden. Die Standards sollten Transaktionsnamen, Tabellennamen, Resource Classes, etc. betreffen. Solche Standards helfen dabei, Fehler bei RACF-Definitionen zu vermeiden (siehe M 2.285 *Festlegung von Standards für z/OS-Systemdefinitionen*).

Rollen einführen

- Es sollte überlegt werden, ob die Einführung von Rollen-Konzepten (siehe M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*) die Verwaltung der Benutzer erleichtert.

Externalisierung der Sicherheitsmechanismen

- Sicherheitsmechanismen sollten bei Transaktionsmonitoren immer so aktiviert werden, dass das entsprechende Regelwerk extern definiert werden kann. Der Einsatz externer Sicherheitsfunktionen, wie RACF-Definitionen, sollte immer eventuell vorhandenen internen Funktionen vorgezogen werden.

IMS TM (*Transaction Monitor*, vorher *DC* genannt)

Die folgenden Empfehlungen gelten für den IMS Transaktionsmonitor. Je nach Einsatzszenario sind in der Regel weitere Sicherheitsmechanismen erforderlich.

- IMS sollte über die Definition im *IMS Security Makro* so eingestellt werden, dass IMS RACF verwendet (Parameter *TYPE = RACFAGN / RACFTERM / RACFCOM*). Das IMS System muss durch die *RCLASS* Definition so definiert werden, dass dieser Name (die IMS-ID) in RACF als *Resource Class* geführt werden kann. Ist mehr als ein IMS im z/OS-System in Betrieb, sollte überlegt werden, ob die standardmäßig in RACF vorhandenen Namen benutzt werden sollen (z. B. AIMS, TIMS usw.) oder ob eigene (unterschiedliche) Namen vergeben werden sollten. Bei der Benutzung von eigenen Namen müssen diese als *Resource Classes* in RACF eingetragen werden.

  Über das IMS Security Makro können u. a. die folgenden Prüfungen aktiviert werden (Benutzung der Default IMS-ID IMS):

  - AGN Prüfung über RACF (über Klasse AIMS), Ablegen der gültigen User-IDs für IMS in RACF (RDEFINE)
  - Transaktions-Autorisierung (über Klasse TIMS oder GIMS und SECLVL=TRANAUTH im Security Makro)
  - Terminal Security (SECLVL=SIGNON / FORCSIGN im Security Macro und Resource Class TERMINAL in RACF)
  - Kommando Autorisierung (über Klasse CIMS oder DIMS)

  Existiert ein Parallel Sysplex mit Datasharing, sollte als RCLASS Wert die IMS-ID des Master-IMS benutzt werden.
- Es sollte überlegt werden, ob zur Signon Verifizierung ein Exit (DFSSGNX0) eingesetzt werden sollte (falls die RACF Prüfung nicht ausreichend granular ist).
- Es müssen in RACF Standard Profile für die einzelnen Resource Classes eingerichtet werden, zu denen die Applikations-Anwender zugelassen werden können. Es ist empfehlenswert, vor Beginn der Definitionen Standards zu entwickeln, die die Definitionen erleichtern.
- Es sollte überlegt werden, ob die Sicherheitsanforderungen eine Terminal-Security über RACF notwendig machen (Class Terminal). Vorsicht ist geboten bei Einführung eines restriktiven Schutzes gegen nicht definierte Terminals, z. B. mit dem RACF Kommando SETROPTS TERMINAL(NONE): Es müssen mindestens einige Terminals für die Benutzung von RACF unter TSO freigeschaltet sein, da sich sonst niemand mehr auf dem System anmelden kann!

  RACF Terminal Security
- Das Mapping von RACF-Resource Classes auf die internen IMS Security Regeln erfolgt über Definitionen, die über den SMU-Prozess (Security Management Utility) verarbeitet werden. Aus der Definitionsdatei wird über einen Preprocessor und nachfolgendem Assembly und Link ein Loadmodule erzeugt, das auf dem IMS Matrix Dataset gestellt wird und in

dem u. a. die IMS Security Definitionen in Kontrollblockform zur Verfügung stehen. Die Datei des Quellcodes darf nur von Mitarbeitern zugreifbar sein, die diese Datei im Rahmen ihrer Tätigkeit benötigen.

- Zugriffe auf IMS aus dem TCP/IP-Netz (z. B. aus dem Internet) erfolgen über die OTMA-Schnittstelle (*OpenTransaction Manager Access*). Zur Absicherung dieser Verbindung muss über den Parameter *OTMASE=xxx* mindestens *CHECK* (besser *FULL*) sichergestellt werden, dass RACF zur Verifizierung eingesetzt wird. IMS Kommandos werden dabei gegen die Klasse *CIMS*, Transaktionen gegen *TIMS* geprüft. Die Gültigkeit der Verbindung sollte über Profile in der *FACILITY* Klasse in RACF sichergestellt werden.
- Es ist zu überlegen, ob die IMS Programme (Control Region, Message Processing Region, Utilities) zur Erhöhung der Sicherheit über die RACF Klasse *Program* geschützt werden sollen.
- Die IMS Dateien müssen über RACF Dataset Profile so geschützt werden, dass nur Mitarbeiter Zugriff zu den Dateien haben, die sie im Rahmen ihrer Tätigkeit auch benötigen. Anwender von IMS benötigen keinen Zugriff auf die IMS Dateien. Zu schützende Dateien sind z. B.
  - APF-Dateien (Authorized Programming Facility)
  - System-Dateien
  - Anwender-Dateien wie z. B. PSB-, DBD-, ACB- und PGM-LIB

  Der Zugriff auf APF- und System-Dateien darf nur für die STC-User-IDs (*Started Task Control*) und autorisierte Mitarbeiter freigegeben werden. Normale Anwender benötigen keinen Zugriff auf diese Dateien (siehe auch M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen*).

  Der Zugriffsschutz von Anwender-Dateien muss durch RACF Definitionen erfolgen (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).
- MVS Kommandos für IMS sollten über RACF geschützt werden (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).
- Die Started Tasks sollten über die RACF Klasse *STARTED* abgesichert werden (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).
- Bei besonders hohen Sicherheitsanforderungen an IMS kann auch der Zugang zur IMS Kontroll-Region generell durch die RACF *Resource Class* APPL auf der Basis des VTAM LU-Namens abgesichert werden. Da jeder Anwender hierbei entweder als einzelner User oder in Gruppen definiert werden muss, ist zu beachten, dass dadurch ein erhöhter Administrationsaufwand entsteht. Dies gilt besonders für Installationen mit vielen Anwendern.

CICS

Die folgenden Empfehlungen gelten für den CICS Transaktionsmonitor. Je nach Einsatzszenario sind in der Regel zusätzliche Sicherheitsmechanismen erforderlich. Weitere Informationen sind in der IBM Dokumentation *CICS RACF Security Guide* zu finden:

- Sollen die CICS-Regions im Modus *Non-Swappable* laufen (PPT-Eintrag im SCHEDnn Parmlib-Member), muss sichergestellt werden, dass die Option *NOPASS* für das Modul DFHSIP im PPT-Eintrag (Program Property Table) **nicht** gesetzt wird. Die Option NOPASS umgeht Passwort- und RACF-Prüfungen.
- Die Started Task User-IDs müssen so definiert werden, wie M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF* beschrieben ist. Die User-IDs von CICS Started Tasks dürfen nicht das Attribut *OPERATIONS* besitzen.
- Die CICS Dateien müssen über RACF Dataset Profile so geschützt werden, dass nur Mitarbeiter Zugriff auf die Dateien haben, die sie im Rahmen ihrer Tätigkeit auch benötigen. Zu schützende Dateien sind z. B.
  - APF-Dateien (Authorized Programming Facility)
  - System-Dateien
  - Anwender-Dateien wie z. B. PSB-, DBD-, ACB- und PGM-LIB
- Der Zugriff auf APF- und System-Dateien darf nur für die STC-User-IDs (*Started Task Control*) und autorisierte Mitarbeiter freigegeben werden. Normale Anwender benötigen keinen Zugriff auf diese Dateien (siehe auch in M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen*).

  Der Zugriff auf Anwender-Dateien muss im Rahmen der RACF Regeln erfolgen (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).
- MVS Kommandos für CICS sollten über RACF geschützt werden (siehe dies M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).
- Die Aktivierung von RACF für die CICS-Security erfolgt in der SIT (*System Initialization Table*) durch Setzen des Parameters SEC=*YES*. In der SIT kann auch definiert werden, ob Transaktionsschutz, Programmschutz oder Feldschutz von Eingabemasken über RACF aktiviert werden soll. Es muss sichergestellt werden, dass diese Modifikationen nur von autorisierten Mitarbeitern durchgeführt werden können. Dabei ist zu beachten, dass die Auswahl der SIT sowohl über *SYSIN* Eingabe als auch über einen Parameter im *EXEC Statement* der Prozedur (in der *Job Control Language*) definiert werden kann. Das SIT-Modul muss in eine APF-Bibliothek eingestellt und über RACF Profile so geschützt werden, dass nur die für diesen Bereich zuständigen Mitarbeiter Zugriff haben (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*). Auch die Quell-Datei der SIT darf nur zugreifbar sein für die dazu befugten Mitarbeiter und muss mit entsprechenden RACF Dateiprofilen geschützt werden.
- Die Kommando Security muss bei der Definition der Transaktionen eingeschaltet sein (*CMDSEC Parameter*). Es ist zu überlegen, ob durch SECPRFX=*YES* die Systeme voneinander unterschieden werden sollen. Dies ist empfehlenswert bei verschiedenen CICS-Jobs in einem System.
- Die Prozeduren der CICS Regions stehen auf einer (oder mehreren) Prozedur-Bibliothek(en). Diese müssen durch RACF so geschützt werden, dass nur Mitarbeiter diese Prozeduren verändern können, die im Rahmen ihrer Tätigkeit darauf Zugriff haben müssen. Es ist zu überlegen, ob eine separate *PROCLIB* (mit entsprechender Verknüpfung zu den anderen

PROCLIBs) das Sicherheitsniveau erhöht und das Missbrauchsrisiko durch getrennte Zugriffsdefinitionen dadurch verringert werden kann.

- Die Anmeldung an CICS muss über die Eingabe von RACF User-ID und Passwort erfolgen. Es ist zu empfehlen, eine Signon-Maske für die Anmeldung an CICS vorzusehen. Für jede CICS Region muss daher ein Default-User in RACF definiert sein. Die in der Default-User-ID im CICS-Segment definierten Vorgaben werden von CICS für alle Terminal Sessions verwendet, bis ein Signon mit der persönlichen User-ID durchgeführt wurde. Es wird empfohlen, die Default-User-ID nur mit sehr geringen Rechten auszustatten.
- Die *General Resource Classes* Txxxxxxx (*Member Class*) und Gxxxxxxx (*Group Class*) sollten für Transaktionssicherheit, die Klassen Cxxxxxxx (*Member Class*) und Vxxxxxxx (*Group Class*) für Kommando Sicherheit aktiviert werden (über das Kommando *SETROPTS*).
- Sicherheitsmechanismen in der Anwendung (Applikation) sollten nur dort implementiert werden, wo keine adäquaten Sicherheitsfunktionen von RACF oder anderen Sicherheitssystemen zur Verfügung stehen.
- Es ist zu überlegen, ob ein Terminalschutz auf Basis der VTAM-LU (Logical Unit) aktiviert werden soll. Diese Maßnahme erhöht den Schutz, bedeutet jedoch mehr Verwaltungsaufwand.
- Der Zugang zu der CICS Region kann über den VTAM ACB-Namen (*Access Control Block*) über RACF kontrolliert werden. Sollte diese Kontrolle eingesetzt werden, empfiehlt es sich, ein Gruppenkonzept aufzubauen, um den Verwaltungsaufwand möglichst gering zu halten.
- Für die CICS Transaktionen und System Kommandos sind unterschiedliche Gruppen zu bilden. Alle CICS Administrations-Transaktionen und alle kritischen CICS Kommandos sollten so geschützt werden, dass nur die Mitarbeiter Zugriff zu diesen Transaktionen haben, die sie im Rahmen von Administrationstätigkeiten auch benötigen. Eine Vertretungsregelung sollte vorhanden sein. Es ist zu überlegen, ob es erforderlich ist, weitere CICS *Resource Classes* einzusetzen (siehe *CICS RACF Security Guide*).
- **CICS System Definitionen**

  CICS Systemdefinitionen können entweder über die RCT (*Resource Control Table*) oder über die CSD (*CICS System Definitions*) vorgenommen werden. Während die ältere RCT noch als Loadmodule via *Assembly* und *Link* erstellt wird, wird die CSD durch den RDO Dialog (*Resource Definition Online*) über die Transaktionen CEDA, CEDB und CEDC als VSAM-Datei erstellt und von CICS eingelesen. In beiden Fällen müssen sowohl die relevanten Dateien als auch die Transaktionen durch RACF Profile so geschützt werden, dass nur CICS-Administratoren Zugriff auf diese Definitionen haben. Hier wird u. a. auch das CICS-DB2 Attachment über das Makro *DB2CONN* definiert, in dem z. B. der Name des DB2 Subsystems, die Berechtigungen auf bestimmte Kennungen oder Relationen zwischen Transaktion, DB2 Plan und Programm festgelegt werden.

Es ist zu überlegen, ob CEDC (die nur lesende Aktionen durchführt) auch geschützt werden soll. Dies hängt vom Inhalt der Daten ab.

DB2

Die folgenden Empfehlungen gelten für das DB2-Datenbanksystem. Je nach Einsatzszenario sind in der Regel zusätzliche Sicherheitsmechanismen erforderlich. Weitere Informationen sind in der IBM Dokumentation *DB2 UDB Administration Guide* zu finden:

- Für jedes DB2-Subsystem muss ein Eintrag in der RACF *Router Table* vorgenommen werden, da diese Einträge standardmäßig nicht mit ausgeliefert werden.
- Die General Resource Class *DSNR* muss über das Kommando SETROPTS aktiviert werden. Die Profile müssen gemäß DB2 Dokumentation definiert und Zugriffe dazu über *PERMIT* Kommandos eingerichtet werden. Vorher sollte ein Gruppenkonzept entwickelt werden, wie es beispielhaft in der IBM Dokumentation *DB2 UDB Administration Guide* beschrieben ist. Ist eine VTAM LU 6.2 Verbindung (*Virtual Telecommunication Access Management*) im Einsatz, sollte überlegt werden, ob ein zusätzlicher Schutz über die Klasse *APPCLU* zweckmäßig ist.
- Die DB2 Dateien müssen über RACF Dataset Profile so geschützt werden, dass nur Mitarbeiter Zugriff auf die Dateien haben, die sie im Rahmen ihrer Tätigkeit auch benötigen. Zu schützende Dateien sind z. B.
  - APF-Dateien (Authorized Programming Facility)
  - System-Dateien
  - Anwender-Dateien als Datenbanken

  Der Zugriff auf APF- und System-Dateien darf nur für die STC-User-IDs (*Started Task Control*) und autorisierte Mitarbeiter freigegeben werden. Andere Anwender benötigen keinen Zugriff auf diese Dateien (siehe auch M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen*).

  Der Zugriff auf Anwender-Dateien muss im Rahmen der RACF Regeln erfolgen (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).
- Der Zugriff auf die Prozedurbibliotheken der DB2 *Started Tasks* ist durch RACF Dateiprofile zu schützen (siehe M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen*).
- MVS Kommandos für DB2 sollten über RACF geschützt werden (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).
- Die DB2 Started Task User-IDs müssen in der RACF Klasse *STARTED* als *Protected User* definiert werden. Die User-IDs benötigen Zugriffe auf die Dateien der Started Task Prozeduren.
- Alle DB2 Dateien sollten über RACF *Dataset* Profile abgesichert werden, wobei normale Benutzer keinen direkten Zugriff auf die Datenbank haben sollten. Direkte Zugriffe sollten auf die Administratoren beschränkt bleiben.

- Es ist zu empfehlen, keine DB2 *GRANT PUBLIC* Genehmigung auf DB2-Katalog-Tabellen zu erteilen. Statt dessen sollten Zugriffsrechte auf der Ebene von Benutzergruppen vergeben werden.
- Es wird empfohlen, die internen System-Tabellen nur über DB2-Admin Kommandos (GRANT in DB2) zu schützen. Zugriffsrechte auf User-Tabellen sollten über RACF Gruppen vergeben werden. Dabei muss die RACF Gruppe in DB2 durch entsprechende GRANTs autorisiert werden. Die Autorisierung einzelner User-IDs oder (besser) ganzer Gruppen lässt sich durch das RACF Kommando *Permit* realisieren. Alle Sicherheitsdefinitionen sollten möglichst zu RACF verlegt werden.

Ergänzende Kontrollfragen:

- Wird zum Schutz der Transaktionen und der Transaktionsmonitore ein Sicherheitssystem wie RACF eingesetzt?
- Sind die Started Tasks von IMS, CICS oder DB2 über RACF gesichert?
- Gibt es ein Gruppenkonzept für den IMS Transaktionsmonitor?
- Werden die CICS General Resource Classes eingesetzt?
- Sind alle DB2 Dateien über RACF Dataset Profile abgesichert?

M 2.297 Deinstallation von z/OS-Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Wird ein z/OS-System nicht mehr benötigt, so reicht es nicht, das System einfach auszuschalten. Beim Abbau eines z/OS-Systems oder eines *Parallel-Sysplexes* sollten die folgenden Empfehlungen beachtet werden:

Festplatten löschen

Alle Festplatten, die sensitive Daten wie Kundendaten enthalten, müssen so gelöscht werden, dass ihr Inhalt nicht mehr reproduziert werden kann. Hierfür kann ein Programm wie ICKDSF eingesetzt werden. Das Löschen kann u. U. auch durch die Herstellerfirma durchgeführt werden. Sind Festplatten, auch einzelne, defekt und müssen deshalb vom Hersteller ausgetauscht werden, ist sicherzustellen, dass die ausgetauschte Festplatte durch den Hersteller vernichtet wird. Dies sollte vertraglich vereinbart werden. Entsprechendes gilt auch für den Austausch eines kompletten Festplattenschranks. Vor der Weitergabe von Datenträgern an Dritte muss in jedem Fall geprüft werden, ob der Schutzbedarf der gespeicherten Daten dies zulässt (siehe auch M 2.167 *Sicheres Löschen von Datenträgern*).

Kennungen löschen

Alle Kennungen des deinstallierten Systems müssen gelöscht werden, sofern dies nicht schon automatisch durch den Abbau erfolgt. Wenn ein System aus einem *Parallel-Sysplex* herausgelöst wird, so sind die Kennungen und Aliase auf den anderen Systemen des *Parallel-Sysplex* zu löschen.

Die betroffenen Kennungen müssen aus den Verwaltungssystemen (z. B. Benutzerverwaltung) entfernt werden.

System-Namen entfernen

Die System-Namen (*SYSIDs*) müssen aus den System-Listen entfernt werden. Falls ein System aus einem *Parallel-Sysplex* genommen wird, muss der System-Name aus den *Sysplex*-Definitionen entfernt werden.

System entfernen

Das System muss aus dem Passwort-Synchronisierungsverfahren entfernt werden, falls ein solches Verfahren in Betrieb ist (siehe M 2.294 *Synchronisierung von z/OS-Passwörtern und RACF-Kommandos*).

Terminal-Monitor-Programme

Das System muss aus allen Terminal-Monitor-Programmen, z. B. TPX (*Terminal Productivity Executive*) oder NV/AS (*NetView/Access*), entfernt werden.

NJE-Definitionen korrigieren

Das System muss aus den NJE-Definitionen (*Network Job Entry*) des JES2/3 entfernt werden.

Berichtswesen

Das Berichtswesen ist darauf zu überprüfen, ob Definitionen entfernt und eventuell Tabellen gelöscht werden müssen.

Automation

Vorhandene Automationsverfahren sind darauf zu untersuchen, ob Definitionen angepasst werden müssen.

Lizenzschlüsselverwaltung

Da sich durch den Abbau die Anzahl der Systeme reduziert hat, sollte geprüft werden, ob Software-Lizenzen nicht mehr benötigt werden und daher abbestellt werden können.

Ergänzende Kontrollfragen:

- Werden sensitive Daten auf frei werdenden Festplatten vollständig gelöscht?
- Trägt das Löschverfahren dem Schutzbedarf der gespeicherten Informationen Rechnung?
- Wird das zu deinstallierende System aus allen relevanten Tabellen entfernt?

M 2.298 Verwaltung von Internet-Domainnamen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT

Internet-Domainnamen (*Domains*) müssen bei Registrierungsstellen (*Registrars*) angemeldet werden. Eine Registrierungsstelle kann Namen für eine oder mehrere sogenannte Top-Level-Domains (beispielsweise die "klassischen" Domains *.com*, *.org*, *.gov* und die diversen Länder-Domains wie *.de* für Deutschland, *.at* für Österreich und *.ch* für die Schweiz) vergeben. Domains werden jeweils für einen bestimmten Zeitraum registriert. Ist dieser Zeitraum abgelaufen, so muss die Registrierung gegen Zahlung einer Gebühr verlängert werden. Wird die Verlängerung einer Registrierung vergessen, so kann dies unangenehme Folgen haben (siehe G 2.100 *Fehler bei der Beantragung und Verwaltung von Internet-Domainnamen*). Es muss daher sichergestellt sein, dass die Registrierungen für alle Domains, die von einer Organisation benutzt werden, regelmäßig und rechtzeitig verlängert werden. Dazu sollte in jeder Organisation eine Stelle festgelegt werden, die die Verwaltung der Domainnamen bei den verschiedenen Registrierungsstellen koordiniert.

Neben der Verwaltung der Domainnamen und der Sicherstellung der rechtzeitigen Verlängerung der Registrierungen sollten beim Management von Internet-Domainnamen auch folgende Punkte berücksichtigt werden:

DNS Nameserver

Primary Nameserver in verschiedene Subnetze

Bei der Registrierung eines Domainnamens müssen mindestens zwei DNS-Nameserver (*Primary Nameserver*) angegeben werden, die für die Zuordnung von Rechnernamen zu IP-Adressen zuständig sind. Ein Nameserver wird oft vom Internet-Zugangsprovider betrieben, kann aber auch von der Organisation selbst betrieben werden. Bei der Festlegung der Nameserver sollte zumindest darauf geachtet werden, dass die *Primary Nameserver* in verschiedenen Class-C Netzen liegen. Ist dies nicht der Fall, so kann ein Denial of Service Angriff auf den Router, mit dem dieses Netz ans Internet angebunden ist, die komplette Domain lahm legen, da keine Namen aus dieser Domain mehr aufgelöst werden können. Bei hohen Anforderungen an die Verfügbarkeit der Namensauflösung sollten die *Primary Nameserver* idealerweise in verschiedenen Netzen mit Anbindung über unterschiedliche Provider angesiedelt werden

Domainnamen

Domains mit Firmen- und Produktnamen

Zu Anfang des "Internet-Zeitalters" reichte es meist aus, wenn eine Organisation eine einzige Internet-Domain betrieb. Mit der wachsenden Popularität des World-Wide-Web wurde es üblich, nicht nur eine Domain mit beispielsweise dem eigenen Firmennamen zu betreiben, sondern auch für bekannte Produkte Domains einzurichten.

Domain-Grabbing vorbeugen

Um zu verhindern, dass Domains mit dem Namen eigener Produkte und Dienstleistungen von Anderen registriert werden, die unter dieser Adresse dann eventuell pornographische oder andere anstößige Inhalte verbreiten, die von Besuchern dann mit der eigenen Organisation in Verbindung gebracht werden, sollten soweit möglich nicht nur der eigene Firmenname und die

Namen bekannter eigener Produkte in der korrekten Schreibweise registriert werden, sondern jeweils auch Varianten davon, etwa mit oder ohne Bindestrichen bei zusammengesetzten Namen. Diese Namen sollten unter den verschiedenen "relevanten" Top-Level-Domains (etwa *.de*, *.com*, *.org*, *.info*) registriert werden. Außerdem sollte geprüft werden, ob nicht auch bestimmte falsch geschriebene Varianten (etwa bestimmte "Buchstabendreher") von Produkt- oder Firmennamen registriert werden sollten. Der dadurch entstehende Mehraufwand ist gering im Vergleich zu dem Aufwand, gegebenenfalls die "Herausgabe" einer Domain gerichtlich erzwingen zu müssen.

Für solche "sicherheitshalber" registrierten Domains sollte zumindest ein minimales Webangebot eingerichtet werden, das den Domainnamen nennt, auf dem das eigentliche Angebot eingerichtet ist und eine Weiterleitung dort hin anbietet. Gegebenenfalls kann auch einfach der Haupt-Webserver der Organisation über eine entsprechende Namensauflösung auch als Webserver für diese Domain agieren.

Registrierungsstellen und Registrierungszeiträume

Für mehrere Top-Level Domains (etwa *.com* und *.org*) existieren verschiedene Registrierungsstellen. Ein Wechsel der Registrierungsstelle ist jederzeit möglich, aber meist mit Kosten verbunden.

Übersicht über Laufzeiten, Preise und Kontakte behalten

Es ist wichtig, für alle registrierten Domains einen Überblick über die jeweilige Laufzeit der Registrierung, den Preis für die Verlängerung und die Bankverbindung der Registrierungsstelle zu haben, um eine rechtzeitige Verlängerung der Registrierung sicher zu stellen.

Vertragsgestaltung mit Internetdienstleistern

Wenn die Domains der Organisation nicht in Eigenregie registriert und verwaltet werden, sondern dies über einen Internetdienstfeister geschieht, so muss bei der Vertragsgestaltung darauf geachtet werden, dass die Organisation selbst die Kontrolle über die Domains behält. Dies kann beispielsweise bei einem eventuellen Wechsel des Registrars oder bei der Auflösung von Namensstreitigkeiten von Bedeutung sein.

Für den Fall von Fehlern und Versäumnissen des Dienstleisters im Bezug auf die Verwaltung von Domainnamen sollten entsprechende Regelungen getroffen werden, da in solchen Fällen erheblicher Schaden entstehen kann (siehe G 2.100 *Fehler bei der Beantragung und Verwaltung von Internet-Domainnamen*).

Falls die Nameserver nicht in der Organisation selbst betrieben, sondern bei einem Dienstleister gehostet werden, sollten in den Service-Level-Agreements insbesondere Vereinbarungen über die Anforderungen an die Verfügbarkeit der Nameserver und an Bearbeitungszeiten für Änderungen im DNS der Organisation getroffen werden.

Ergänzende Kontrollfragen:

- Welche Domainnamen wurden registriert?
- Existiert ein Überblick über Laufzeiten, Preise und Kontakte für die Domainregistrierungen?
- Wo werden die Nameserver der Organisation betrieben?

M 2.299 Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Da das Sicherheitsgateway für die Sicherheit des Netzes eine zentrale Rolle spielt, ist der sichere und ordnungsgemäße Betrieb besonders wichtig. Dieser kann nur sichergestellt werden, wenn das Vorgehen in die bestehenden sicherheitstechnischen Vorgaben integriert ist.

Die zentralen sicherheitstechnischen Anforderungen (das zu erreichende Sicherheitsniveau) ergeben sich aus der organisationsweiten Sicherheitsleitlinie und sollten in einer spezifischen Sicherheitsrichtlinie für den Betrieb des Sicherheitsgateways formuliert werden, um die übergeordnet und allgemein formulierte Sicherheitsleitlinie im gegebenen Kontext zu konkretisieren und umzusetzen.

In diesem Zusammenhang ist zu prüfen, ob neben der organisationsweiten Sicherheitsleitlinie weitere übergeordnete Vorgaben wie beispielsweise IT-Richtlinien, Passwortrichtlinien oder Vorgaben zur Internetnutzung zu berücksichtigen sind.

Die Sicherheitsrichtlinie muss allen Personen und Gruppen, die an der Beschaffung und dem Betrieb des Sicherheitsgateways beteiligt sind, bekannt sein und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die Sicherheitsrichtlinie sollte zunächst das generell zu erreichende Sicherheitsniveau spezifizieren und grundlegende Aussagen zum Betrieb des Sicherheitsgateways treffen. Nachfolgend sind einige Punkte aufgeführt, die berücksichtigt werden sollten:

- Allgemeine Konfigurationsstrategie: Da das Sicherheitsgateway eine zentrale Rolle bei der Absicherung des Netzes spielt, muss es selbst (bzw. die einzelnen Komponenten) besonders sicher konfiguriert sein.
- Regelungen für die Arbeit der Administratoren und Revisoren:
  - Über welche Zugangswege dürfen Administratoren und Revisoren auf die Systeme zugreifen (beispielsweise nur lokal an der Konsole, über ein eigenes Administrationsnetz oder über verschlüsselte Verbindungen)?
  - Welche Vorgänge werden müssen dokumentiert werden? In welcher Form wird die Dokumentation erstellt und gepflegt?
  - Gilt für bestimmte Änderungen ein Vieraugenprinzip? Für besonders sicherheitskritische Änderungen an den Einstellungen des Sicherheitsgateway ist dies dringend empfohlen.
  - Nach welchem Schema werden Administrationsrechte vergeben?
- Vorgaben für Beschaffung von Geräten anhand eines Anforderungsprofils

- Vorgaben für die Installation und Konfiguration einzelner Komponenten des Sicherheitsgateways
  - Vorgehen bei der Erstinstallation
  - Überprüfung der Default-Einstellungen hinsichtlich Sicherheitsgefährdungen
  - Regelungen zur physikalischen Zugriffskontrolle
  - Verwendung und Konfiguration von Konsole und sonstigen Zugriffsarten
  - Regelungen zur Benutzer- und Rollenverwaltung, Berechtigungsstrukturen (Ablauf und Methoden der Authentisierung und Autorisierung, Berechtigung zu Installation, Update, Konfigurationsänderungen etc.). Nach Möglichkeit sollte ein Rollenkonzept für die Administration erarbeitet werden.
  - Regelungen zu Erstellung und Pflege von Dokumentation, Form der Dokumentation: Verfahrensanweisungen, Betriebshandbücher
- Vorgaben für den sicheren Betrieb
  - Absicherung der Administration (beispielsweise: Zugriff nur über abgesicherte Verbindungen)
  - Einsatz von Verschlüsselung (Standards, Schlüsselstärken, Einsatzbereiche)
  - Vorgaben zu Passwortnutzung (Passwortregeln, durch Passwörter zu schützende Bereiche, Regeln und Situationen für Passwortänderungen, gegebenenfalls Hinterlegung von Passwörtern)
  - Werkzeuge für Betrieb und Wartung, Integration in ein bestehendes Netzmanagement
  - Berechtigungen und Vorgehensweisen bei Softwareupdates und Konfigurationsänderungen
- Protokollierung
  - Welche Ereignisse werden protokolliert?
  - Wo werden die Protokolldateien gespeichert?
  - Wie und in welchen Abständen werden die Protokolle ausgewertet?
- Datensicherung und Recovery
  - Einbindung in das organisationsweite Datensicherungskonzept
- Störungs- und Fehlerbehandlung, Incident Handling
  - Regelungen für die Reaktion auf Betriebsstörungen und technische Fehler (lokaler Support, Fernwartung)
  - Regelungen für Sicherheitsvorfälle
- Notfallvorsorge
  - Einbindung in das organisationsweite Notfallvorsorgekonzept

- Revision und Audit (Verantwortlichkeiten, Vorgehen, Integration in ein übergreifendes Revisionskonzept)

Die Verantwortung für die Sicherheitsrichtlinie liegt beim IT-Sicherheitsmanagement, Änderungen und Abweichungen hiervon dürfen nur in Abstimmung mit dem IT-Sicherheitsmanagement erfolgen.

Bei der Erstellung einer Sicherheitsrichtlinie ist es empfehlenswert, so vorzugehen, dass zunächst ein Maximum an Forderungen und Vorgaben für die Sicherheit der Systeme aufgestellt wird. Diese können anschließend den tatsächlichen Gegebenheiten angepasst werden. Idealerweise wird so erreicht, dass alle notwendigen Aspekte berücksichtigt werden. Für jede im zweiten Schritt verworfene oder abgeschwächte Vorgabe sollte der Grund für die Nicht-Berücksichtigung dokumentiert werden.

Ergänzende Kontrollfragen:

- Wurde eine Sicherheitsrichtlinie für den Betrieb des Sicherheitsgateways erstellt?
- Wann wurde die Sicherheitsrichtlinie zum letzten Mal aktualisiert?
- Wurde ein Sicherheitsniveau in der Sicherheitsrichtlinie definiert?
- Wurden in der Sicherheitsrichtlinie Vorgaben zur Einrichtung, zum Betrieb und zur Störungsbehandlung von Komponenten des Sicherheitsgateways beschrieben?
- Wurden in der Sicherheitsrichtlinie unterschiedliche Einsatzzwecke der Komponenten berücksichtigt?

M 2.300 Sichere Außerbetriebnahme oder Ersatz von Komponenten eines Sicherheitsgateways

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsbeauftragter

Verantwortlich für Umsetzung: Administrator

Sollen Komponenten des Sicherheitsgateway außer Betrieb genommen oder ersetzt werden, so müssen von den Geräten alle sicherheitsrelevanten Informationen gelöscht werden. Dies gilt besonders dann, wenn die Komponenten ausgesondert und an Dritte weitergegeben (beispielsweise verkauft) werden oder wenn ein Gerät im Rahmen eines Garantieaustausches oder einer Reparatur an den Hersteller oder eine Service-Firma übergeben wird, aber selbst dann, wenn die Geräte intern weiter verwendet oder verschrottet werden.

Je nach Einsatzzweck der Komponenten können beispielsweise folgende Informationen und Daten auf den Geräten gespeichert sein:

- Konfigurationsdateien, aus denen Informationen über die Netzstruktur der Organisation (wie IP-Adressen, Routing-Tabellen, SNMP-Community Strings, Access-Control-Lists oder ähnliches) entnommen werden können
- Passwortdateien
- Protokolldateien, die sicherheitsrelevante Informationen oder personenbezogene Daten enthalten
- Benutzerdaten, beispielsweise aus Web-Cache- oder E-Mail-Spool-Verzeichnissen
- potentiell gefährliche Dateien (Schadsoftware) aus "Quarantäne-Verzeichnissen"
- Zertifikate und Schlüssel (etwa SSL-Zertifikate bei SSL-Proxies oder Schlüssel für den Zugang per SSH)

Daten löschen, Erfolg überprüfen

Wegen der Sensibilität dieser Informationen ist darauf zu achten, dass die Dateien vor der Außerbetriebnahme oder dem Austausch defekter oder veralteter Geräte gelöscht beziehungsweise unlesbar gemacht werden. Nach dem Löschen der Daten muss überprüft werden, ob das Löschen auch erfolgreich war. Die Vorgehensweise hängt dabei stark von der Art und vom Verwendungszweck des Gerätes ab. In der Sicherheitsrichtlinie für das Sicherheitsgateway sollten hierfür entsprechende Verantwortlichkeiten definiert werden.

Die entsprechenden Dateien sind je nach Gerät und Einsatzzweck eventuell in mehreren unterschiedlichen Verzeichnissen gespeichert, beispielsweise befinden sich bei ALGs die verschiedenen Konfigurationsdateien meist an anderen Stellen als die Cache-Dateien, Spool- oder Quarantäneverzeichnisse. Vor der Außerbetriebnahme sollte daher geklärt werden, welche sicherheitsrelevanten Dateien an welchen Stellen gespeichert sind.

Festplatten löschen

Bei "normalen" Rechnern, die als Komponenten des Sicherheitsgateway eingesetzt waren, sollten die Festplatten mit einem geeigneten Tool so gelöscht werden, dass keine Wiederherstellung der Dateien mehr möglich ist. Die kann beispielsweise dadurch geschehen, dass der Rechner von einem

externen Boot-Medium gestartet wird und die Festplatten mit Zufallsdaten überschrieben werden. Dabei ist es empfehlenswert, den Überschreibvorgang mehrfach zu wiederholen.

Bei Appliances hängt die Vorgehensweise davon ab, ob in dem Gerät eine Festplatte eingebaut ist oder ob die Daten in einem nichtflüchtigen Speicher gespeichert werden. Oft bieten die Geräte eine "Factory-Reset" Option, mit der sämtliche Konfigurationseinstellungen auf die Werte des Auslieferungszustands zurückgesetzt werden können. Auch nach dem Ausführen eines "Factory-Reset" sollte überprüft werden, ob die Daten wirklich gelöscht beziehungsweise zurückgesetzt wurden oder ob bestimmte Daten oder Dateien noch vorhanden sind.

Notfalls Speicher unbrauchbar machen

Sind auf dem Gerät besonders sicherheitskritische Informationen gespeichert und kann nicht mit hinreichender Sicherheit gewährleistet werden, dass die Daten wirklich gelöscht sind, so kann es erforderlich sein, die Speicherbausteine oder Festplatten physisch zu zerstören bzw. unbrauchbar zu machen.

Auch Backup-Medien berücksichtigen

Neben den Informationen, die auf dem Gerät selbst gespeichert sind sollte auch überprüft werden, ob auf den Backup-Medien sensitive Informationen enthalten sind. Falls es nicht aus anderen Gründen (beispielsweise Archivierung, Aufbewahrungspflicht aufgrund gesetzlicher Regelungen) erforderlich ist, die Backup-Medien aufzubewahren, so sollten die Medien nach der Außerbetriebnahme des Gerätes ebenfalls gelöscht werden.

Auch Beschriftungen entfernen

Oft sind die Komponenten des Sicherheitsgateways von außen mit IP-Adressen, Hostnamen oder sonstigen technischen Informationen beschriftet. Auch diese Beschriftungen sollten vor der Entsorgung entfernt werden.

Ergänzende Kontrollfragen:

- Ist die sichere Entsorgung von Geräten in der Sicherheitsrichtlinie für das Sicherheitsgateway berücksichtigt?
- Werden Konfigurationsdateien und Log-Dateien vor der Entsorgung sicher gelöscht bzw. unlesbar gemacht?
- Wird die Beschriftung von den Geräten vor der Entsorgung entfernt?

M 2.301 Outsourcing des Sicherheitsgateway

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Der Aufbau und Betrieb eines Sicherheitsgateway bedeutet einen nicht unerheblichen finanziellen und personellen Aufwand. Trotzdem kann auf ein Sicherheitsgateway nicht verzichtet werden, wenn LANs an nicht vertrauenswürdige Netze (insbesondere an das Internet) angeschlossen werden sollen. Oft wird daher überlegt, den Betrieb einer Sicherheitsgateway einem externen Dienstleister zu überlassen. Dabei sind verschiedene Varianten denkbar:

- **Betrieb vor Ort, Administration durch Externe**

  Das Sicherheitsgateway wird innerhalb der Räumlichkeiten des Auftraggebers betrieben und administriert. Damit wird ein externer Sicherheitsgateway-Administrator beauftragt.

  Diese Lösung bringt oft nicht einmal einen Kostenvorteil. Nachteilig ist hier, wie bei allen anderen Lösungen, dass Externe sicherheitsrelevante Aufgaben übernehmen und intern kein entsprechendes Wissen aufgebaut wird, so dass eine wirksame Kontrolle äußerst schwierig ist.

- **Remote Management**

  Das Sicherheitsgateway wird innerhalb der Räumlichkeiten des Auftraggebers aufgestellt und betrieben, aber über Fernzugriff administriert.

  Dabei ist eine starke Authentisierung sowie die Verschlüsselung der Verbindung unerlässlich. Die Dienstleister sollten nur auf die Sicherheitsgateway selber zugreifen dürfen, nicht auf weitere Daten und Verzeichnisse im LAN. Wie im Baustein B 4.4 *Remote Access* beschrieben, sollten weitere organisatorische Vorkehrungen getroffen werden, um einen möglichen Missbrauch einzudämmen. Dazu gehören beispielsweise

  - das Verhängen einer Zeitsperre bei fehlerhaften Zugangsversuchen,
  - das Sperren des Fernwartungszugangs im Normalbetrieb und explizite Freigabe für eine genau definierte Zeitspanne,
  - Einschränkung der Rechte der externen Administratoren, so dass z. B. die Sicherheitsrichtlinien nicht niedriger eingestellt werden können,
  - "Zwangslogout" bei Leitungsunterbrechung; wird die Verbindung zwischen Fernwartungsstelle und PC-Gateway auf irgendeine Weise unterbrochen, so muss der Zugriff auf das System durch ein "Zwangslogout" beendet werden.

- **Hosting**

  Bei dieser Lösung wird die Sicherheitsgateway beim Dienstleister aufgestellt und gepflegt. Vom internen LAN zum Sicherheitsgateway muss dabei eine feste, geschützte Verbindung vorhanden sein.

Hierbei muss eine hohe Verfügbarkeit sowohl der Verbindung als auch des Sicherheitsgateway-Systems gewährleistet werden, da bei deren Ausfall keine externen Verbindungen mehr möglich sind.

Im Allgemeinen sollen auch weitere Komponenten, die der Kommunikation zwischen geschütztem und externem Netz dienen, eingesetzt werden. Dazu gehören z. B. Informationsserver für die Bereitstellung von Informationen an interne oder externe Benutzer, Mailserver und DNS-Server. Diese werden üblicherweise in einer DMZ des Sicherheitsgateway aufgestellt (siehe auch M 2.77 *Integration von Servern in das Sicherheitsgateway*). In diesem Fall müssten sie also beim externen Dienstleister betrieben werden. Dies kann die Kosten erheblich in die Höhe treiben.

Sowohl beim Remote Management als auch beim Hosting eines Sicherheitsgateways sollte eine Ausweich-Verbindung zum Dienstleister vorhanden sein, um bei einem Ausfall der Hauptanbindung die Administration bzw. die Internet-Anbindung zu gewährleisten. Für die Ausweich-Verbindung muss sichergestellt sein, dass für diese Verbindung mindestens das selbe Sicherheitsniveau gewährleistet ist, wie für die Hauptverbindung.

Bei den verschiedenen Dienstleistungsangeboten ist zu hinterfragen,

- wie viel technisches, aber auch wie viel sicherheitsrelevantes Wissen beim Anbieter vorhanden ist und wie dieses aktuell gehalten wird,
- ob und wie lange das Sicherheitsgateway-System unbeaufsichtigt betrieben wird,
- wie der Personaleinsatz gesteuert wird, da ja üblicherweise mehrere Kunden betreut werden.

Auch wenn die Betreuung des Sicherheitsgateways einem Dienstleister überlassen wird, muss trotzdem intern eine Sicherheitsgateway-Sicherheitspolicy erstellt werden, die mit den Sicherheitszielen der Organisation abgestimmt ist (siehe auch M 2.71 *Festlegung einer Policy für ein Sicherheitsgateway*). Beim Outsourcing eines Sicherheitsgateways sollte in den Service-Level Agreements insbesondere schriftlich fixiert werden,

- welche Reaktionszeiten bei Ausfällen oder Angriffen gewährleistet werden müssen,
- welche Verfügbarkeit zu gewährleisten ist (Performance, maximale Ausfallrate),
- was protokolliert werden darf bzw. muss,
- welche Sicherheitsmaßnahmen gewährleistet werden müssen. Dazu gehören insbesondere alle in Baustein B 3.301 *Sicherheitsgateway (Firewall)* aufgeführten Maßnahmen.

Baustein 1.11 Outsourcing betrachten!

Für das Outsourcing einer so sicherheitskritischen Komponente wie dem Sicherheitsgateway muss in jedem Fall der Baustein B 1.11 *Outsourcing* angewandt werden. Beim Dienstleister sollte idealerweise ebenfalls ein vollständiges Informationssicherheitsmanagement-System z. B. basierend auf IT-Grundschutz existieren. Es wird empfohlen, beim Outsourcing des

Sicherheitsgateways zumindest zu prüfen, ob das Sicherheitsmanagement des Dienstleisters den Anforderungen des Bausteins B 1.11 *Outsourcing* genügt.

Ergänzende Kontrollfragen:

- Wurde die Entscheidung über das Sicherheitsgateway-Outsourcing mit dem IT-Sicherheitsmanagement abgestimmt?
- Wurde der Baustein B 1.11 *Outsourcing* angewandt?

M 2.302 Sicherheitsgateways und Hochverfügbarkeit

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Ein Sicherheitsgateway sollte immer die einzige Schnittstelle zwischen dem externen und dem zu schützenden Netz darstellen. Damit stellt natürlich das Sicherheitsgateway einerseits einen potentiellen Flaschenhals und zum anderen eine mögliche Bruchstelle für den gesamten Netzverkehr einer Organisation dar. Somit werden an die Verfügbarkeit von Sicherheitsgateways häufig hohe Anforderungen gestellt.

Die wichtigsten Komponenten eines Sicherheitsgateways sollten somit redundant ausgelegt werden. Dies sind vor allem diejenigen Komponenten, die zum Abruf oder zum Versand von Informationen unbedingt überquert werden müssen. In diese Kategorie fallen in der Regel Paketfilter, Application-Level-Gateway und evtl. VPN-Komponenten. Bei anderen Komponenten (z. B. Virenscanner oder Intrusion-Detection-System) muss die Bedeutung für die Sicherheit des zu schützenden Netzes im Einzelfall betrachtet werden.

Es gibt verschiedene Möglichkeiten, die Verfügbarkeit von Komponenten eines Sicherheitsgateways zu steigern:

Cold-Standby:

Beim Cold-Standby wird neben dem eigentlichen Produktivsystem ein zweites baugleiches Ersatzsystem bereitgehalten, das aber nicht in Betrieb ist. Wenn das erste System ausfällt, kann das Ersatzsystem manuell hochgefahren und ins das Sicherheitsgateway integriert werden.

Vorteile einer Cold-Standby Lösung	Nachteile einer Cold-Standby Lösung
- Der Aufwand zur Neuinstallation bzw. zum Neuaufbau eines Sicherheitsgateways ist relativ gering. - Die geringe Komplexität des Sicherheitsgateways erschwert Fehlkonfigurationen.	- Zum bestehenden System muss ein zweites System vorgehalten werden und ständig auf dem aktuellen Konfigurations- und Patch-Stand gehalten werden. - Das Cold-Standby-System kann Fehlfunktionen nicht selbständig erkennen und muss manuell aktiviert werden. Es liegt in der Verantwortung der Administratoren, die Funktion des Wirksystems permanent zu überwachen und im Notfall einzuschreiten. - Je nach eingesetztem Produkt erfordert das Hochfahren einer Komponente des Sicherheitsgateways die Anwesenheit eines Administrators, da manche Systeme ohne Benutzerinteraktion über Tastatur nicht in den Betriebszustand starten. Das Einschalten von Komponenten über eine webgesteuerte Steckdose ist in diesem Fall ausgeschlossen.

Tabelle 1: Vor- und Nachteile einer Cold-Standby Lösung

Hot-Standby:

Bei einem Hot-Standby steht ebenfalls ein Ersatzsystem (meist mit der gleichen Konfiguration wie das im Regelbetrieb befindliche System) bereit. Dieses läuft aber ständig parallel mit, wobei eine Komponenten die andere überwacht. Bei einer Fehlfunktion kann dann das Ersatzsystem unmittelbar die Funktion des Wirksystems übernehmen. Dies kann automatisiert erfolgen oder auch nach Benutzerinteraktion. Eine Benutzerinteraktion kann verhindern, dass eine Umschaltung auf das Hot-Standby-System - die zusätzliche Komplikationen mit sich bringen kann - bei extrem kurzen Ausfällen erfolgt.

Um die Ausfallzeiten möglichst gering zu halten, muss der Zustand der wichtigsten Komponenten beim Hot-Standby-Betrieb des Sicherheitsgateways in möglichst kurzen Zeitabständen überprüft werden.

Vorteile einer Hot-Standby Lösung	Nachteile einer Hot-Standby Lösung
- Es ist keine Interaktion durch den Administrator an der Konsole notwendig. - Da die Funktionen des ausgefallenen Systems von der Ersatzkomponenten automatisch übernommen wird, gibt es keine oder nur kurze Ausfallzeiten.	- Gegenüber Cold-Standby wird das Sicherheitsgateway sehr komplex, da alle beteiligten Komponenten durch zusätzliche Überwachungskomponenten ständig auf korrekte Funktion überprüft werden müssen. - Für jede relevante Komponente des Sicherheitsgateways muss eine eigene Überwachungskomponente beschafft und betreut werden.

Tabelle 2: Vor- und Nachteile einer Hot-Standby Lösung

Parallelbetrieb:

Bei einem Parallelbetrieb arbeiten zwei oder mehr Sicherheitsgateways ständig nebeneinander im Wirkbetrieb. Durch einen Parallelbetrieb wird nicht nur eine Lastverringerung und Performancesteigerung erreicht, vielmehr verringern sich auch die Probleme bei Ausfällen. Je nach gewählter Lastverteilungsmethode kann ein System im Fehlerfall die Aufgaben des gerade nicht zur Verfügung stehenden Systems übernehmen. Daraus resultiert natürlich ein kurzfristiger Performance-Verlust, aber die Funktionalität bleibt vollständig erhalten.

Dabei muss allerdings sichergestellt sein, dass alle Systeme konsistent gehalten werden. Bei Sicherheitsgateways muss hier vor allem auf korrekte Zeitsynchronisierung und die Konsistenz der Regelbasis geachtet werden. Außerdem muss gewährleistet sein, dass ein- und ausgehende Anfragen immer von den selben Komponenten bearbeitet werden, da sonst evtl. Verbindungen abgebrochen werden. Dies betrifft besonders Application-Level-Gateways und Paketfilter mit Stateful-Inspection-Funktion.

Beim Parallelbetrieb sind zwei Varianten zu unterschieden:

Statischer Parallelbetrieb

Bei dieser Variante ändert sich die Konfiguration (insbesondere die Routing-Informationen) der Komponenten des Sicherheitsgateways nicht. Eine Variante des statischen Parallelbetriebs könnte beispielsweise darin bestehen, dass über die parallelen Komponenten des Sicherheitsgateways unterschiedliche Dienste geleitet werden, also z. B. HTTP über einen Kommunikationsstrang und SMTP über einen parallelen Kommunikationsstrang. Diese Konfiguration erhöht zwar die Performance des Gesamtsystems, ist aber beim Ausfall einzelner Komponenten problematisch, da die Komponenten unterschiedlich konfiguriert sind und nicht ohne Weiteres durch die jeweils parallele Komponente ersetzt werden können. Aus diesem Grund ist von einer solchen Struktur und Konfiguration des Sicherheitsgateways in der Regel abzuraten.

Dynamischer Parallelbetrieb/Loadbalancing

Bei dieser Betriebsart wird die Konfiguration der Komponenten des Sicherheitsgateways den Performanceanforderungen im Betrieb angepasst. Ein Beispiel hierfür ist das Loadbalancing, bei dem Datenströme in Abhängigkeit von der Auslastung der an der Kommunikation beteiligten Komponenten geroutet werden.

Unbedingt zu beachten ist beim Loadbalancing, dass sich durch die automatischen Konfigurationsänderungen auf den beteiligten Komponenten keine Änderungen des Sicherheits-Regelwerks für das gesamte Sicherheitsgateway ergeben.

Loadbalancing kann Teil einer High-Availibility-Lösung (**HA-Lösung**) sein. Bei einer HA-Lösung wird die Verfügbarkeit von Komponenten des Sicherheitsgateways überwacht und es werden beim Ausfall ggf. Ersatzsysteme genutzt, die den Ausfall kompensieren sollen. Das oben angesprochene Loadbalancing dient in diesem Zusammenhang eigentlich nur der Performancesteigerung und führt alleine noch nicht zu Hochverfügbarkeit, es muss zusätzlich dafür gesorgt werden, dass bei einem Systemausfall die Ersatzsysteme den Ausfall automatisch ohne Zutun des Administrators auffangen. Eine ständige Überwachung der HA-Komponenten ist dabei ebenso wichtig wie ein automatisches Fail-Over im Bedarfsfall.

Vor- und Nachteile einer HA-Lösung sind mit denen eines Hot-Standby-Systems zu vergleichen. Vorteilhaft gegenüber Hot-Standby ist zusätzlich jedoch, dass sämtliche Komponenten des Sicherheitsgateways genutzt werden und sich somit eine Lastverteilung ergibt, die die Verfügbarkeit des Sicherheitsgateways sicherstellen kann.

Anforderungen an HA-Lösungen:

An eine HA-Lösung sollten folgende Forderungen gestellt werden:

Keine Sicherheitseinbußen bei Fail-Over!

- Auch nach einem automatischen Fail-Over muss das Sicherheitsgateway die Sicherheitsanforderungen der Sicherheitsleit- bzw. -richtlinie erfüllen ("Fail safe" bzw. "Fail secure").
- Die HA-Realisierung darf den Betrieb des Sicherheitsgateways bzw. dessen Sicherheitsfunktionen nicht behindern.
- Mindestens Paketfilter und Application-Level-Gateway sollten hochverfügbar ausgelegt werden, da eine Kommunikation bei einem Ausfall der Komponenten in der Regel nicht mehr möglich ist. Ähnliches gilt für VPN-Komponenten.
- Es sollten zwei voneinander unabhängige Zugangsmöglichkeiten zum externen Netz bestehen, z. B. zwei Internetzugänge von unterschiedlichen Providern.
- Interne und externe Router müssen redundant ausgelegt sein, z. B. unter Verwendung von Protokollen wie "Virtual Router Redundancy Protocol" (VRRP) oder das proprietäre "Hot Standby Routing Protocol" (HSRP).

- Die Funktionsüberwachung sollte anhand einer Vielzahl von Parametern erfolgen und sich nicht auf ein einzelnes Kriterium verlassen (wie z. B. eine einfache Erreichbarkeitsprüfung durch Testen der Verfügbarkeit der Netzschnittstelle ("ping")). Ist eine Komponente mittels "ping" erreichbar, könnte beispielsweise überprüft werden, ob die konfigurierten Dienste in der intendierten Art und Weise arbeiten.
- Fehlkonfigurationen bei Inbetriebnahme oder Fehlfunktionen einer Komponente im Wirkbetrieb werden bei HA-Lösungen evtl. nicht sofort sichtbar, da Funktionen teilweise von der parallel installierten Komponente übernommen werden. So z. B. fällt es unter Umständen nicht sofort auf, wenn auf einem ALG die Filterung auf aktive Inhalte ausgeschaltet ist und die Anfragen vom korrekt konfigurierten System bearbeitet werden. Deshalb ist eine regelmäßige Kontrolle der Protokolldateien und der Warnmeldungen der HA-Lösung wichtig.

HA bei Paketfiltern ist meist einfach

Besonders einfach ist eine HA-Lösung dann, wenn nur ein einstufiger Aufbau bestehend aus einem Paketfilter hochverfügbar ausgelegt werden soll. Viele kommerzielle Produkte bieten hierfür eine einfache Lösung, die im Wesentlichen in der Aktivierung einer entsprechenden HA-Option in der Administrationsoberfläche besteht.

Aufwändiger ist eine HA-Lösung bei mehrstufigen Sicherheitsgateways (z. B. zusammengesetzt aus Paketfiltern und Application-Level-Gateway). Hier muss jede Komponente hochverfügbar ausgelegt sein, was einen erheblichen Mehraufwand bedeutet. In der Regel müssen hier neben der Überwachungsfunktion noch dynamische Routingprotokolle (z. B. "Open Shortest Path First", OSPF) verwendet werden, die den Netzverkehr je nach Bedarf in die richtige Richtung lenken.

Dynamische Routing-Protokolle sind jedoch aus Sicht der Sicherheit nicht unproblematisch. Zu den Problemen siehe auch G 5.51 *Missbrauch der Routing-Protokolle* und M 5.112 *Sicherheitsaspekte von Routing-Protokollen*. Sollen zur Realisierung einer HA-Lösung dynamische Routing-Protokolle eingesetzt werden, so sollte im Rahmen einer ergänzenden Sicherheitsanalyse geprüft werden, ob das erforderliche Sicherheitsniveau noch erreicht wird.

In der P-A-P-Kette eines mehrstufigen Sicherheitsgateways muss eine Komponente die Überwachungsfunktion übernehmen. Diese Komponente entscheidet, ob der P-A-P-Strang funktionsfähig ist oder nicht. Für diese Aufgabe bietet sich eine eigenständige Überwachungskomponente an, die für nichts anderes als die Funktionskontrolle zuständig ist.

Ist die Integration einer eigenständigen Überwachungskomponente nicht möglich, so bietet es sich an, dem Application-Level-Gateway diese Aufgabe zu übertragen. Dies bietet zum einen den Vorteil, dass viele Funktionen des Sicherheitsgateways auf dem ALG implementiert sind, also von der Überwachungssoftware dann lokal ausgewertet werden können. Zum anderen ist das ALG oftmals an zentraler Stelle in das Sicherheitsgateway integriert, bietet also einen direkten Zugang zu den anderen Komponenten des Sicherheitsgateways.

Problematisch ist allerdings, dass ALGs oftmals das Aufspielen von Fremdsoftware zu verhindern versuchen, um eine Kompromittierung des Systems zu verhindern. Tatsächlich ist natürlich nicht auszuschließen, dass die eingesetzte Überwachungssoftware fehlerbehaftet ist und die Sicherheit des ALGs stark herabsetzt.

Ergänzende Sicherheitsanalyse

Hochverfügbarkeitslösungen sind immer auf spezielle Anforderungen zugeschnitten und Mischformen aus den oben beschriebenen Typen sind durchaus denkbar. Grundsätzlich wird für denn Fall, dass die Anforderungen an die Verfügbarkeit des Sicherheitsgateways eine Hochverfügbarkeitslösung notwendig erscheinen lassen, eine ergänzende Sicherheitsanalyse dringend empfohlen.

Ergänzende Kontrollfragen:

- Wird eine HA-Lösung eingesetzt? Falls ja, welche Art?
- Wie wird sichergestellt, dass bei einem automatischen Fail-Over das Sicherheitsniveau nicht sinkt?

M 2.303 Festlegung einer Strategie für den Einsatz von PDAs

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Bevor in einer Organisation PDAs eingesetzt werden, muss festgelegt sein, welche generelle Strategie die Organisation im Hinblick auf die Nutzung der Geräte einnimmt. Insbesondere sind dafür die folgenden Fragen zu beantworten:

- Für welche Anwendungen sollen die PDAs eingesetzt werden?
- Werden den Mitarbeitern dienstliche PDAs zur Verfügung gestellt?
- Wird die Nutzung privater PDAs der Mitarbeiter erlaubt oder sogar offiziell unterstützt?

Insbesondere die Frage, für welche Zwecke PDAs eingesetzt werden sollen, ist für die späteren Entscheidungen wichtig, denn sie kann einen entscheidenden Einfluss auf die Auswahl anzuschaffender Geräte haben und muss in jedem Fall bei der Formulierung der Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung berücksichtigt werden.

Klassifikation der Daten

Jeder Benutzer und jede Institution sollte sich Gedanken darüber machen, welche Daten auf einem PDA gespeichert werden dürfen und welchen Schutzbedarf diese haben. In einem Unternehmen oder einer Behörde sollte dies nicht nur für Daten auf PDAs, sondern generell geklärt werden. So gibt es in Anwendungsfeldern und Geschäftsprozessen Daten, die einen höheren Schutzbedarf haben oder die besonderen Restriktionen unterliegen, z. B. personenbezogene, finanzrelevante, vertrauliche oder Copyright-geschützte Daten.

Daher sollten in einer Institution alle Arten von Daten danach kategorisiert sein, wie schutzbedürftig sie sind und welche Beschränkungen im Umgang mit ihnen beachtet werden sollten (siehe hierzu auch M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*).

Damit die Mitarbeiter mit diesen Einstufungen auch sinnvoll umgehen können, empfiehlt es sich, diesen hierzu leicht verständliche Tabellen und Beispiele an die Hand zu geben, in denen erläutert ist, welche Arten von Daten auf den verschiedenen IT-Systemen oder Anwendungen gespeichert oder verarbeitet werden dürfen und auch, an wen diese weitergegeben werden dürfen.

Nutzung von privaten PDAs

Aufgrund einer unzureichenden Ausstattung oder eines hohen Benutzerdruckes kann es vorkommen, dass private PDAs für dienstliche Zwecke benutzt werden. Das IT-Sicherheitsmanagement bzw. die IT-Verantwortlichen sollten aber auf jeden Fall sicherstellen, dass auch die private Nutzung innerhalb der Institution nicht "wild" erfolgt, sondern klar geregelt ist. Sollen PDAs nur für Anwendungen wie Termin- und Adressverwaltung oder für

E-Mail-Kommunikation eingesetzt werden, so kann die Nutzung privater PDAs normalerweise erlaubt werden, wenn keine sonstigen Gründe dagegen sprechen.

Bei hohem Schutzbedarf möglichst kein privaten PDAs

Falls die PDAs für eine Anwendung eingesetzt werden sollen, aus der sich für die Geräte ein hoher Schutzbedarf ergibt, so ist es sehr fraglich, ob dafür die Nutzung privater PDAs zugelassen werden sollte. Der Grund dafür ist insbesondere, dass private Geräte weitgehend dem Einfluss der zentralen Konfiguration und Administration entzogen sind und es deswegen praktisch keine Möglichkeit gibt, für die Geräte ein akzeptables Sicherheitsniveau zu gewährleisten. Es wird dringend empfohlen, in diesem Fall keine Nutzung privater PDAs zuzulassen.

Bei der Entscheidung sollte auch berücksichtigt werden, dass die Entscheidung, private PDAs zuzulassen, auch Auswirkungen auf die spätere IT-Strategie einer Organisation haben kann.

Beispiel:

In einem Unternehmen wurden zwar keine PDAs für die Mitarbeiter angeschafft, die Mitarbeiter wurden aber dennoch bei der Beschaffung privater Geräte und der Anbindung an die Arbeitsplatz-PCs beraten. Als das Unternehmen die PCs von Windows NT nach Windows 2000 migrierte, stellte sich heraus, dass es unter Windows 2000 keine passenden Treiber für die vorhandenen PDAs existierten. Durch die massiven Benutzerbeschwerden stand das Unternehmen vor der Wahl, den Benutzern neue PDAs zu finanzieren oder diesen weiter NT-basierte PCs zur Verfügung zu stellen.

Wenn ein Verbot ausgesprochen wird, private PDAs für Dienstzwecke zu benutzen oder sie in das Büro mitzubringen, sollte immer bedacht werden, dass solche Verbote überwacht werden müssen und dass sie auch ineffektiv sein können.

Die Entscheidung sollte zusammen mit den Entscheidungsgründen dokumentiert und den Mitarbeitern auf geeignete Art und Weise kommuniziert werden.

Ergänzende Kontrollfragen:

- Werden dienstliche PDAs angeschafft?
- Ist die Nutzung privater PDAs erlaubt?

M 2.304 Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Wenn in einer Institution entschieden wurde, PDAs einzusetzen, so müssen diese in die allgemeine Sicherheitsstrategie eingebunden werden.

Bei der Nutzung von PDAs gibt es eine Vielzahl von Möglichkeiten, diese vor Missbrauch zu schützen. Damit diese Möglichkeiten auch genutzt werden, sollte eine Sicherheitsrichtlinie erstellt werden, in der alle umzusetzenden Sicherheitsmechanismen beschrieben werden. Jede Institution sollte sich die Möglichkeiten und Risiken des PDA-Einsatzes bewusst machen. Hierbei sollten zwei Sicherheitsaspekte im Vordergrund stehen:

- die Sicherheit der auf PDAs gespeicherten Daten und
- die Auswirkung der PDA-Nutzung auf die Sicherheit anderer IT-Systeme innerhalb einer Institution.

Aufbauend auf die PDA-Sicherheitsrichtlinie sollte für die Benutzer ein kurzes und übersichtliches Merkblatt für die sichere Nutzung von PDAs erstellt werden.

Schutz vor Missbrauch

Ein PDA hat nicht nur für den Besitzer den Vorteil, leicht zu transportieren und unauffällig zu verwahren zu sein, sondern auch für einen Dieb. Daher sollte auch ein PDA stets sicher aufbewahrt werden. Bei Dienstreisen sollten sie nicht unbeaufsichtigt gelassen werden. Insbesondere sollten sie nicht in Fahrzeugen zurückgelassen werden.

Praktisch alle Varianten von PDAs und Organizern lassen sich durch PINs oder Passwörter gegen unbefugten Zugriff absichern. Leider sind nicht alle vom Hersteller angebotenen Sicherheitsmechanismen so sicher, wie es wünschenswert wäre. Daher sollten sich PDA-Benutzer informieren, wie zuverlässig die vorhandenen Sicherheitsmechanismen sind, z. B. über das Internet.

Solange keine besseren Sicherheitstools installiert sind, sollten aber auf jeden Fall die vorhandenen Sicherheitsmechanismen genutzt werden (siehe auch M 4.228 *Nutzung der Sicherheitsmechanismen von PDAs*). Alle Benutzer sollten sich aber über deren Wirkung und insbesondere deren Grenzen im Klaren sein. Dabei sollten die Passwörter und PINs sorgfältig ausgewählt werden, also auch lang genug sein, damit sie nicht einfach überwunden werden können. Die Passwörter dürfen keinesfalls zusammen mit dem PDA aufbewahrt werden.

Sensibilisierung der Benutzer

Alle PDA-Benutzer sollten nicht nur über die Vorteile von PDAs aufgeklärt werden, sondern auch über potentielle Risiken und Probleme bei der Nutzung sowie über den Nutzen, aber auch die Grenzen der eingesetzten Sicherheitsmaßnahmen.

Da auch für die Betriebssysteme von PDAs (beispielsweise Palm OS, Windows CE bzw. Windows Mobile, Symbian OS) immer wieder neue Sicherheitslücken offengelegt werden, sollte sich das IT-Sicherheitsmanagement regelmäßig über aktuelle Risiken informieren. Gegebenenfalls ist es angebracht, die Mitarbeiter regelmäßig über die neu bekanntgewordenen Gefahren zu informieren und damit auch zu sensibilisieren.

Regelungen zur PDA-Nutzung

Allgemeine Regelungen

Auf einem PDA sind Daten in der Regel schlechter geschützt als auf IT-Systemen innerhalb der Organisation. Unabhängig davon, ob privat oder dienstlich angeschaffte PDAs genutzt werden, sollte der Arbeitgeber daher schriftlich regeln,

- welche Daten nicht auf einem PDA gespeichert werden dürfen,
- dass Daten nicht überall eingegeben bzw. abgerufen werden sollten, da sie dabei unter Umständen mitgelesen werden können,
- wie, wann und durch wen Datensicherungen des PDAs durchzuführen sind,
- unter welchen technischen Einsatzbedingungen die PDAs eingesetzt werden dürfen. Hierzu gehören vor allem die Festlegung von Sicherheitsmaßnahmen, die Auswahl und Installation der erforderlichen Sicherheitshard- und -software sowie Vorgaben für die sichere Konfiguration der betroffenen IT-Systeme.

Ein PDA sollte möglichst nicht unbeaufsichtigt bleiben. Falls ein PDA in einem Kraftfahrzeug zurückgelassen werden muss, so sollte das Gerät von außen nicht sichtbar sein. Das Abdecken des Gerätes oder das Einschließen in den Kofferraum bieten Abhilfe. Ein PDA stellt einen Wert dar, der potentielle Diebe anlocken könnte.

Wird ein PDA in fremden Büroräumen benutzt, so sind die Sicherheitsregelungen der besuchten Organisation zu beachten.

In fremden Räumlichkeiten wie Hotelzimmern sollte ein PDA nicht ungeschützt liegen gelassen werden. Alle Passwort-Schutzmechanismen sollten spätestens jetzt aktiviert werden. Das Verschließen des Gerätes in einem Schrank behindert Gelegenheitsdiebe.

Nutzung von privaten PDAs

Bei der Nutzung von privaten PDAs in einer Behörde oder einem Unternehmen sind unter anderem die folgenden Punkte zu regeln:

- Die sinnvolle Nutzung von PDAs erfordert im Allgemeinen eine Synchronisation mit einem PC, beispielsweise für Terminkalender, Adressbücher, E-Mail-Unterstützung und mehr. Daher muss geklärt werden, ob die Installation der dafür benötigten Hard- und Software erlaubt wird, und wer die Installation vornimmt. Dies sollte nicht den Benutzern selbst überlassen werden.
- Es muss geklärt werden, inwieweit der Benutzer-Support bei Problemen, die sich aus der Nutzung von privaten PDAs ergeben, Hilfestellung leistet. Ebenso sollte im Vorfeld abgesprochen werden, wie private PDAs in die IT-Strategie der Institution eingebunden werden.

Nutzung von dienstlichen PDAs

Bei der Nutzung von dienstlichen PDAs sind unter anderem die folgenden Punkte zu regeln:

- Es muss geklärt werden, ob dienstliche PDAs auch mit privaten PCs synchronisiert werden dürfen. Dies erleichtert einerseits Terminabstimmungen, andererseits könnte dadurch Schadsoftware in die dienstlichen Systeme eingeschleppt werden und interne Dokumente könnten auf die privaten PCs gelangen.
- Die Benutzer sollten darauf hingewiesen werden, wie sie sorgfältig mit den PDAs umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten (z. B. Akkupflege, Aufbewahrung außerhalb von Büro- oder Wohnräumen, Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen).
- Die Verwaltung, Wartung und Weitergabe von PDAs sollte geregelt werden.

Einbindung in andere Sicherheitslösungen

Bei der Benutzung von PDAs muss nicht nur überlegt werden, ob der Einsatz von Sicherheitssoftware zum Schutz des PDAs selber sinnvoll ist, sondern auch, wie der PDA mit der Sicherheitssoftware der Einsatzumgebung zusammenarbeitet. Dazu zwei Beispiele:

- Der Benutzer liest und schreibt auf seinem Desktop-PC häufig E-Mails, die verschlüsselt bzw. signiert sind. Außerdem möchte er seinen PDA nutzen, um unterwegs E-Mail zu bearbeiten. Mit verschlüsselten bzw. signierten Mails kann er aber aus verschiedenen Gründen Probleme bei der Weiterverwendung auf dem PDA bekommen. So gibt es beispielsweise bisher nur sehr wenige Verschlüsselungs- bzw. Signaturanwendungen, die sowohl mit den einschlägigen Mailprogrammen auf Office-Systemen als auch auf PDAs kompatibel sind. Bei solchen Anwendungen werden außerdem oft Chipkarten oder andere Sicherheitstoken als sicherer Speicherplatz für die benötigten kryptographischen Schlüssel eingesetzt. Nur die wenigsten PDAs lassen sich aber um Chipkarten-Leseeinrichtungen erweitern. Viele PKI-Anwendungen arbeiten außerdem serverbasiert, benötigen also Zugriff auf einen Server, um beispielsweise Zertifikate überprüfen oder öffentliche Schlüssel von Kommunikationspartnern abrufen zu können.
- Im Unternehmen werden alle Daten, sowohl auf den Clients als auch den Servern, ausschließlich verschlüsselt gespeichert. Wenn Benutzer nun interne Daten auf PDAs transferieren wollen, kann zum einem passieren, dass sie unterwegs feststellen, dass sie zugriffsgeschützte Dateien geladen haben, die sie auf dem PDA nicht lesen können. Dies ist der für die Vertraulichkeit der Daten bessere Fall. Typischerweise werden die auf den PDA übertragenen Daten dort nämlich nicht oder nur schwach verschlüsselt, so dass sie weniger stark geschützt sind als auf den internen Systemen.

Auch solche Fälle, also die Einbindung von PDA-Applikationen in andere Sicherheitssoftware im Unternehmen, muss daher unbedingt in der PDA-Sicherheitsrichtlinie geregelt werden, um zu vermeiden, dass durch die PDA-Nutzung das festgelegte Sicherheitsniveau reduziert wird.

Wo nötig: Nutzungsverbot von PDAs

Es sollte überlegt werden, ob die Nutzung oder sogar das Mitbringen von PDAs in allen oder bestimmten Bereichen einer Behörde oder eines Unternehmens eingeschränkt werden sollte. Dies kann z. B. dort sinnvoll sein, wo das Mitschneiden von Gesprächen oder das Fotografieren unterbunden werden soll.

Wenn die IT-Sicherheitsrichtlinie der Institution es nicht zulässt, dass fremde IT-Systeme wie beispielsweise PDAs mitgebracht werden, muss an allen Eingängen deutlich darauf hingewiesen werden. Dies sollte dann auch regelmäßig kontrolliert werden. Für die Besucher sollte in diesem Fall eine Möglichkeit geschaffen werden, mitgebrachte Mobiltelefone, PDAs oder Notebooks sicher aufzubewahren. Beispielsweise können an den Eingängen Schließfächer zur Verfügung gestellt werden.

Ergänzende Kontrollfragen:

- Existiert eine aktuelle Sicherheitsrichtlinie für die PDA-Nutzung?
- Wie wird die Einhaltung der Sicherheitsrichtlinie für die PDA-Nutzung überprüft?
- Besitzt jeder PDA-Benutzer ein Exemplar dieser PDA-Richtlinie oder ein Merkblatt mit einem Überblick der wichtigsten Sicherheitsmechanismen?
- Ist die Sicherheitsrichtlinie für die PDA-Nutzung Inhalt der Schulungen zu IT-Sicherheitsmaßnahmen?
- Werden die Benutzer von PDAs auf die Regelungen hingewiesen, die von ihnen einzuhalten sind?
- Werden die Benutzer von PDAs auf die geeignete Aufbewahrung hingewiesen?

M 2.305 Geeignete Auswahl von PDAs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Beschaffungsstelle, Administrator

PDAs gibt es in verschiedensten Varianten und Geräteklassen. Diese unterscheiden sich nicht nur in ihren Abmessungen und Leistungsumfang, sondern auch bei Sicherheitsmechanismen und Bedienkomfort. Zudem stellen sie unterschiedliche Voraussetzungen an Hard- und Software-Komponenten im Einsatzumfeld.

Bei der Vielzahl verschiedener PDA-Modelle mit den unterschiedlichsten Betriebssystemen, sind Kompatibilitätsprobleme bei Hardware, Software auf PDA und PC sowie Schnittstellen naheliegend.

Anforderungsliste zur Produkt-Bewertung

Wenn einmal beschlossen worden ist, innerhalb einer Institution PDAs einzusetzen, sollte daher eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Aufgrund der Bewertung sollten dann die zu beschaffenden Produkte ausgewählt werden. Die Praxis zeigt, dass es aufgrund verschiedener Einsatzanforderungen durchaus sinnvoll sein kann, mehrere Gerätetypen für die Beschaffung auszuwählen. Die Gerätevielfalt sollte aber zur Vereinfachung des Supports eingeschränkt werden.

Außerdem muss sichergestellt werden, dass eine Möglichkeit zur zentralen und effektiven Verwaltung der einzelnen Endgeräte und der darauf verwendeten Software vorhanden ist. Auch sollte die notwendige Serverinfrastruktur einen möglichst geringen administrativen Aufwand erfordern.

Manche Funktionen von PDAs sind nur in Verbindung mit externen Dienstleistern nutzbar. Über einen externen Dienstleister sollten keine internen Daten ausgetauscht werden, wenn die Vertraulichkeit und Integrität der Daten nicht gewährleistet ist. Eine Übertragung über ein Mobilfunknetz ist beispielsweise zwar meist zunächst verschlüsselt ("Luftschnittstelle"), die Daten werden dann aber oft innerhalb des Netzes des Mobilfunkanbieters unverschlüsselt übertragen und auf dem Server des Dienstbetreibers unverschlüsselt gespeichert. Im Zweifelsfall sollen solche Dienste daher nicht genutzt werden.

Zunächst sollte eine Anforderungsanalyse durchgeführt werden. Ziel der Anforderungsanalyse ist es einerseits, alle im konkreten Fall in Frage kommenden Einsatzszenarien zu bestimmen und andererseits daraus Anforderungen an die benötigten Hard- und Softwarekomponenten abzuleiten.

Die folgende Liste gibt einen groben Überblick über mögliche allgemeine Bewertungskriterien, erhebt jedoch keinen Anspruch auf Vollständigkeit und kann um weitere allgemeine Anforderungen erweitert werden.

1 Allgemeine Kriterien

1.1 Wartung

- Lässt sich das Produkt einfach warten?
- Bietet der Hersteller regelmäßige Software-Updates an?
- Wird für das Produkt die Möglichkeit des Abschlusses von Wartungsverträgen angeboten?

1.2 Zuverlässigkeit/Ausfallsicherheit

- Wie zuverlässig und ausfallsicher ist das Produkt?
- Ist das Produkt im Dauerbetrieb einsetzbar?
- Gibt es einen im Produkt integrierte Backup-Mechanismus?
- Kann eine automatische Datensicherung durchgeführt werden?

1.3 Benutzerfreundlichkeit

- Können Benutzer die Systeme ohne größere Schulungsmaßnahmen effektiv, sicher und fehlerfrei nutzen?
- Ist die Synchronisations-Software so konfigurierbar, dass die Benutzer möglichst wenig mit technischen Details belastet werden? Ist die Sicherheit dabei trotzdem immer gewährleistet?
- Sind Abmessungen und Gewicht bezogen auf den Einsatzzweck angemessen? Ist die Akku-Laufzeit ausreichend für die tägliche Arbeit?

1.4 Kosten

- Wie hoch sind die Anschaffungskosten der Hard- und Software?
- Wie hoch sind die voraussichtlichen laufenden Kosten der Hard- und Software (Wartung, Betrieb, Support)?
- Wie hoch sind die voraussichtlichen laufenden Kosten für das Personal (Administrator/Support)?
- Müssen zusätzliche Soft- oder Hardware-Komponenten angeschafft werden (z. B. Docking-Station, Konvertierungssoftware)?

2. Funktion

2.1 Installation und Inbetriebnahme

- Lässt sich das Produkt einfach installieren, konfigurieren und nutzen?
- Kann das Gerät sowie die Synchronisations-Software so konfiguriert werden, dass die vorgegebenen Sicherheitsziele erreicht werden können?
- Können wichtige Konfigurationsparameter vor Veränderungen durch unbefugte Benutzer geschützt werden?
- Arbeitet das Produkt mit gängiger Hard- und Software zusammen (Betriebssysteme, Treiber)?

2.2 Administration

- Enthält die mitgelieferte Produktdokumentation eine genaue Darstellung aller technischen und administrativen Details?
- Können die PDAs über eine zentral gesteuerte Management-Software administriert werden? Ist die administrative Schnittstelle so gestaltet, dass auf fehlerhafte, unsichere oder inkonsistente Konfigurationen hingewiesen wird oder diese verhindert werden?

Ist einfache Administration möglich?

2.3 Protokollierung

- Bietet das Produkt Protokollierung an?
- Ist der Detailgrad der Protokollierung konfigurierbar?
- Werden durch die Protokollierung alle relevanten Daten erfasst?

2.4 Kommunikation und Datenübertragung

- Unterstützt der PDA alle benötigten Datenübertragungstechniken (z. B. Infrarot, Bluetooth oder GSM)?

2.5 Sicherheit: Kommunikation, Authentisierung und Zugriff

- Hat der PDA geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer?
- Können mit dem Produkt die Daten zu anderen Endgeräten gesichert übertragen werden? Gilt dies für alle Schnittstellen, also z. B. auch für drahtlose Verbindungen?
- Können zusätzliche Sicherungsmechanismen (z. B. Verschlüsselungs- oder Virensuchprogramme) genutzt werden?
- Erlaubt die Produktarchitektur die nachträgliche Installation neuer Sicherheitsmechanismen?
- Wird dem mobilen Benutzer nur nach erfolgreicher Authentisierung der Zugang zu lokalen Endgeräten erlaubt?
- Gibt es benutzerfreundliche Möglichkeiten zur Datensicherung?

Eigenwillige Mitarbeiter

Trotz einer Produktauswahl durch das IT-Management sollte immer damit gerechnet werden, dass Mitarbeiter andere PDAs bevorzugen und versuchen, diese im Betrieb einzusetzen und eventuell sogar Unterstützung dafür einfordern. Hierfür sollte eine geeignete Vorgehensweise definiert werden.

Ergänzende Kontrollfragen:

- Wurde eine Anforderungsanalyse durchgeführt?
- Wurde eine Bewertung der relevanten Geräte anhand dieser Anforderungen durchgeführt?
- Wurde die Beschaffungsentscheidung mit den Administratoren und dem technischen Personal abgestimmt?

M 2.306 Verlustmeldung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Bei Ausfall, Defekt, Zerstörung oder Diebstahl eines IT-Systems sollte dies umgehend gemeldet werden. Hierfür sollte es in jeder Organisation klare Meldewege und Ansprechpartner geben. Vor allem bei einem Diebstahl muss schnell gehandelt werden, da es hier nicht nur um die Wiederbeschaffung der Geräte geht, sondern auch darum, potentiellen Missbrauch der betroffenen Informationen zu verhindern.

Auf gestohlenen Geräten wie Laptops oder PDAs können sich vertrauliche Daten befinden, nach deren Verlust umgehend gehandelt werden muss, beispielsweise:

- Zugangsdaten wie Passwörter: Alle Zugangsdaten auf eventuell betroffenen IT-Systemen müssen umgehend geändert werden.
- als vertraulich eingestufte Informationen (z. B. Patientenakten): Alle betroffenen Bereiche (z. B. Fachabteilung, Kunden, etc.) müssen benachrichtigt werden, um entsprechende Maßnahmen ergreifen zu können.

Wenn verloren geglaubte Geräte wieder auftauchen, ist dies nicht nur ein Grund zur Freude, sondern sollte auch nachdenklich stimmen. Vor der erneuten Inbetriebnahme sollten die Geräte auf eventuelle Manipulationen untersucht werden (z. B. ob Schrauben geöffnet oder Siegel entfernt wurden). Außerdem sollten sie neu installiert werden, um sicherzustellen, dass sich keine manipulierten Programme auf diesen befinden (siehe dazu M 4.28 *Software-Reinstallation bei Benutzerwechsel eines Laptops*).

Ergänzende Kontrollfragen:

- Wissen die Benutzer wie und wo sie Verlustmeldungen abgeben können?

M 2.307 Geordnete Beendigung eines Outsourcing-Dienstleistungsverhältnisses

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung, IT-Verfahrensverantwortlicher

Die Empfehlungen dieser Maßnahme lassen sich in der Regel nur umsetzen, wenn bereits im Vertrag mit dem Outsourcing-Dienstleister alle relevanten Themen bei Vertragsende geregelt wurden.

Wird das Dienstleistungsverhältnis beendet, müssen die betroffenen Dienstleistungen wie beispielsweise der IT-Betrieb geordnet zurück in eigene Verantwortung oder auf einen anderen Dienstleister übergehen. Es müssen Vorkehrungen getroffen werden, dass durch das Vertragsende des Dienstleistungsvertrags nicht die Geschäftstätigkeit beeinträchtigt wird.

- Der Übergang auf einen anderen Dienstleister ist ein neues Outsourcing-Verfahren. Die Maßnahmen des Outsourcing-Bausteins sind entsprechend anzuwenden.
- Bei Insourcing sind die relevanten Maßnahmen des Outsourcing-Bausteins analog anzuwenden. Für Strategie, IT-Sicherheitskonzept für Insourcing, Migration und Notfallvorsorge gelten die gleichen Anforderungen wie bei einem "klassischen" Outsourcing-Verfahren.

Folgende Gesichtspunkte sind zu beachten:

- Eigentumsrechte an Hard- und Software (Schnittstellenprogramme, Tools, Batchabläufe, Makros, Lizenzen, Backups) müssen geregelt werden.
- Die Weiterverwendung der vom Dienstleister eingesetzten Tools, Prozeduren, Skripte, Batchprogramme ist für den Fall der Beendigung des Dienstleistungsverhältnisses zu regeln.
- IT-Systeme, IT-Anwendungen und Arbeitsabläufe müssen ausreichend dokumentiert sein.
- Alle notwendigen Daten müssen vom Dienstleister an den Auftraggeber übertragen bzw. übergeben werden.
- Alle Datenbestände beim Dienstleister müssen sicher gelöscht werden.
- Interne oder externe Mitarbeiter, die Aufgaben des Dienstleisters übernehmen, müssen eingewiesen und geschult werden.
- Es ist empfehlenswert, vertraglich eine Übergangsfrist zu vereinbaren, in der der ehemalige Dienstleister noch für Rückfragen und Hilfestellungen zur Verfügung steht.

Ergänzende Kontrollfragen:

- Wurden die im Dienstleistungsvertrag vereinbarten Rechte und Pflichten bei Vertragsende berücksichtigt?

M 2.308 Auszug aus Gebäuden

Verantwortlich für Initiierung: Leiter Innerer Dienst, Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Innerer Dienst, Mitarbeiter

Wenn ein Gebäude ganz oder teilweise wegen Auszug geräumt wird, sind folgende Dinge zu beachten:

- Im Vorfeld des Auszugs ist ein Bestandsverzeichnis aller für die IT-Sicherheit relevanten Dinge (Hardware, Software, Datenträger, Paperware etc.) zu erstellen.
- Jeder Beschäftigte ist schriftlich darüber zu informieren, für welche Dinge er zuständig ist. Dadurch wird vermieden, dass sich ein Mitarbeiter sehr wohl um seine eigenen Dinge kümmert, Dinge für die vermeintlich jemand anderer zuständig ist, hingegen liegen bleiben.
- Nicht mehr benötigte Alt-Geräte, Datenträger etc. sind vor dem Auszug entsprechen der Maßnahme M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* zu entsorgen. Keinesfalls dürfen alte Betriebsmittel einfach zurückgelassen werden, auch wenn der Vermieter, Nachmieter oder Käufer deren weitere Verwendung wünscht oder eine Entsorgung zusagt.
- Nach absolviertem Auszug sind ALLE Räume daraufhin zu überprüfen, ob auch tatsächlich keine sicherheitskritischen Dinge zurückgelassen wurden. Besonders in entlegenen Abstellbereichen wie Keller und Dachböden werden häufig Dinge vergessen.

  Alle Gegenstände der dienstlichen Nutzung sind konsequent einzusammeln, zu entfernen und gegebenenfalls nachträglich einer sicheren Entsorgung zuzuführen.

Die Empfehlungen aus M 2.177 *Sicherheit bei Umzügen* sollten berücksichtigt werden.

Ergänzende Kontrollfragen:

- Werden für den Auszug Bestandsverzeichnisse erstellt und verteilt?
- Wird das Gebäude nach erfolgtem Auszug nach zurückgelassenen Dingen durchsucht?

M 2.309 Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Leiter IT

IT-Geräte, die außerhalb der eigenen Institution eingesetzt werden, sind mehr Risiken ausgesetzt, als solche, die sich innerhalb geschützter Räumlichkeiten befinden. Trotzdem gibt es eine Vielzahl von Möglichkeiten, mobile IT-Systeme unterwegs zu schützen. Damit diese Möglichkeiten auch genutzt werden, sollte eine Sicherheitsrichtlinie erstellt werden, in der alle umzusetzenden Sicherheitsmechanismen beschrieben sind. Zusätzlich sollte für die Benutzer ein kurzes und übersichtliches Merkblatt für die sichere Nutzung von mobilen IT-Systemen erstellt werden.

Sensibilisierung der Benutzer

Je kleiner und leichter IT-Systeme werden, desto leichtfertiger wird erfahrungsgemäß damit umgegangen. Daher sollten Mitarbeiter für den Wert mobiler IT-Systeme und den Wert der darauf gespeicherten Informationen sensibilisiert werden. Da es bei mobilen IT-Systemen eine große Bandbreite von Varianten und Kombinationsmöglichkeiten gibt (von Handy über PDA zu Laptop mit WLAN-Schnittstelle), sollten sie vor allem über die spezifischen Gefährdungen und Maßnahmen der von ihnen benutzten Geräte aufgeklärt werden.

Sorgfalt bei der Weitergabe von Informationen

Die Mitarbeiter sollten auch darüber aufgeklärt werden, dass sie vertrauliche Informationen unterwegs nicht mit jedem austauschen und dies unterwegs auch nicht in Hör- und Sichtweite von Externen machen sollten. Insbesondere sollte die Identität des Kommunikationspartners hinterfragt werden, bevor detaillierte Auskünfte gegeben werden (siehe auch G 3.45 *Unzureichende Identifikationsprüfung von Kommunikationspartnern*).

Regelungen zur Nutzung mobiler IT-Systeme

Ebenso sind bei der Nutzung von mobilen IT-Systemen diverse Punkte zu regeln:

- Die Benutzer müssen darüber informiert sein, welche Informationen mit mobilen IT-Systemen unterwegs verarbeitet werden dürfen. Die Daten sollten dementsprechend klassifiziert sein, um Einschränkungen den Benutzern transparent zu machen (siehe auch M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*). Dienstgeheimnisse dürfen nicht auf mobilen IT-Systemen verarbeitet werden.
- Daten, die ein hohes Maß an Sicherheit verlangen (z.B. Angebote, Konstruktionsdaten, Wirtschaftsdaten des Unternehmens) sollten stets verschlüsselt auf dem mobilen IT-System abgelegt werden.
- Beim Einsatz mobiler IT-Systeme ist zu klären, ob mobile Mitarbeiter von unterwegs Zugriff auf interne Daten ihrer Institution erhalten. Falls dies vorgesehen ist, muss dieser Zugriff angemessen geschützt werden (siehe hierzu auch M 5.121 *Sichere Kommunikation von unterwegs* und M 5.122 *Sicherer Anschluss von Laptops an lokale Netze*).

- Es muss geklärt werden, ob diese auch für private Zwecke benutzt werden dürfen, beispielsweise für private Schreiben oder ein Spielchen nach Feierabend.
- Die Benutzer sollten darauf hingewiesen werden, wie sie sorgfältig mit den mobilen IT-Systemen umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten (z. B. Akkupflege, Aufbewahrung außerhalb von Büro- oder Wohnräumen, Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen).
- Die Verwaltung, Wartung und Weitergabe von mobilen IT-Systemen sollte geregelt werden.
- Bei jedem Benutzerwechsel müssen alle benötigten Passwörter gesichert weitergegeben werden (siehe M 2.22 *Hinterlegen des Passwortes*).

Mobile IT-Systeme sollten möglichst nicht unbeaufsichtigt bleiben. Falls ein mobiles IT-System in einem Kraftfahrzeug zurückgelassen werden muss, so sollte das Gerät von außen nicht sichtbar sein. Das Abdecken des Gerätes oder das Einschließen in den Kofferraum bieten Abhilfe. Ein mobiles IT-System stellt einen Wert dar, der potentielle Diebe anlocken könnte.

Werden mobile IT-Systeme in fremden Büroräumen vor Ort benutzt, so sind die Sicherheitsregelungen der besuchten Organisation zu beachten.

In fremden Räumlichkeiten wie Hotelzimmern sollten mobile IT-Systeme nicht ungeschützt ausliegen. Alle Passwort-Schutzmechanismen sollten spätestens jetzt aktiviert werden. Das Verschließen des Gerätes in einem Schrank behindert Gelegenheitsdiebe.

Entsorgung von Datenträgern und Dokumenten

Auch unterwegs gibt es häufiger Material, das entsorgt werden soll, schon alleine, damit das Gepäck noch tragbar bleibt. Während es aber innerhalb der eigenen Institution eingeübte Verfahren gibt, wie alte oder unbrauchbare Datenträger und Dokumente entsorgt werden (siehe auch M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*), ist dies unterwegs nicht immer möglich. Daher ist vor der Entsorgung ausgedienter Datenträger und Dokumente genau zu überlegen, ob diese sensible Informationen enthalten könnten. Ist dies der Fall, müssen die Datenträger und Dokumente im Zweifelsfall wieder mit zurück transportiert werden. Dies ist auch dann der Fall, wenn die Datenträger defekt sind, da Experten auch hieraus wieder wertvolle Informationen zurückgewinnen können. Auch Shredder-Einrichtungen in fremden Institutionen sollten mit Vorsicht betrachtet werden, da hier nicht unbedingt ersichtlich ist, wer die Entsorgung durchführt bzw. wie zuverlässig diese ist.

Nutzungsverbot von mobilen IT-Systemen

Es sollte überlegt werden, ob die Nutzung oder sogar das Mitbringen von mobilen IT-Systemen in allen oder bestimmten Bereichen einer Behörde oder eines Unternehmens eingeschränkt werden sollte. Dies kann z. B. für Besprechungsräume sinnvoll sein (siehe dazu beispielsweise M 5.80 *Schutz vor Abhören der Raumgespräche über Mobiltelefone*). Wenn die IT-Sicherheitspolitik der Institution es nicht zulässt, dass mobile IT-Systeme

mitgebracht werden, muss an allen Eingängen deutlich darauf hingewiesen werden. Dies sollte dann auch regelmäßig kontrolliert werden.

Ergänzende Kontrollfragen:

- Existiert eine aktuelle Sicherheitsrichtlinie für die Nutzung von mobilen IT-Systemen?
- Wie wird die Einhaltung der Sicherheitsrichtlinie für die Nutzung von mobilen IT-Systemen überprüft?
- Besitzt jeder Benutzer von mobilen IT-Systemen ein Exemplar dieser Richtlinie oder ein Merkblatt mit einem Überblick der wichtigsten Sicherheitsmechanismen?
- Ist die Sicherheitsrichtlinie für die Nutzung von mobilen IT-Systemen Inhalt der Schulungen zu IT-Sicherheitsmaßnahmen?
- Werden die Benutzer von mobilen IT-Systemen auf die Regelungen hingewiesen, die von ihnen einzuhalten sind?
- Werden die Benutzer von mobilen IT-Systemen auf die geeignete Aufbewahrung hingewiesen?

M 2.310 Geeignete Auswahl von Laptops

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator, Beschaffungsstelle, Leiter IT

Laptops gibt es in verschiedensten Varianten und Geräteklassen. Diese unterscheiden sich nicht nur in ihrem Abmessungen und Leistungsmerkmalen, sondern auch den Sicherheitsmechanismen und Bedienkomfort. Zudem stellen sie unterschiedliche Voraussetzungen an Hard- und Software-Komponenten im Einsatzumfeld.

Bei der Vielzahl verschiedener Laptop-Modelle mit den unterschiedlichsten Betriebssystemen, sind Kompatibilitätsprobleme bei Hardware, Software auf Laptop und PC sowie Schnittstellen naheliegend.

Wenn einmal beschlossen worden ist, innerhalb einer Institution Laptops einzusetzen, sollte daher eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Aufgrund der Bewertung sollten dann die zu beschaffenden Produkte ausgewählt werden. Die Praxis zeigt, dass es aufgrund verschiedener Einsatzanforderungen durchaus sinvoll sein kann, mehrere Gerätetypen für die Beschaffung auszuwählen. Die Gerätevielfalt sollte aber zur Vereinfachung des Supports eingeschränkt werden.

Zunächst sollte eine Anforderungsanalyse durchgeführt werden. Ziel der Anforderungsanalyse ist es einerseits, alle im konkreten Fall in Frage kommenden Einsatzszenarien zu bestimmen und andererseits daraus Anforderungen an die benötigten Hard- und Softwarekomponenten abzuleiten.

Die folgende Liste gibt einen groben Überblick über mögliche allgemeine Bewertungskriterien, erhebt jedoch keinen Anspruch auf Vollständigkeit und kann um weitere allgemeine Anforderungen erweitert werden.

1 Allgemeine Kriterien

1.1 Wartbarkeit

- Ist das Produkt einfach wartbar?
- Bietet der Hersteller regelmäßige Software-Updates an?
- Wird für das Produkt die Möglichkeit des Abschlusses von Wartungsverträgen angeboten?

1.2 Zuverlässigkeit/Ausfallsicherheit

- Wie zuverlässig und ausfallsicher ist das Produkt?
- Ist das Produkt im Dauerbetrieb einsetzbar?
- Gibt es einen im Produkt integrierte Backup-Mechanismus? Kann eine automatische Datensicherung durchgeführt werden?

1.3 Benutzerfreundlichkeit

- Lässt sich das Produkt einfach installieren, konfigurieren und nutzen?

- Ist die Synchronisations-Software so konfigurierbar, dass die Benutzer möglichst wenig mit technischen Details belastet werden? Ist die Sicherheit dabei trotzdem immer gewährleistet?
- Sind Abmessungen und Gewicht bezogen auf den Einsatzzweck angemessen? Ist die Akku-Laufzeit ausreichend für die tägliche Arbeit?

1.4 Kosten

- Wie hoch sind die Anschaffungskosten der Hard- und Software?
- Wie hoch sind die voraussichtlichen laufenden Kosten der Hard- und Software (Wartung, Betrieb, Support)?
- Wie hoch sind die voraussichtlichen laufenden Kosten für das Personal (Administrator/Support)?
- Müssen zusätzliche Soft- oder Hardware-Komponenten angeschafft werden (z. B. Docking-Station, Konvertierungssoftware)?

2. Funktion

2.1 Installation und Inbetriebnahme

- Kann das Gerät sowie die Synchronisations-Software so konfiguriert werden, dass die vorgegebenen Sicherheitsziele erreicht werden können?
- Können wichtige Konfigurationsparameter vor Veränderungen durch Benutzer geschützt werden?
- Arbeitet das Produkt mit gängiger Hard- und Software zusammen (Betriebssysteme, Treiber)?

2.2 Administration

- Enthält die mitgelieferte Produktdokumentation eine genaue Darstellung aller technischen und administrativen Details?
- Können die Laptops über eine zentral gesteuerte Management-Software administriert werden? Ist die administrative Schnittstelle so gestaltet, dass auf fehlerhafte, unsichere oder inkonsistente Konfigurationen hingewiesen wird oder diese verhindert werden?

2.3 Protokollierung

- Bietet das Produkt Protokollierung an?
- Ist der Detailgrad der Protokollierung konfigurierbar? Werden durch die Protokollierung alle relevanten Daten erfasst?
- Ist der Zugriff auf die Protokolldaten mit einem Zugriffsschutz versehen?

- Bietet das Produkt die Möglichkeit an, die Protokolldaten nicht nur lokal zu speichern, sondern auch auf entfernten Rechnern (zentrales Protokoll)?

2.4 Kommunikation und Datenübertragung

- Unterstützt der Laptop alle benötigten Datenübertragungstechnologien (z. B. Infrarot, Bluetooth oder GSM)?

2.5 Sicherheit: Kommunikation, Authentisierung und Zugriff

- Hat der Laptop geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer?
- Können mit dem Produkt die Daten zu anderen Endgeräten gesichert übertragen werden?
- Können zusätzliche Sicherungsmechanismen (z. B. Verschlüsselungs- oder Virensuchprogramme) genutzt werden?
- Erlaubt die Produktarchitektur die nachträgliche Installation neuer Sicherheitsmechanismen?
- Wird dem mobilen Benutzer nur nach erfolgreicher Authentisierung der Zugang zu lokalen Endgeräten erlaubt?
- Ist die Systemarchitektur so aufgebaut, dass neue Authentisierungsmechanismen nachträglich integriert werden können?

Sind alle Anforderungen an das zu beschaffende Produkt dokumentiert, so müssen die am Markt erhältlichen Produkte dahin gehend untersucht werden, inwieweit sie diese Anforderungen erfüllen. Es ist zu erwarten, dass nicht jedes Produkt alle Anforderungen gleichzeitig oder gleich gut erfüllt. Daher sollten die einzelnen Anforderungen mit Gewichten versehen werden, die reflektieren, wie wichtig die Erfüllung der jeweiligen Anforderung ist. Aufgrund der durchgeführten Produktbewertung (gemäß dem erstellten Anforderungskatalog) kann dann eine fundierte Kaufentscheidung getroffen werden.

Ergänzende Kontrollfragen:

- Wurde eine Anforderungsanalyse durchgeführt?
- Wurde eine Bewertung der relevanten Geräte anhand dieser Anforderungen durchgeführt?
- Wurde die Beschaffungsentscheidung mit den Administratoren und dem technischen Personal abgestimmt?

M 2.311 Planung von Schutzschränken

Verantwortlich für Initiierung: Leiter IT, Leiter Beschaffung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Beschaffungsstelle, Haustechnik

Der Einsatz von Schutzschränken kann aus verschiedenen Gründen sinnvoll sein, z. B. als Ersatz für einen Serverraum oder um die Schutzwirkung eines Serverraums zu erhöhen. Da die Kosten für Schutzschränke nicht unerheblich sind, sollte zunächst ein Konzept erstellt werden, das auf den Anforderungen aus den geplanten Einsatzszenarien beruht. Dafür ist unter anderem zu hinterfragen, welche Komponenten durch den Schutzschrank gegen welche Bedohungen geschützt werden sollen, also z. B. ob sie ihren Inhalt gegen die Einwirkung von Feuer bzw. gegen unbefugten Zugriff schützen sollen.

Außerdem ist ein Kostenvergleich dringend empfehlenswert. Zu vergleichen sind die Kosten, die die Beschaffung und der Unterhalt eines Schutzschrankes verursachen, mit den Kosten für die Errichtung eines Serverraums bzw. Datenträgerarchivs und dessen Unterhalt.

Bei der Planung des Raumes, in dem der Schutzschrank aufgestellt wird, ist durch Maßnahmen zum Brandschutz bis hin zur Installation einer Gefahrenmeldeanlage, gegebenenfalls innerhalb des Schutzschranks, dafür zu sorgen, dass eine hinreichende physische Sicherheit bereitgestellt wird. Dazu gehört auch, dass nach Möglichkeit keine wasserführenden Leitungen vorhanden sein sollten, da Undichtigkeiten größere Schäden verursachen können, gegen die nicht jeder Schutzschrank ausreichend abgesichert ist. Soll der Schutzschrank als Serverschrank eingesetzt werden, sind je nach Schutzbedarf zusätzliche Maßnahmen wie Überspannungsschutz, Not-Aus-Schalter, Klimatisierung, USV und eventuell auch eine Fernanzeige von Störungen vorzusehen.

Ergänzende Kontrollfragen:

- Wird vor einer Beschaffung eine Anforderungsanalyse für den Einsatz eines Schutzschranks durchgeführt?

M 2.312 Konzeption eines Schulungs- und Sensibilisierungsprogramms zur IT-Sicherheit

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter Personal, IT-Sicherheitsmanagement-Team

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement-Team, Vorgesetzte

Ein gutes Schulungs- und Sensibilisierungsprogramm zur IT-Sicherheit sollte jeden im Unternehmen bzw. in der Behörde einbeziehen. Dabei sollte das Bewusstsein aller Mitarbeiter für Gefährdungen geschärft bzw. geschaffen werden, um Sicherheitsproblemen vorzubeugen und um aus eigenen und externen Sicherheitsproblemen zu lernen.

Unterstützung der Führungsebene einholen

Für die Durchführung von Schulungs- und Sensibilisierungsmaßnahmen ist unbedingt die Unterstützung des Managements erforderlich, damit der notwendige Nachdruck für alle sichtbar ist und die benötigten Ressourcen zur Verfügung stehen (siehe auch M 3.44 *Sensibilisierung des Managements für IT-Sicherheit*).

Im Folgenden werden die wichtige Schritte bei der Konzeption eines Schulungs- und Sensibilisierungsprogramms beschrieben.

1. Lernziele definieren (Ableiten aus IT-Sicherheitszielen)

Als erstes muss definiert werden, welche Ziele erreicht werden sollen. Wichtig ist vor allem, dass die IT-Sicherheitsziele der jeweiligen Institution hier einfließen. Typische Ziele von Sensibilisierungs- und Schulungsmaßnahmen zur IT-Sicherheit sind die folgenden:

- Aufmerksamkeit für IT-Sicherheit zu gewinnen und Interesse daran wecken,
- Grundwissen zu IT-Sicherheit zu vermitteln,
- die für die Fachaufgaben der Benutzer benötigten IT-Sicherheitskenntnisse zu vermitteln,
- Praxiswissen zu vermitteln, so dass Mitarbeiter in sicherheitskritischen Situation richtig reagieren,

kontinuierliche Verhaltensänderungen zu erzielen.

Außerdem sollten die Erfolgskriterien für die Schulungs- und Sensibilisierungsprogramme skizziert werden, auch wenn diese unbestreitbar nur schwer zu beschreiben oder zu quantifizieren sind.

2. Zielgruppenorientiertes Training und Sensibilisierung

Die Zielgruppe für jede Maßnahme im Bereich IT-Sicherheitstraining ist im Voraus zu bestimmen, da IT-Benutzer im allgemeinen unterschiedliche Bedürfnisse und Vorkenntnisse haben und auch teilweise über verschiedene Methoden anzusprechen sind. Hier sind beispielsweise zu unterscheiden:

Managementebene

- Der Erfolg ganzer Sensibilisierungsprogramme hängt oft davon ab, wie gut diese von der Managementebene aufgenommen werden. Daher ist eine

gründliche Vorbereitung der Sensibilisierungsmaßnahmen für die Managementebene enorm wichtig.

- Diese Zielgruppe hat oft wenig Zeit, daher sollten alle Sensibilisierungsmaßnahmen kurz und prägnant sein.

Mitarbeiter

- Die Mitarbeiter sind diejenigen, deren Verhalten die stärksten direkten Auswirkungen auf die tägliche IT-Sicherheit innerhalb der Institution hat. Hier ist zu berücksichtigen, dass der Wissenstand über IT sehr unterschiedlich sein kann. Beispielsweise haben Software-Entwickler andere IT Kenntnisse als Mitarbeiter der Personalverwaltung und benötigen unterschiedliche Inhalte um zum Thema IT-Sicherheit sensibilisiert und geschult zu werden.

Administratoren

- Administratoren und Support-Mitarbeiter müssen tiefgehende Fachkenntnisse der von ihnen betreuten IT-Systeme und IT-Anwendungen haben, so dass sie auch in der Lage sind, Sicherheitsprobleme zu erkennen und zu beheben sowie diesen vorzubeugen.

Externe Mitarbeiter

- In vielen Fällen werden interne Daten, Anwendungen und Systeme für Mitarbeiter anderer Institutionen zur Verfügung gestellt. Vertraulichkeitserklärungen bieten ein Mittel, um externe Mitarbeiter zum sicheren Umgang mit der internen Informationstechnik zu verpflichten und zu sensibilisieren.

Das IT-Sicherheitstraining muss in Umfang und Inhalt auf die Bedeutung und Komplexität des IT-Einsatzes bei den jeweiligen Zielgruppen abgestimmt werden. Daher sollten zunächst die Mitarbeiter einer Institution in Zielgruppen eingeteilt werden, für die jeweils passende IT-Sicherheitstrainingsmaßnahmen ausgewählt werden.

3. Lernbedürfnisse identifizieren

Um die Inhalte für die Schulungs- und Sensibilisierungsmaßnahmen zielgerecht festlegen zu können, müssen die Lernbedürfnisse identifiziert werden. Es sollte erörtert werden, wer welche Kenntnisse über IT-Sicherheit haben und welche IT-Sicherheitsmaßnahmen beherrschen sollte. Insbesondere sind folgende Bereiche auf jeden Fall zu berücksichtigen:

- Sensibilisierung für alle Mitarbeiter, aber insbesondere Managementebene,
- Einarbeitung neuer Mitarbeiter,
- Grundlagenwissen für alle Mitarbeiter,
- Spezialkenntnisse für bestimmte Gruppen wie z. B. Sicherheitsspezialisten und Administratoren.

Der Wissensbedarf sollte dabei an den Sicherheitszielen der Behörde oder des Unternehmens ausgerichtet werden.

4. Lerninhalte festlegen

Keep it short and simple!

Alle Mitarbeiter sollten alle internen IT-Sicherheitsleitlinien, Regelungen, Verfahren kennen, die für ihren Arbeitsplatz relevant sind. Sie sollten nicht nur auf deren Existenz hingewiesen werden, sondern auch deren Inhalte, Hintergründe und Einflüsse auf die Arbeitsumgebung kennen. Dafür ist natürlich auch wichtig, dass es nicht zu viele Vorgaben, Regeln und Dokumente zu IT-Sicherheit gibt. Hier wie überall sollte das Regelwerk einfach und überschaubar gehalten werden

- Inhalte zu Grundlagen der IT-Sicherheit sind in den Maßnahmen M 3.26 *Einweisung des Personals in den sicheren Umgang mit IT* und M 3.5 *Schulung zu IT-Sicherheitsmaßnahmen* spezifiziert.
- Für Inhalte zu Spezialthemen können die Maßnahmen M 3.45 *Planung von Schulungsinhalten zur IT-Sicherheit* und M 3.49 *Schulung zur Vorgehensweise nach IT-Grundschutz* herangezogen werden. Wenn für die Trainingsmaßnahmen auf externe Veranstalter zurückgegriffen wird, können diese auch hier als Checkliste genutzt werden, um zu prüfen, ob vorkonfektionierte Seminare die benötigten Inhalte haben.

Übung der Anwendung von IT-Sicherheitsvorgaben

Damit das Einhalten der IT-Sicherheitsvorgaben während des täglichen Betriebes nicht als Hürde empfunden wird, muss dieses vorher ausreichend geübt werden. Anderenfalls wird aufgrund von Termindruck möglicherweise auf die IT-Sicherheitsvorkehrungen erst einmal verzichtet. So geraten sie langfristig in Vergessenheit.

Einbindung in bestehende Schulungsmaßnahmen

Die Schulungsmaßnahmen zur IT-Sicherheit müssen in enger Abstimmung mit den sonstigen Schulungsmaßnahmen der Institution, vor allem mit den IT-Schulungen erstellt werden. Dabei sollte überlegt werden, inwieweit es möglich ist, Schulungsthemen zur IT-Sicherheit in letztere zu integrieren. Eine solche Einbindung hat den Vorteil, dass IT-Sicherheit unmittelbar als Bestandteil des IT-Einsatzes wahrgenommen wird. Dafür müssen allerdings die Dozenten ausreichend qualifiziert sein. Außerdem muss IT-Sicherheitsaspekten genügend Platz und Zeit eingeräumt werden. Eine Kurz-Abhandlung des Themas etwa am Freitag zwischen 13 und 14 Uhr genügt nicht.

5. Methoden und Medien auswählen

Zunächst muss geklärt werden, ob die Sensibilisierung und Ausbildung zu Sicherheitsfragen durch eigene Mitarbeiter oder Externe durchgeführt werden soll und in welcher Form die Ausbildung erfolgen soll (siehe auch M 3.48 *Auswahl von Trainern oder Schulungsanbietern*). Typische Varianten sind folgende:

- Informationsbörse zu IT-Sicherheit im Intranet,
- Mitarbeiterzeitung,
- E-Mails zu aktuellen Sicherheitsfragen, Anmelde-Bildschirm mit Sicherheitsinformationen,
- Rundschreiben und Zeitschriften mit sicherheitsrelevanten Themen,
- Poster und Broschüren,

- Werbematerialen zur IT-Sicherheit,
- interne Informationsveranstaltungen,
- externe Seminare, Messen und Konferenzen,
- Videos, die Spezialthemen zur IT-Sicherheit aufzeigen,
- E-Learning-Programme,
- Planspiele zur IT-Sicherheit (siehe M 3.47 *Durchführung von Planspielen zur IT-Sicherheit*).

Alle bereits im Unternehmen oder in der Behörde vorhandenen Schulungsprogramme und -materialien sollten darauf untersucht werden, ob sie sich als erfolgreich erwiesen haben und als Vorbild übernommen werden können und ob Sicherheitsthemen in andere Programme integriert werden können.

Für Sensibilisierungsprogramme sollten kreative und phantasiereiche pädagogische Materialien gewählt werden, die zur verantwortungsbewussten IT-Nutzung anregen.

Bei der Auswahl von E-Learning-Anwendungen sollte auch berücksichtigt werden, dass diese als IT-Anwendungen selber wieder keine negativen Auswirkungen auf die IT-Sicherheit in der eingesetzten IT-Umgebung haben dürfen. Wenn E-Learning-Angebote nicht nur im Intranet, sondern auch über das Internet präsentiert werden sollen, sollte beispielsweise auf aktive Inhalte (Java, Javascript, ActiveX, etc.) verzichtet werden. Wenn dies nicht machbar ist, können sie nur über dedizierte, nicht ins Netz integrierte Internet-PCs abgerufen werden. Grundsätzlich sollten E-Learning-Anwendungen wie jede andere Anwendung auch vor ihrem Einsatz getestet und nur freigegeben werden, wenn keine Sicherheitsbedenken bestehen.

6. Durchführung

Alle Ausbildungsangebote sollten auf die vorliegenden Bedürfnisse abgestimmt sein und modularisierbar sein, so dass jede Zielgruppe ausreichend und in angemessener Tiefe geschult werden kann.

7. Erfolg und Effektivität kontrollieren

Bei allen Maßnahmen zur Schulung und Sensibilisierung für IT-Sicherheit muss zum einen sichergestellt werden, dass diese für sich zielgruppengerecht und effektiv waren, zum anderen aber auch, dass alle betroffenen Mitarbeiter erreicht wurden. Dabei dürfen auch Personen nicht vergessen werden, die nur zeitweise bei der Institution oder bei einem Unterauftragnehmer arbeiten. Jede Organisation sollte einen Überblick über den Ausbildungsstand ihrer Mitarbeiter haben, beispielsweise über Schulungsnachweise.

Um die Effektivität der Trainingsmaßnahmen nachzuprüfen, können verschiedene Verfahren gewählt werden. Die klassische Methode ist der Einsatz von Fragebögen, mit denen die Teilnehmer die Qualität der Schulung bewerten können, bzw. über die Gelerntes hinterfragt, Verständnisprobleme aufgezeigt und Bedürfnisse für weitere Schulungen festgestellt werden können. Wenn regelmäßig externe Anbieter Schulungen für Mitarbeiter durchführen, sollten diese unbedingt auch intern bewertet werden, um

Zufriedenheit und Lernerfolge bei diesen Anbietern feststellen zu können.

Eine sichtbare Änderung der Einstellung der Mitarbeiter gegenüber Sicherheitsmaßnahmen, z. B. ob sich Benutzer in Arbeitspausen abmelden oder sie Bildschirmschoner zum Zugriffsschutz aktivieren, kann ebenfalls als Maßstab für den Erfolg der Trainingsmaßnahmen verwendet werden. Dies darf allerdings nicht als Überwachung von Mitarbeitern missbraucht werden.

In die Planung von Sicherheitskampagnen sollte auch der Personal- bzw. Betriebsrat rechtzeitig einbezogen werden, da auch typisches Fehlverhalten von Mitarbeitern angesprochen werden muss. Dies sollte aber natürlich nie auf konkrete Einzelfälle innerhalb der eigenen Institution bezogen sein.

8. Wissen regelmäßig aktualisieren

In dem sich dynamisch entwickelnden IT-Bereich verliert einmal erworbenes Wissen rasch an Wert. Neue IT-Anwendungen und IT-Systeme, aber auch neue Bedrohungen, Schwachstellen und mögliche Abwehrmaßnahmen machen eine ständige Auffrischung und Erweiterung des Wissens über IT-Sicherheit erforderlich. Das diesbezügliche Schulungsangebot sollte sich daher nicht ausschließlich an neue Mitarbeiter richten, sondern auch für erfahrenere IT-Benutzer in regelmäßigen Abständen Auffrischungs- und Ergänzungskurse vorsehen. Weiterhin ist es vor diesem Hintergrund wichtig, die Schulungskonzepte einer regelmäßigen Aktualisierung zu unterziehen und sie nötigenfalls an neue Gegebenheiten anzupassen (siehe hierzu auch M 2.198 *Sensibilisierung der Mitarbeiter für IT-Sicherheit*).

Ergänzende Kontrollfragen:

- Ist eine Bedarfsanalyse zum vorhandenen Wissenstand und Wissensbedarf zu IT-Sicherheit durchgeführt worden?
- Gibt es Schulungsprogramme zur eingesetzten IT und zur IT-Sicherheit für alle Mitarbeiter einer Institution?
- Wird das IT-Sicherheitsmanagement-Team bei der Planung und Durchführung von IT-Schulungen eingebunden?
- Werden die Trainingsprogramme regelmäßig aktualisiert?

M 2.313 Sichere Anmeldung bei Internet-Diensten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Bei vielen Internet-Diensten müssen Benutzer sich anmelden, um diese nutzen zu können. Dazu ist in der Regel mindestens die Angabe eines Benutzernamens und eines Passwortes erforderlich, häufig werden aber auch mehr Informationen erfragt, wie z. B. Vor- und Familienname, Arbeitgeber, E-Mail-Adresse, etc.

Jeder Benutzer sollte sich genau überlegen, welche Angaben hier gemacht werden, da dies zum Beispiel ungewollte Werbeaktionen auslösen kann. Um dies zu vermeiden, sollten möglichst wenig detaillierte Informationen weitergegeben werden. Außerdem sollten die Datenschutz-Hinweise genau gelesen werden. Die Benutzer sollten bei jeder Angabe personenbezogener Daten überlegen, inwieweit sie diese wirklich an den Dienstleister weitergeben wollen und welcher weiteren Verwendung sie dabei zustimmen. Falls eine funktionierende E-Mail-Adresse benötigt wird, kann hierbei auf Wegwerf-E-Mail-Adressen zurückgegriffen werden, die gegebenenfalls über kostenfreie Internet-Dienste erzeugt werden können.

Falls bestimmte Internet-Dienste regelmäßig beruflich genutzt werden, sollten von der Institution möglichst Vorgaben für die Mitarbeiter erarbeitet werden, wie die einzelnen Felder beim Anmeldevorgang auszufüllen sind.

Das Passwort für den jeweiligen Internet-Dienst sollte angemessen sorgfältig ausgesucht werden (siehe dazu auch M 2.11 *Regelung des Passwortgebrauchs*). Vor allem sollten solche Passwörter nicht mit einem Passwort übereinstimmen, das wichtige Daten schützen soll, also z. B. den Büro-Rechner.

Falls bei der Anmeldung personenbezogene Daten angegeben werden müssen, so sollte dies möglichst nur SSL-gesichert erfolgen (siehe auch M 5.66 *Verwendung von SSL*). Wenn die Nutzung eines Angebots die Angabe sensitiver Daten über eine ungesicherte Verbindung erfordert, so sollte sorgfältig abgewogen werden, ob dieses Angebot wirklich genutzt werden soll.

Viele Internet-Dienste bieten eine Recovery-Funktion für Passwörter an, also eine Rettungsmöglichkeit, wenn ein Benutzer sein Passwort vergisst. Hierfür müssen im Vorfeld oft einige Fragen beantwortet werden. Die Antworten werden vom Dienstleister gespeichert und der Benutzer wird danach gefragt, wenn er sein eigentliches Passwort vergessen hat. Die Fragen sind häufig vorgefertigt, oft wird z. B. nach dem Namen der Mutter oder des Haustieres, der Lieblingsfarbe oder des Geburtsortes gefragt. Leider bieten nur wenige Dienstleister die Möglichkeit, die Frage selbst vorzugeben.

Hinweis: Bei vielen Angriffen über Social Engineering oder Phishing wird nicht plump nach Passwörtern gefragt, sondern anscheinend unverfänglich nach dem Haustier oder der Lieblingsfarbe. Daher ist es sinnvoll, bei Recovery-Funktionen keine wahrheitsgemäßen Antworten zu geben, sondern solche, auf die kein Angreifer kommt, die man sich aber selbst merken kann.

Ergänzende Kontrollfragen:

- Werden für Internet-Dienste andere Passwörter gewählt als für den eigenen Büro-Arbeitsplatz?

M 2.314 Verwendung von hochverfügbaren Architekturen für Server

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Die Verfügbarkeit von Geschäftsprozessen, Anwendungen und Diensten hängt oft von der Funktion eines zentralen Servers ab. Je mehr Anwendungen aber auf einem Server laufen, desto ausfallsicherer muss dieser sein. Ein Server enthält in der Regel verschiedene potentielle Fehlerquellen ("Single Points of Failure"), also Komponenten, deren Ausfall den Ausfall des Gesamtsystems auslösen kann: CPU, Festplatten, Stromversorgung, Lüfter, Backplane, etc. Die Wiederherstellung des Gesamtsystems kann in diesem Fall erhebliche Zeit in Anspruch nehmen. Neben der Vorhaltung von Ersatzteilen können zusätzlich folgende Möglichkeiten zur Steigerung der Verfügbarkeit eingesetzt werden:

- Cold-Standby
- Hot-Standby (manuelles Umschwenken)
- Cluster (automatisches Umschwenken)
  - Load balanced Cluster
  - Failover Cluster

Jede einzelne dieser Techniken bietet ein unterschiedliches Niveau an Verfügbarkeit und ist in der Regel mit unterschiedlichen Kosten verbunden.

Cold-Standby

Beim Cold-Standby wird neben dem eigentlichen Produktivsystem ein zweites baugleiches Ersatzsystem bereitgehalten, das aber nicht aktiv ist. Wenn das erste System ausfällt, kann das Ersatzssystem manuell hochgefahren und ins Netz integriert werden.

Nach der Vorhaltung von einzelnen Ersatzteilen ist dies die einfachste Redundanz-Lösung, die mit den entsprechenden Vorteilen und Nachteilen verbunden ist:

Vorteile einer Cold-Standby Lösung	Nachteile einer Cold-StandbyLösung
- Cold-Standby Lösungen bringen keine Komplexitätserhöhung für das Gesamtsystem mit sich. - Die Kosten für ein Cold-Standby System belaufen sich lediglich auf die Kosten der zusätzlichen Hardware und sind so mit am geringsten unter den vorgestellten Möglichkeiten. - Neuaufsetzen oder Änderungen im System sind ohne Verfügbarkeitseinbußen möglich. Der Produktivbetrieb wird dafür während der Änderungen auf das Cold-Standby System umgelegt.	- Zum bestehenden System muss ein zweites System vorgehalten werden. - Das Ersatzsystem muss ständig auf dem aktuellen Konfigurations- und Patch-Stand gehalten werden. - Da das Ersatzsystem manuell aktiviert werden muss, müssen Administratoren das System kontinuierlich überwachen und im Notfall einschreiten. - Wenn die Applikationsdaten nicht auf einem externen Speichersystem liegen, so dass der Zugriff direkt aus dem Ersatzsystem möglich ist, dann müssen diese auf das Cold-Standby System migriert werden.

Tabelle: Vor-und Nachteile einer Cold-Standby Lösung

Der Einsatz eignet sich gut für Server mit Anwendungen, bei denen kurze bzw. begrenzte Ausfallzeiten, bis der Eingriff des Administrators möglich ist, unkritisch sind. Beispiele dafür sind:

- Server in kleineren Netzen (Intranet)
- Wenig frequentierte Server im Internet

Hot-Standby (manuelles Umschwenken)

Bei einem Hot-Standby steht ebenfalls ein Ersatzsystem bereit, das aber neben dem Produktivsystem parallel in Betrieb gehalten wird. Die Funktion des Produktivsystems wird überwacht, bei Ausfall wird das Ersatzsystem aktiv. Der Wechsel kann automatisch erfolgen oder auch manuell. Für den automatischen Wechsel sind zusätzliche Funktionalitäten im Gesamtsystem erforderlich z. B. die automatische Erkennung von Ausfällen. Dieser Fall wird im nächsten Abschnitt unter "Cluster" behandelt.

Um die Ausfallzeiten möglichst gering zu halten, muss der Zustand des Ersatzsystems kontinuierlich überprüft werden.

Vorteile einer Hot-Standby Lösung	Nachteile einer Hot-Standby Lösung
- Die Ausfallzeiten sind im Vergleich zu Cold-Standby geringer. - Wie beim Cold-Standby ist diese Lösung auch relativ kostengünstig, verglichen mit höherwertigen Hochverfügbarkeitslösungen, die im Folgenden beschrieben werden. - Das Ersatzsystem ist in Betrieb und kann auch zu Datenreplikation benutzt werden. - Neuaufsetzen oder Änderungen im System sind ohne Verfügbarkeitseinbuße möglich. Der Produktivbetrieb wird dafür während der Änderungen auf das Hot-Standby System umgelegt.	- Es wird auch hier immer nur die Hälfte der vorhandenen Hardware genutzt. - Das Ersatzsystem muss ständig auf dem aktuellen Stand gehalten werden. - Im Falle der manuellen Aktivierung des Hot-Standby Systems ist eine kontinuierliche Überwachung von einem Systemverantwortlichen erforderlich.

Tabelle: Vor- und Nachteile einer Hot-Standby Lösung

Der Einsatz von Hot-Standby Systemen eignet sich für Anwendungen, bei denen kurze Ausfallzeiten unkritisch sind. Die Problematik der Systemüberwachung und der Aktivschaltung des Hot-Standby Servers muss dabei mitbedacht werden. Mögliche Einsatzbereiche sind z. B. für:

- Webserver mit oft variierendem Content
- Server in kleineren Netzen (Application-Server, Mailserver)
- Datenbank-Server und Fileserver (z. B. sekundärer Server repliziert primären Server ständig und wird im Fehlerfall als primärer Server geschaltet).

Cluster (automatisches Umschwenken)

Ein Cluster besteht aus einer Gruppe von zwei oder mehreren Rechnern, die zur Steigerung der Verfügbarkeit oder auch der Leistung einer Anwendung oder eines Dienstes parallel betrieben werden. Die Anwendung oder der Dienst kann dabei auf einem der Rechner aktiv durchgeführt werden oder auf mehreren verteilt (Performance-Steigerung).

Cluster werden je nach Funktionsart in

- Load balanced Cluster
- Failover Cluster und

unterschieden.

Load balanced Cluster

Beim Load balanced Cluster werden Instanzen einer Anwendung oder eines Dienstes in Abhängigkeit von der Auslastung unter den Servern verteilt. Wenn dies für eine Anwendung oder einen Dienst möglich ist, dann kann damit nicht nur eine Lastverteilung (Load balancing) und somit eine Performancesteigerung erreicht werden, sondern auch die Probleme bei Ausfällen werden verringert. Eine der Voraussetzungen für den Einsatz von Load balancing ist, dass die jeweiligen Anwendungen oder Dienste keinen schreibenden Datenzugriff benötigen dürfen.

Eine Redundanz kann in diesem Fall geschaffen werden, indem Systeme mit ähnlicher Leistung mit Hilfe eines Load-Balancing Prozesses "nebeneinander" gestellt werden und dafür gesorgt wird, dass beim Ausfall eines Servers die anderen Server diesen Ausfall auffangen.

Vorteile eines Load balanced Clusters	Nachteile eines Load balanced Clusters
- Es können damit sowohl Verfügbarkeitssteigerung als auch Leistungssteigerung erreicht werden. - Alle verfügbare Ressourcen werden dauerhaft genutzt. - Die Lösung ist hochgradig skalierbar. - Die Komplexität des Gesamtsystems ist geringer als bei einem Failover Cluster.	- Der Einsatz ist nicht für alle Arten von Anwendungen möglich. Insbesondere Anwendungen, die keine reinen Lesezugriffe verwenden und zugleich den Zugriff aller Server auf die gleichen Speicherressourcen verlangen, sind für Load Balancing nicht geeignet.

Tabelle: Vor- und Nachteile eines Load balanced Clusters

Wenn neben der Verfügbarkeit die Performance hohen Stellenwert hat und die Applikation einen verteilten Einsatz erlaubt, bietet ein Load balanced Cluster eine optimale Lösung. Das kann z. B. der Fall sein für:

Web-Server, für Front-end Applikationen mit ausschließlichen Lesezugriffen (z. B. Web-Server-Farmen) Failover Cluster

Als Failover Cluster wird hier ein Cluster bezeichnet, wenn bei Ausfall eines der Cluster-Systeme automatisch der aktive Betrieb der Anwendung oder des Dienstes von einem anderen Teil des Clusters übernommen wird (Takeover). Die automatische Übernahme von Diensten beim Ausfall einer Systemkomponente durch eine funktional äquivalente Komponente wird Failover genannt. Für die Failover-Funktionalität ist eine dedizierte "heartbeat" (Herzschlag) Verbindung üblich, die die Kommunikation zwischen den Cluster-Servern gewährleistet. Die Cluster-Server müssen neben der Verbindung mit dem Client-Netz auch mit dem Administrationsnetz dediziert verbunden sein, um einen direkten Zugriff im Notfall zu gewähren.

Ein automatisches Failover setzt voraus, dass alle Software- und Hardware-Komponenten geeignet überwacht werden. Daher ist es wichtig sicherzustellen, dass der Failover Mechanismus auf keine falschen Annahmen basiert.

Folgende Punkte müssen beim Einsatz eines Failover-Clusters berücksichtigt werden:

- **Zugriff auf gemeinsamen Speicher:**

  Neben den servereigenen Festplatten, die das Betriebssystem und die für den Betrieb notwendigen Daten enthalten, ist es in einem Cluster ratsam, die Anwendungsdaten auf gemeinsamen Speicher zu verwalten. Der Zugriff auf diese Festplatten wird dem Teil des Clusters gewährt, der gerade aktiv ist. Es ist auch möglich, statt gemeinsamen Festplatten replizierte Festplatten zu verwenden. Dies ist dann sinnvoll, wenn das Failover von einem entfernten Standort aus stattfindet. Bei einem lokalen Failover sollte überlegt werden, ob die durch die Replikation erzeugte Komplexität und entstandene Abhängigkeiten nicht eine zusätzliche Bedrohung für die Verfügbarkeit darstellen.

- **Portabilität der Anwendung:**

  Die Installation und Inbetriebnahme einer Anwendung auf zwei oder mehreren Servern parallel erfordert in den meisten Fällen den Einsatz zusätzlicher Lizenzen. Darüber hinaus muss überprüft werden, ob die Applikation eine Failover-Funktionalität erlaubt.

- **NSPoF (No Single Points of Failure):**

  Wenn die Failover-Funktionalität des Clusters durch den Ausfall einer einzigen Komponente gestört werden kann, widerspricht dies dem eigentlichen Zweck der Cluster-Architektur. Um Single Points of Failure zu vermeiden, muss das Gesamtsystem analysiert werden und der Ausfall einzelner Komponenten (Netzteile, Systemspeicher, Hauptspeicher, Netzwerkkarten, Switche, Hubs etc.) in Betracht gezogen werden.

- **Betriebssystem und Konfiguration der Cluster-Server:**

  Die Cluster-Server sollten mit gleichen Betriebssystemversionen, Patches, Libraries und Applikationsversionen ausgestattet sein. Eine möglichst identische Hardware- und Software-Konfiguration kann ein möglichst

identisches Verhalten im Falle eines Failovers gewährleisten. Darüber hinaus reduziert sich im Falle von identischen Systemen die Komplexität des Gesamtsystems (Einsatz der gleichen Failover Software, Netz-Schnittstellen, Kompatibilität der gemeinsamen Speichersystems, Administration, Service).

- **Dedizierte und redundante Verbindung zwischen den Servern:**

  Die Kommunikation zwischen den Cluster-Servern muss unabhängig von der Netzlast, möglichst verzögerungsfrei erfolgen, damit das Failover schnellstmöglichst stattfinden kann. Die Redundanz ist aufgrund der hohen Verfügbarkeitsanforderungen ebenfalls erforderlich.

- **Einsatz von ausgereiften Software-Produkten für das Failover Management:**

  Die Entscheidung, ob ein Failover stattfinden muss oder nicht, ist eine sehr komplexe. Neue oder selbstentwickelte Tools können Fehler enthalten und dadurch letztendlich die Verfügbarkeit des Gesamtsystems reduzieren.

- **Ausführliches Testen aller möglichen Failover-Aspekten:**

  Ein ausführliches Testen ist unter anderem auch dazu notwendig, um festzustellen, dass keine unerwarteten Fehlerquellen (Single Points of Failure) vorhanden sind. Insbesondere muss das Monitoring der Server und das Failover-Management auf alle möglichen Fehler getestet werden.

Vorteile eines Failover Clusters	Nachteile eines Failover Clusters
- Durch das automatische Takeover kann die Verfügbarkeit erheblich gesteigert werden. - Es sind keine manuellen Eingriff nötig.	- Diese Lösung ist hoch komplex. - Failover Cluster sind nicht gut skalierbar. - Es wird immer nur ein Teil der Ressourcen genutzt. - Es entstehen hohe Kosten aufgrund zusätzlicher Hardware und Software

Tabelle: Vor- und Nachteile eines Failover Clusters

Wie aus der Gegenüberstellung der Vorteile und Nachteile hervorgeht, ist der Einsatz eines Failover Clusters nur dann sinnvoll, wenn eine oder mehrere Applikationen sehr hohe Verfügbarkeitsanforderungen haben. Neben dem hohen Kostenaufwand sind sehr gute Kenntnisse des verantwortlichen Personals sowohl über die eingesetzten Betriebssysteme und Applikationen als auch über die Failover-Funktionalität erforderlich. Der Einsatz von Failover Lösungen für Server macht zudem nur dann Sinn, wenn auch alle Abhängigkeiten wie beispielsweise Netzanbindung oder Verfügbarkeit der Clients auch mit den entsprechenden Redundanzen ausgelegt sind.

Bereiche, für die typischerweise bei hohen Verfügbarkeitsanforderungen Failover Cluster eingesetzt werden, sind z. B.:

- Datenbank Anwendungen
- File Storage
- Anwendungen mit dynamischem Inhalt
- Mail Server

Wenn Geschäftsprozesse, Anwendungen oder Dienste hohe Anforderungen an die Verfügbarkeit haben, sollte auf jeden Fall überlegt werden, wodurch diese Anforderungen abgedeckt werden können. Die IT- bzw. IT-Sicherheitsverantwortlichen sollten für die entsprechenden Server ein Konzept erarbeiten und angemessene Architekturen auswählen.

Wie aus der Gegenüberstellung der Vorteile und Nachteile hervorgeht, ist der Einsatz eines Failover Clusters nur dann sinnvoll, wenn eine oder mehrere Applikationen sehr hohe Verfügbarkeitsanforderungen haben. Neben dem hohen Kostenaufwand sind sehr gute Kenntnisse des verantwortlichen Personals sowohl über die eingesetzten Betriebssysteme und Applikationen als auch über die Failover-Funktionalität erforderlich. Der Einsatz von Failover Lösungen für Server macht zudem nur dann Sinn, wenn auch alle Abhängigkeiten wie beispielsweise Netzanbindung oder Verfügbarkeit der Clients auch mit den entsprechenden Redundanzen ausgelegt sind.

Bereiche, für die typischerweise bei hohen Verfügbarkeitsanforderungen Failover Cluster eingesetzt werden, sind z. B.:

Ergänzende Kontrollfragen

- Welche Redundanzen sind für hochverfügbare Server vorhanden?
- Wird im Falle eines manuellen Umschwenken der Dieste oder Anwendungen sichergestellt, dass die Verfügbarkeitsanforderungen gewährleistet sind?
- Wie wird sichergestellt, dass ein Failover ausschließlich nur dann stattfindet, wenn es notwendig ist?

M 2.315 Planung des Servereinsatzes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Eine grundlegende Voraussetzung dafür, dass ein Server sicher betrieben werden kann ist ein angemessenes Maß an Planung im Vorfeld.

Die Planung für den Einsatz eines Servers kann in mehreren Schritten nach dem Prinzip des Top-Down-Entwurfs erfolgen: Ausgehend von einem Grobkonzept für das Gesamtsystem werden konkrete Planungen für Teilkomponenten in spezifische Teilkonzepten festgelegt. Die Planung betrifft dabei nicht nur Aspekte, die klassischerweise mit dem Begriff Sicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen.

Grobkonzept

Im Grobkonzept sollten beispielsweise folgende typische Fragestellungen behandelt werden:

- Welche Aufgaben soll das zu planende System erfüllen? Welche Dienste sollen von dem Server bereitgestellt werden? Gibt es besondere Anforderungen an die Verfügbarkeit des Systems oder an die Vertraulichkeit oder Integrität der gespeicherten oder verarbeiteten Daten?

  Diese Vorgaben kommen aus der übergreifenden Planung und werden von den allgemeinen Zielvorgaben bestimmt. Je genauer die Rahmenbedingungen bekannt und je präziser die Vorgaben formuliert sind, desto einfacher werden die folgenden Planungsschritte.

- Sollen in dem System bestimmte Hardwarekomponenten eingesetzt werden? Dies kann beispielsweise für die Auswahl des Betriebssystems wichtig sein.

- Welche Anforderungen an die Hardware (CPU, Arbeitsspeicher, Kapazität der Festplatten, Kapazität des Netzes etc.) ergeben sich aus den allgemeinen Anforderungen?

- Handelt es sich bei dem eingesetzten Netz um einen homogenen oder heterogenen Rechnerverbund?

- Ersetzt das System ein altes, vorhandenes? Sollen von dem alten System Datenbestände oder Hardwarekomponenten übernommen werden?

- Sollen auf dem Rechner weitere Betriebssysteme mittels Multiboot installiert werden?

Teilkonzepte

Die folgenden Teilkonzepte sollten bei der Planung des Servereinsatzes berücksichtigt werden:

- **Authentisierung und Benutzerverwaltung**: Welche Arten der Benutzerverwaltung und Benutzerauthentisierung sollen auf dem System genutzt werden? Werden Benutzer nur lokal verwaltet oder soll ein zentrales Verwaltungssystem genutzt werden? Soll das System auf einen zentralen, netzbasierten Authentisierungsdienst zugreifen, oder wird nur eine lokale Authentisierung benötigt? Mehr Informationen dazu finden sich in M 4.133 *Geeignete Auswahl von Authentikations-Mechanismen*.

- **Benutzer- und Gruppenkonzept**: Ausgehend vom organisationsweiten Benutzer-, Rechte- und Rollenkonzept müssen entsprechende Regelungen für das System erstellt werden (siehe auch M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile* und M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*).

- **Administration**: Wie soll das System administriert werden? Werden alle Einstellungen lokal vorgenommen oder der Server in ein zentrales Administrations- und Konfigurationsmanagement integriert?

- **Partitions- und Dateisystem-Layout**: In der Planungsphase sollte eine erste Abschätzung des benötigten Plattenplatzes durchgeführt werden. Zur einfacheren Administration und Wartung ist es empfehlenswert, so weit wie möglich eine Trennung von Betriebssystem (Systemprogramme und -konfiguration), Anwendungsprogrammen und -daten (beispielsweise Datenbank-Server und Daten) und gegebenenfalls Benutzerdaten vorzunehmen. Verschiedene Betriebssysteme bieten hierfür unterschiedliche Mechanismen an (Aufteilung in Laufwerke unter Windows, Filesysteme unter Unix). Oft kann es sinnvoll sein, bestimmte Daten sogar auf einer eigenen Festplatte oder einem eigenen Plattensystem zu speichern. Dies erlaubt es beispielsweise, bei einer Neuinstallation oder einem Update des Systems die Daten auf den anderen Partitionen ohne Umkopieren zu übernehmen.

  Trennung von Programmen, System- und Benutzerdaten

  Falls auf dem Server Daten mit hohem Schutzbedarf bezüglich der Vertraulichkeit gespeichert werden, so wird der Einsatz verschlüsselter Dateisysteme dringend empfohlen. Dabei brauchen nicht notwendigerweise alle Dateisysteme verschlüsselt zu werden, sondern es wird oft ausreichend sein, für den Teil des Dateisystems eine Verschlüsselung vorzusehen, auf dem die Daten selbst gespeichert werden. Dies wird durch eine entsprechende Planung des Partitions- und Dateisystemlayouts erleichtert. Bei der Auswahl einer Verschlüsselung von einzelen Dateien und Verzeichnissen sollte den Anwendern die Auswahl abgenommen werden, ob die Dateien verschlüsselt werden oder unverschlüsselt abgelegt werden.

  Bei hohem Schutzbedarf möglichst verschlüsselte Dateisysteme vorsehen

  In der Planungsphase sollte die vorgesehene Aufteilung der Partitionen und deren Größe dokumentiert werden.

- **Netzdienste und Netzanbindung**: In Abhängigkeit von den Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit der Daten, die auf dem Server gespeichert oder verarbeitet werden sollen, muss die Netzanbindung des Servers geplant werden.

  Generell wird empfohlen, einen Server nicht direkt im selben IP-Subnetz zu platzieren wie die Clients, die auf den Server zugreifen sollen. Wenn der Server zumindest durch einen Router von den Clients getrennt ist, dann bestehen wesentlich besser Möglichkeiten zur Steuerung des Zugriffs und zur Erkennung von Anomalien im Netzverkehr, die auf mögliche Probleme hindeuten.

  Ein Server, der Daten mit einem hohen Schutzbedarf bezüglich Vertraulichkeit oder Integrität speichert oder verarbeitet, sollte in einem eigenen IP-Subnetz angesiedelt werden und zumindest durch einen

  Bei besonderem Schutzbedarf eigenes Teilnetz und Paketfilter

Paketfilter vom Rest des Netzes getrennt werden. Bei einem sehr hohen Schutzbedarf sollte ein Application Level Gateway eingesetzt werden.

Bei normalem Schutzbedarf kann ein Server, der ausschließlich von Clients aus dem internen Netz genutzt wird, ausnahmsweise auch im selben Teilnetz angesiedelt werden. Es wird jedoch empfohlen, auch in diesem Fall den Server bei anstehenden Umstellungen in der Netzstruktur in ein eigenes Teilnetz zu verlegen.

Abhängigkeiten berücksichtigen

Abhängig vom festgelegten Einsatzzweck des Rechners wird außerdem eventuell der Zugriff auf bestimmte Dienste im Netz (etwa Web-, File-, Datenbank-, Druck-, DNS oder Mailserver) benötigt. Dies muss bereits im Rahmen der Planung berücksichtigt werden, damit nicht zu einem späteren Zeitpunkt Schwierigkeiten beispielsweise durch zu geringe Übertragungskapazitäten oder Probleme mit zwischengeschalteten Sicherheitsgateways entstehen.

Zusätzliche Dienste zur Administration etc.

Neben dem eigentlichen Dienst, für den ein Server aufgesetzt wird, werden oft noch andere Dienste benötigt, um den Server effizient nutzen und administrieren zu können. Beispielsweise wird für eine Administration über das Netz ein sicherer Zugang (beispielsweise SSH, siehe auch M 5.64 *Secure Shell*) benötigt, oder die Dateien für ein Webangebot können über das Netz auf den Webserver übertragen werden. Wenn die dadurch entstehende Netzkommunikation über unsichere Netze stattfindet, so müssen geeignete sichere Protokolle benutzt werden. Außerdem dürfen die Dienste nur autorisierten Benutzern und Rechnern zur Verfügung gestellt werden. Dies kann durch eine Passwortvergabe, durch den Einsatz eines Paketfilters (siehe beispielsweise M 4.238 *Einsatz eines lokalen Paketfilters* oder Baustein B 3.301 *Sicherheitsgateway (Firewall)*) oder anderer Mechanismen realisiert werden. Kein Dienst sollte in einem unsicheren Netz wie dem Internet bereitgestellt werden, wenn dies nicht ausdrücklich vorgesehen ist.

Übersicht über Netzdienste und Netzverbindungen erstellen

In der Planungsphase sollte eine Übersicht über die vorgesehenen und benötigten Netzdienste sowie über die in diesem Zusammenhang nötigen Netzverbindungen erstellt werden. Allgemein ist es wichtig, bereits in der Planungsphase zu überlegen, wie groß die Abhängigkeit eines Systems vom Funktionieren der Netzanbindung sein darf.

- **Tunnel oder VPN**: Falls bereits in der Planungsphase absehbar ist, dass auf das System über unsichere Netze zugegriffen werden muss, sollten frühzeitig geeignete Lösungen untersucht werden. Beispielsweise kann der Zugriff über ein VPN erfolgen.
- **Monitoring**: Um die Verfügbarkeit und Auslastung des Systems und der angebotenen Dienste zu beobachten, kann ein Monitoring-System eingesetzt werden. Dafür wird auf einem weiterem Server ein Monitoring-Daemon installiert, dem ein lokal installierter Agent die zu überwachenden Daten sendet. Im weiterem besteht die Möglichkeit, die Aktivitäten von Netzdiensten, die von externen Systemen angeboten werden, zu überwachen. Bei Problemen kann zum Beispiel automatisch ein Administrator alarmiert werden.

- **Protokollierung**: Die Protokollierung von Meldungen des Systems und der eingesetzten Dienste spielt eine wichtige Rolle, beispielsweise bei der Diagnose und Behebung von Störungen oder bei der Erkennung und Aufklärung von Angriffen. In der Planungsphase sollte entschieden werden, welche Informationen mindestens protokolliert werden sollen, und wie lange die Protokolldaten aufbewahrt werden sollen. Außerdem muss festgelegt werden, ob die Protokolldaten lokal auf dem System oder auf einem zentralen Logserver im Netz gespeichert werden sollen.

  Sinnvoller Weise sollte bereits in der Planungsphase festgelegt werden, wie und zu welchen Zeitpunkten Daten ausgewerten werden sollen.

Auch an die Auswertung der Logdateien denken

- **Hochverfügbarkeit**: Falls an die Verfügbarkeit des Systems und seiner Dienste besondere Anforderungen gestellt werden, so sollte bereits in der Planungsphase überlegt werden, wie diese Anforderungen erfüllt werden können (siehe auch M 6.43 *Einsatz redundanter Windows NT/2000 Server*).

Alle Entscheidungen, die in der Planungsphase getroffen wurden, müssen so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Dabei ist zu beachten, dass meist andere Personen neben dem Autor diese Informationen auswerten müssen. Daher ist auf passende Strukturierung und Verständlichkeit zu achten.

Ergänzende Kontrollfragen:

- Welche Dokumentation existiert über die Planung des Servers?

M 2.316 Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement, Administrator

Die Sicherheitsvorgaben für jeden Server ergeben sich aus der organisationsweiten Sicherheitsrichtlinie. Ausgehend von der allgemeinen Richtlinie müssen die Anforderungen für den gegebenen Kontext konkretisiert werden und in einer Sicherheitsrichtlinie für den Server oder eine Gruppe von Servern zusammengefasst werden. In diesem Zusammenhang ist zu prüfen, ob neben der organisationsweiten Sicherheitsleitlinie weitere übergeordnete Vorgaben wie IT-Richtlinien, Passwortrichtlinien oder Vorgaben zur Internetnutzung zu berücksichtigen sind.

Die Sicherheitsrichtlinie muss allen Personen und Gruppen, die an der Beschaffung und dem Betrieb der Server beteiligt sind, bekannt sein und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die Sicherheitsrichtlinie sollte das generell zu erreichende Sicherheitsniveau spezifizieren und grundlegende Festlegungen zum Betrieb des Servers treffen. Zur Verbesserung der Übersichtlichkeit kann es sinnvoll sein, für verschiedene Einsatzgebiete gesonderte Sicherheitsrichtlinien zu entwickeln.

Allgemeine Strategie: Liberal oder Restiktiv?

Als erstes sollte die allgemeine Konfigurations- und Administrationsstrategie ("Liberal" oder "Restriktiv") festgelegt werden, da die weiteren Entscheidungen von dieser Festlegung wesentlich abhängen.

Für Server, die lediglich Daten mit normalem Schutzbedarf speichern und verarbeiten, kann eine relativ liberale Strategie gewählt werden, was in vielen Fällen die Konfiguration und Administration vereinfacht. Generell ist es aber auch in diesen Fällen empfehlenswert, die Strategie nur "so liberal wie nötig" auszulegen.

Bei einem Server, auf dem Daten mit hohem Schutzbedarf gespeichert oder verarbeitet werden, wird grundsätzlich eine restriktive Strategie empfohlen. Für Server mit besonderem Schutzbedarf bezüglich eines der drei Grundwerte sollte unbedingt eine restriktive Konfigurations- und Administrationsstrategie umgesetzt werden.

Nachfolgend sind einige Punkte aufgeführt, die berücksichtigt werden sollten:

- Regelungen zur physikalischen Zugriffskontrolle: Ein Server sollte grundsätzlich in einem abschließbaren Rechnerraum oder Serverschrank aufgestellt oder eingebaut werden. Dabei ist zu regeln, wer Zutritt zu dem Raum beziehungsweise Zugriff auf den Server selbst erhält.
- Regelungen für die Arbeit der Administratoren und Revisoren:
  - Nach welchem Schema werden Administrationsrechte vergeben? Welcher Administrator darf welche Rechte ausüben und wie erlangt er diese Rechte?

  - Über welche Zugangswege dürfen Administratoren und Revisoren auf die Syteme zugreifen (beispielsweise nur lokal an der Konsole, über ein eigenes Administrationsnetz oder über verschlüsselte Verbindungen)?
  - Welche Vorgänge müssen dokumentiert werden? In welcher Form wird die Dokumentation erstellt und gepflegt?
  - Gilt für bestimmte Änderungen ein Vier-Augen-Prinzip?
- Vorgaben für die Installation und Grundkonfiguration
  - Welche Installationsmedien werden zur Installation verwendet?
  - Soll ein zentraler Authentisierungsdienst genutzt werden oder erfolgt die Benutzerverwaltung und -authentisierung nur lokal?
  - Regelungen zur Benutzer- und Rollenverwaltung, Berechtigungsstrukturen (Ablauf und Methoden der Authentisierung und Autorisierung, Berechtigung zu Installation, Update, Konfigurationsänderungen etc.). Nach Möglichkeit sollte ein Rollenkonzept für die Administration erarbeitet werden.
  - Vorgaben für die zu installierenden Softwarepakete.
  - Falls bei der Planung für den Server festgelegt wurde, dass Teile des Dateisystems verschlüsselt werden sollen, so ist es empfehlenswert, an dieser Stelle festzulegen, wie dies zu geschehen hat:
    - Welche Teile des Dateisystems sollen verschlüsselt werden?
    - Welcher Mechanismus zur Einbindung des verschlüsselten Dateisystems soll verwendet werden?
    - Welche Kryptoalgorithmen und Schlüssellängen sollen verwendet werden?
    - Welche Daten sollen in den verschlüsselten Dateisystemen gespeichert werden?
    - Wie werden die verschlüsselten Dateisysteme in das Backup einbezogen?

    Besondere Sorgfalt bei verschlüsselten Dateisystemen

    Es empfiehlt sich, beim Einsatz verschlüsselter Dateisysteme hierfür ein eigenes Konzept zu erstellen und die Details der Konfiguration besonders sorgfältig zu dokumentieren, da im Fall von Problemen (Verlust des Schlüssels oder der Passphrase zum Schlüssel, inkorrekte Konfiguration oder ähnliches) die Daten auf den verschlüsselten Dateisystemen sonst vollständig verloren sein können.
  - Regelungen zu Erstellung und Pflege von Dokumentation
- Vorgaben für den sicheren Betrieb
  - Welcher Benutzerkreis darf sich lokal auf dem System anmelden?
  - Welche Benutzer erhalten Zugriff über das Netz? Welche Protokolle dürfen verwendet werden?

  - Auf welche Ressourcen dürfen die Benutzer zugreifen?
  - Vorgaben für die Passwortnutzung (Passwortregeln, Regeln und Situationen für Passwortänderungen, gegebenenfalls Hinterlegung von Passwörtern)
  - Wer darf das System herunterfahren?
- Netzkommunikation und -dienste
  - Soll ein lokaler Paketfilter aufgesetzt werden?
  - Welche Netzdienste werden von dem Server angeboten?
  - Welche Authentisierungsverfahren sollen für die angebotenen Dienste gewählt werden?
  - Auf welche externen Netzdienste soll von dem Rechner aus zugegriffen werden können?
  - Soll ein verteiltes Dateisystem eingebunden werden?

  Verteilte Dateisysteme, bei denen die Nutzdaten unverschlüsselt übertragen werden, sollten nur im internen Netz verwendet werden. Soll ein verteiltes Dateisystem über ein unsicheres Netz hinweg genutzt werden, so muss es durch zusätzliche Maßnahmen (kryptographisch geschütztes VPN, Tunneling) gesichert werden.

Vorsicht bei Nutzung von verteilten Dateisystemen

- Protokollierung
  - Welche Ereignisse werden protokolliert?
  - Wo werden die Protokolldateien gespeichert? Werden sie lokal gespeichert oder soll ein zentraler Server eingesetzt werden, an dem die einzelnen Systeme im Netz ihre Protokollierungsinformationen schicken?
  - Wie und in welchen Abständen werden die Protokolle ausgewertet?
  - Wer hat Zugriff auf die Logdateien?
  - Ist gewährleistet, dass personenbezogene Informationen nicht an unbefugte Personen gelangen?
  - Wie lange sollen die Logdateien gespeichert werden?

Anhand der oben genannten Punkte kann eine Checkliste erstellt werden, die bei Audits oder Revisionen hilfreich sein kann.

Die Verantwortung für die Sicherheitsrichtlinie liegt beim IT-Sicherheitsmanagement, Änderungen und Abweichungen hiervon dürfen nur in Abstimmung mit dem IT-Sicherheitsmanagement erfolgen.

Bei der Erstellung einer Sicherheitsrichtlinie ist es empfehlenswert, so vorzugehen, dass zunächst ein Maximum an Forderungen und Vorgaben für die Sicherheit der Systeme aufgestellt wird. Diese können anschließend den tatsächlichen Gegebenheiten angepasst werden. Idealerweise wird so erreicht, dass alle notwendigen Aspekte berücksichtigt werden. Für jede im zweiten Schritt verworfene oder abgeschwächte Vorgabe sollte der Grund für die Nicht-Berücksichtigung dokumentiert werden.

Ergänzende Kontrollfragen:

- Wurde eine Sicherheitsrichtlinie für den Betrieb des Servers erstellt?
- In welcher Form wurde die Dokumentation der Sicherheitsrichtlinie vorgenommen?
- Wann wurde die Sicherheitsrichtlinie zum letzten Mal aktualisiert?
- Wurde ein Sicherheitsniveau in der Sicherheitsrichtlinie definiert?

M 2.317 Beschaffungskriterien für einen Server

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsbeauftragter

Verantwortlich für Umsetzung: Beschaffer

Die Beschaffung eines Servers betrifft sowohl die Hard- als auch die Software, aus der der Server aufgebaut werden soll. Werden bei der Beschaffung eines Servers Fehler gemacht, so kann dies schwerwiegende Folgen auf den sicheren Betrieb eines Netzes haben, da mit ungeeigneter Hard- und Software das angestrebte Sicherheitsniveau unter Umständen nur schwer erreichbar ist.

Bevor ein Server beschafft wird, muss daher eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Aufgrund der Bewertung kann dann eine fundierte Kaufentscheidung erfolgen, die sicherstellt, dass der Server im praktischen Betrieb den Anforderungen genügt.

Auch rein funktionale Merkmale von Servern können Auswirkungen auf die IT-Sicherheit haben. Meist ist dann der Grundwert Verfügbarkeit betroffen, beispielsweise wenn ein Server wegen unzureichender Speicherausstattung nicht die geforderten Antwortzeiten oder Durchsatzraten erreicht. Außerdem spielt die Unterstützung durch den Hersteller eine nicht zu vernachlässigende Rolle, wenn es beispielsweise darum geht, dass zeitnah Patches für Sicherheitslücken zur Verfügung gestellt werden.

Zentrale Sicherheitsanforderungen

Aus dem Blickwinkel der IT-Sicherheit sind zentrale Anforderungen an Server, dass

- Hard- und Software so ausgelegt sind, dass die Anforderungen an die Verfügbarkeit des Servers und die Integrität der Daten erfüllt werden können,
- die Administration über sichere Protokolle möglich ist,
- die Benutzerverwaltung es erlaubt, das organisationsweite Rollenkonzept entsprechend umzusetzen, und
- dass es gegebenenfalls möglich ist, besonders sensitive Daten zu verschlüsseln.

Nachfolgend werden einige Anforderungen aufgelistet, die bei der Beschaffung von Servern berücksichtigt werden sollten:

1. Grundlegende funktionale Anforderungen
   - Unterstützt das Gerät alle benötigten Hardwareschnittstellen?
   - Unterstützt die Software alle benötigten Protokolle und Datenformate?
2. Sicherheit
   - Unterstützt das System sichere Protokolle zur Administration?

   Wenn Server nicht über ein eigenes Administrationsnetz administriert werden, muss die Administration mit Hilfe von sicheren Netzprotokollen möglich sein.

3. Wartbarkeit

   - Bietet der Hersteller regelmäßige Updates und schnell verfügbare Sicherheitspatches für die Software an?

   Es ist insbesondere wichtig, dass der Hersteller zeitnah auf bekannt gewordene Sicherheitsmängel reagiert.

   - Wird für das Produkt die Möglichkeit des Abschlusses von Wartungsverträgen angeboten?

   Oft ist der Zugriff auf Updates und Unterstützungsleistungen vom Hersteller nur in Verbindung mit einem gültigen Wartungsvertrag möglich.

   - Können im Rahmen der Wartungsverträge maximale Reaktionszeiten für die Problembehebung festgelegt werden?

   Ein Wartungsvertrag ist nur dann geeignet, wenn mit den garantierten Reaktions- und Wiederinbetriebnahmezeiten die festgelegten Ansprüche an die Verfügbarkeit der Geräte abgedeckt werden können.

   - Bietet der Hersteller einen technischen Kundendienst (Hotline) an, der in der Lage ist, sofort bei Problemen zu helfen?

   Dieser Punkt sollte Bestandteil des abgeschlossenen Wartungsvertrags sein. Beim Abschluss des Vertrags ist auf die Sprache der zur Verfügung gestellten Hotline des Herstellers zu achten.

4. Zuverlässigkeit/Ausfallsicherheit

   - Gibt es verlässliche Informationen zur Zuverlässigkeit und Ausfallsicherheit von Hard- und Software?
   - Bietet der Hersteller gegebenenfalls Hochverfügbarkeitslösungen an?

   Wenn die Verfügbarkeitsanforderungen nicht über Wartungsverträge abgedeckt werden können, sollte das System Hochverfügbarkeitslösungen unterstützen.

5. Benutzerfreundlichkeit

   - Lässt sich das Produkt einfach installieren, konfigurieren, administrieren und benutzen?

   Es sollten darüber hinaus Schulungen für das Produkt angeboten werden.

6. Kosten

   - Wie hoch sind die Anschaffungskosten für Hard- und Software?
   - Wie hoch sind die voraussichtlichen laufenden Kosten (Wartung, Betrieb, Support)?

   Diese Kosten müssen bereits in der Beschaffungsphase mit berücksichtigt werden. Der Inhalt der Wartungs- und Supportverträge sollte geprüft werden (Reaktionszeiten, Hotline, Qualifikation des Personals, etc.).

   - Wie hoch sind die voraussichtlichen laufenden Kosten für das Personal?

- Müssen zusätzliche Soft- oder Hardware-Komponenten angeschafft werden?

Diese Frage sollte bereits in der Planungsphase beantwortet werden. Wenn beispielsweise bereits ein Netz-Management-System im Einsatz ist, sollte die Kompatibilität mit den zu beschaffenden Geräten geprüft werden.

Zudem sollte der Aufwand zur Integration in eine bestehende Infrastruktur beachtet werden.

- Wie hoch sind die Kosten für die Schulung von Administratoren?
- Mit welchen Kosten muss gerechnet werden, wenn wegen erhöhter Kapazitätsanforderungen ein Upgrade der Hardware notwendig ist?

Die Kosten können in diesem Fall erheblich höher ausfallen, als die Kosten für die Hardware selbst, da in etlichen Lizenzmodellen von Softwareanbietern der Lizenzpreis von der Anzahl der Prozessoren oder dem Prozessortakt abhängt, so dass bei einem Hardwareupgrade auch gleichzeitig eine neue Programmlizenz erforderlich sein kann.

7. Protokollierung

- Welche Möglichkeiten der Protokollierung sind vorhanden?

Die angebotenen Möglichkeiten zur Protokollierung müssen mindestens die in der Sicherheitsrichtlinie festgelegten Anforderungen erfüllen. Insbesondere sind die folgenden Punkte relevant:

- Ist der Detailgrad der Protokollierung konfigurierbar?
- Werden durch die Protokollierung alle relevanten Daten erfasst?
- Unterstützt das System zentrale Protokollierung (z. B. syslog)?
- Kann die Protokollierung so erfolgen, dass die Bestimmungen des Datenschutzes erfüllt werden können?
- Werden Alarmierungsfunktionen unterstützt?

8. Infrastruktur

- Abmessungen und Kompatibilität mit Schutzschränken

Auch der Platzbedarf eines Servers ist bei der Beschaffung zu berücksichtigen. Kann das Gerät in die vorgesehenen Schutzschränke eingebaut werden (Formfaktor, Gewicht, Befestigungselemente)?

- Stromversorgung und Abwärme

Vom Hersteller sollten Angaben zum Stromverbrauch und zu den Anforderungen an die Umgebungstemperatur verfügbar sein. Reicht die vorhandene Kapazität der Stromversorgung und der USV aus? Reicht die vorhandene Kühlleistung zur Abfuhr der Abwärme des Geräts aus?

Die Anforderungen und die auf ihrer Basis getroffenen Auswahlentscheidungen sollten so dokumentiert werden, dass zu einem späteren Zeitpunkt nachvollziehbar ist, wie die Entscheidung zu Stande gekommen ist.

Ergänzende Kontrollfragen:

- Sind die Anforderungen an den Server dokumentiert?

M 2.318 Sichere Installation eines Servers

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Nachdem die Planung des Servers (siehe M 2.315 *Planung des Servereinsatzes*) abgeschlossen und eine Sicherheitsrichtlinie (siehe M 2.316 *Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server*) erstellt wurde, kann mit der Installation des Systems begonnen werden.

Installationskonzept

Es ist empfehlenswert, zunächst ein kurzes Installationskonzept entsprechend den funktionalen Anforderungen aus der Planung und den Vorgaben der Sicherheitsrichtlinie zu erstellen. Prinzipiell ist es vorteilhaft, die Installation in zwei Phasen vorzunehmen: Zunächst wird ein Grundsystem installiert und konfiguriert, anschließend werden die weiteren benötigten Dienste und Anwendungen eingerichtet. Die Installationsprogramme der meisten Betriebssysteme unterstützen diese Vorgehensweise mehr oder weniger gut.

Referenz-System

Die beschriebenen Schritte brauchen nicht notwendigerweise alle für jeden Server erneut durchgeführt zu werden. Dies könnte sogar insofern kontraproduktiv sein, als die ständige Wiederholung die Gefahr von Fehlern erhöht. Es wird daher empfohlen, die beschriebenen Schritte einmal besonders sorgfältig auf einem Referenz-System durchzuführen, die nötigen Konfigurationen genau zu dokumentieren und so ein angepasstes Installationskonzept für das betreffende Betriebssystem zu erhalten. Dabei muss beachtet werden, dass dieses Installationskonzept auch bei Änderungen am Betriebssystem, die kein komplett neues Release darstellen (Service-Packs, Update-Releases oder ähnliches) überprüft und gegebenenfalls angepasst werden muss.

Installation

Diese Maßnahme beinhaltet nur Empfehlungen für die ersten Schritte einer Installation und nicht für die endgültige Konfiguration für den geplanten Einsatzzweck. Die weitergehenden Konfigurationsschritte sind sehr stark vom jeweiligen System und Einsatzgebiet abhängig und werden in eigenen Maßnahmen behandelt.

Dokumentation

Während der Installation und der späteren Konfiguration sollten zumindest die wichtigen Schritte so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Beispielsweise kann eine Installations-Checkliste erstellt werden, auf der beendete Schritte abgehakt und vorgenommene Einstellungen vermerkt werden können. Eine entsprechende Dokumentation ist für eine Fehleranalyse oder spätere Neuinstallation hilfreich. Dabei sollte beachtet werden, dass neben dem Autor auch weitere, auf diesem Gebiet eventuell weniger spezialisierte, Administratoren auf die Dokumentation zurückgreifen müssen. Daher ist es wichtig, dass die Dokumenation gut strukturiert und verständlich ist.

Offline-Installation

Die Installation und Grundkonfiguration sollte möglichst "offline" oder zumindest in einem sicheren Netz (Installations- oder Administrationsnetz) erfolgen. Dies ist wichtig, weil während der Installation meist noch keine Passwörter vergeben wurden und keine Schutzmechanismen aktiv, aber eventuell schon Zugriffe möglich sind. Falls die Installation teilweise über das

Netz erfolgen soll (beispielsweise Nachladen von Paketen), so sollte wenn möglich ein Installationsserver im Administrationsnetz genutzt werden.

Verwendung sicherer Informationsquellen

Insbesondere beim Betriebssystem selbst ist es wichtig, dass die installierte Version aus einer vertrauenswürdigen Quelle stammt. Dies ist besonders wichtig, wenn beispielsweise CD-Images aus dem Internet heruntergeladen wurden. In diesem Fall sollte unbedingt geprüft werden, ob digitale Signaturen der Pakete verfügbar sind, die zur Verifikation von Integrität und Authentizität der Pakete verwendet werden können (siehe auch M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*). Pakete und CD-Images, für die keine digitalen Signaturen oder wenigstens Prüfsummen existieren, sollten möglichst nicht eingesetzt werden.

Partitionierung und Filesystemlayout

Bei der Einrichtung der Festplattenpartitionen muss das in der Planungsphase (siehe M 2.315 *Planung des Servereinsatzes*) erstellte Konzept umgesetzt werden. Wenn ein verschlüsseltes Dateisystem eingesetzt werden soll, so muss es meist initialisiert werden, bevor Daten hineinkopiert werden können, denn oft lässt sich ein Dateisystem nicht im Nachhinein verschlüsseln. Auch einige Raid-Systeme und -Level erfordern eine Konfiguration, die abgeschlossen sein muss, bevor die betreffenden Dateisysteme eingerichtet werden können.

Einrichtung der Hardware und des Bootloaders

Während der ersten Installationsphase braucht prinzipiell nur derjenige Teil der Hardware konfiguriert zu werden, der für das Booten des Systems (beispielsweise RAID-Laufwerke, verschlüsselte Dateisysteme oder ähnliches) und die Fortführung der Installation (gegebenenfalls Netzwerkkarten) benötigt wird. Die restliche Hardware kann in der zweiten Phase der Installation eingerichtet werden.

Am Ende der Grundinstallation steht meist die Installation und Konfiguration eines Bootloaders, der dafür sorgt, dass beim Starten des Systems das Betriebssystem geladen wird. Meist bietet der Bootloader ein Auswahlmenü, das die Auswahl zwischen verschiedenen installierten Betriebssystemen oder Konfigurationen erlaubt. Bei der Konfiguration des Bootloaders muss mit entsprechender Sorgfalt vorgegangen werden, damit das System überhaupt starten kann. Die vorgenommene Konfiguration sollte dokumentiert werden. Manche Systeme bieten zu diesem Zeitpunkt der Installation auch die Möglichkeit, eine Bootdiskette zu erstellen, mit der das System im Notfall gestartet werden kann.

Bei Systemen, die nicht physisch gegen unautorisierten Zugriff geschützt sind, sollte der Bootloader nach Möglichkeit mit einem Passwort abgesichert werden.

Protokollierung früh aktivieren

Sofern dies nicht bereits automatisch geschehen ist, sollte spätestens beim Abschluss der Grundinstallation auch die Protokollierung der Systemereignisse aktiviert werden. Die Protokolldaten können bei Problemen bei der weiteren Installation und Konfiguration wertvolle Informationen liefern.

Aktualisierung

Aktualisierung der Pakete

Wird das System von einer CD, DVD oder einem anderen "Offline-Medium" installiert, so sollte nach der Grundinstallation überprüft werden, ob zwischenzeitlich Aktualisierungen oder Sicherheitspatches vom Hersteller oder Distributor veröffentlicht wurden (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems* und M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*).

Installation des jeweiligen Serverprogramms

Nachdem das Betriebssystem installiert wurde und die Grundkonfiguration und Aktualisierung abgeschlossen sind, können die jeweiligen Serverprogramme installiert und konfiguriert werden. Hierfür wird ein analoges Vorgehen wie für das Betriebssystem selbst empfohlen.

Ergänzende Kontrollfragen:

- Wurde ein Installationskonzept erstellt?
- Wird ein Bootloader eingesetzt? Falls ja, welcher?
- Wurden die Pakete nach der Installation aktualisiert?

M 2.319 Migration eines Servers

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Sollen die Dienste des Servers von einem anderen System übernommen werden, so muss der Übergang geplant werden. Insbesondere dann, wenn besondere Anforderungen an die Verfügbarkeit der Dienste bestehen, ist eine besonders sorgfältige Planung erforderlich.

In den meisten Fällen ist es empfehlenswert, den "Funktionsübergang" auf das Ersatzsystem außerhalb der normalen Betriebszeiten durchzuführen. Falls dies nicht möglich ist müssen Maßnahmen getroffen werden, die sicher stellen, dass weder Daten beim Funktionsübergang verloren gehen, noch untragbare Ausfallzeiten entstehen.

Für die Migration wichtiger Server muss deswegen vorab ein entsprechendes Migrationskonzept erstellt werden. Dabei sollten insbesondere folgende Punkte mit berücksichtigt werden:

- Migration der Daten und Konfiguration

  Nach der Übertragung der Daten auf das neue System muss überprüft werden, ob die Daten vollständig und korrekt übertragen wurden.

  Vorsicht bei Versionsänderungen

  Wenn auf dem neuen System eine neue Version der Serversoftware eingesetzt werden soll, so muss sichergestellt sein, dass die neue Version mit den vorhandenen Datenbeständen korrekt umgehen kann. Dies betrifft nicht nur die Aufgabe, Daten der alten Version korrekt einzulesen, sondern insbesondere auch, diese Daten zu modifizieren oder neue Datensätze hinzuzufügen. Gerade in solchen Fällen tauchen oft Probleme auf, so dass gründliche Tests empfohlen werden.

  Außerdem ist es wichtig, dass die Konfiguration des alten Dienstes auf dem neuen System korrekt übernommen oder zumindest "funktional äquivalent nachgebaut" werden kann.

- Kompatibilität des Dienstes

  Es muss sichergestellt sein, dass der Dienst auf dem Ersatzsystem mit dem ursprünglichen Dienst kompatibel ist. Dies ist insbesondere dann von Bedeutung, wenn im Rahmen der Migration auf dem neuen System eine neue Version des Serverprogramms eingesetzt werden soll, auf die jedoch weiter mit Clients der alten Version zugegriffen wird. Selbst dann, wenn ein Hersteller Berichte von Referenzkunden über erfolgreiche Migrationen vorlegt oder "problemlose Abwärtskompatibilität", "vollständige Rückwärtskompatibilität mit früheren Versionen" oder ähnliches zusichert, wird dingend empfohlen, vorab entsprechende Tests durchzuführen.

- Kryptographische Schlüssel

  Achtung bei Verschlüsselung

  Falls Teile der Daten oder der Dateisysteme eines Servers verschlüsselt sind, so kommt der Sicherung oder Übertragung der entsprechenden Schlüssel besondere Bedeutung zu: Oft sind diese an einer anderen Stelle auf dem System gespeichert als die Nutzdaten selbst. Beispielsweise dann, wenn die Daten mit Hilfe systemnaher Programme blockweise direkt

kopiert werden oder die Festplatten aus dem alten in das neue System umgebaut werden, muss sichergestellt sein, dass auch die Schlüssel mit übertragen werden, da sonst kein Zugriff mehr auf die verschlüsselten Daten möglich ist.

- Umstellung von Namen und Adressen

  Adressänderungen

  Falls auf einen Server nur über seine IP-Adresse oder einen DNS-Namen zugegriffen wird, so ist eine Migration meist relativ unproblematisch, da in diesem Fall einfach das Ersatzsystem die IP-Adresse des alten Systems übernehmen kann. Problematischer wird es beispielsweise, wenn das neue System den selben DNS-Namen bekommen soll, aber nicht die IP-Adresse übernehmen kann. Denn es dauert eine gewisse Zeit, bis die Änderung der Adresse bei allen Clients "angekommen" ist. Solche Latenzzeiten müssen bei der Planung der Migration berücksichtigt werden.

  Falls auf das System anders zugegriffen wird (beispielsweise wenn die Adresse von einem anderen Verzeichnisdienst aufgelöst wird), so muss berücksichtigt werden, dass auch die Änderung auf diesem Weg eventuell ebenfalls eine gewisse Latenzzeit hat, bevor sie wirksam wird.

  Das größte Problem entsteht dann, wenn Clients auf den Servern über eine Anwendung zugreifen, bei der die IP-Adresse oder der Name des Servers in einer lokalen Konfigurationsdatei oder -datenbank gespeichert sind. Falls eine größere Anzahl Clients manuell umkonfiguriert werden müssen, so kann dies eine erhebliche Zeit in Anspruch nehmen und muss vorab geplant werden.

- Dauerhafte Verbindungen

  Falls es Clients gibt, die länger bestehende oder gar dauerhafte Netzverbindungen zu dem Dienst aufbauen, der auf einen neuen Rechner migriert werden muss (dies ist beispielsweise bei manchen Datenbankanwendungen er Fall), so muss dies bei der Migration berücksichtigt werden. Gegebenenfalls müssen diese Verbindungen auf den betreffenden Clients manuell beendet werden. Auch hierfür ist eine entsprechende Planung erforderlich.

Für die Durchführung der Migration ist es empfehlenswert, im Rahmen der Erarbeitung des Migrationskonzeptes eine Checkliste zu erstellen, die bei der Umstellung Schritt für Schritt durchgegangen werden kann. Bei der Planung der Migration und der Erstellung der Checkliste muss darauf geachtet werden, dass jeder Schritt nur von den vorhergehenden Schritten abhängig ist.

Bei hohen Anforderungen an die Verfügbarkeit des Dienstes sollte der gesamte Übergang vorab in einer Testumgebung unter möglichst realistischen Bedingungen geprobt werden, um mögliche Probleme frühzeitig zu identifizieren und zu beseitigen.

Ergänzende Kontrollfragen:

- Wurde ein Migrationskonzept erstellt?

M 2.320 Geregelte Außerbetriebnahme eines Servers

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Soll ein Server außer Betrieb genommen werden, so darf dies nicht unvorbereitet und ohne Ankündigung für die Benutzer geschehen, sondern es muss eine Reihe von Maßnahmen ergriffen werden, um sicher zu stellen, dass

- keine wichtigen Daten verloren gehen,
- keine Dienste oder Systeme beeinträchtigt werden, die von dem Server abhängen, und dass
- keine sensitiven Daten auf den Datenträgern des Servers zurück bleiben.

Dazu ist es insbesondere wichtig, einen Überblick darüber zu haben, welche Daten wo auf dem System gespeichert sind und von wo aus darauf zugegriffen wird. Ausgehend von diesen Informationen sollte eine Planung für die Außerbetriebnahme des Servers erfolgen. Dabei sollten die folgenden Punkte berücksichtigt werden:

- Datensicherung

  Vor der Außerbetriebnahme des Servers müssen Daten, die noch benötigt werden, entweder extern gesichert bzw. archiviert (beispielsweise auf Magnetbändern, CD- oder DVD-ROMs) oder auf ein Ersatzsystem übertragen werden. Nach der Sicherung sollte überprüft werden, dass wirklich alle Daten korrekt gesichert wurden. Weitere Informationen zu diesem Themenkomplex finden sich in den Bausteinen B 1.4 *Datensicherungskonzept* und B 1.12 *Archivierung*.

- Ersatzsystem

  Wenn die von dem Server bereitgestellten Dienste weiter benötigt werden, so muss rechtzeitig ein angemessenes Ersatzsystem bereitgestellt werden. Für die entsprechende Planung, Beschaffung und Inbetriebnahme müssen entsprechende Ressourcen zur Verfügung stehen, siehe auch M 2.319 *Migration eines Servers*.

- Information der Benutzer

  Falls das System ersatzlos abgeschaltet wird, so müssen die Benutzer rechtzeitig über die bevorstehende Abschaltung informiert werden und gegebenenfalls die Gelegenheit erhalten, eigene Daten zu sichern.

- Entfernen von Verweisen auf das System

  Im Zuge der Außerbetriebnahme eines Systems müssen auch Verweise auf das System gelöscht werden. Dazu gehört beispielsweise das Löschen des DNS-Eintrags und der Einträge in sonstigen Verzeichnisdiensten sowie in Abhängigkeit vom Einsatzzweck weitere Verweise. Wird beispielsweise ein Webserver außer Betrieb genommen, so sollten Verweise auf diesen Server, die noch in eigenen Webseiten enthalten sind, gelöscht werden.

Sicheres Löschen von Daten

- Löschen der Daten auf dem abzuschaltenden System

  Es muss sichergestellt werden, dass keine schützenswerten Informationen mehr auf den Festplatten vorhanden sind. Dazu genügt es nicht, die Platten einfach neu zu formatieren, sondern sie müssen mindestens einmal vollständig überschrieben werden. Es ist zu beachten, dass weder das logische Löschen mit den Löschfunktionen des Betriebssystems noch das Neuformatieren der Platten die Daten tatsächlich von den Festplatten entfernt. Mit geeigneter Software können Daten in solchen Fällen, oft sogar ohne großen Aufwand, wieder rekonstruiert werden. Weitere Hinweise finden sich in M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* und in M 2.167 *Sicheres Löschen von Datenträgern*.

- Löschen von Datensicherungsmedien

  Nach der Außerbetriebnahme eines Systems müssen gegebenenfalls auch die entsprechenden Datensicherungsmedien gelöscht oder unbrauchbar gemacht werden, wenn die darauf gespeicherten Daten nicht mehr benötigt werden.

- Entfernen sonstiger Informationen

  Oft enthalten Serversysteme weitere Daten (beispielsweise Konfigurationsdaten), die in einem nichtflüchtigen Speicher abgelegt sind, oder sind von außen beschriftet (beispielsweise mit dem Rechnernamen, der IP-Adresse und weiteren technischen Informationen). Diese Informationen sollten nach Möglichkeit vor der Weitergabe des Gerätes entfernt werden, da ein Angreifer auch aus solchen Informationen eventuell Hinweise für mögliche Angriffe ziehen kann.

Es wird empfohlen, anhand der oben gegebenen Empfehlungen eine Checkliste zu erstellen, die bei der Außerbetriebnahme eines Systems abgearbeitet werden kann. Auf diese Weise kann vermieden werden, dass einzelne Schritte vergessen werden.

Ergänzende Kontrollfragen:

- Wie wird bei der Außerbetriebnahme eines Systems vorgegangen?

M 2.321 Planung des Einsatzes von Client-Server-Netzen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Eine grundlegende Voraussetzung dafür, dass Clients sicher betrieben werden können, ist ein angemessenes Maß an Planung im Vorfeld.

Die Planung des Einsatzes kann in mehreren Schritten nach dem Prinzip des Top-Down-Entwurfs erfolgen: Ausgehend von einem Grobkonzept für das Gesamtsystem werden konkrete Planungen für Teilkomponenten in spezifische Teilkonzepten festgelegt. Die Planung betrifft dabei nicht nur Aspekte, die klassischerweise mit dem Begriff Sicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen.

Grobkonzept

Im Grobkonzept sollten beispielsweise folgende typische Fragestellungen behandelt werden:

- Welche Aufgaben sollen die Clients erfüllen? Auf welche Dienste muss von den Clients zugegriffen werden können? Gibt es besondere Anforderungen an die Verfügbarkeit der Systeme oder an die Vertraulichkeit oder Integrität der gespeicherten oder verarbeiteten Daten?
- Sollen in dem System bestimmte Hardware-Komponenten eingesetzt werden? Dies kann beispielsweise für die Auswahl des Betriebssystems wichtig sein.
- Welche Anforderungen an die Hardwareausstattung (CPU, Arbeitsspeicher, Kapazität der Festplatten, Kapazität des Netzes etc.) ergeben sich aus den allgemeinen Anforderungen?
- Handelt es sich bei dem Netz, in dem die Clients eingesetzt werden sollen, um einen homogenen oder heterogenen Rechnerverbund?
- Dienen die Clients als Ersatz für vorhandene Systeme? Sollen von den alten Systemen Datenbestände oder Hardware-Komponenten übernommen werden?
- Sollen auf den Rechnern weitere Betriebssysteme mittels Multiboot installiert werden?

Es wird empfohlen, ein oder mehrere generische Anforderungsprofile (beispielsweise "Allgemeiner Büro-PC", "Entwicklungsrechner" oder "Administrations-Client") zu erstellen, die bei konkreten Planungen als Grundlage dienen können.

Teilkonzepte

Die folgenden Teilkonzepte sollten bei der Planung berücksichtigt werden:

- **Authentisierung und Benutzerverwaltung**: Welche Arten der Benutzerverwaltung und Benutzer-Authentisierung sollen genutzt werden? Werden Benutzer nur lokal verwaltet oder soll ein zentrales Verwaltungssystem genutzt werden? Soll das System auf einen zentralen, netzbasierten Authentisierungsdienst zugreifen oder wird nur eine lokale Authentisierung benötigt? Mehr Informationen dazu finden sich in M 4.133 *Geeignete Auswahl von Authentikationsmechanismen* und M 4.250 *Auswahl eines zentralen, netzbasierten Authentisierungsdienstes*.

- **Benutzer- und Gruppenkonzept**: Ausgehend vom organisationsweiten Benutzer-, Rechte- und Rollenkonzept müssen entsprechende Regelungen für die Clients erstellt werden (siehe auch M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile* und M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*).
- **Administration**: Wie sollen die Systeme administriert werden? Werden alle Einstellungen lokal vorgenommen oder werden die Clients in ein zentrales Administrations- und Konfigurationsmanagement integriert?
- **Partitions- und Dateisystem-Layout**: In der Planungsphase sollte eine erste Abschätzung des benötigten Plattenplatzes durchgeführt werden. Zur einfacheren Administration und Wartung ist es empfehlenswert, so weit wie möglich eine Trennung von Betriebssystem (Systemprogramme und -konfiguration), Anwendungsprogrammen und -daten (beispielsweise Datenbank-Server und Daten) und gegebenenfalls Benutzerdaten vorzunehmen. Verschiedene Betriebssysteme bieten hierfür unterschiedliche Mechanismen an (Aufteilung in Laufwerke unter Windows, Dateisysteme unter Unix). Oft kann es sinnvoll sein, bestimmte Daten sogar auf einer eigenen Festplatte oder einem eigenen Plattensystem zu speichern. Dies erlaubt es beispielsweise, bei einer Neuinstallation oder einem Update des Systems die Daten auf den anderen Partitionen ohne Umkopieren zu übernehmen.

  Trennung von Programmen, System- und Benutzerdaten

  In der Planungsphase sollte die vorgesehene Aufteilung der Partitionen und deren Größe dokumentiert werden.

  Falls auf den Clients Daten mit hohem Schutzbedarf bezüglich der Vertraulichkeit gespeichert werden, so wird der Einsatz verschlüsselter Dateisysteme dringend empfohlen. Dabei brauchen nicht notwendigerweise alle Dateisysteme verschlüsselt zu werden, sondern es wird oft ausreichend sein, für den Teil des Dateisystems eine Verschlüsselung vorzusehen, auf dem die Daten selbst gespeichert werden. Dies wird durch eine entsprechende Planung des Partitions- und Dateisystemlayouts erleichtert.

  Bei hohem Schutzbedarf möglichst verschlüsselte Dateisysteme vorsehen

  Bei besonderen Anforderungen an die Vertraulichkeit der Daten, die auf den Clients gespeichert sind, kann es erforderlich werden, die Systeme mit einem Verschlüsselungsprogramm auszustatten, das die gesamte Festplatte verschlüsselt und bereits vor dem Start des Betriebssystems eine Benutzer-Authentisierung (beispielsweise über eine Chipkarte) durchführt ("Pre-Boot-Authentication").
- **Netzdienste und Netzanbindung**: In Abhängigkeit von den Sicherheitsanforderungen der Daten, auf die von den Clients aus zugegriffen werden muss, muss die Netzanbindung der Clients geplant werden.

  Abhängig vom festgelegten Einsatzzweck der Rechner wird außerdem eventuell der Zugriff auf weitere Dienste im Netz benötigt. Dies muss bereits im Rahmen der Planung berücksichtigt werden, damit nicht zu einem späteren Zeitpunkt Schwierigkeiten beispielsweise durch zu geringe Übertragungskapazitäten oder Probleme mit zwischengeschalteten Sicherheitsgateways entstehen.

- **Monitoring**: Falls besondere Anforderungen an die Verfügbarkeit der Clients bestehen, so kann ein Monitoring-System eingesetzt werden. Dafür wird auf einem Server ein Monitoring-Daemon installiert, dem ein lokal installierter Agent die zu überwachenden Daten, beispielsweise zur Systemauslastung oder zum verbleibenden freien Speicherplatz, sendet. Bei Problemen kann zum Beispiel automatisch ein Alarm generiert werden.
- **Protokollierung**: Auch bei Clients spielt die Protokollierung eine wichtige Rolle, beispielsweise bei der Diagnose und Behebung von Störungen oder bei der Erkennung und Aufklärung von Angriffen. In der Planungsphase sollte entschieden werden, welche Informationen mindestens protokolliert werden sollen, und wie lange die Protokolldaten aufbewahrt werden sollen. Außerdem muss festgelegt werden, ob die Protokolldaten lokal auf den Systemen oder auf einem zentralen Logserver im Netz gespeichert werden sollen.

  Sinnvollerweise sollte bereits in der Planungsphase festgelegt werden, wie und zu welchen Zeitpunkten Protokolldaten ausgewertet werden sollen.

Auch an die Auswertung der Logdateien denken

- **Hochverfügbarkeit**: Falls an die Verfügbarkeit der Clients besondere Anforderungen gestellt werden, so sollte bereits in der Planungsphase überlegt werden, wie diese Anforderungen erfüllt werden können.

Alle Entscheidungen, die in der Planungsphase getroffen wurden, müssen so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Dabei ist zu beachten, dass meist andere Personen neben dem Autor diese Informationen auswerten müssen. Daher ist auf passende Strukturierung und Verständlichkeit zu achten.

Ergänzende Kontrollfragen:

- Wurde der Einsatz von Clients vor Beschaffung und Installation geplant?
- Welche Dokumentation existiert über die Planung der Clients?

M 2.322 Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement, Administrator

Die Sicherheitsvorgaben für alle Clients ergeben sich aus der organisationsweiten Sicherheitsrichtlinie. Ausgehend von der allgemeinen Richtlinie müssen die Anforderungen für den gegebenen Kontext konkretisiert werden und in einer Sicherheitsrichtlinie für die jeweilige Gruppe von Clients zusammengefasst werden. In diesem Zusammenhang ist zu prüfen, ob neben der organisationsweiten Sicherheitsleitlinie weitere übergeordnete Vorgaben wie IT-Richtlinien, Passwortrichtlinien oder Vorgaben zur Internet-Nutzung zu berücksichtigen sind.

Die Sicherheitsrichtlinie muss allen Anwendern und anderen Personen, die an der Beschaffung und dem Betrieb der Clients beteiligt sind, bekannt sein und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die Sicherheitsrichtlinie sollte das generell zu erreichende Sicherheitsniveau spezifizieren und grundlegende Festlegungen treffen. Zur Verbesserung der Übersichtlichkeit kann es sinnvoll sein, für verschiedene Einsatzgebiete gesonderte Sicherheitsrichtlinien zu entwickeln.

Allgemeine Strategie: Liberal oder Restriktiv?

Als erstes sollte die allgemeine Konfigurations- und Administrationsstrategie ("Liberal" oder "Restriktiv") festgelegt werden, da die weiteren Entscheidungen von dieser Festlegung wesentlich abhängen.

Für Clients mit normalem Schutzbedarf kann eine relativ liberale Strategie gewählt werden, was in vielen Fällen die Konfiguration und Administration vereinfacht. Generell ist es aber auch in diesen Fällen empfehlenswert, die Strategie nur "so liberal wie nötig" auszulegen.

Bei Clients mit einem hohem Schutzbedarf wird grundsätzlich eine restriktive Strategie empfohlen. Für Clients mit besonderem Schutzbedarf bezüglich eines der drei Grundwerte sollte unbedingt eine restriktive Konfigurations- und Administrationsstrategie umgesetzt werden.

Nachfolgend sind einige Punkte aufgeführt, die berücksichtigt werden sollten:

- Regelungen für die Arbeit der Benutzer der Clients
  - Soll das System nur von einem einzelnen Benutzer genutzt werden, oder ist ein Betrieb mit wechselnden Benutzern vorgesehen?
  - Dürfen Benutzer bestimmte Konfigurationseinstellungen selbst ändern (beispielsweise Bildschirmhintergrund, Bildschirmschoner oder ähnliches) oder werden alle Einstellungen zentral vorgegeben?
  - Dürfen Benutzer auf bestimmte Bereiche des Systems keinen Zugriff haben?

Diese Vorgaben haben in der Regel sowohl Auswirkungen auf die Rechtevergabe im System selbst als auch auf die Vorgaben für die Installation und Grundkonfiguration.

  - Sind die Benutzer gehalten, den Rechner abends herunterzufahren und auszuschalten, oder muss er rund um die Uhr in Betrieb sein?

  Für das Ausschalten von Client-Rechnern bei Arbeitsschluss sprechen beispielsweise Brandschutz und Stromersparnis. Darüber hinaus sind etwa Festplatten, die in Client-Computern eingesetzt werden, meist nicht mehr für einen Dauerbetrieb geeignet. Ein durchgehender Betrieb der Rechner kann dennoch erwünscht sein, beispielsweise wenn über Nacht automatische Datensicherungen laufen oder die Rechner für andere Anwendungen genutzt werden.

- Regelungen für die Arbeit der Administratoren und Revisoren:
  - Nach welchem Schema werden Administrationsrechte vergeben? Welcher Administrator darf welche Rechte ausüben und wie erlangt er diese Rechte?
  - Über welche Zugangswege dürfen Administratoren und Revisoren auf die Systeme zugreifen?
  - Welche Vorgänge und Ereignisse müssen dokumentiert werden? In welcher Form wird die Dokumentation erstellt und gepflegt?
  - Gilt für bestimmte Änderungen ein Vier-Augen-Prinzip?
- Vorgaben für die Installation und Grundkonfiguration
  - Welche Installationsmedien werden zur Installation verwendet?
  - Soll ein zentraler Authentisierungsdienst genutzt werden oder erfolgt die Benutzerverwaltung und -authentisierung nur lokal?
  - Regelungen zur Benutzer- und Rollenverwaltung, Berechtigungsstrukturen (Ablauf und Methoden der Authentisierung und Autorisierung, Berechtigung zu Installation, Update, Konfigurationsänderungen etc.). Nach Möglichkeit sollte ein Rollenkonzept für die Administration erarbeitet werden.
  - Vorgaben für die zu installierenden Softwarepakete.
  - Falls bei der Planung für die Clients festgelegt wurde, dass Teile des Dateisystems verschlüsselt werden sollen, so sollte an dieser Stelle festgelegt werden, wie dies zu geschehen hat.

Besondere Sorgfalt bei verschlüsselten Dateisystemen

Beim Einsatz verschlüsselter Dateisysteme sollte hierfür ein eigenes Konzept erstellt und die Details der Konfiguration besonders sorgfältig dokumentiert werden, da im Fall von Problemen (Verlust des Schlüssels oder der Passphrase zum Schlüssel, inkorrekte Konfiguration oder ähnliches) die Daten auf den verschlüsselten Dateisystemen sonst vollständig verloren sein können.

- Regelungen zu Erstellung und Pflege von Dokumentation
- Vorgaben für den sicheren Betrieb

- Welcher Benutzerkreis darf sich auf dem System anmelden?
- Erhalten Benutzer Zugriff auf ein oder mehrere LANs oder das Internet? Welche Protokolle dürfen verwendet werden? Bei Clients,die als Arbeitsplatzrechner in einer Organisation genutzt werden, ist es in der Regel nicht notwendig und oft auch nicht wünschenswert, dass normale Benutzer über das Netz auf einen anderen Arbeitsplatzrechner zugreifen.
- Auf welche Ressourcen dürfen die Benutzer zugreifen?
- Es müssen Vorgaben für die Passwortnutzung erstellt werden (Passwortregeln, Regeln und Situationen für Passwortänderungen, gegebenenfalls Hinterlegung von Passwörtern).
- Wer darf das System herunterfahren?
- Soll das System mit einer Boot-Sperre versehen werden, die ein Starten von externen Medien wie Disketten, CD-ROMs oder USB-Memory-Sticks verhindert?

  Es wird empfohlen, für den Normalbetrieb eine solche Sperre vorzusehen, die nur im Rahmen einer Störungssuche und -beseitigung vom Administrator aufgehoben werden kann, wenn er das System mit dem Notfall-Bootmedium (siehe M 6.24 *Erstellen eines Notfall-Bootmediums*) startet.

- Netzkommunikation und -dienste
  - Soll ein lokaler Paketfilter aufgesetzt werden?
  - Auf welche externen Netzdienste soll von dem Rechner aus zugegriffen werden können?
  - Soll ein verteiltes Dateisystem eingebunden werden?

    Vorsicht bei Nutzung von verteilten Dateisystemen

    Verteilte Dateisysteme, bei denen die Nutzdaten unverschlüsselt übertragen werden, sollten nur im internen Netz verwendet werden. Soll ein verteiltes Dateisystem über ein unsicheres Netz hinweg genutzt werden, so muss es durch zusätzliche Maßnahmen (kryptographisch geschütztes VPN, Tunneling) gesichert werden.

- Protokollierung
  - Welche Daten werden protokolliert? Wie und in welchen Intervallen werden die Protokolldaten ausgewertet? Wer führt die Auswertung durch?

Anhand der oben genannten Punkte kann eine Checkliste erstellt werden, die bei Audits oder Revisionen hilfreich sein kann.

Die Verantwortung für die Sicherheitsrichtlinie liegt beim IT-Sicherheitsmanagement. Änderungen und Abweichungen hiervon dürfen nur in Abstimmung mit dem IT-Sicherheitsmanagement erfolgen.

Bei der Erstellung einer Sicherheitsrichtlinie ist es empfehlenswert, so vorzugehen, dass zunächst ein Maximum an Forderungen und Vorgaben für die Sicherheit der Systeme aufgestellt wird. Diese können anschließend den

tatsächlichen Gegebenheiten angepasst werden. Idealerweise wird so erreicht, dass alle notwendigen Aspekte berücksichtigt werden. Für jede im zweiten Schritt verworfene oder abgeschwächte Vorgabe sollte der Grund für die Nicht-Berücksichtigung dokumentiert werden.

Im Bezug auf Regelungen für die Benutzer sollte jedoch beachtet werden, dass diese nur so weit sinnvoll sind, wie sie im normalen Arbeitsalltag anwendbar sind, aber auch wie sie überwacht und durchgesetzt werden können. Beispielsweise ist es bei Zugriffsbeschränkungen nicht zielführend, den Benutzern nur in der Sicherheitsrichtlinie den Zugriff auf bestimmte Verzeichnisse zu verbieten, diese aber nicht auch durch eine entsprechende Rechtevergabe tatsächlich vor dem Zugriff zu schützen. Zugriffsbeschränkungen, die bei der Erstellung der Sicherheitsrichtlinie festgelegt wurden, sollten daher immer so weit wie möglich über entsprechende Vorgaben für die Installation und Konfiguration der Rechner umgesetzt werden.

Zu starke Einschränkungen können kontraproduktiv sein

Bei der Formulierung der Sicherheitsrichtlinie für Clients ist es auch wichtig, eine Balance zwischen Sicherheit (durch Einschränkungen der Funktionalität und restriktive Vergabe von Benutzerrechten) und Benutzerfreundlichkeit wichtig. Werden die Benutzer durch Regelungen, die für sie nicht transparent sind und die eventuell sogar als Schikane empfunden werden, zu sehr eingeschränkt, so kann sie dies im Gegenzug dazu verleiten, diese Beschränkungen mit besonderer Kreativität zu umgehen.

Dies unterscheidet die Sicherheitsrichtlinie für Clients von den entsprechenden Richtlinien etwa für Server oder aktive Netzkomponenten, bei denen in der Regel nur technisch versierte Anwender und Administratoren angesprochen sind, denen viele Einschränkungen eher plausibel gemacht werden können.

Ergänzende Kontrollfragen:

- Wurde eine Sicherheitsrichtlinie für den Betrieb der Clients erstellt?
- In welcher Form wurde die Dokumentation der Sicherheitsrichtlinie vorgenommen?
- Wann wurde die Sicherheitsrichtlinie zum letzten Mal aktualisiert?
- Wurde ein Sicherheitsniveau in der Sicherheitsrichtlinie definiert?

M 2.323 Geregelte Außerbetriebnahme eines Clients

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Bei der Außerbetriebnahme eines Clients muss vor allem sichergestellt werden, dass

- keine wichtigen Daten, die eventuell auf dem Client gespeichert sind, verloren gehen, und dass
- keine sensitiven Daten auf den Datenträgern des Rechners zurück bleiben.

Dazu ist es insbesondere wichtig, einen Überblick darüber zu haben, welche Daten wo auf dem System gespeichert sind.

- Datensicherung

  Vor der Außerbetriebnahme des Rechners müssen lokal gespeicherte Daten, die noch benötigt werden, entweder extern gesichert bzw. archiviert (beispielsweise auf Magnetbändern, CD- oder DVD-ROMs) oder auf ein Ersatzsystem übertragen werden. Nach der Sicherung sollte überprüft werden, dass wirklich alle Daten korrekt gesichert wurden.

  In diesem Zusammenhang kann es sinnvoll sein, den Benutzern für die Sicherung eventuell gespeicherter lokaler Daten ein geeignetes Laufwerk, beispielsweise einen externen CD- oder DVD-Brenner, zur Verfügung zu stellen.

  Weitere Informationen zu diesem Themenkomplex finden sich in den Bausteinen B 1.4 *Datensicherungskonzept* und B 1.12 *Archivierung*.

- Austragen des Systems aus Verzeichnisdiensten und Datenbanken

  Etwaige Berechtigungen im Netz, die an den Client-Rechner selbst (und nicht an einen Benutzer) gekoppelt sind, müssen gelöscht werden. Beispiele hierfür sind Einträge auf Proxyservern am Sicherheitsgateway oder Zugriffsrechte auf Netzdienste, die anhand der IP-Adresse gewährt werden. Ist der Client in netzweiten Verzeichnisdiensten oder Datenbanken eingetragen (etwa in einer Windows Domäne, Active Directory, NIS oder ähnlichen), so müssen die zugehörigen Einträge gelöscht oder zumindest die entsprechenden Konten deaktiviert werden.

- Löschen der Daten auf dem System

  Sicheres Löschen von Daten

  Es muss sichergestellt werden, dass keine schützenswerten Informationen mehr auf den Festplatten vorhanden sind. Dazu genügt es nicht, die Platten einfach neu zu formatieren, sondern sie müssen mindestens einmal vollständig überschrieben werden. Es ist zu beachten, dass weder das logische Löschen mit den Löschfunktionen des Betriebssystems noch das Neuformatieren der Platten die Daten tatsächlich von den Festplatten entfernt. Mit geeigneter Software können Daten in solchen Fällen, oft sogar ohne großen Aufwand, wieder rekonstruiert werden. Weitere Hinweise finden sich in M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln* und in M 2.167 *Sicheres Löschen von Datenträgern*.

- Löschen von Datensicherungsmedien

Nach der Außerbetriebnahme eines Systems müssen gegebenenfalls auch die entsprechenden Datensicherungsmedien gelöscht werden, wenn die darauf gespeicherten Daten nicht mehr benötigt werden.

- Entfernen sonstiger Informationen

  Sind auf einem Rechner noch an anderen Stellen als auf der Festplatte (etwa in einem nichtflüchtigen Speicher) potentiell sensitive Daten gespeichert (beispielsweise bestimmte Konfigurationsdaten), so müssen auch diese vor der Weitergabe des Geräts entfernt werden.

Es wird empfohlen, anhand der oben gegebenen Empfehlungen eine Checkliste zu erstellen, die bei der Außerbetriebnahme eines Systems abgearbeitet werden kann. Auf diese Weise kann vermieden werden, dass einzelne Schritte vergessen werden.

Ergänzende Kontrollfragen:

- Wie wird bei der Außerbetriebnahme eines Systems vorgegangen?

M 2.324 Einführung von Windows XP planen

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement, Administrator

Die geregelte und sichere Einführung von Windows XP Systemen setzt eine umfangreiche Planung voraus. In der Planungsphase werden die notwendigen Voraussetzungen für einen sicheren Betrieb von Windows XP Systemen geschaffen.

Die einzelnen Planungsschritte sind abhängig von den geplanten Einsatzszenarien der Windows XP Systeme. Die Einführung muss in ihren einzelnen Schritten möglichst detailliert geplant werden. Hierbei müssen nicht nur die Inhalte, sondern auch interne Prozesse und Abläufe der Organisation berücksichtigt werden. Alle Inhalte und Prozesse sind zu definieren, dokumentieren und allen Beteiligten zugänglich zu machen.

Generell muss ausreichend Zeit für die Einführung von Windows XP eingeplant werden. Dabei ist ein Zeitraum von einem halben Jahr für größere Unternehmen und Behörden durchaus als realistischer Planungszeitraum einzukalkulieren. Im Laufe der Planung muss erfahrungsgemäß außerdem mehrfach der Zeitplan angepasst werden.

Die im folgenden genannten sicherheitsrelevanten Aspekte müssen bei der Einführung von Windows XP berücksichtigt werden.

Neuinstallation oder Migration/Upgrade

Für die Einführung von Windows XP stehen verschiedene Verfahren zur Verfügung. Zum einen kann die Einführung durch einen parallelen Aufbau der Windows XP-Infrastruktur (neue Clients werden parallel zu bestehenden eingeführt) erfolgen. Zum anderen kann dies durch eine Migration bzw. ein Update vorhandener Client-Rechner geschehen.

Eine generelle Empfehlung für die Einführung kann nicht gegeben werden, da dies von den lokalen Gegebenheiten abhängt. Im Allgemeinen muss das Verfahren immer auf das Unternehmen bzw. die Behörde zugeschnitten werden.

In erster Linie muss entschieden werden, ob bei der Einführung von Windows XP die Client-Rechner komplett neuinstalliert oder migriert werden. In der Praxis werden häufiger bereits bestehende Client-Systeme migriert anstatt eine vollständige Neuinstallation durchzuführen. Nicht nur die Neuinstallation, sondern auch die Migration von Windows NT 4.0/2000 Professional Clients auf Windows XP Professional bedarf einer ausgiebigen Planung, insbesondere, wenn nicht nur die Clients sondern auch die Domänen (also Domänen-Controller) migriert (z. B. auf Windows Server 2003) werden. Die Migration muss in ihren einzelnen Schritten möglichst detailliert geplant werden, da durch Planungsdefizite in der Zeit der Umstellung leicht Sicherheitslücken entstehen können.

Werden nicht nur Clients, sondern auch Domänen von älteren Windows-Versionen migriert, müssen zusätzlich die entsprechenden Migrationsaspekte auf Server-Seite berücksichtigt werden (siehe M 2.233 *Planung der Migration von Windows NT auf Windows 2000*).

Es ist zu beachten, dass in der Migrationphase unter Umständen erweiterte Zugriffsberechtigungen (z. B. für ein spezielles Migrationsteam) und schwächere Sicherheitseinstellungen wegen potentieller Kompatibilitäts-probleme gewählt werden müssen. Diese Einstellungen müssen nach dem Abschluss der Migration auf das höchstmögliche Sicherheitsniveau gebracht werden. Die zusätzlichen migrationspezifischen Berechtigungen sind nach der Migration zu entziehen. Generell gilt, dass nach der erfolgten Migration dasselbe Sicherheitsniveau erreicht werden muss wie bei einer Neu-installation. Nach Abschluss der Migration hat ein Soll-Ist-Abgleich aller Sicherheitseinstellungen wie z. B. Berechtigungen und Gruppenmitglied-schaften stattzufinden.

Die Zeitspanne für die Migration muss festgelegt und eingehalten werden. Die Migration darf nicht zu einem "Normalzustand" werden. Dies hat insbesondere sicherheitsrelevante Auswirkungen, da die Sicherheit während der Migration üblicherweise abgeschwächt wird.

Einsatz in gemischten Umgebungen planen

Beim Einsatz von Windows XP Clients in gemischten Umgebungen (z. B. zusammen mit NT 4.0 Rechnern) können Abschwächungen der Sicherheitseinstellungen notwendig sein (z. B. kein durchgehendes digitales Signieren der Netzkommunikation). Diese sind bei der Planung zu berücksichtigen. Insbesondere muss dafür Sorge getragen werden, dass nach der Realisierung einer homogenen Umgebung (d. h. ausschließlich Windows XP Clients, Windows 2000/2003 Domain Controller und Server) die Sicherheitseinstellungen auf das höhere Niveau anzuheben sind.

Werden Windows XP Clients in NT-Umgebungen eingesetzt, stehen Active Directory-basierte Gruppenrichtlinien nicht zur Verfügung. In diesem Fall müssen lokale Sicherheitsrichtlinien zur Umsetzung der gewünschten Sicherheitseinstellungen verwendet werden. Für diesen Fall muss insbesondere der Verteilungsmechanismus für die Richtlinieneinstellungen geplant worden sein. Zusätzlich muss ein Konzept zur Pflege der lokalen Sicherheitsrichtlinien in der Planungsphase erstellt werden.

Active-Directory-bezogene Planung

Bei der Einführung von Windows XP in einer Active Directory Umgebung ist es nicht ausreichend, ausschließlich die Client-Seite zu betrachten. Auch die Server-Seite ist zu berücksichtigen. Hierbei müssen vor allem die Änderungen im Active Directory geplant werden sowie ein Abgleich der Sicherheitseinstellungen auf Client- und Server-Seite erfolgen.

So sind beispielsweise entsprechende Gruppen- und OU-Strukturen (Organisationseinheit, Organizational Unit) im Active Directory zu entwerfen. Denn eine geeignete OU-Struktur begünstigt einen einfacheren und damit wegen der größeren Transparenz einen sichereren Betrieb der Windows XP Systeme in einer Unternehmensumgebung.

Des Weiteren ist die Gruppenrichtlinien-Struktur im Active Directory zu planen. Über den Einsatz von Gruppenrichtlinien-spezifischen Mechanismen wie etwa das Blockieren der Vererbung oder das sogenannte Security Filtering muss in der Planungsphase entschieden werden. Dabei ist die Verarbeitungsreihenfolge für Gruppenrichtlinien zu berücksichtigen.

Die generellen Active Directory-Planungsmaßnahmen sind unter anderem in M 2.229 *Planung des Active Directory* zusammengefasst.

Sicherheitskonzept/Windows XP Sicherheitsrichtlinie

Das Planen und Erstellen eines Sicherheitskonzeptes bzw. einer Sicherheitsrichtlinie im Vorfeld der Einführung von Windows XP ist immens wichtig. Durch die Sicherheitsrichtlinie sind alle sicherheitsrelevanten Aspekte des Windows XP Betriebs zu berücksichtigen. Weitere Anforderungen an das Sicherheitskonzept sind in der Maßnahme M 2.325 *Planung der Windows XP Sicherheitsrichtlinie* zusammengefasst.

Benutzerkonzept

Bei der Planung des Benutzerkonzepts muss der Umgang mit lokalen und domänen-weiten Benutzerkonten geregelt werden. Beim Einsatz von Windows XP in einer Windows 2000/2003 Domäne muss auch über den Einsatz von servergespeicherten Benutzerprofilen (Roaming User Profile) entschieden werden. Die Nutzung von servergespeicherten Benutzerprofilen hat vor allem Auswirkungen auf die Backup-Strategie, sowie auf den Einsatz des Windows Encrypting File System (EFS).

Administrationskonzept

Ein Administrationskonzept ist im Vorfeld der Einführung von Windows XP zu erstellen. Insbesondere muss die entfernte Administration der Clients und der Umgang mit lokalen administrativen Konten geregelt werden. Die Fragen der personellen und organisatorischen Zuständigkeiten müssen ebenfalls im Konzept Berücksichtigung finden. Das Trennen von Verantwortlichkeiten (Segregation of Duties) ist im Administrationskonzept zu verankern. Die entsprechende Umsetzung ist sowohl auf der organisatorischen als auch der technischen Ebene zu planen.

Werden die Windows XP Systeme in einer Active Directory Umgebung eingesetzt, so müssen die Fragen der administrativen Zuständigkeiten und Grenzen, sowie die Vergaberichtlinien für administrative Berechtigungen auf Client- und Benutzer-Objekte im Active Directory geklärt werden.

Protokollierungs-/Audit-Konzept

Um die Sicherheit eines Windows XP Systems gewährleisten zu können, muss überwacht werden, ob die festgelegten Sicherheitsrichtlinien (siehe M 2.325 *Planung der Windows XP Sicherheitsrichtlinie*) eingehalten werden. Insbesondere ist auf organisatorischer und technischer Ebene zu regeln, wie die gesammelten Daten regelmäßig ausgewertet werden. Die Sicherheitsaspekte, die bei der Protokollierung zu beachten sind, sind in der Maßnahme M 4.148 *Überwachung eines Windows 2000/XP Systems* aufgeführt.

Datenablage, Datensicherung und Verschlüsselung

Es ist festzulegen, wo die Benutzerdaten gespeichert werden (siehe M 2.138 *Strukturierte Datenhaltung*). Es wird grundsätzlich empfohlen, keine Daten auf Client-Rechnern abzulegen. Dann muss jedoch eine geeignete serverseitige Infrastruktur vorhanden sein. Die Maßnahmen M 5.37 *Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz* und M 2.67 *Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste* sind dabei zu beachten. Nach welcher Strategie verfahren werden soll, ist anhand der konkreten Umstände im Einzelfall festzulegen. In bestimmten Einsatzszenarien, wie beispielsweise bei der Verwendung mobiler Computer, ist die Datenablage auf Clients hingegen notwendig und erwünscht. In solchen Fällen muss die client-seitige Datenablage und ihr (kryptographischer) Schutz geplant werden. Die Umsetzung der technischen Maßnahmen, die die Sicherheit der lokalen Datenablage gewährleisten (z. B. Festplattenverschlüsselung, EFS, Verschlüsselung der Offline-Dateien), muss vor der Einführung geplant werden.

Um eine saubere Trennung von benutzer- und projektspezifischen Daten, sowie von Programmen und Daten des Betriebssystems durchzusetzen, muss eine geeignete Verzeichnisstruktur geplant werden, durch die eine projekt- und benutzerbezogene Dateiablage unterstützt wird. So können beispielsweise zwei Hauptverzeichnisse *\Projekte* und *\Benutzer* angelegt werden, unter denen dann die Dateien und Verzeichnisse der Projekte bzw. Benutzer in jeweils eigenen Unterverzeichnissen abgelegt werden.

Bei der Einführung von Windows XP muss auch eine entsprechende Datensicherungsstrategie festgelegt werden. Für jedes System und für jede Datenart muss die Verfahrensweise der Datensicherung festgelegt werden. Die jeweilige Umsetzung hängt vor allem von der Art der Daten ab, die auf einem Client abgelegt sind. Werden auf einem Client keine Daten abgelegt, nur Standard-Software eingesetzt und haben die Benutzer servergespeicherte Profile, so kann unter Umständen auf client-seitige Datensicherung verzichtet werden. Werden dagegen auf einem Windows XP Client-Rechner Daten abgelegt, müssen diese Daten bei Sicherungen berücksichtigt werden. Weitere Informationen zu diesem Thema werden in den Maßnahmen M 6.32 *Regelmäßige Datensicherung* und M 6.33 *Entwicklung eines Datensicherungskonzepts* gegeben.

Die Verwendung von EFS muss beim Festlegen der Backup-Strategie berücksichtigt werden. Wird EFS eingesetzt, so muss generell die Maßnahme M 6.56 *Datensicherung bei Einsatz kryptographischer Verfahren* beachtet werden. Insbesondere ist jedoch durch das Backup-Konzept der Umgang mit dem Schlüsselmaterial bei Wiederherstellungsoperationen zu regeln (siehe dazu auch M 4.147 *Sichere Nutzung von EFS unter Windows 2000/XP*).

Roll-out

Die Abläufe bei der Installation, also die Roll-out-Phase, müssen bei der Planung berücksichtigt werden. Unter anderem sind die personellen Zuständigkeiten beim Roll-out eindeutig zu definieren. Es ist zusätzlich ein Roll-out-Notfallkonzept zu erstellen. Durch dieses Notfallkonzept muss sichergestellt werden, dass bei einer fehlgeschlagenen Umstellung für ein System der produktive Zustand schnell wiederhergestellt werden kann.

Weitere Konzepte

Neben den oben aufgeführten Konzepten können je nach Einsatzszenario auch weitere Konzepte notwendig werden, wie z. B. ein Namenskonzept (Namenskonventionen für die Rechner, Benutzergruppen und die Benutzer), ein Softwareverteilungskonzept oder ein Konzept zur Anwendungsmigration. Insbesondere die Anwendungsmigration kann Auswirkungen auf die Sicherheit eines Windows XP Systems haben (z. B. Abschwächung der Zugriffsrechte auf die Registrierung) und ist daher sorgfältig zu planen.

Diese weiteren Konzepte sind dann ebenfalls in der Planungsphase zu berücksichtigen. In der Regel bestehen hier bereits entsprechende Konzeptionen im Unternehmen oder in der Behörde, die jedoch auf ihre Eignung im Windows XP Umfeld hin geprüft werden müssen.

Nicht zuletzt sollte geplant werden, welche Benutzer bzw. Administratoren geschult werden müssen und wann dies zu erfolgen hat. Insbesondere die Administratoren sind hinsichtlich der Verwaltung und der Sicherheit von Windows XP gründlich zu schulen. Erst nach ausreichender Schulung sollte daher der Windows XP-Betrieb aufgenommen werden.

Ergänzende Kontrollfragen

- Wurde die Planung der Windows XP Einführung bedarfsgerecht durchgeführt?
- Sind alle für den konkreten Einsatz notwendigen Konzepte entworfen?

M 2.325 Planung der Windows XP Sicherheitsrichtlinie

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Eine der wichtigsten organisatorischen Aufgaben bei der Einführung von Windows XP ist es, eine entsprechende Windows XP Sicherheitsrichtlinie zu planen und zu definieren. Diese Richtlinie legt die später umzusetzenden Sicherheitsbestimmungen für Windows XP Systeme fest.

Die in der XP-Sicherheitsrichtlinie definierten Anforderungen werden durch die entsprechenden Sicherheitseinstellungen auf Betriebssystemebene und/oder durch organisatorische Maßnahmen umgesetzt. In Fällen, in denen technische Maßnahmen nicht ausreichen, ist eine Kombination notwendig, so dass eine technische Umsetzung durch zusätzliche organisatorische Maßnahmen begleitet und unterstützt wird. Nach Möglichkeit sollte eine technische Lösung gegenüber einer organisatorischen immer bevorzugt werden.

Die zu erstellende XP-Sicherheitsrichtlinie hat sich an den bisher geltenden Sicherheitsrichtlinien des jeweiligen Unternehmens bzw. der jeweiligen Behörde zu orientieren und darf diesen nicht widersprechen. In der Regel werden die existierenden Regelungen für Windows XP angepasst oder sinngemäß erweitert. Dabei sind insbesondere Windows XP-spezifische Technologien (z. B. Remote Desktop) zu berücksichtigen. Generell gilt, dass sich die Planung der Windows XP Infrastruktur an der jeweiligen übergreifenden Sicherheitsrichtlinie orientiert, dabei jedoch auch über einen Feedback-Prozess Einfluss auf diese Sicherheitsrichtlinie besitzt. Nicht zuletzt ist beim Erstellen der XP-Sicherheitsrichtlinie darauf zu achten, dass geltende rechtliche Bestimmungen berücksichtigt werden. Die XP-Sicherheitsrichtlinie ist zu dokumentieren und im erforderlichen Umfang den Benutzern des Client-Server-Netzes mitzuteilen. Alle Administratoren sollten sie kennen und umsetzen.

Die folgenden Themenbereiche bieten einen groben Überblick über die abzudeckenden Bereiche einer solchen Richtlinie. Je nach Unternehmen oder Behörde und umzusetzenden Einsatzszenarien müssen natürlich noch weitere Aspekte in Betracht gezogen werden.

Physische Sicherheit

Die Fragen der physischen Sicherheit müssen bei der Planung der XP-Sicherheitsrichtlinie berücksichtigt werden, da es sich bei Windows XP um ein Client-Betriebssystem handelt, welches auch auf mobilen Rechnern zum Einsatz kommen kann. Daher müssen die generellen Emfehlungen zu physischen Sicherheit aus den Bausteinen B 3.201 *Allgemeiner Client* und B 3.202 *Allgemeines nicht vernetztes IT-System* umgesetzt werden.

Verantwortlichkeiten

Die Verantwortlichkeiten für den Betrieb der Windows XP Systemen müssen durch die XP-Sicherheitsrichtlinie geregelt werden. Es ist festzulegen, welche Verantwortung die einzelnen Administratoren zu übernehmen haben. Dies können zum Beispiel Verantwortlichkeiten sein für:

- Änderungen der Windows XP Sicherheitsparameter (lokal),
- Änderungen der Windows XP Sicherheitsparameter im Active Directory,
- die Verwaltung der Windows XP Systeme im Active Directory,
- die Auswertung der Protokolldaten,
- die Vergabe von Zugriffsrechten und Systemberechtigungen,
- das Hinterlegen und den Wechsel von Passwörtern und
- die Durchführung von Datensicherungen und Datenwiederherstellungen.

Auch die Endbenutzer müssen in einem Client-Server-Netz Verantwortlichkeiten übernehmen, sofern sie imstande sein sollen, bestimmte administrative Tätigkeiten auszuführen. In der Regel beschränken sich diese Verantwortlichkeiten jedoch auf die Vergabe von Zugriffsrechten auf die eigenen Dateien, sofern diese explizit festgelegt und nicht von Voreinstellungen des übergeordneten Verzeichnisses übernommen werden.

Die Administration der Systeme sollte von geschulten Netzadministratoren erfolgen, wobei im Rahmen der Notfallvorsorge für eine geeignete Stellvertreterregelung zu sorgen ist.

Benutzerkonten

Vor der Einrichtung von Benutzerkonten muss die Entscheidung getroffen werden, ob die Konten lokal oder im Active Directory angelegt werden. Aus Gründen der einfacheren Verwaltung wird grundsätzlich empfohlen, die Benutzerkonten im Active Directory anzulegen.

Des Weiteren sollten die Restriktionen, die für Konten gelten sollen, festgelegt werden. Dies betrifft insbesondere die Regelungen für Passwörter und für die Reaktion des Systems auf Anmelde-Fehlversuche.

Berechtigungskonzept

Die XP-Sicherheitsrichtlinie muss unter anderem auch ein Berechtigungskonzept beinhalten. Das Berechtigungskonzept legt vor allem Rechte sowohl normaler als auch administrativer Benutzer fest.

Problematisch ist dabei die Tatsache, dass Windows XP nicht rollenfähig ist. Daher muss ein entsprechendes Gruppenkonzept geplant und (lokal oder in der Domäne) umgesetzt werden. Dies erfordert im Wesentlichen eine Abbildung der Organisationshierarchie und der existierenden Rollen auf die jeweiligen Gruppen. Durch die Vergabe entsprechender Berechtigungen an die Gruppen sowie gegebenenfalls die Definition entsprechender Richtlinien (z. B. Software Restriction Policies) wird das Berechtigungskonzept umgesetzt. Dies erfordert eine entsprechende Planung bzw. Erfassung der Verantwortlichkeiten und Prozesse.

Folgende Bereiche müssen durch das Berechtigungskonzept abgedeckt sein:
- Systemberechtigungen und Benutzerrechte (z. B. lokale oder entfernte Anmeldung auf einem Rechner, das Herunterfahren eines Systems),
- Zugriffsberechtigungen auf Netzwerkfreigaben (insbesondere wenn Peer-to-Peer-Funktionalität benutzt wird),
- Zugriffsberechtigungen auf Dateien (Anwendungs- und Systemdateien),
- Zugriffsberechtigungen auf Registry-Einträge.

Benutzerrechte müssen sorgfältig geplant werden, da sie Vorrang vor anderen Rechten haben, insbesondere allen Datei- und Verzeichnisberechtigungen. Benutzerrechte beziehen sich damit auf das gesamte XP-System. Die Vergabe der Benutzerrechte erfolgt über Gruppenrichtlinien, die bei Mitgliedern einer Active-Directory-basierten Domäne im Active Directory und bei anderen Systemen lokal definiert werden (siehe M 2.326 *Planung der Windows XP Gruppenrichtlinien*). Bei der Vergabe ist darauf zu achten, dass Berechtigungen und Rechte vorzugsweise Gruppen und nicht einzelnen Benutzern zugewiesen werden.

Kommunikationssicherheit

Auch Anforderungen an die Sicherheit bei der Datenübertragung müssen ein Bestandteil der XP-Sicherheitsrichtlinie sein. Es ist empfehlenswert, Grundanforderungen an die Übertragungssicherheit in der Sicherheitsrichtlinie zu formulieren (Sollzustand) und anschließend Ausnahmen zu erfassen, die aufgrund lokaler Gegebenheiten notwendig sind. Bei der Definition der Anforderungen und zugehöriger Ausnahmen sind vor allem die Fragen der erforderlichen Authentizität, Vertraulichkeit, Integrität und Verfügbarkeit zu berücksichtigen.

Die technische Umsetzung der Anforderungen kann je nach verwendeten Mechanismen und den lokalen Gegebenheiten auf unterschiedliche Art und Weise erfolgen. Zwei der möglichen Umsetzungen werden in M 5.123 *Absicherung der Netzwerkkommunikation unter Windows XP* und M 5.90 *Einsatz von IPSec unter Windows 2000/XP* beschrieben.

Protokollierung

Windows XP stellt, wie auch Windows 2000, sehr ausführliche Möglichkeiten zur Protokollierung sicherheitsrelevanter Ereignisse (erfolgreiche und/oder fehlgeschlagene Versuche) zur Verfügung. Diese sind jedoch bei vollständiger Nutzung in der Lage, das System weitgehend mit der Protokollierung auszulasten und dabei große Mengen an Plattenplatz zu verbrauchen. Bei der Definition der Protokolleinstellungen ist das Gesamtkonzept der Systemüberwachung (siehe M 4.148 *Überwachung eines Windows 2000/XP Systems*) zu berücksichtigen.

Einsatzszenarien-spezifische Aspekte

Je nach Einsatzszenario entstehen weitere, für dieses Szenario spezifische Aspekte, die bei der Planung berücksichtigt sein müssen. Insbesondere durch die Verwendung von Peer-to-Peer-Diensten entstehen neue Sicherheitsaspekte, die durch die Sicherheitsrichtlinien abgedeckt sein müssen (siehe auch M 5.37 *Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz* und M 2.67 *Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste*). Auf die Verwendung von Peer-to-Peer-Funktionalitäten sollte nach Möglichkeit verzichtet werden, da diese die Sicherheit des Client-Server-Netzes beinträchtigen können.

Die für den mobilen Betrieb eines Windows XP Systems zu berücksichtigenden Aspekte werden in M 2.328 *Einsatz von Windows XP auf mobilen Rechnern* beschrieben.

Ein weiteres Beispiel für szenariospezifische Sicherheitsaspekte ist die Verwendung von EFS, das zusätzliche sicherheitsrelevante Anforderungen aufwirft (siehe M 4.147 *Sichere Nutzung von EFS unter Windows 2000/XP*).

Ergänzende Kontrollfragen

- Sind alle relevanten Bereiche durch die XP-Sicherheitsrichtlinie abgedeckt?
- Wurde der Feedback-Prozess bei der Umsetzung der XP-Sicherheitsrichtlinie berücksichtigt?
- Ist die erstellte XP-Sicherheitsrichtlinie dokumentiert und den Benutzern bzw. Administratoren mitgeteilt worden?
- Sind alle Benutzer in die Windows XP Sicherheitsrichtlinie eingewiesen worden?

M 2.326 Planung der Windows XP Gruppenrichtlinien

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Wie bereits unter Windows 2000 steht zur Konfiguration von Windows XP Systemen der Mechanismus der Gruppenrichtlinien zur Verfügung. Die unter Windows 2000 eingeführten Richtlinien wurden um Windows-XP-spezifische Inhalte erweitert , so dass mehr als 200 neue Richtlinien neu dazugekommen sind (insgesamt mehr als 900 Richtlinien).

Gruppenrichtlinien dienen dazu, einen Satz von Konfigurationseinstellungen, insbesondere auch Sicherheitseinstellungen, auf eine Gruppe von Objekten anzuwenden. Ein so genanntes Gruppenrichtlinienobjekt (englisch Group Policy Object, GPO) fasst dabei einen vorgegebenen Satz von Konfigurationsparametern zusammen. Für jeden Parameter kann ein konkreter Wert angegeben werden, der unter Umständen nur aus einem beschränkten Wertebereich stammt. Generell kann auch der Wert *nicht definiert* gewählt werden, dann gelten automatisch die Standardeinstellungen für diese Parameter.

Die Gruppenrichtlinien sind der primäre Mechanismus zur Umsetzung der in der Maßnahme M 4.244 *Sichere Windows XP Systemkonfiguration* empfohlenen Sicherheitseinstellungen. Sie können zur Definition der Parametereinstellungen für einen konkreten Rechner oder Benutzer lokal auf dem Rechner (lokale GPO) und beim Betrieb in einer Active Directory-basierten Umgebung noch zusätzlich auf der Standort-, Domänenebene bzw. auf der Ebene einzelner Organisationseinheiten eingesetzt werden.

Die Parameter innerhalb eines Gruppenrichtlinienobjektes sind baumartig oder dateisystemartig thematisch zusammengefasst. Dabei ergibt sich eine generelle Zweiteilung auf oberster Ebene in Einstellungen für Rechner und Benutzer. Dies ermöglicht sowohl die Definition von rechner- als auch benutzerbasierten Einschränkungen. Durch die im Benutzerteil einer Gruppenrichtlinie definierten Einstellungen werden unter anderem auch anwendungsspezifische Einschränkungen festgelegt. Durch den Import zusätzlicher administrativer Vorlagen können weitere Anwendungen, wie z. B. Microsoft Office, über die Gruppenrichtlinien zentral konfiguriert werden. Im Allgemeinen wird der Einsatz von benutzerspezifischen und anwendungsspezifischen Gruppenrichtlinien zum Einsatz empfohlen.

Benutzer- und Rechnerteile einer Gruppenrichtlinie lassen sich einzeln deaktivieren, so dass der jeweils deaktivierte Teil bei der Anwendung der Gruppenrichtlinie nicht ausgewertet wird. Dies schafft in einigen Einsatzszenarien Geschwindigkeitsvorteile. Über die Deaktivierung eines nicht genutzten Teils einer Gruppenrichtlinie ist im Allgemeinen in Abhängigkeit von aktuellen Gegebenheiten zu entscheiden.

Werden Gruppenrichtlinien festgelegt, muss auf die Unterschiede zwischen lokalen Gruppenrichtlinien und Richtlinien im Active Directory geachtet werden. Nicht alle Einstellungen, die in einer Active Directory-basierten GPO vorgenommen werden können, können auch in einer lokalen Gruppenrichtlinie definiert werden. So fehlen in der lokalen Gruppenrichtlinie z. B. die Kerberos- und die Systemdienst-Richtlinien. Einzelne Richtlinien wie z. B. *Kennwörter für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern* sind nur beim Einsatz in einer Domäne wirksam. Bei der Festlegung einzelner Parametereinstellungen muss folglich stets der Geltungsbereich einzelner Richtlinien berücksichtigt werden.

Gruppenrichtlinien-Bereiche

Folgende Bereiche existieren im Computer-Teil einer Gruppenrichtlinie: *Softwareeinstellungen, Windows-Einstellungen|Skripts, Windows-Einstellungen|Sicherheitseinstellungen, Administrative Vorlagen*. Die Softwareeinstellungen sind vor allem beim Einsatz in einer Domäne relevant. Mit ihrer Hilfe kann über die Gruppenrichtlinien Software installiert, aktualisiert oder deinstalliert werden. Über die Skript-Richtlinien können Skripte spezifiziert werden, die beim Starten bzw. Herunterfahren des Systems ausgeführt werden.

Die Sicherheitseinstellungen-Richtlinien unterteilen sich in weitere Bereiche: *Kontorichtlinien (Kennwortrichtlinien, Kontosperrungsrichtlinien, Kerberos-Richtlinie), Lokale Richtlinien (Überwachungsrichtlinien, Zuweisen von Benutzerrechten, Sicherheitsoptionen), Ereignisprotokoll, Eingeschränkte Gruppen, Systemdienste, Registrierung, Dateisystem, Richtlinien öffentlicher Schlüssel, Richtlinien für Softwareeinschränkung, IP-Sicherheitsrichtlinien*. Bei der Festlegung von Richtlinien für Sicherheitseinstellungen ist zu beachten:

- Kontorichtlinien werden in einer Active Directory Umgebung nur auf Domänenebene durchgesetzt.
- Die Verwendung von Richtlinien für eingeschränkte Gruppen verhindert nicht, dass Modifikationen an Gruppenmitgliedschaften durchgeführt werden können. Die unerlaubten Modifikationen werden bei der nächsten Anwendung der Richtlinien nur rückgängig gemacht.

Der Bereich Administrative Vorlagen wird für die Konfiguration der Windows-Komponenten, des Systems, des Netzes sowie weiterer Anwendungen verwendet.

Anwendungsspezifische Richtlinien

Anwendungsspezifische Richtlinien werden im Bereich *Computerkonfiguration|Administrative Vorlagen* und *Benutzerkonfiguration|Administrative Vorlagen* definiert. Dabei können nicht nur Windows Komponenten wie NetMeeting, Internet Explorer, Windows Explorer, Windows Messenger konfiguriert werden, sondern auch andere Anwendungen, die ihre eigenen administrativen Vorlagen mitbringen, wie es bei Microsoft Office der Fall ist. Solche zusätzlichen administrativen Vorlagen müssen durch Administratoren explizit in eine Gruppenrichtlinie importiert werden.

Für die meisten Behörden und Unternehmen ist es empfehlenswert, alle vorhandenen Möglichkeiten zur zentralisierten anwendungsspezifischen Konfiguration auszunutzen, um durch die zentralisierte Vorgabe von sicherheitsrelevanten Einstellungen viele Sicherheitsrisiken zu beseitigen. Welche Komponenten und/oder Anwendungen zentral durch GPOs konfiguriert werden, ist in Abhängigkeit von der lokalen Umgebung festzulegen. Auch an dieser Stelle sollte die Grundsatzregel gelten, dass alle nicht benötigten Anwendungen bzw. Komponenten zu deaktivieren sind (z. B. Windows Messenger). Die erforderlichen Anwendungen und Komponenten sind so restriktiv wie möglich zu konfigurieren. Wird z. B. Microsoft NetMeeting benötigt, jedoch kein Desktop Sharing verwendet, so ist dieses Merkmal durch die Definition entsprechender Richtlinien zu deaktivieren.

Benutzerspezifische Richtlinien

Windows XP ermöglicht (wie auch schon Windows 2000) die Definition benutzerspezifischer Gruppenrichtlinien, die auf Benutzerbasis angewandt werden. Speziell beim Einsatz in einer Active Directory Umgebung kann dies Sicherheitsvorteile bringen, indem Einschränkungen in Abhängigkeit vom Benutzertyp definiert werden und beispielsweise zwischen normalen und administrativen Benutzern unterschieden wird. Jede Differenzierung lässt sich durch eine geeignete OU-Struktur und die Definition entsprechender Gruppenrichtlinien umsetzen.

Auch die Arbeitsumgebung eines Benutzers kann unter Windows XP durch die Verwendung von Gruppenrichtlinien in ihrer Funktionalität eingeschränkt werden. Insbesondere wird an dieser Stelle empfohlen, durch die Definition der geeigneten Parametereinstellungen die Konfiguration der MMC, des Startmenüs, der Taskleiste, des Desktops, der angezeigten Systemsteuerungskomponenten sowie der zugelassenen Windows-Anwendungen vorzunehmen.

Für die Arbeitsumgebung eines normalen Benutzers sollten nach Möglichkeit folgende Einschränkungen vorgenommen werden:
- Anzeige ausschließlich zugelassener Systemsteuerungskomponenten,
- Sperren der meisten MMC Snap-Ins (das *Zertifikate* Snap-In sollte zugelassen bleiben, wenn Zertifikate zum Einsatz kommen),
- Einschränkungen des Taskplaners,
- Deaktivierung oder Einschränkung des Active Desktops,
- Einschränkungen im Bereich der Start- und Taskleiste.

Bei der Definition von Richtlinien *Nur zugelassene Windows-Anwendungen ausführen* und *Angegebene Windows-Anwendungen nicht ausführen* ist zu beachten, dass diese Einschränkungen nur für den Start der Anwendungen mit dem Windows Explorer gelten. Der Start einer "verbotenen" Anwendung durch den Taskmanager, von der Kommandozeile oder aus einem anderen Programm heraus wird damit also nicht verhindert. Hierfür stehen je nach Notwendigkeit andere Mittel wie Richtlinien für Softwareeinschränkung (englisch Software Restriction Policy) zur Verfügung.

Außerdem sollten die anwendungsspezifischen Richtlinien zur Einschränkung der Anwendungen/Systemkomponenten auf Benutzerbasis verwendet werden.

Einsatz außerhalb von Active Directory-basierten Umgebungen

Beim Einsatz von Windows XP als Stand-alone-Rechner oder in einer Windows NT Domäne sind die zentralen Konfigurationsmöglichkeiten mittels globaler Gruppenrichtlinien nicht verfügbar. In diesem Fall müssen die lokalen Gruppenrichtlinien eines jeden Rechners zur Umsetzung der definierten sicherheits-relevanten Parametereinstellungen benutzt werden. Grundlage ist dabei der in der Planungsphase festgelegte Mechanismus zur Pflege von lokalen Gruppenrichtlinien auf mehreren Rechnern.

Einsatz in Active Directory-basierten Umgebungen

Beim Einsatz von Windows XP Systemen in Active-Directory-basierten Umgebungen (Windows 2000/2003 Domänen) ist der Einsatz lokaler Gruppenrichtlinien auf einzelnen Rechnern ebenfalls möglich. In diesem Fall werden jedoch die Vorteile der zentralen Administration nicht genutzt. Folglich ist es grundsätzlich empfehlenswert, die Active Directory-basierten Gruppenrichtlinien auf der Standort-, Domänenebene bzw. auf Ebene einzelner Organisationseinheiten für die Umsetzung der Sicherheitseinstellungen zu benutzen. Lokale Gruppenrichtlinien auf einzelnen Rechnern sollten aufgrund ihrer schlechten zentralen Verwaltbarkeit nach Möglichkeit nicht eingesetzt werden. Ist jedoch der gemeinsame Einsatz lokaler und Active-Directory-basierter Gruppenrichtlinien aus bestimmten Gründen erforderlich, so müssen die Parametereinstellungen aller Gruppenrichtlinien aufeinander abgestimmt werden.

Die Verwendung von Active-Directory-basierten Gruppenrichtlinien macht die Planung ihres Einsatzes in der Domäne (Windows 2000/2003) erforderlich. Weitere Informationen zu Windows 2000 Active-Directory-basierten Gruppenrichtlinien sind in der Maßnahme M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000* zusammengefasst. Im allgemeinen müssen folgende Aspekte der Verwendung von Active-Directory-basierten Gruppenrichtlinien bedacht werden:

- OU- und Gruppenstruktur im Active Directory,
- Hierarchie der GPOs im Active Directory und generell das GPO-Konzept,
- Vererbung der Gruppenrichtlinien,
- Blockieren und Erzwingen der GPO-Überdeckung,
- Priorisierung bzw. die Festlegung der Reihenfolge bei Abarbeitung mehrerer GPOs,
- Berechnung der jeweils gültigen Einstellungen für einen Gruppenrichtlinienparameter und die GPO Abarbeitungsreihenfolge,
- Steuerung der Abarbeitung von Gruppenrichtlinien,
- Linken der Gruppenrichtlinien,
- GPO-Schutz.

Im Folgenden werden nur die davon abweichenden bzw. ergänzenden Informationen und Empfehlungen gegeben.

Windows XP bringt Änderungen und Neuerungen in der Gruppenrichtlinien-Funktionalität. Neue Features sind durch die aktualisierten clientseitigen Erweiterungen, .adm-Dateien (administrative Vorlagen) und das aktualisierte GPO Snap-in realisiert. Um die neuen Windows XP-spezifischen Merkmale auch in einer Windows 2000 Domäne zu nutzen, müssen die bestehenden Windows 2000 Gruppenrichtlinien aufgerüstet werden. Ein Upgrade erfolgt durch die Anwendung neuer .adm-Dateien und wird beim Laden der zu aktualisierenden Gruppenrichtlinie auf einem Windows XP Domänenmitglied mittels des *Gruppenrichtlinien* Snap-ins realisiert.

Das Upgrade der Gruppenrichtlinien muss unter Umständen wiederholt werden, wenn etwa ein neues Service Pack (SP) auf Windows 2000 Domain Controller angewandt wird. So ist beispielsweise die erneute Aktualisierung der Gruppenrichtlinien nach Installation des Windows 2000 SP4 notwendig.

Die Verwaltung der Windows XP-spezifischen Richtlinien im Active Directory sollte ausschließlich mit einem Windows XP Domänenmitglied erfolgen. Bei der Verwendung des Windows 2000 Gruppenrichtlinien Standard-Snap-ins sind Kompatibilitätsprobleme zu erwarten, die zwar nicht die Funktion der Gruppenrichtlinien, jedoch das Einsehen und das Modifizieren von GPOs beeinträchtigen können.

Die computerspezifischen Gruppenrichtlinien werden während des Boot-Vorgangs angewandt, die benutzerspezifischen Gruppenrichtlinien erst bei der Benutzeranmeldung. Dabei besitzt die benutzerspezifische Gruppenrichtlinie den Vorrang und überschreibt gegebenenfalls Einstellungen, die in der Computer-Richtlinie definiert sind. Für Active Directory-basierte Gruppenrichtlinien bietet sich der sogenannte Loopback-Verarbeitungsmodus an. Dieser stellt sicher, dass eine Computer-Richtlinie nicht von benutzerspezifischen Gruppenrichtlinien ausgehebelt werden kann. Dieser Verarbeitungsmodus sollte vor allem aktiviert werden, wenn sich die Einstellungen ausdrücklich auf den Computer beziehen und von Benutzern unabhängig sein sollen (z. B. ein Windows XP System als Kiosk). Es gibt zwei Varianten der Loopback-Verarbeitung: *Ersetzen* und *Zusammenführen*. Im *Ersetzen*-Modus werden keine benutzerspezifischen Einstellungen gesammelt und die Computer-spezifische Gruppenrichtlinie wird angewandt. Der *Zusammenführen*-Modus führt die Einstellungen der Benutzer GPO mit den Einstellungen der Computer GPO zusammen. Ob eine Gruppenrichtlinie im Loopback-Verarbeitungsmodus und in welcher Variante eingesetzt werden soll, hängt immer vom jeweiligen Einsatzszenario und den Anforderungen der bestehenden Umgebung ab. Je nach Szenario kann dieser Modus sicherheitsrelevante Vorteile bringen, eine allgemeine Empfehlung ist jedoch an dieser Stelle nicht möglich.

Wird eine GPO gleichzeitig auf Windows XP und Windows 2000 Systemen in einer Domäne angewandt, muss auf die Anwendbarkeit der Parametereinstellungen auf diese unterschiedlichen Systeme geachtet werden. Grundsätzlich gilt, dass Windows XP-spezifische Parametereinstellungen von Windows 2000 Systemen ignoriert werden. Das unterschiedliche Verhalten der beiden Betriebssysteme bei gleichen Einstellungen (wie z. B. EFS Richtlinien, M 4.147 *Sichere Nutzung von EFS unter Windows 2000/XP*) ist ebenfalls zu berücksichtigen. Die Information, ab welcher Betriebssystemversion die zu definierenden Einstellungen angewandt werden, ist bei der Festlegung der Gruppenrichtlinien wesentlich, um potentielle Probleme zu vermeiden.

Auch bei Verwendung von Windows XP mit verschiedenen Service Packs ergeben sich Unterschiede bei der Anwendung von Parametereinstellungen einer GPO. So sind für Systeme mit Windows XP Service Pack 2 zusätzliche Sicherheitseinstellungen möglich, die von Systemen ohne Service Pack 2 ignoriert werden. Auch hier gilt: die Information, ab welcher Version die zu definierenden Einstellungen angewandt werden, ist somit bei der Festlegung der Gruppenrichtlinien unbedingt zu beachten.

Die beiden Mechanismen *Sicherheitsfilter* (englisch *Security Filtering*) und *WMI Filter* ermöglichen es, Gruppenrichtlinien differenziert anzuwenden. Der *Security Filtering* Mechanismus gibt Sicherheitsgruppen an, für die die jeweilige Gruppenrichtlinie gilt. Standardmäßig wird eine Gruppenrichtlinie auf *Authentifizierte Benutzer* angewandt. *WMI Filter* steuern die Anwendung einer Gruppenrichtlinie in Abhängigkeit von der Beschaffenheit des Rechners (z. B. Betriebssystem, Service Pack Version, Festplattenplatz). Es sollte beachtet werden, dass Windows 2000-basierte Rechner die definierten *WMI Filters* nicht auswerten und die Gruppenrichtlinie somit immer zum Einsatz kommt. Beide Mechanismen ermöglichen im allgemeinen eine flexible Steuerung der Anwendung einer Gruppenrichtlinie auf ein Benutzer- oder Computer-Objekt im Active Directory. Ihr Einsatz erfordert jedoch genaue Planung und ausreichendes Testen im Vorfeld.

Sicherheitsvorlagen

Die Parametereinstellungen in Gruppenrichtlinien können nicht nur direkt mit dem entsprechenden MMC Snap-In, sondern auch durch den Import einer entsprechenden Sicherheitsvorlage vorgenommen werden. Sicherheitsvorlagen werden zur Konfiguration der Sicherheitseinstellungen verwendet. Sie werden in textbasierter Form in Richtliniendateien gespeichert (INF-Dateien) und können mit dem MMC Snap-In *Sicherheitsvorlagen* oder mit einem gewöhnlichen Texteditor bearbeitet werden. Eine Vielzahl definierter Sicherheitsvorlagen sind sowohl von Microsoft als auch von Drittanbietern frei verfügbar.

Als grundsätzliche Vorgehensweise kann folgendes vorgeschlagen werden:

- Eine bestehende Sicherheitsvorlage wird ausgewählt (z. B. von Microsoft). Die Wahl einer Vorlage mit einem höheren Sicherheitsniveau wie *hisecws* wird dabei empfohlen, da es aus Sicherheitssicht vorteilhafter ist, "sicherere" Einstellungen bei Notwendigkeit abzuschwächen als umgekehrt.

- Die Vorlage muss an lokale Anforderungen angepasst werden, die vorgenommenen Änderungen sind dabei zu begründen und zu dokumentieren.
- Die erstellte Vorlage wird in die entsprechende Gruppenrichtlinie importiert. Um beim Import einer Sicherheitsvorlage in eine Gruppenrichtlinie sicherzustellen, dass alle Einstellungen überschrieben werden, wird die Verwendung der Option *Datenbank vor dem Importieren aufräumen* empfohlen.

Eine weitere Verwendungsmöglichkeit finden die Sicherheitsvorlagen bei der Sicherheitsanalyse vorgenommener Einstellungen. Die aktuell auf einem Computer gültigen Einstellungen können mit denjenigen innerhalb einer INF-Datei verglichen werden. Dies kann entweder mittels des *Sicherheitskonfiguration und -analyse* Snap-Ins der MMC oder mittels des *secedit* Kommandozeilenwerkzeuges erfolgen.

Durch das Anwenden der Sicherheitsvorlage *secsetup.inf*, die sich im Verzeichnis *%SystemRoot%\repair* befindet, können die Standardeinstellungen von Windows XP wiederhergestellt werden.

Definition eigener administrativer Vorlagen

Die sicherheitsrelevanten Einstellungen in Gruppenrichtlinien sind nicht nur im Bereich *Windows-Einstellungen*, sondern auch im Bereich der administrativen Vorlagen zu finden. Administrative Vorlagen bestehen aus einzelnen Parametern, die die Einstellungen zugehöriger Registry-Schlüssel konfigurieren. Die entsprechenden ADM-Dateien bestimmen die einzelnen Parameter, die sich innerhalb der administrativen Vorlagen konfigurieren lassen. Windows XP beinhaltet standardmäßig mehrere ADM-Dateien, die beispielsweise Konfigurationsmöglichkeiten für Internet Explorer beinhalten. Es ist zu beachten, dass die administrativen Vorlagen lediglich Einstellungsparameter und keine Einstellungen definieren und somit nicht zum Speichern und Verteilen der Einstellungen verwendet werden.

Es ist auch möglich, eigene administrative Vorlagen zu definieren. Diese Vorgehensweise empfiehlt sich vor allem, wenn in einem Unternehmen bzw. einer Behörde ein reger Gebrauch von direkten Registry-Einstellungen gemacht wird. Durch die einmalige Definition einer administrativen Vorlage können die entsprechenden Registry-Einstellungen komfortabel über den Gruppenrichtlinien-Mechanismus verteilt werden. Dies stellt unter anderem auch sicher, dass die Registry-Einstellungen tatsächlich auf allen Zielrechnern umgesetzt werden.

Testen der festgelegten Gruppenrichtlinien

Die festgelegten Windows XP Gruppenrichtlinien müssen getestet werden, bevor sie in einer Produktivumgebung eingesetzt werden. Die Tests müssen gewährleisten, dass einerseits die benötigte Funktionalität nicht eingeschränkt wurde und dass andererseits alle sicherheitsrelevanten Einschränkungen korrekt umgesetzt werden.

Ergänzende Kontrollfragen

- Erfolgte eine geeignete Verteilung der Sicherheitseinstellungen auf mehrere GPOs?
- Wurde sichergestellt, dass auf allen Rechnern die richtigen GPOs angewandt werden?
- Sind organisatorische Aspekte für die GPO-Erstellung und -Pflege berücksichtigt worden?

M 2.327 Sicherheit beim Fernzugriff unter Windows XP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Mit Windows XP wurden zwei neue Mechanismen zur Fernsteuerung eines Rechners eingeführt: der Remotedesktop und die Remoteunterstützung. Der Remotedesktop basiert auf der Technologie der Terminaldienste (RDP-Protokoll) und macht eine Anmeldung am System über ein Netz möglich. Die Remoteunterstützung erweitert den Remotedesktop um die Möglichkeit, innerhalb einer bestehenden Sitzung auf die Bildschirminhalte zuzugreifen und gegebenenfalls auch die Steuerung des Rechners zu übernehmen.

Der Remotedesktop wird primär für Wartungsarbeiten auf Windows XP Rechnern über ein Netz eingesetzt. Der Einsatz der Remoteunterstützung ist bei Unternehmen und Behörden vor allem in Szenarien denkbar, wo Mitarbeiter eines internen oder externen Support-Zentrums einem Benutzer die notwendige Hilfestellung geben sollen.

Bei der Benutzung des Remotedesktops ist zu beachten, dass immer nur genau ein Benutzer auf dem Zielrechner angemeldet sein kann. Der Remotedesktop ist in dieser Hinsicht nicht als Ersatz für Terminaldienste zu verstehen.

Die Aktivierung und Deaktivierung des Remotedesktops bzw. der Remoteunterstützung kann mittels entsprechender Gruppenrichtlinienobjekte (*Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Terminaldienste, Benutzerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Terminaldienste* und *Computerkonfiguration* | *Administrative Vorlagen* | *System* | *Remote Unterstützung*) oder lokal über die Systemsteuerung (*System* | *Remote*) erfolgen.

Beim Einsatz von diesen beiden Technologien muss auf folgendes geachtet werden:

- Es sollte starke Verschlüsselung (128-bit, Einstellung *Höchste Stufe*) verwendet werden. Diese muss in der Richtlinie *Verschlüsselungsstufe der Clientverbindung* (festzulegen unter *Computerkonfiguration* | *Windows-Einstellungen* | *Administrative Vorlagen* | *Terminaldienste* | *Verschlüsselung und Sicherheit*) aktiviert werden.
- Es sollte keine automatische Kennwortanmeldung benutzt werden. Dies muss durch die Aktivierung der Richtlinie *Clients bei der Verbindungsherstellung immer zur Kennworteingabe auffordern* unter *Computerkonfiguration* | *Windows-Einstellungen* | *Administrative Vorlagen* | *Terminaldienste* | *Verschlüsselung und Sicherheit* ausgeschaltet werden.
- Die Umleitungen von Zwischenablage, Drucker, Dateiablagen und Smartcard-Anschlüssen, die unter *Computerkonfiguration* | *Windows-Einstellungen* | *Administrative Vorlagen* | *Terminaldienste* | *Client/Server-Datenumleitung* aktiviert und deaktiviert werden, sollten nach Möglichkeit vermieden. werden.

Die Gruppe der berechtigten Benutzer für den Remotedesktop-Zugriff wird entweder über die Zuweisung entsprechender Benutzerrechte in den Richtlinien (Rechte *Anmeldung über Terminaldienste zulassen*, *Anmeldung über Terminaldienste verweigern*) oder über die Systemsteuerung spezifiziert. Standardmäßig ist der entfernte Zugriff für die Gruppe der Administratoren sowie die Gruppe *Remotedesktopbenutzer*, die nach der Installation leer ist, möglich.

Für den Aufbau einer Remoteunterstützungs-Sitzung können folgende zwei Möglichkeiten verwendet werden:
- Die Sitzung wird standardmäßig nur nach einer expliziten Einladung zu Remoteuntertüstzung, die vom Benutzer erstellt wird, aufgebaut.
- Bei geeigneter Konfiguration kann ein Helfer dem Benutzer seine Unterstützung aktiv anbieten.

Der aktuell angemeldete Benutzer muss dem Aufbau einer Sitzung explizit zustimmen. Der Benutzer stellt wegen fehlender Authentisierung die Schwachstelle beim Verbindungsaufbau dar. Aus diesem Grund erfordert der Remoteunterstützungs-Mechanismus einen Umgang mit Bedacht.

Durch die Definition entsprechender Richtlinien ist beim Einsatz der Remoteunterstützung folgendes zu gewährleisten:

- Eine Sitzung sollte nur nach einer expliziten Einladung initiiert werden. Soll das Anbieten der Remoteunterstützung möglich sein, darf der Verbindungsaufbau nur bestimmten Benutzergruppen erlaubt werden (z. B. Support-Mitarbeiter). Die Definition erfolgt hierbei in Form von <*Domänenname*>\<*Benutzername*> oder <*Domänenname*>\<*Gruppenname*>. Eine Auswahl aus vorhandenen Benutzern bzw. Gruppen ist nicht möglich.
- Die maximale Gültigkeitsdauer der Einladung muss auf eine für das Unternehmen bzw. die Behörde annehmbare Größe eingestellt werden.
- Wird eine Einladung zu Remoteunterstützung in einer Datei abgespeichert, so sollte ein Kennwort vergeben werden, um die Gefahr einer unautorisierten Verwendung der Einladung zu verringern.
- Die Steuerungsart (*Helfer dürfen den Computer nur ansehen* bzw. *Helfer dürfen den Computer remote steuern*) sollte nach Möglichkeit restriktiv (*Helfer dürfen den Computer nur ansehen*) gesetzt werden.

Beim Einsatz von Remotedesktop und/oder Remoteunterstützung sind die Auswirkungen auf die Konfiguration und Verwaltung von Firewalls zu berücksichtigen. Grundsätzlich wird empfohlen, keine Remotedesktop- bzw. Remoteunterstützungs-Verbindungen von außerhalb des eigenen Netzes zuzulassen.

Zusammengefasst gilt, dass der Einsatz von Fernsteuerungsmechanismen sehr sorgfältig abgewogen werden muss. Insbesondere aufgrund der bestehenden Unterschiede bei der Benutzerauthentisierung sollten die Vor- und Nachteile des jeweiligen Mechanismus in Betracht gezogen werden. Wird in einem Unternehmen oder einer Behörde kein Gebrauch von Remotedesktop bzw. Remoteunterstützung gemacht, so sind diese unbedingt zu deaktivieren.

Basiseinstellungen für GPOs

Die nachfolgenden Einstellungen gelten nur für den Einsatz beider Fernsteuerungsmechanismen. Soll einer der beiden oder gar beide Mechanismen nicht verwendet werden, so ist dieser zu deaktivieren. Hierfür ist die Modifikation der unten angegebenen Richtlinieneinstellungen notwendig.

Die nachfolgende Tabelle listet Gruppenrichtlinieneinstellungen für Computer auf, die für die Benutzung von Remotedesktop und Remoteunterstützung konfiguriert werden sollten.

Richtlinie	Status	Einstellung
Computerkonfiguration | Windows-Einstellungen | Administrative Vorlagen | Terminaldienste | Verschlüsselung und Sicherheit | Verschlüsselungsstufe der Clientverbindung festlegen	Aktiviert	Höchste Stufe
Computerkonfiguration | Windows-Einstellungen | Administrative Vorlagen | Terminaldienste | Verschlüsselung und Sicherheit | Clients bei der Verbindungsherstellung immer zur Kennworteingabe auffordern	Aktiviert	
Computerkonfiguration | Windows-Einstellungen | Administrative Vorlagen | Terminaldienste | Client/Server-Datenumleitung | *	Aktiviert/ Deaktiviert	
Computerkonfiguration | Administrative Vorlagen | System | Remote Unterstützung |Remoteunterstützung anbieten	Deaktiviert	
Computerkonfiguration | Administrative Vorlagen | System | Remote Unterstützung | Angeforderte Remoteunterstützung	Aktiviert	Helfer dürfen den Computer remote steuern Maximale Gültigkeitsdauer: 8 Stunden

Tabelle: Gruppenrichtlinieneinstellungen für Computer

Die nachfolgende Tabelle listet Gruppenrichtlinieneinstellungen für Benutzer auf, die für die Benutzung von Remotedesktop und Remoteunterstützung konfiguriert werden sollten.

Richtlinie	Status	Einstellung
Benutzerkonfiguration | Windows-Einstellungen | Administrative Vorlagen | Terminaldienste | Regeln für Remoteüberwachung von Terminaldienste-Benutzersitzungen festlegen	Aktiviert	Vollzugriff mit Erlaubnis des Benutzers
Benutzerkonfiguration | Windows-Einstellungen | Administrative Vorlagen | Terminaldienste |Client | Speichern von Kennwörtern nicht zulassen	Aktiviert	

Tabelle: Gruppenrichtlinieneinstellungen für Benutzer

Ergänzende Kontrollfragen

- Wurde der Einsatz von Fernsteuerungsmechanismen von Windows XP sorgfältig abgewogen?
- Wurden die Fernsteuerungsmechanismen vollständig deaktiviert, wenn deren Einsatz nicht vorgesehen ist?
- Sind die Benutzer im sicheren Umgang mit der Remoteunterstützung geschult worden?

M 2.328 Einsatz von Windows XP auf mobilen Rechnern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Beim Einsatz von Windows XP auf mobilen Rechnern ist wie für alle anderen mobilen PCs der Baustein B 3.203 Laptop zu beachten.

Datenverschlüsselung

Mobile Computer befinden sich häufig in Umgebungen, die deutlich niedrigere Sicherheit als geschützte Büroumgebungen bieten. Daher sollten die auf dem mobilen Rechner befindlichen schützenswerten Daten verschlüsselt werden (siehe auch M 4.29 *Einsatz eines Verschlüsselungsproduktes für tragbare PCs*). Neben einer Reihe von Drittprodukten können zur Verschlüsselung auch die integrierten Windows XP Mechanismen eingesetzt werden:

- Das verschlüsselnde Dateisystem (EFS, Encrypting File System),
- Verschlüsselung der Offlinedateien.

Informationen zur sicheren Nutzung von EFS sind in der Maßnahme M 4.147 *Sichere Nutzung von EFS unter Windows 2000/XP* zu finden.

Das Konzept der Offlinedateien wurde mit Windows 2000 eingeführt. Offlinedateien sind im Grunde genommen Kopien von Dokumenten, die sich auf einer Netzwerkfreigabe befinden. Sie werden auf dem lokalen Computer in einer Datenbank gespeichert, so dass der Zugriff auf Dokumente auch dann erhalten bleibt, wenn die Netzwerkfreigabe nicht erreichbar ist.

Die Möglichkeit, diese Offlinedateien zu verschlüsseln, wurde unter Windows XP eingeführt. Der gesamte Speicher für Offlinedateien, der Dateien aller Benutzer beinhaltet, wird mit einem computerspezifischen Schlüssel verschlüsselt. Die Verschlüsselung ist transparent für Benutzer und kann nur von Administratoren aktiviert bzw. deaktiviert werden. Die Aktivierung kann durch die Ordner-Eigenschaften im Windows Explorer unter *Extras* | *Ordneroptionen* | *Offlinedateien* | *Offlinedateien verschlüsseln, um Daten zu schützen* oder in Gruppenrichtlinien unter *Computerkonfiguration* | *Administrative Vorlagen* | *Netzwerk* | *Offlinedateien* | *Offlinedateicache verschlüsseln* erfolgen. Die Aktivierung der Offlinedateien-Verschlüsselung empfiehlt sich insbesondere für den Fall, wenn zu synchronisierende Originaldokumente verschlüsselt sind und die lokalen Offline-Kopien in entschlüsselter Form vorliegen können.

Die Strategie zum Schutz der auf einem mobilen Rechner befindlichen Daten (Windows XP EFS, Offlinedateien-Verschlüsselung oder Verschlüsselung mit einem Drittprodukt) ist nach Bedarf anhand der konkreten Umstände und im Einzelfall festzulegen.

Lokale Firewall

Im Gegensatz zu stationären organisationsinternen Desktops, besteht bei mobilen Clients die Möglichkeit, dass sie direkt an das Internet angeschlossen werden. Schutz durch eine lokal installierte Firewall ist in diesem Fall unabdingbar.

Mit Windows XP wurde eine neue Funktionalität eingeführt - die Internet Connection Firewall (ICF), die mit dem Service Pack 2 in Windows-Firewall umbenannt wurde. Die Windows-Firewall ist ein zustandsbehafteter Paketfilter, der jedes TCP/IP oder UDP Paket analysiert und entsprechend der Konfiguration abarbeitet.

Windows XP Service Pack 2 enthält unter anderem folgende Verbesserungen für die ICF/Windows-Firewall:
- Standardmäßig aktiviert für alle Interfaces
- Schutz schon beim Booten
- Zentrale Konfiguration über GPOs
- Quell-Adresseneinschränkung für Port
- Kommandozeilenunterstützung
- Lock-Down Modus
- Ausnahmelisten für Applikationen
- Mehrere Policy Profile möglich
- RPC Unterstützung
- Rücksetzen auf Herstellerkonfiguration
- Unterstützung der unbeaufsichtigten Installation

Die Windows-Firewall filtert ausschließlich eingehende Verbindungen. Ausgehende Pakete werden hingegen keinen Restriktionen unterworfen. Dies bedeutet, dass z. B. eine Einschränkung der zugreifbaren Internetserver mit der Windows-Firewall nicht möglich ist. Programme, die für den Internet-Zugriff berechtigt sein sollen, können nicht festgelegt und kontrolliert werden. Daher bietet die Windows-Firewall keinen Schutz vor Trojanern, die sich bereits auf dem Rechner befinden.

Der Einsatz von der ICF (vor Service Pack 2) im Unternehmens- oder Behördenkontext ist durch die fehlenden zentralen Konfigurationsmöglichkeiten nur schwer möglich. Durch die Gruppenrichtlinie *Computerkonfiguration* | *Administrative Vorlagen* | *Netzwerk* | *Netzwerkverbindungen* | *Verwendung des Internetverbindungsfirewalls im eigenen DNS-Domänennetzwerk nicht zulassen* lässt sich die ICF lediglich komplett deaktivieren. Die Konfiguration der ICF erfolgt für jede Netzschnittstelle gesondert lokal auf dem Windows XP System.

Mit Einführung von Service Pack 2 besteht für Administratoren jetzt auch die Möglichkeit zur zentralen Verwaltung der Windows-Firewall durch Gruppenrichtlinien unter *Computerkonfiguration* | *Administrative Vorlagen* | *Netzwerk* |*Netzwerkverbindungen* | *Windows-Firewall*. Bei der Konfiguration der Windows-Firewall können verschiedene Profile angelegt werden, so dass die Windows-Firewall je nach aktueller Umgebung (organisationsinternes Netz oder mobiler Einsatz) unterschiedlich konfiguriert werden kann. Denkbar ist an dieser Stelle, dass in einem organisationsinternen Netz gewisse Ausnahmen für den eingehenden Verkehr zugelassen werden (z. B. für den Fernzugriff auf den Rechner). Hingegen für den mobilen Einsatz sollte die Windows-Firewall keine Ausnahmen zulassen und den gesamten eingehenden Verkehr blockieren. Ist ein Domain Controller in der Reichweite des Clients, so wird das Domänenprofil angewandt, ansonsten wird das mobile Profil aktiviert.

Die Windows-Firewall wird nach der Installation des Service Packs 2 standardmäßig auf allen vorhandenen Netzschnittstellen aktiviert. Dies kann, je nach vorhandenem Kontext im jeweiligen Unternehmen oder in der Behörde, unter Umständen auch zu Problemen führen (siehe auch M 2.329 *Einführung von Windows XP SP2*).

Sowohl die ICF als auch die Windows-Firewall bieten die Möglichkeit der Protokollierung an. Diese ist nach der Firewall-Aktivierung standardmäßig deaktiviert und muss explizit aktiviert werden. Dabei ist die Aktivierung der Protokollierung getrennt für angenommene und verworfene Pakete möglich, so dass die Protokollierung den individuellen Bedürfnissen angepasst werden kann. Die Protokollierung erfolgt im vom W3C standardisierten Extended Log File Format. Ist die maximale Größe der Protokolldatei erreicht, so wird eine Kopie der Datei mit der angehängten Dateinamenerweiterung *old* erzeugt. Erreicht die Protokolldatei erneut die Maximalkapazität, werden die gesicherten Protokolldaten überschrieben und gehen verloren. Aus diesem Grund ist auf die ausreichende Größe der Protokolldatei zu achten. Da die Protokollierungsdaten lokal abgelegt werden, muss ein Mechanismus zum Sammeln der Daten realisiert werden. Windows XP stellt in dieser Hinsicht keinen eigenen Mechanismus zur Verfügung.

Sollen Windows XP Rechner vor Angriffen aus dem lokalen Netz oder Internet (mobiler Einsatz) geschützt werden, ist der Einsatz einer Personal Firewall eines Drittanbieters in der Regel empfehlenswerter, da diese meist einen erweiterten Funktionsumfang besitzt (z. B. Filtern ausgehender Verbindungen oder Einschränkung berechtigter Programme für den Internet-Zugriff).

Ist keine Personal Firewall installiert und aktiviert, so sollte bei einem mobilem IT-System zumindest die Windows-Firewall (bzw. ICF vor SP2) eingerichtet werden (siehe auch Maßnahmen M 5.91 *Einsatz von Personal Firewalls für Internet-PCs*).

Ergänzende Kontrollfragen:

- Welche Mechanismen werden zum Schutz der Windows XP Systeme vor Angriffen verwendet?

M 2.329 Einführung von Windows XP SP2

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator

Seit August 2004 ist das Windows XP Service Pack 2 von Microsoft erhältlich (siehe hierzu auch h*ttp://www.bsi.bund.de/fachthem/betriebssysteme/winxp/spzwei/sp_zwei.htm*). Am 12.April 2005 endet der Zeitraum, in dem die Installation von SP2 mit einem speziellen Tool von Microsoft trotz aktivierten internetbasierten Windows-Update-Dienstes verhindert werden kann. Nur Organisationen, die einen eigenen Update-Server betrieben, können die Installation von SP2 weiterhin verhindern.

Das Service Pack 2 enthält neben Fehlerkorrekturen und Verbesserungen an vorhandenen Mechanismen auch einige sicherheitsrelevante Änderungen oder Erweiterungen. Zu nennen sind hier beispielsweise:

- Insgesamt mehr als 600 neue Sicherheitsrichtlinien (Windows-Firewall, Security Center, Internet Explorer usw.)
- Verbesserungen in der Windows-Firewall (früher Internet Connection Firewall, ICF), vor allem die Möglichkeit zur zentralen Administration.
- Verbesserungen im Internet Explorer: Add-on Management, Pop-up Blocker, Zone Elevation Blocking, konsistente MIME-Verarbeitung, Restriktivere Behandlung von ActiveX-Steuerelementen.
- Integration von Virenschutzsoftware von Drittherstellern in das sogenannte "Sicherheitscenter", das zur zentralen Verwaltung und Überwachung von Windows Sicherheitseinstellungen gedacht ist.
- Speicherschutz gegen Buffer Overflows: Der Systemkern und die Bibliotheken wurden mit spezifischen Compiler-Flags übersetzt, das einen Schutz gegen Buffer Overflows gewährleisten soll. Dieses "No Execute" Flag (NX) wird von einigen aktuellen Prozessoren benutzt.
- Markierung von heruntergeladenen Dateien und Anhängen auf NTFS-Laufwerken (Attachment Execution Service).
- Die Benutzung von Raw-Sockets und die direkte Manipulation von IP-Paketen wurden deutlich eingeschränkt, Denial-of-Service Vorkehrungen sind in den TCP/IP Stack integriert.
- USB-Schreibschutz wurde implementiert, so dass mit einer geeigneten Konfiguration nur lesender Zugriff auf USB-Speichergeräte wie USB-Sticks und USB-Platten möglich ist (so wird ein unberechtigter Datenexport auf USB-Medien verhindert).

Die Konfiguration neuer Einstellungen und insbesondere Gruppenrichtlinieneinstellungen muss im Vorfeld der SP2-Installation festgelegt werden. Änderungen in Gruppenrichtlinien können weitreichende Auswirkungen in Unternehmen und Behörden mit Windows XP Clients haben und müssen daher von Administratoren unbedingt sorgfältig durchgeführt werden.

Problemen vorbeugen

Aufgrund der umfangreichen Veränderungen besteht insbesondere bei größeren Installationen in Unternehmen oder Behörden die Gefahr, dass die Installation des Service Packs 2 zu Problemen führen kann. Dies ist besonders dann kritisch, wenn Anwendungen nicht mehr lauffähig sind oder Firewall- und Antivirus-Programme betroffen werden. Um diese Probleme zu vermeiden, muss die Einführung von SP2 genauestens geplant und zunächst ausgiebig getestet werden. Vor allem die Funktionsfähigkeit der Anwendungssoftware muss im Vorfeld überprüft werden.

Folgende Probleme können durch die Installation von Service Pack 2 verursacht werden:

- Probleme bei der Verwaltung der GPOs mit alten Werkzeugen, da neue administrative Vorlagen lange Zeichenketten enthalten
- MMC Snap-In *Gruppenrichtlinienergebnissatz* funktioniert bei Remote-Anfragen nicht mehr aufgrund der standardmäßig nach der Installation aktivierten Firewall
- Probleme bei DCOM-Anwendungen, da ein neues DCOM-Authentisierungsmodell eingeführt wurde (z. B. bei Delegation von Gruppenrichtlinienergebnissatz-Aufgaben an nicht-administrative Benutzer)
- Anwendungsprobleme aufgrund der standardmäßig aktivierten Firewall
- Anwendungsprobleme aufgrund der Änderungen am TCP/IP-Stack (Einschränkung der Benutzung von Raw-Sockets)
- Skript- und ActiveX-Fehlermeldungen, Bilddarstellungsprobleme beim Öffnen gespeicherter Web-Seiten in Anwendungen (unter anderem auch in Microsoft Office Produkten)
- Zusatzsoftware wird automatisch mit installiert (Windows Movie Maker). Diese muss unter Umständen wieder entfernt werden.

Zu den genannten Problemen gibt es mittlerweile im Internet und Fachzeitschriften eine Vielzahl von Lösungsvorschlägen, über die sich die Administratoren vor dem Auspielen von SP 2 informieren sollten.

Ergänzende Kontrollfragen:

- Wurde die Anwendungskompatibilität überprüft?
- Ist die Festlegung der Konfiguration für neue Einstellungen erfolgt?

M 2.330 Regelmäßige Prüfung der Windows XP Sicherheitsrichtlinien und ihrer Umsetzung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator,

Um Verstöße gegen die geltenden Windows XP Sicherheitsrichtlinien feststellen zu können, sind regelmäßige Überprüfungen notwendig. Diese Prüfungen sollten ein fester Bestandteil eines organisatorischen Prozesses sein. Die Ergebnisse der Überprüfungen sind zu dokumentieren, um auch Wiederholungsfälle feststellen zu können.

Folgende Aspekte sind dabei zu berücksichtigen:

- Die existierenden Sicherheitsrichtlinien müssen auf ihre Aktualität und Konsistenz überprüft werden. Im Laufe der Zeit werden natürlich neue Erkenntnisse über sicherheitsrelevante Aspekte von Windows XP gewonnen, diese sind bei der Überprüfung der Sicherheitsrichtlinien angemessen zu berücksichtigen. Die Sicherheitsrichtlinien müssen gegebenenfalls angepasst und neu umgesetzt werden.
- Die Windows XP Sicherheitsrichtlinien müssen sorgfältig umgesetzt werden. Zur Ermittlung aktuell umgesetzter Einstellungen bzw. ihrer etwaigen Unterschiede von den in Sicherheitsrichtlinien definierten Parameterwerte können automatisierte Tools wie *secedit* eingesetzt werden (siehe auch Maßnahme M 4.243 *Windows XP Verwaltungswerkzeuge*).
- Zugriffsberechtigungen im Dateisystem, Registry und Netzwerkfreigaben müssen auf ihre Konsistenz hin geprüft werden. Benutzer dürfen nur die benötigten Berechtigungen besitzen.
- Benutzerberechtigungen (Systemberechtigungen) sind ebenfalls zu überprüfen.
- Änderungen, die sich aus der Installation neuer und dem Entfernen alter Software (Windows-Komponenten oder Anwendungssoftware von Drittherstellern) ergeben, sind angemessen zu berücksichtigen. Die dadurch resultierenden Änderungen der Sicherheitseinstellungen (Gruppenrichtlinienobjekte, Zugriffsberechtigungen usw.) sind umzusetzen, wobei für kritische Änderungen eine Sicherheitsanalyse durchzuführen ist.

Des weiteren ist die Maßnahme M 2.10 *Überprüfung des Hard- und Software-Bestandes* bei Überprüfungen zu beachten, um die Nutzung von nicht-freigegebener Software fest- und abstellen zu können.

Ergänzende Kontrollfragen:

- Wurde ein interner organisatorischer Prozess für die regelmäßige Prüfung der Windows XP Sicherheitsrichtlinien und ihrer Umsetzung definiert?
- Sind Maßnahmen definiert worden, um Verstöße gegen existierende Sicherheitsrichtlinien erkennen und abstellen zu können?

M 2.331 Planung von Besprechungs-, Veranstaltungs- und Schulungsräumen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter Organisation

Verantwortlich für Umsetzung: Leiter Organisation, Mitarbeiter

Von der geplanten Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen hängt nicht nur die Wahl der Ausstattung, sondern auch die erforderlichen Sicherheitsmaßnahmen ab. Daher sollte zunächst dokumentiert werden, welche Nutzungsarten für welche Räume vorgesehen sind und basierend auf den Anforderungen aus den geplanten Einsatzszenarien die Einrichtung auszuwählen und organisatorische und technische Nutzungsregelungen festzulegen.

Die Lage von Besprechungs-, Veranstaltungs- und Schulungsräumen sollte möglichst so gewählt werden, dass Fremde nicht unnötig durchs Haus laufen müssen, also möglichst nah zu/zum

- Eingang
- Sanitären Einrichtungen
- Kantine

Der Weg zu einem Besprechungs-, Veranstaltungs- und Schulungsraum sollte möglichst nicht in die Nähe von oder gar durch besonders sicherheitsrelevante Bereiche führen. Ebenso sollten Besprechungs-, Veranstaltungs- und Schulungsräume so ausgewählt und eingerichtet sein, dass sie zu möglichst geringen Störungen des normalen Betriebs führen.

Die Wege zu einem Besprechungs-, Veranstaltungs- und Schulungsraum, zu den sanitären Einrichtungen und zur Kantine sollten gut erkennbar markiert sein. Dadurch wird es vermieden, dass sich Personen auf der Suche danach verlaufen. Ebenso entzieht es Personen, die sich absichtlich "versehentlich" verlaufen, die Argumentationsgrundlage.

Es sollte ein Raumbuchungssystem eingesetzt werden, aus dem auch nachträglich ersichtlich ist, wer die Räume genutzt hat. Dadurch können auch Ausweichmöglichkeiten leicht erkannt werden.

Ergänzende Kontrollfragen:

- Ist dokumentiert, für welche Räume welche Nutzungsarten vorgesehen sind?
- Sind Besprechungs-, Veranstaltungs- und Schulungsräume so angelegt worden, dass sie zu möglichst geringen Störungen des normalen Betriebs führen?

M 2.332 Einrichtung von Besprechungs-, Veranstaltungs- und Schulungsräumen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement, Leiter Organisation

Verantwortlich für Umsetzung: Leiter Haustechnik, Leiter Organisation

Besprechungs-, Veranstaltungs- und Schulungsräume sind entweder für einen der genannten Zwecke fest einzurichten oder (bei wechselnder Nutzung) so zu möblieren, dass sie der jeweils aktuellen Nutzung optimal angepasst werden können.

In Schulungsräumen sind die Arbeitsplätze hinsichtlich Zahl und Anordnung der IT-Geräte sowie Platzangebot so zu gestalten, dass gegenseitige Störungen vermieden werden und dass an jedem Platz ausreichend Fläche vorhanden ist, um Unterlagen, Schreibblöcke etc. problemlos handhaben zu können.

Die Besprechungs-, Veranstaltungs- und Schulungsräume müssen geeignet ausgestattet werden. Dazu gehören beispielsweise Kommunikations- und Medienunterstützung wie Beamer oder Flipcharts. Für die Einrichtung sollten unter anderem folgende Aspekte berücksichtigt werden:

- Es sollten sich sinnvollerweise dort Stromanschlüsse befinden, wo Beamer, Laptops oder andere Verbraucher aufgestellt werden sollen. Sie sollten auch in genügender Anzahl für typischerweise mitgebrachte IT-Systeme wie Laptops vorhanden sein. Dies dient auch der IT-Sicherheit, da sonst IT-Geräte durch wilde Verkabelung und Unachtsamkeit hinunterfallen oder anderweitig Schaden nehmen können.
- Die Stromversorgung eines Besprechungs-, Veranstaltungs- und Schulungsraums ist aus der letzten Unterverteilung heraus getrennt von anderen Räumen aufzubauen. Dadurch wirken sich Beeinträchtigungen der Energieversorgung nicht auf andere Räume aus. Optimal ist eine eigene Unterverteilung im Besprechungs-, Veranstaltungs- und Schulungsraum. Damit entfällt die Notwendigkeit, nach dem Ansprechen eines Sicherungselements die irgendwo anders im Gebäude befindliche Unterverteilung zu suchen.
- Es sollte mindestens ein Festnetz-Telefonanschluß vorhanden sein, um die Erreichbarkeit auch während Veranstaltungen zu gewährleisten. Dies ist insbesondere wichtig, wenn Mobiltelefone während Veranstaltungen ungenutzt bleiben sollen oder sogar ein Handy-Verbot ausgesprochen wurde. Für interne Verbindungen ist er dauerhaft freizuschalten. Für externe kommende und gehende Verbindungen ist er zum Schutz gegen Missbrauch nur bei Bedarf durch befugte Personen freizuschalten.
- Es muss überlegt werden, ob Netzsteckdosen für den Anschluss ans Internet oder interne Netze eingerichtet werden sollen. Da dies für interne Netze eine Vielzahl von Gefährdungen mit sich bringen kann, müssen solche Netzzugänge entsprechend abgesichert sein (siehe auch M 2.204 *Verhinderung ungesicherter Netzzugänge*). Wenn ein Internet-Zugang erforderlich ist, sollte überlegt werden, diesen nicht über das Intranet, sondern getrennt zu führen.

- Bei der Einrichtung eines WLANs in Besprechungs-, Veranstaltungs- und Schulungsräumen müssen alle erforderlichen Sicherheitsmaßnahmen eingesetzt werden.

Ergänzende Kontrollfragen:

- Sind Besprechungs-, Veranstaltungs- und Schulungsräume so eingerichtet, dass sie eine optimale und sichere Umgebung für Gespräche mit Externen bieten?

M 2.333 Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter Organisation

Verantwortlich für Umsetzung: Leiter Organisation, Benutzer

Für die Nutzung dieser Räume sollte es in jeder Organisation feste Regeln geben. Diese sollte unter anderem Verhaltenshinweise genereller Art für die Benutzer umfassen, aber auch solche zur Benutzung sowohl fest installierter als auch mitgebrachter Geräte.

Dabei sollten unter anderem folgende Aspekte berücksichtigt werden:

- Externe Teilnehmer von Besprechungen oder Schulungen sollten außerhalb der Besprechungs- und Schulungsräume nicht unbeaufsichtigt bleiben (siehe auch M 2.16 *Beaufsichtigung oder Begleitung von Fremdpersonen*).
- Es muss geklärt werden, unter welchen Rahmenbedingungen Externe mitgebrachte IT-Systeme wie Handys oder Laptops einsetzen dürfen.
- Vorhandene Festnetz-Telefonanschlüsse müssen vor Missbrauch geschützt werden, beispielsweise indem die Anwahl externer Nummern nur nach einer Passwort-Eingabe möglich ist.
- Im Raum sollten die Telefonnummern von Ansprechpartnern für Probleme wie IT-Support oder Schlüsselverwaltung ausgehängt oder ausgelegt sein. Die Ansprechpartner müssen jederzeit während der üblichen Bürozeiten erreichbar sein.
- Wenn im Raum ein Beamer und weitere Geräte fest eingerichtet sind, müssen die erforderlichen Sicherheitsmaßnahmen zum Schutz dieser Geräte vor Diebstahl getroffen werden. Beispielsweise können diese mit Diebstahlsicherungen wie Stahlkabeln versehen werden. Auch verschließbare Schränke für Materialen sind sinnvoll.
- Nach Ende jeder Veranstaltung sollte alles Material entfernt werden, das sensitive Informationen enthalten könnte. Daher sollte z. B. benutztes Flipchart-Papier mitgenommen und Tafeln gesäubert werden. Auch im Papierkorb gelandete Entwürfe dürfen nicht vergessen werden.

Aufräumen schützt Informationen

- In Besprechungs-, Veranstaltungs- und Schulungsräumen sind häufig fest installierte IT-Systeme wie z. B. Schulungsrechner vorhanden. Hierfür ist folgendes zu beachten:
  - Die IT in Besprechungs- und Schulungsräumen muss entsprechend den Erfordernissen konfiguriert und administriert werden (siehe auch M 4.225 *Einsatz eines Protokollierungsservers in einem Sicherheitsgateway*). Es ist festzulegen, wer für die Administration der Schulungsrechner zuständig ist. Außerdem müssen Ansprechpartner für immer wieder gerne auftretende Probleme benannt sein. Diese müssen auch kurzfristig helfen können.

  - In Räumen mit Schulungsrechnern sollte nichts mitgebracht werden dürfen, was die Funktionsfähigkeit der IT-Systeme beeinträchtigen könnte, also weder Getränke noch klebrige Pausenriegel. Das heißt dann auch, dass Kaffeepausen außerhalb des Raumes stattfinden müssen.
- Es muss klare Regelungen für Zugriffe auf LAN- und TK-Schnittstellen aus Besprechungs- und Schulungsräumen geben.
- Außerdem sollten Hinweise auf Fluchtwege und das richtige Verhalten bei Bränden nicht vergessen werden (siehe M 1.6 *Einhaltung von Brandschutzvorschriften*).

Bei aufgetretenen Problemen wie fehlendem Papier für Flipcharts oder defekten Geräten sollten die zuständigen Ansprechpartner informiert werden, damit diese zeitnah behoben werden können.

Abschließen von Besprechungs-, Veranstaltungs- und Schulungsräumen

Bei Besprechungs-, Veranstaltungs- und Schulungsräumen stehen grundsätzlich zwei Lösungen für den Verschluss solcher Räume im Widerspruch. Wird der Raum außer bei Benutzung ständig verschlossen gehalten, ist zwar die darin befindliche IT gut gegen eine Reihe von Gefährdungen geschützt, eine spontane Nutzung des Raumes ist allerdings nicht möglich. Ständig offene Besprechungs-, Veranstaltungs- und Schulungsräume hingegen sind zwar jederzeit nutzbar, zugleich ist aber das Risiko für die IT deutlich höher. Sie abzuschließen hat außerdem den Vorteil, dass die Einrichtung der Schulungsräume sich eher in dem gewünschten Zustand befindet. Aus Sicht der IT-Sicherheit sind Besprechungs-, Veranstaltungs- und Schulungsräume also außerhalb der Nutzungszeit verschlossen zu halten. Gleichzeitig ist natürlich sicherzustellen, dass der Zutritt bei Bedarf angemessen rasch und einfach zu realisieren ist. Die Schlüssel für die Besprechungs-, Veranstaltungs- und Schulungsräume sollten von einer zentralen Stelle verwaltet werden (z. B. Pforte oder innerem Dienst).

Wohin mit Laptops und Dokumenten?

In Besprechungs-, Veranstaltungs- und Schulungsräume gibt es meistens keine Möglichkeit, Unterlagen, IT-Systeme und ähnliches gesondert einzuschließen. Daher sollte es möglich sein, solche Räume zumindest dann, wenn alle Teilnehmer einer Veranstaltung den Raum verlassen, abzuschließen oder ihn durch einen internen Mitarbeiter beaufsichtigen zu lassen.

M 2.334 Auswahl eines geeigneten Gebäudes

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter Innerer Dienst

Verantwortlich für Umsetzung: Innerer Dienst

Neben der Standortplanung (siehe M 1.16 *Geeignete Standortauswahl*), die das Umfeld eines Gebäudes betrachtet, muss ein Gebäude hinsichtlich seiner inneren Eignung beurteilt werden. Grundsätzlich ist natürlich schon bei der Gebäudeauswahl zu prüfen, ob alle für die spätere Nutzung relevanten Maßnahmen dann auch umgesetzt werden können.

Für einige dieser Maßnahmen können die Voraussetzung nachträglich jedoch nur mit extrem hohem Aufwand oder gar nicht geschaffen werden. Diese Maßnahme soll daher bei der Auswahl eines bestehende Gebäudes helfen, typischerweise erst später auftretende Probleme im Vorfeld so weit wie möglich zu vermeiden. Sie kann aber auch bei der Planung eines Neubaus hilfreich sein.

Einzelne Aspekte sind je nachdem, ob das Gebäude gekauft oder gemietet wird, unterschiedlich relevant. Aus Sicht der IT-Sicherheit ist unter anderem folgendes hinsichtlich des Zustandes der Bausubstanz zu beachten:

- Ermöglicht die Statik (maximale Deckentraglast, tragende Wände) die Einrichtung von Räumen mit hoher Flächenlast (Serverraum, RZ, USV etc.) dort, wo sie arbeitsökonomisch und aus Sicht der IT-Sicherheit sinnvoll anzuordnen wären (siehe auch M 1.13 *Anordnung schützenswerter Gebäudeteile*, M 1.47 *Eigener Brandabschnitt* (für RZ))?
- Lassen sich die vorhandenen oder zusätzlich erforderliche Erschließungswege (Flure, Treppenhäuser, Aufzüge) so nutzen und einrichten, dass Maßnahmen wie z. B. M 2.17 *Zutrittsregelung und -kontrolle* auch sinnvoll umzusetzen sind?

  Ist es auf Grund der Erschließungswege möglich, Bereiche mit hohen Sicherheitsanforderungen von solchen mit niedrigen zu getrennt, so dass z. B. Schulungsräume außerhalb des Entwicklungsbereiches liegen?
- Lassen sich die vorhandenen oder zusätzlich erforderliche Erschließungswege (Flure, Treppenhäuser, Aufzüge) jederzeit für den Transport auch größerer IT-Komponenten nutzen? Ist dies nicht gewährleistet, kann der Wiederanlauf nach einem Hardwareschaden unter Umständen stark verzögert werden.
- Gibt es (Bau-)Auflagen (Wegerechte, Denkmalschutz etc.), die einer bedarfsgerechten Nutzung des Gebäudes hinderlich sein können? Besonders auf Wegerechte Dritter ist hier zu achten, da diese mit erforderlichen zutrittsgeschützten Bereichen kollidieren können.
- Ist eine Raumverteilung möglich, so dass die Maßnahmen M 1.8 *Raumbelegung unter Berücksichtigung von Brandlasten* und M 1.51 *Brandlastreduzierung* umgesetzt werden können?
- Lassen sich die Maßnahmen M 1.3 *Angepasste Aufteilung der Stromkreise* und M 1.39 *Verhinderung von Ausgleichsströmen auf Schirmungen* mit vertretbarem Aufwand umsetzen?

- Gibt es einen äußeren Blitzschutz? Wenn ja, hat dies Einfluss auf Details der Umsetzung der Maßnahmen M 1.25 *Überspannungsschutz* und M 1.39 *Verhinderung von Ausgleichsströmen auf Schirmungen*?

Bei Mietobjekten sind zusätzlich folgende Aspekte zu berücksichtigen:

- Erhält der Mieter alle für die geeignete Herrichtung des Gebäudes erforderlichen Rechte? Welche Rechte und Einspruchsmöglichkeiten behält sich der Vermieter vor?
- Müssen Sicherheitseinrichtung nach Ende des Mietverhältnisses zurückgebaut werden? Es muss in der Planungsphase sichergestellt werden, dass wegen solcher Zusatzkosten nicht auf erforderliche Sicherheitsmaßnahmen verzichtet wird.
- Wenn das Gebäude gleichzeitig von Dritten genutzt wird, ist zu klären, in wie weit dadurch die Umsetzung von Maßnahmen erschwert oder gar verhindert wird.
- Erhält man als Mieter ein Mitspracherecht bei einer späteren Neuvermietung dritt-genutzter Gebäudeteile? Es kann durchaus sein, dass ein neuer Mitnutzer des Gebäudes als sicherheitskritischer angesehen werden muss als der bisherige.

  Beispiel: Die Personalabteilung eines kleinen Schulbuch-Verlages zieht aus und als Nachmieter richtet dort eine politisch oder gesellschaftlich sehr umstrittene Organisation ein Büro ein.

Ergänzende Kontrollfragen:

- Werden Sicherheitsaspekte bei der Auswahl eines geeigneten Gebäudes berücksichtigt?

M 2.335 Festlegung der IT-Sicherheitsziele und -strategie

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter

Informationssicherheit ist ein wichtiger Erfolgsfaktor, um die Ziele und Aufgaben eines Unternehmens bzw. einer Behörde erfüllen zu können. Informationssicherheit ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess, der auch als solches in allen Geschäftsprozessen und den Köpfen aller Mitarbeiter verankert werden muss. Der IT-Sicherheitsprozess muss durch die Behörden- bzw. Unternehmensleitung initiiert und etabliert werden. Zunächst müssen angemessene IT-Sicherheitsziele sowie eine Strategie festgelegt werden. Neben den strategischen Leitaussagen müssen konzeptionelle Vorgaben erarbeitet und die organisatorischen Rahmenbedingungen geschaffen werden, um das ordnungsgemäße und sichere IT-gestützte Arbeiten des Unternehmens oder der Behörde zu ermöglichen.

IT-Sicherheitsziele

Die IT-Sicherheitsziele sollten zu Beginn jedes Sicherheitsprozesses sorgfältig bestimmt werden. Anderenfalls besteht die Gefahr, dass IT-Sicherheitskonzepte erarbeitet werden, die die eigentlichen Anforderungen der Behörde bzw. des Unternehmens verfehlen. IT-Sicherheit hilft, die grundlegenden Ziele und Aufgaben eines Unternehmens bzw. einer Behörde zu erreichen. Die Grundlage für die Definition der IT-Sicherheitsziele bilden daher die generellen Ziele der Institution sowie die wesentlichen Geschäftsprozesse und Informationen. Angemessene und erreichbare IT-Sicherheitsziele sind Voraussetzung für alle weiteren Schritte im IT-Sicherheitsprozess. Die Ziele müssen realistisch, praxisorientiert, überzeugend und verständlich sein. Hieraus lässt sich dann im Rahmen der IT-Sicherheitskonzeption ableiten, welchen Schutzbedarf die einzelnen IT-Anwendungen, IT-Komponenten und Netze haben und welche Sicherheitsmaßnahmen daher umzusetzen sind.

Bei der Umsetzung von IT-Sicherheitsmaßnahmen muss in der Regel immer ein Kompromiss zwischen Kosten und Aufwand gefunden werden. Es sollte daher transparent sein, welche Informationen und Geschäftsprozesse zur Aufgabenerfüllung beitragen und welcher Wert diesen beigemessen wird, um daraus angemessene IT-Sicherheitsziele zu formulieren

Die IT-Sicherheitsziele müssen von der Unternehmens- oder Behördenleitung getragen und verantwortet werden. Sie sollten von der IT-Sicherheitsorganisation unter Beteiligung der Leitungsebene erarbeitet und dokumentiert werden. Je nach Organisationsstruktur ist es ratsam, die Leiter von größeren Geschäftsbereichen (z. B. Abteilungsleiter oder Bereichsleiter) in die Beratungen einzubeziehen.

Eine detaillierte Beschreibung, wie und in welcher Beschreibungstiefe IT-Sicherheitsstrategie und -ziele festgehalten werden sollten, findet sich im BSI-Standard 100-2 *Vorgehensweise nach IT-Grundschutz*.

Aufrechterhaltung und Verbesserung der IT-Sicherheitsstrategie

IT-Sicherheitsziele und -strategie sollten regelmäßig daraufhin beleuchtet werden, ob sie noch aktuell und angemessen sind. Insbesondere bei Ände

rungen von Rahmenbedingungen, von Geschäftsprozessen oder des IT-Umfeldes müssen die IT-Sicherheitsziele und -strategie überprüft und eventuell angepasst werden.

Der IT-Sicherheitsprozess kann nur dann langfristig erfolgreich sein, wenn die Wirksamkeit und Effizienz der IT-Sicherheitsstrategie regelmäßig von der Leitungsebene überprüft wird. Die daraus resultierenden Verbesserungen gehen in die Anpassung des Sicherheitsprozesses ein.

Ergänzende Kontrollfragen:

- Wurden IT-Sicherheitsziele ermittelt?
- Ist ein adäquater IT-Sicherheitsprozess etabliert?
- Wie werden die IT-Sicherheitsziele und -strategie aktuell gehalten?

M 2.336 Übernahme der Gesamtverantwortung für IT-Sicherheit durch die Leitungsebene

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung

IT-Sicherheit ist Chefsache!

Die Führung und Lenkung eines Unternehmens oder einer Behörde und die damit verbundenen Leitungsaufgaben beinhalten eine hohe Verantwortung. Diese Verantwortung bezieht sich nicht nur auf den Grad der Zielerreichung wie beispielsweise den Geschäftserfolg, sondern auch auf die Früherkennung und Minimierung von möglichen Risiken für den Betrieb. Dazu gehören neben anderen Risiken auch solche, die aus unzureichender IT-Sicherheit entstehen.

Ein angemessenes IT-Sicherheitsniveau zu gewährleisten, ist eine komplexe Aufgabe. Dies erfordert ein systematisches Vorgehen, einen kontinuierlichen und zielgerichteten IT-Sicherheitsprozess. Es ist Aufgabe der Leitungsebene jeder Institution, diesen Prozess zu initiieren, zu steuern und zu kontrollieren. Bei kleineren Institutionen wird dies häufig durch ein Mitglied der Leitungsebene persönlich übernommen. In mittleren und großen Institutionen wird die Aufgabe "IT-Sicherheit" an eine dedizierte Person, den IT-Sicherheitsbeauftragten, delegiert. Je nach Größe und Art der Institution werden noch weitere Personen mit Sicherheitsaufgaben betraut, die diese ausschließlich oder zusätzlich zu anderen Aufgaben wahrnehmen. Hierfür ist es sinnvoll, eine geeignete Organisationsstruktur aufzubauen, um die verschiedenen Teilaufgaben im Bereich Sicherheit adäquat zu steuern. Dabei verbleibt die Gesamtverantwortung immer bei der Leitungsebene, unabhängig davon, an wie viele Personen Sicherheitsaufgaben delegiert wurden.

Motivation der Leitungsebene

Die Geschäftsführung sollte regelmäßig über mögliche Risiken und Konsequenzen aufgrund fehlender IT-Sicherheit aufgeklärt werden. Dazu ist es empfehlenswert, die Leitungsebene auf folgende Punkte aufmerksam zu machen (siehe auch M 3.44 *Sensibilisierung des Managements für IT-Sicherheit*):

- Darstellung der Sicherheitsrisiken und der damit verbundenen Kosten
- Auswirkungen von IT-Sicherheitsvorfällen auf die kritischen Geschäftsprozesse
- Gesetzliche und vertragliche Sicherheitsanforderungen
- Übersicht über Standard-Vorgehensweisen zur IT-Sicherheit für die Branche

Auch wenn die Leitungsebene für die Erreichung der Sicherheitsziele verantwortlich ist, muss der Sicherheitsprozess von allen Beschäftigten in einer Institution mitgetragen und mitgestaltet werden. Daher sollten folgende Prinzipien eingehalten werden:

- Übernahme der Gesamtverantwortung für IT-Sicherheit
  Die Initiative für IT-Sicherheit geht von der Behörden- bzw. Unternehmensleitung aus. Die Aufgabe "IT-Sicherheit" wird durch die Behörden- bzw. Unternehmensleitung aktiv unterstützt.

- **IT-Sicherheit integrieren**
  IT-Sicherheit muss in alle Prozesse und Projekte integriert werden, die IT nutzen. Darüber hinaus müssen alle Beteiligten über den IT-Sicherheitsprozess ausreichend informiert und motiviert werden, damit sie diesen auch einhalten.
- **Zuständigkeiten definieren**
  Die Behörden- bzw. Unternehmensleitung benennt die für IT-Sicherheit zuständigen Mitarbeiter und stattet sie mit den erforderlichen Kompetenzen und Ressourcen aus.
- **Lenken und Überwachen**
  Die Leitungsebene muss aktiv den IT-Sicherheitsprozess initiieren, lenken und überwachen. Dazu muss das Management die Auswirkungen von IT-Sicherheitsvorfällen auf die Geschäftstätigkeit kennen, Sicherheitsziele vorgeben und Rahmenbedingungen schaffen, die es ermöglichen, diese Ziele zu erreichen.
- **Angemessene Ziele setzen**
  Absolute IT-Sicherheit gibt es nicht. Deswegen ist es wichtig, die Sicherheitsziele so zu setzen, dass sie einerseits mit einem vertretbaren Aufwand (Personal, Zeit, Finanzmittel) erreichbar sind und andererseits die Sicherheitsrisiken auf ein akzeptables Maß reduziert werden.
- **Vorbildfunktion**
  Die Leitungsebene übernimmt auch im Bereich IT-Sicherheit eine Vorbildfunktion. Dazu gehört unter anderem, dass auch die Leitungsebene alle vorgegebenen Sicherheitsregeln beachtet.
- **Kontinuierliche Verbesserung**
  Die Angemessenheit und Wirksamkeit aller Elemente des IT-Sicherheitsmanagements muss ständig überprüft werden. Identifizierte Schwachstellen und Verbesserungsmöglichkeiten müssen dann auch konsequent behoben bzw. umgesetzt werden. Wichtig ist auch, zukünftige Entwicklungen, veränderte Rahmenbedingungen und potentielle Gefährdungen frühzeitig zu erkennen.
- **Kommunikation und Wissen**
  Die Leitungsebene und das IT-Sicherheitsmanagement müssen die Mitarbeiter motivieren und für ausreichende Schulungs- und Sensibilisierungsmaßnahmen sorgen. Mitarbeiter müssen vor allem über Sinn und Zweck sowohl von technischen IT-Sicherheitsmaßnahmen als auch von organisatorischen Vorgaben aufgeklärt werden. IT-Anwender sollten in die Umsetzungsplanung von Maßnahmen eingezogen werden. Damit können sie Ideen einbringen und die Praxistauglichkeit von Sicherheitsmaßnahmen beurteilen.

Ergänzende Kontrollfragen:

- Hat die Behörden- bzw. Unternehmensleitung deutlich sichtbar die Verantwortung für IT-Sicherheit übernommen?
- Hat die Behörden- bzw. Unternehmensleitung Sicherheitsverantwortliche benannt?

M 2.337 Integration der IT-Sicherheit in organisationsweite Abläufe und Prozesse

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement-Team

IT-Sicherheit muss in alle Geschäftsprozesse integriert werden. Es muss dabei gewährleistet sein, dass nicht nur bei neuen Projekten, sondern auch bei laufenden Anwendungen alle erforderlichen IT-Sicherheitsaspekte berücksichtigt werden.

Vor allem in größeren Institutionen existiert bereits häufig ein übergreifendes Risikomanagementsystem. Da IT-Risiken zu den wichtigsten operationellen Risiken gehören, sollten die Methoden zum Management von IT-Risiken mit den bereits etablierten Methoden abgestimmt werden. Wichtig ist, dass Arbeitsanweisungen oder Dienstvereinbarungen aus unterschiedlichen Bereichen einer Organisation sich nicht widersprechen dürfen.

Die Bausteine der IT-Grundschutz-Kataloge enthalten ausführliche und konkrete Maßnahmenempfehlungen zur IT-Sicherheitsorganisation. Im Folgenden werden daher nur beispielhaft wichtige übergreifende IT-Sicherheitsmaßnahmen kurz genannt:

Definition von Zuständigkeiten (Funktionstrennung)

Zuständigkeiten und Kompetenzen innerhalb der IT-Sicherheitsorganisation müssen klar definiert und zugewiesen werden. Für alle wichtigen Funktionen sind zudem Vertretungsregelungen sicherzustellen.

Festlegung von Kommunikationswegen

Kommunikationswege müssen geplant, beschrieben, bekannt gemacht und eingerichtet werden. Es muss also für alle Aufgaben und Rollen festgelegt sein, wer wen informiert, bei welchen Aktionen wer informiert werden muss und welchen Umfang dies haben muss.

Zuweisung der Verantwortung für Geschäftsprozesse, Informationen, IT-Anwendungen und IT-Systeme

Für alle wesentlichen Geschäftsprozesse, Informationen, IT-Systeme und IT-Anwendungen, aber auch für Gebäude und IT-Räume müssen verantwortliche Personen benannt werden. Je nach Bereich und Sprachgebrauch werden diese verantwortlichen Personen z. B. als Informationseigentümer, Geschäftsprozessverantwortliche oder Fachverantwortliche bezeichnet. Die Fachverantwortlichen müssen die Erarbeitung und Umsetzung der IT-Sicherheitsstrategie unterstützen. Die Maßnahme M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten gibt weitere Hinweise.

Integration der Mitarbeiter in den Sicherheitsprozess

IT-Sicherheit betrifft ohne Ausnahme alle Mitarbeiter. Jeder Einzelne muss durch verantwortungs- und qualitätsbewusstes Handeln mithelfen, Schäden zu vermeiden und zum Erfolg beitragen. Dies betrifft nicht nur die festangestellten Mitarbeiter, sondern alle, die innerhalb der Institution beschäftigt sind, also beispielsweise auch Pförtner und Praktikanten. Ebenso sollten auch Per

sonen einbezogen werden, die von außerhalb auf Geschäftsprozesse, Anwendungen oder IT-Systeme zugreifen, also z. B. Mitarbeiter von Outsourcing-Dienstleistern. Wichtige Sicherheitsmaßnahmen, die beim Personalmanagement zu beachten sind, also beginnend von der Personalauswahl und Einstellung bis hin zum Wechsel in andere Bereiche oder dem Weggang aus der Institution, sind im Baustein B 3.2 *Personal* beschrieben.

Darüber hinaus müssen alle Mitarbeiter innerhalb ihres Aufgabenbereiches in die erforderlichen Sicherheitsmaßnahmen eingewiesen werden. Sie sollten regelmäßig für IT-Sicherheitsaspekte sensibilisiert werden, um das Bewusstsein für Risiken und Schutzvorkehrungen im alltäglichen Umgang mit Informationen zu schärfen. Auch das Management muss in das Sensibilisierungskonzept einbezogen werden. Vertiefende Ausführungen hierzu finden sich im Baustein B 1.13 *IT-Sicherheitssensibilisierung und -schulung*.

Einbeziehung von IT-Sicherheitsaspekten in alle Geschäftsprozesse

Das Management muss einen Überblick über die geschäftskritischen Informationen, Fachaufgaben und Geschäftsprozesse haben. Die zuständigen Fachverantwortlichen und das IT-Sicherheitsmanagement müssen konkrete Regeln zum Umgang mit den relevanten IT-Sicherheitsaspekten aufstellen (z. B. Schutzmaßnahmen, Klassifizierung und Kennzeichnung von Informationen).

Rechte und Berechtigungen

Zum Schutz der Werte müssen der Zutritt zu Räumen, der Zugang zu IT-Systemen und Anwendungen sowie der Zugriff auf Informationen geregelt werden. Nähere Informationen finden sich z. B. in den Maßnahmen M 2.6 *Vergabe von Zutrittsberechtigungen*, M 2.7 *Vergabe von Zugangsberechtigungen,* M 2.8 *Vergabe von Zugriffsrechten* und M 2.220 *Richtlinien für die Zugriffs- bzw. Zugangskontrolle*.

Änderungsmanagement

Änderungsmanagement beschäftigt sich mit der Planung von Änderungen an Hard- und Software sowie Prozessen. Es muss durch organisatorische Vorgaben sichergestellt werden, dass dabei Sicherheitsgesichtspunkte berücksichtigt werden. Näheres findet sich z. B. in der Maßnahme M 2.221 *Änderungsmanagement*.

Konfigurationsmanagement

Konfigurationsmanagement umfasst alle Maßnahmen und Strukturen, die erforderlich sind, um den Zustand der betrachteten Objekte zu überwachen, beginnend von der Identifikation, über die Bestandsführung und Aktualisierung bis hin zur Außerbetriebnahme. Betrachtete Objekte (Konfigurationselemente) können dabei ganze Infrastrukturbereiche, konkrete IT-Anwendungen und IT-Systeme, aber auch einzelne Komponenten davon (beispielsweise Dokumentationen) sein.

Im Rahmen des Konfigurationsmanagements müssen Prozesse und Regelungen eingeführt werden, die beschreiben, wie Informationen über die Eigenschaften der eingesetzten Konfigurationselemente sowie Informationen über sicherheitsrelevante Störungen, Probleme und Änderungen im Zusammenhang mit Konfigurationselementen verwaltet werden. Typische Tätigkeiten sind

beispielsweise die Aktualisierung der Liste der IT-Systeme oder die Anpassung von sicherheitsrelevanten Dokumentationen nach Änderungen von IT-Anwendungen. Empfehlungen zum Konfigurationsmanagement finden sich in Baustein B 1.9 *Hard- und Software-Management*.

Ergänzende Kontrollfragen:

- Wird der IT-Sicherheitsbeauftragte bzw. das IT-Sicherheitsmanagement-Team an sicherheitsrelevanten Entscheidungen ausreichend beteiligt?
- Werden organisatorische Regelungen und Prozesse, die für die IT-Sicherheit relevant sind, regelmäßig überprüft und verbessert?

M 2.338 Erstellung von zielgruppengerechten IT-Sicherheitsrichtlinien

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement-Team

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement-Team

Zielgruppengerechte Vermittlung von IT-Sicherheitsthemen

Ein wichtiger Erfolgsfaktor für die Erreichung eines angemessenen Sicherheitsniveaus sind verantwortungsbewusste und kompetente Mitarbeiter, die koordiniert zusammenarbeiten. Dabei bringen Management, IT-Benutzer, Administratoren und IT-Sicherheitsexperten sehr individuelle fachliche Voraussetzungen mit und nehmen unterschiedliche Aufgaben wahr. Während die Unternehmens- bzw. Behördenleitung die Gesamtverantwortung trägt, Ziele vorgibt und Rahmenbedingungen definiert, müssen Administratoren technisch hochqualifiziert sein und Detailwissen besitzen, um Systeme bedienen und sicher konfigurieren zu können.

IT-Sicherheitsverantwortliche sind mit den IT-Grundschutz-Katalogen in der Lage, ein ganzheitliches IT-Sicherheitskonzept zu erstellen. Wenn alle Bereiche der IT-Sicherheit damit abgedeckt werden sollen, wird ein IT-Sicherheitskonzept oftmals viele Seiten umfassen.

Die zielgruppengerechte Aufbereitung und Vermittlung der Inhalte des IT-Sicherheitskonzepts ist eine wichtige Aufgabe des IT-Sicherheitsmanagements. Das Ziel ist, dass alle Mitarbeiter die sie betreffenden IT-Sicherheitsaspekte kennen und beachten.

Es empfiehlt sich daher, unterschiedliche Sicherheitsrichtlinien oder sogar ausführliche Teilkonzepte zu erstellen, die einzelne IT-Sicherheitsthemen bedarfsgerecht darstellen. So erhalten Mitarbeiter genau die Informationen, die sie zu einem bestimmten Thema wirklich benötigen.

So können für IT-Systeme oder IT-Dienstleistungen, die sich in einem sicherheitskritischen Bereich befinden, deren Konfiguration kompliziert ist oder deren Anwendung komplex ist, separate IT-System-Sicherheitsrichtlinien mit technischen Anweisungen für Administratoren erstellt werden.

Für IT-Benutzer sollten Sicherheitsthemen dagegen angemessen aufbereitet werden, ohne diese mit unnötigen Details zu konfrontieren, die vom Wesentlichen ablenken, unverständlich sind und verwirren.

Hierarchischer Aufbau von Richtlinien

Bei der Formulierung von Richtlinien hat es sich bewährt, auf verschiedenen Ebenen zu arbeiten.

Zunächst sollten in der ersten Ebene kurz und prägnant die allgemeinen IT-Sicherheitsziele und die IT-Sicherheitsstrategie in einer IT-Sicherheitsleitlinie formuliert werden (siehe M 2.192 *Erstellung einer IT-Sicherheitsleitlinie*). Die Strategie enthält keine technischen Details, wird vom Management verabschiedet und unterliegt weniger Änderungen.

In der nächsten Ebene sollten hieraus grundlegende technische Sicherheitsanforderungen ableitet werden. Zur allgemeinen Sicherheitskonzeption gehören

Dokumente, die verschiedene Aspekte der IT-Sicherheit beschreiben (z. B. eine Richtlinie zur Internetnutzung oder ein Virenschutzkonzept), ohne auf konkrete Produkte einzugehen.

In der dritten Ebene werden technische Details, konkrete Maßnahmen und produktspezifische Einstellungen beschrieben. Sie enthält viele Dokumente, die regelmäßig geändert werden und typischerweise nur von den zuständigen Experten gelesen werden.

Die nachstehende Abbildung stellt den hier beschriebenen Aufbau graphisch dar.

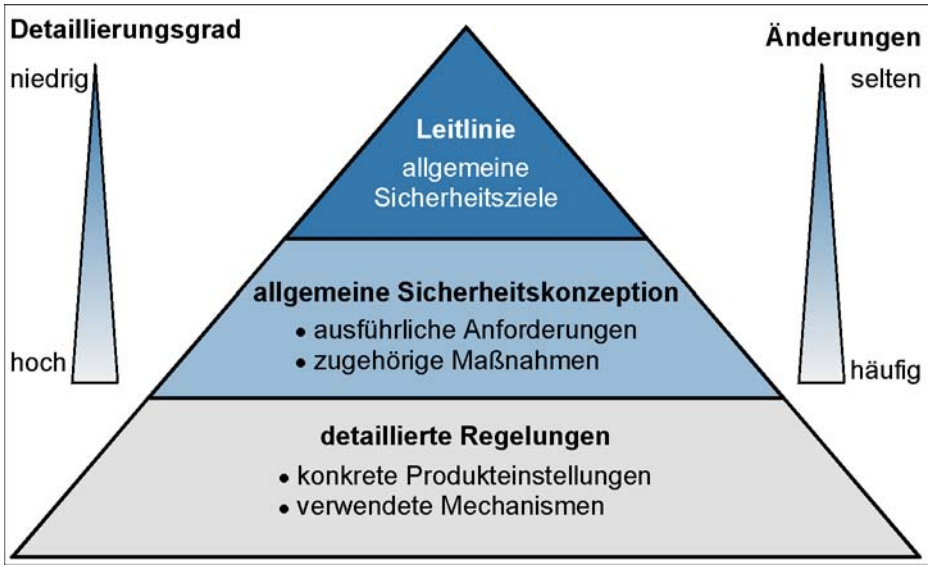


Abbildung: Hierarchischer Aufbau von Richtlinien

Inhalt von speziellen IT-Sicherheitsrichtlinien

geeignete Themenbereiche

Folgende Themen sind beispielsweise geeignet, um sie in speziellen Sicherheitsrichtlinien zielgruppengerecht aufzubereiten:

- Verhaltensregeln und Sicherheitshinweise für IT-Benutzer
- Verhaltensregeln und Sicherheitshinweise für Administratoren
- Sicherheitsgateways (siehe auch M 2.70 *Entwicklung eines Konzepts für Sicherheitsgateways*)
- Virenschutz (siehe auch M 2.154 *Erstellung eines Computer-Virenschutzkonzepts*)
- Notfallvorsorge (siehe auch M 6.3 *Erstellung eines Notfallhandbuchs*)
- Datensicherung (siehe auch M 6.33 *Entwicklung eines Datensicherungskonzepts*)
- Archivierung (siehe auch M 2.243 *Entwicklung des Archivierungskonzepts*)
- Einsatz von E-Mail und Nutzung des Internets (siehe M 2.118 *Konzeption der sicheren E-Mail-Nutzung*)
- Outsourcing (siehe M 2.251 *Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben*)

Sicherheitsrichtlinie zur IT-Nutzung

Oft empfiehlt es sich, die allgemeinen Zielvorgaben der IT-Sicherheitsleitlinie in einer Sicherheitsrichtlinie zur IT-Nutzung zu konkretisieren und die wichtigsten organisationsweiten Maßnahmen des IT-Sicherheitskonzeptes allgemeinverständlich, ohne technische Details, in einer Richtlinie zusammenzufassen. Diese Richtlinie beschreibt die Grundzüge der organisationsweiten IT-Nutzung und führt die Mitarbeiter durch das Sicherheitskonzept.

Folgende Themen könnten in einer allgemeinen Sicherheitsrichtlinie zur IT-Nutzung behandelt werden:

- Umgang mit schützenswerten Informationen (Festlegung von Informationseigentümern, Pflicht zur Klassifizierung von Informationen nach Schutzbedürftigkeit)
- relevante Gesetze und Vorgaben
- Kurzbeschreibung wichtiger Rollen (z. B. IT-Sicherheitsbeauftragter, Administrator, Benutzer)
- Ausbildung des Personals
- Pflicht zur Einrichtung von Vertretungsregelungen
- Anforderungen an die Verwaltung von IT (Beschaffung, Einsatz, Wartung, Revision und Entsorgung)
- grundlegende Sicherheitsmaßnahmen (Zutritt zu Räumen und Zugang zu IT-Systemen, Verschlüsselung, Virenschutz, Datensicherung, Notfallvorsorge)
- Regelungen für spezifische IT-Dienste (Datenübertragung, Internetnutzung)

Musterrichtlinien

Das BSI stellt auf seinen Webseiten im Bereich IT-Grundschutz verschiedene Musterrichtlinien und -konzepte als Beispiele zur Verfügung.

Ergänzende Kontrollfragen:

- Welche IT-Sicherheitsrichtlinien gibt es in der Institution?
- Sind diese IT-Sicherheitsrichtlinien den Betroffenen bekannt?

M 2.339 Wirtschaftlicher Einsatz von Ressourcen für IT-Sicherheit

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter

Damit die gesteckten IT-Sicherheitsziele erreicht werden können, müssen dafür angemessene Ressourcen bereitgestellt werden.

Bereitstellung von Ressourcen für den IT-Betrieb

Eine Grundvoraussetzung für IT-Sicherheit ist ein gut funktionierender IT-Betrieb. Für den IT-Betrieb müssen ausreichende Ressourcen zur Verfügung gestellt werden. Typische Probleme des IT-Betriebs (knappes Budget, überlastete Administratoren und eine unstrukturierte oder schlecht gewartete IT-Landschaft) müssen in der Regel zuerst gelöst werden, damit die eigentlichen IT-Sicherheitsmaßnahmen wirksam und effizient umgesetzt werden können. Ob die bereitgestellten Ressourcen ausreichen, zeigt sich beispielsweise daran, ob die IT-Benutzer angemessen betreut werden oder ob alle Hard- und Software wie vorgesehen getestet wird.

Bereitstellung von Ressourcen für IT-Sicherheit

IT-Sicherheit erfordert ausreichende finanzielle und personelle Ressourcen sowie eine geeignete Ausstattung. Diese müssen dem IT-Sicherheitsmanagement-Team von der Behörden- bzw. Unternehmensleitung in angemessenem Umfang bereitgestellt werden.

Es ist zu empfehlen, dass das IT-Sicherheitsmanagement-Team anhand der IT-Sicherheitsziele die für die Umsetzung aller identifizierten Maßnahmen benötigten Ressourcen aufzeigt. Dies dient einerseits als Grundlage für Management-Entscheidungen über die Zuteilung der Ressourcen und andererseits zur Festlegung der Projektpläne und der Umsetzungszeiträume.

Zugriff auf externe Ressourcen

Die internen IT-Sicherheitsexperten sind häufig mit ihren Routinetätigkeiten so ausgelastet, dass ihnen bei neuen Aufgaben oder Entwicklungen die Zeit fehlt, um alle sicherheitsrelevanten Einflussfaktoren zu analysieren oder um Sicherheitslösungen umzusetzen. Hierzu gehören beispielsweise geänderte gesetzliche Anforderungen, die Einführung neuer IT-Systeme sowie die Verfolgung der aktuellen technischen Entwicklungen. Um Arbeitsspitzen bewältigen zu können, müssen entweder intern zusätzliche Mitarbeiter herangezogen werden, was meistens schwierig ist, oder es muss auf externe Experten zurückgegriffen werden. Bei Bedarf muss dies von den internen IT-Sicherheitsexperten aufgezeigt werden, damit die Leitungsebene die erforderlichen Ressourcen bereit stellt.

Es ist sicherzustellen, dass alle erforderlichen Sicherheitsmaßnahmen umgesetzt werden, sei es durch den Rückgriff auf externe oder interne Kräfte.

Ressourcen für den IT-Sicherheitsbeauftragten

Ohne eine funktionierende IT-Sicherheitsorganisation nützen die teuersten technischen Lösungen nichts. Die Erfahrung zeigt, dass die Berufung eines IT-

Sicherheitsbeauftragten die effektivste IT-Sicherheitsmaßnahme ist. Nach der Bestellung eines IT-Sicherheitsbeauftragten geht in den meisten Organisationen die Anzahl an IT-Sicherheitsvorfällen signifikant zurück. Damit der IT-Sicherheitsbeauftragte eine tatsächliche Verbesserung des IT-Sicherheitsniveaus erreichen kann, muss er

- ausreichend Zeit für seine Arbeit haben,
- ausreichend in alle Geschäftsprozesse, Fachaufgaben und Projekte integriert sein,
- genügenden Zugriff auf alle erforderlichen Ressourcen haben.

In kleineren Organisationen ist es möglich, dass ein Mitarbeiter die Aufgaben des IT-Sicherheitsbeauftragten in Personalunion neben seinen eigentlichen Tätigkeiten wahrnimmt.

Ressourcen für das IT-Sicherheitsmanagement-Team

Ein IT-Sicherheitsmanagement-Team sollte immer dann eingerichtet werden, wenn der IT-Sicherheitsbeauftragte alleine nicht mehr alle Geschäftsprozesse und Projekte betreuen kann, also die Organisation eine gewisse Größenordnung überschritten hat.

Die erstmalige Einrichtung des IT-Sicherheitsprozesses ist meist mit einem erhöhten Aufwand verbunden. Häufig ist es deshalb zweckmäßig, dem IT-Sicherheitsmanagement-Team für diese Phase zusätzliche personelle Ressourcen zur Verfügung zu stellen.

Wirtschaftlichkeitsaspekte in der IT-Sicherheitsstrategie

Die IT-Sicherheitsstrategie sollte von Beginn an auch Wirtschaftlichkeitsaspekte berücksichtigen. Bei der Auswahl der umzusetzenden IT-Sicherheitsmaßnahmen sollten die zur Verfügung stehenden Ressourcen berücksichtigt werden. Wenn für bestimmte Maßnahmen nicht ausreichend technische oder personelle Unterstützung vorhanden ist, muss die Strategie geändert werden. In vielen Fällen lassen sich andere Maßnahmen finden, die zu einem ähnlichen Sicherheitsniveau führen. Wenn aber die formulierten Sicherheitsziele und die vorhandenen finanziellen, technischen oder personellen Möglichkeiten zu weit auseinander liegen, müssen sowohl die Sicherheitsziele als auch die Geschäftsprozesse grundsätzlich überdacht werden. In diesem Fall muss auch die Leitungsebene über diese Diskrepanz informiert werden, damit sie gegebenenfalls Korrekturmaßnahmen veranlassen kann.

Bei der Festlegung von IT-Sicherheitsmaßnahmen sollten auch immer die für die Umsetzung benötigten personellen und finanziellen Ressourcen konkret genannt werden. Hierzu gehört die Benennung von Verantwortlichen und anderen Ansprechpartnern, aber auch die Festlegung genauer Terminpläne und der zu beschaffenden Materialien. Es empfiehlt sich außerdem, bei allen geplanten Sicherheitsmaßnahmen zu dokumentieren, ob die für IT-Sicherheit eingeplanten Ressourcen termingerecht bereitgestellt wurden und was die Gründe für Projektabweichungen waren. Nur so lassen sich nachhaltige Verbesserungen erreichen und Störungen vermeiden.

Ressourcen für die Überprüfung der IT-Sicherheit

Alle IT-Sicherheitsmaßnahmen müssen regelmäßig auf ihre Wirksamkeit und Eignung geprüft werden. Auch hierfür müssen ausreichende Ressourcen bereitgestellt werden. Generell sollten nicht diejenigen, die Sicherheitsmaßnahmen konzipiert haben, deren Wirksamkeit und Eignung prüfen. Hierfür kann auch externer Sachverstand hinzugezogen werden, um Betriebsblindheit zu vermeiden.

Die Frage, ob ausreichende Ressourcen für IT-Sicherheit bereitgestellt werden, ist wesentlich schwieriger zu beantworten als die Überprüfung von rein technischen Aspekten.

Ergänzende Kontrollfragen:

- Gibt es ausreichend Ressourcen für einen ordnungsmäßigen IT-Betrieb?
- Finden regelmäßig Überprüfungen der IT-Sicherheit statt?
- Wurden bei der Festlegung von IT-Sicherheitsmaßnahmen die für die Umsetzung erforderlichen Ressourcen beziffert?
- Wurden für IT-Sicherheit eingeplante Ressourcen tatsächlich termingerecht bereitgestellt? Gab es größere Verzögerung bei der Umsetzung von Maßnahmen, so dass über längere Zeit das angestrebte IT-Sicherheitsniveau nicht eingehalten werden konnte?
- Können der IT-Sicherheitsbeauftragte bzw. das IT-Sicherheitsmanagement-Team ihre Sicherheitsaufgaben wahrnehmen oder werden diese Mitarbeiter durch das Tagesgeschäft oder andere Projekte davon abgehalten?

M 2.340 Beachtung rechtlicher Rahmenbedingungen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung, Leiter Organisation, Vorgesetzte

Bei der Verarbeitung von Informationen sind eine Vielzahl von gesetzlichen oder vertraglichen Rahmenbedingungen zu beachten. Diese variieren sehr stark in Abhängigkeit von der Art der Institution, der Branche und den Geschäftsprozessen.

Typische Bereiche der Informationsverarbeitung, die besonderen gesetzlichen Regelungen unterliegen, sind:

- Schutz personenbezogener Daten,
- Einsatz von kryptographischen Verfahren,
- Schutz von geistigem Eigentum,
- ordnungsgemäßer Betrieb von IT-Systemen.

Abhängig von dem Land, in dem die Informationen verarbeitet werden und ihrem speziellen Einsatzzweck können noch eine Vielzahl von weiteren rechtlichen Regelungen existieren. Diese einzeln zu nennen, würde den Rahmen der IT-Grundschutz-Kataloge sprengen. In diversen Bereichen des IT-Grundschutzes werden länder- oder branchenspezifische Gesetze angesprochen, wie z. B. zu Kryptographie, Outsourcing oder Archivierung. Dies sind aufgrund der Vielzahl möglicher gesetzlicher Rahmenbedingungen jeweils nur Beispiele ohne Anspruch auf Vollständigkeit oder Aktualität.

Zu beachtende gesetzliche und vertragliche Vorschriften für die Informationsverarbeitung, den Betrieb von IT-Systemen und der zugehörigen physischen Infrastruktur müssen identifiziert und dokumentiert werden. Es ist dabei zu beachten, dass gesetzliche Vorschriften sich häufig auf Landes- und Regionalebene unterscheiden. Als Konsequenz müssen für jede Lokation jeweils die dort gültigen Gesetze eingehalten werden. Ebenso ist zu berücksichtigen, dass je nach Einsatzzweck der IT-Systeme (z. B. Büroumgebung, Prozesssteuerung) verschiedene Vorschriften gelten können.

Insbesondere müssen

- alle angewandten IT-Praktiken und Vorgehensweisen,
- alle installierten IT-Systeme (Hardware- und Software) sowie
- die zum Betrieb der IT-Systeme notwendige physikalische Infrastruktur

die gültigen gesetzlichen Vorschriften erfüllen. Alle Änderungen gesetzlicher Auflagen müssen erfasst und die für die Institution relevante Änderungen berücksichtigt werden.

Überprüfung und Durchsetzung

Führungskräfte, welche die rechtliche Verantwortung für die Institution vor Ort tragen, müssen für die Identifizierung und Dokumentation der anzuwendenden gesetzlichen Vorschriften sorgen. Dabei können auch einzelne Bereiche auf benannte Verantwortliche übertragen werden.

So ist der betriebliche Datenschutzbeauftragte dafür verantwortlich, auf die Einhaltung der gültigen Datenschutzvorschriften sowie für die Erstellung und Einhaltung eines institutionsweit gültigen Regelwerks zum Schutz personenbezogener Daten hinzuwirken. Die IT-Leitung muss für die Definition und Dokumentation des Lizenzmanagements sorgen.

Natürlich ist auch jeder einzelne Mitarbeiter und insbesondere das Führungspersonal für die Umsetzung der Regelungen zu rechtlichen Aspekten und für die Überwachung der Einhaltung verantwortlich (siehe auch M 3.2 *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*).

Ergänzende Kontrollfragen:

- Sind alle relevanten rechtlichen Vorgaben identifiziert und dokumentiert worden?
- Sind die Verantwortlichkeiten und Zuständigkeiten für die Einhaltung rechtlicher Vorgaben definiert?

M 2.341 Planung des SAP Einsatzes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Leiter IT

Vor der Installation und Inbetriebnahme eines SAP Systems müssen umfangreiche Planungen erfolgen. Eine sorgfältige Planung ist nicht nur unter Sicherheitsgesichtspunkten notwendig. Auch die Geschäftsprozesse und -abläufe, die durch das SAP System automatisiert und unterstützt werden sollen, müssen vollständig, korrekt und im notwendigen Detailgrad erfasst werden. Nur so ist eine erfolgreiche Umsetzung innerhalb eines SAP Systems möglich. Selbst eine Planungsphase von mehreren Monaten kann für große Systeme bei Neuplanung knapp bemessen sein.

Schon in der Konzeptionsphase sollten der Datenschutzbeauftragte und der Personal- oder Betriebsrat beteiligt werden. Zum einen werden mit SAP-Systemen in der Regel auch immer personenbezogene Daten verarbeitet, z. B. mit dem Modul HR oder im Rahmen der Protokollierung (siehe unten). Zum anderen sollte die notwendige Umstellung von Geschäftsprozessen und Arbeitsabläufen begleitet werden.

Planungen sind für jedes SAP System individuell durchzuführen, da sich jedes SAP System im Einsatzszenario unterscheidet. Auch für das Test- und Abnahme-System und das Entwicklungs-System, die einem Produktiv-System zugeordnet sind, sollte aufgrund der unterschiedlichen Verwendungszwecke eine individuelle Planung erfolgen. Es ist dabei zu beachten, dass jeweils auch die Abhängigkeiten zwischen SAP Systemen berücksichtigt werden müssen. Dies gilt besonders für die verschiedenen Ausprägungen (Entwicklung, Test und Abnahme, Produktion) eines SAP Systems, aber auch für unterschiedliche SAP Systeme in einem Verbund. Insofern muss eine auf die Zusammenarbeit der individuellen Systeme abgestimmte Gesamtplanung erfolgen.

Konzepte in der Planungsphase

Im Folgenden ist eine Liste von SAP Sicherheitsteilkonzepten angegeben, die im Hinblick auf die Sicherheit eines SAP Systems in der Planungsphase zu erstellen sind und die auch kontinuierlich gepflegt werden müssen. Die Liste ist nicht vollständig und muss auf die lokalen Gegebenheiten und Anforderungen angepasst werden, mindestens erforderlich sind aber die folgenden SAP Sicherheitsteilkonzepte:

- Planung der technischen Konfiguration
- Administrationskonzept
- Konzept zur Benutzerverwaltung
- Berechtigungskonzept
- Ressourcen-Planung
- Planung der SAP Systemlandschaft
- Audit- und Logging-Konzept
- Änderungsmanagement-Konzept
- Backup-Konzept
- Notfallvorsorge-Konzept

Generell sind bei der Konzeption die bestehenden Sicherheitskonzepte der Behörde oder des Unternehmens zu berücksichtigen.

Planen der technischen Konfiguration

Aufbauend auf den vorstehend genannten Konzepten muss die technische Umsetzung durch die SAP Systemkonfiguration (Customizing) erfolgen. Dazu sind für den ABAP-Stack die notwendigen technischen Konfigurationsschritte im Rahmen eines projektbezogenen Implementation Guide (IMG) festzulegen. Die notwendigen Schritte für die gewünschte Konfiguration werden in der Regel aus dem SAP Referenz-IMG ausgewählt (siehe, M 4.258 *Sichere Konfiguration des SAP ABAP-Stacks*). Für den Java-Stack existiert der IMG-Mechanismus nicht, trotzdem sind die erforderlichen Konfigurationsschritte zu planen, um die gewünschten Konfiguration zu erhalten (siehe auch auch M 4.266 *Sichere Konfiguration des SAP Java-Stacks*).

Bei der Planung der technischen Konfiguration ist zu berücksichtigen, dass Rückkopplungsprozesse notwendig sind, um auf Änderungen reagieren zu können, die sich im Rahmen der Implementierung ergeben. In der Planungsphase können die SAP Systemdokumentationen herangezogen werden, um die notwendigen technischen Konfigurationen zu bestimmen und zu planen. Diese sind über das SAP Help Portal help.sap.com zugreifbar. Nach der Installation kann die technische Konfiguration, sofern notwendig, angepasst werden.

Administrationskonzept

Ein gutes Konzept für die Administration eines SAP Systems trägt wesentlich zur Sicherheit bei. Im Administrationskonzept ist festzulegen, wer welche administrativen Aufgaben wahrnimmt. Die technische Umsetzung muss dann dafür Sorge tragen, dass jeder nur die ihm zugeordneten Aufgaben wahrnehmen kann. Generell sollten dabei die nachfolgend beschriebenen Empfehlungen und Aspekte berücksichtigt werden.

Es muss immer ein Konzept für die Stacks (ABAP, Java) erstellt werden, die für ein SAP System installiert sind. Es muss ausgeschlossen sein, dass ein Stack installiert ist und kein Administrationskonzept vorliegt.

Funktionstrennung für administrative Aufgaben

In großen Unternehmen und Behörden empfiehlt sich, die Administration auf mehrere Personen aufzuteilen und so eine Funktionstrennung herbeizuführen. Generell sollte immer eine Trennung der Basis-Administration und der Administration auf Applikations- und Modul-Ebene umgesetzt werden.

Weiterhin empfiehlt sich mindestens eine Aufteilung in Administratoren für Benutzerverwaltung, Berechtigungsverwaltung, Verwaltung der System-Protokollierung, Backup und Änderungsmanagement. Je nach personeller Ausstattung kann die Trennung auch weiter fortgesetzt werden - etwa auf Basis einzelner Schnittstellen (z. B. RFC, ICF, SOAP) oder Dienste (z. B. Batch-Verarbeitung). Bei der Planung des Konzeptes sollten auch die relevanten Verantwortlichen für Geschäftsprozesse und Informationen einbezogen werden. Nur so ist sichergestellt, dass das Konzept auf die Anforderungen zugeschnitten ist, die sich aus den Geschäftsprozessen ergeben.

Bei der Aufteilung der administrativen Tätigkeiten ist jedoch zu bedenken, dass weder für den ABAP-Stack noch für den Java-Stack eine solche detaillierte Trennung vorkonfiguriert ist. Daher muss mit erhöhtem

Konfigurationsaufwand gerechnet werden, wenn eine feinere Trennung erreicht werden soll.

Funktionstrennung in kleinen Institutionen

In kleinen Unternehmen und Behörden, die oft nur einen einzigen Administrator beschäftigen, ist eine Funktionstrennung schon aufgrund fehlender personeller Alternativen nicht möglich. In diesem Fall sollten die Folgen eines internen Angriffs oder mangelnder Systemkenntnis jedoch sorgsam bedacht und abgeschätzt werden. Hier kann eine regelmäßige externe Sicherheitsprüfung helfen, die Systemsicherheit aufrecht zu erhalten. Generell müssen auch interne Sicherheitskontrollen definiert werden, um das Risiko zu vermindern. Es ist dabei zu berücksichtigen, dass diese Kontrollen sowie deren Umsetzung und Durchführung auch verwaltet werden müssen.

Der ABAP-Stack eines SAP Systems darf nicht durch einen Benutzer mit SAP_ALL Berechtigungen administriert werden. Diese Administrationsvariante birgt zu viele Sicherheitsrisiken. Erfolgt die Basis-Administration durch genau einen Administrator, so kann folgendes Vorgehen sinnvoll sein:

- Dem zur Administration genutzten Konto werden die Berechtigungsobjekte aus dem Profil SAP_ALL über eine Profil-Kopie zugeordnet.
- Alle Berechtigungsobjekte, die nicht für die Basis-Administration benötigt werden - dies sind in der Regel Berechtigungen, die in Applikationen oder Modulen Verwendung finden - werden aus der Profil-Kopie gelöscht.

Damit besitzt der Administrator nicht automatisch alle Applikationsberechtigungen. Auch wenn nur ein Administrator genutzt wird, empfiehlt es sich, im Rahmen des Administrationskonzeptes festzulegen, welche administrativen Aufgaben der Administrator wahrnehmen darf und welche nicht. Die verbleibenden Berechtigungsobjekte sind dann entsprechend anzupassen. Auf diese Weise können bestimmte administrative Operationen durch den Administrator nur dann ausgeführt werden, wenn beispielsweise eine Genehmigungskette durchlaufen wurde.

Im Administrationskonzept sind auch Verfahrens- und Vorgehensweisen für die Notfall-Administration festzulegen.

Konzept zur Benutzerverwaltung

Verwaltung eines einzelnen SAP Systems

Die Komplexität des Benutzerverwaltungskonzeptes wird dadurch bestimmt, ob nur ein einziges oder mehrere SAP Systeme verwaltet werden sollen. Muss nur ein System verwaltet werden, so ist durch das Benutzerverwaltungskonzept Folgendes festzulegen:

- Welche Konventionen für die Benutzernamen werden eingesetzt, so dass Benutzernamen eindeutig sind?
- Wer besitzt innerhalb der Benutzerverwaltung welche Rechte?
- Welche Benutzertypen werden wie eingesetzt?
- Wie werden die Benutzer in Gruppen aufgeteilt?
- Wie werden privilegierte Standardbenutzer geschützt?
- Welche Benutzer sind Mitglied der Gruppe SUPER?

- Welche Prozesse sind für die Benutzerverwaltung (z. B. Beantragung, Genehmigung, Anlegen, Verändern, Löschen) vorgesehen?

Es ist darauf zu achten, dass für alle anfallenden Verwaltungsarbeiten Prozesse definiert werden (z. B. Anlegen von Benutzern, Ändern oder Zuordnen von Rollen) und diese vollständig spezifiziert sind. Zusätzlich sind die jeweiligen Verantwortlichkeiten vollständig festzulegen. So wird verhindert, dass sich durch unklare Verantwortlichkeiten oder unvollständig definierte Prozesse Sicherheitslücken einschleichen.

User Management Engine

Für den Java-Stack besteht zwar die Möglichkeit, unterschiedliche Benutzerspeicher einzusetzen, generell kann jedoch der Einsatz der "User Management Engine" (UME) empfohlen werden, da diese die größte Flexibilität in der Konfiguration anbietet. In der Regel sollte die UME dann so konfiguriert werden, dass der zugehörige ABAP-Stack als Benutzerspeicher genutzt wird. So wird sichergestellt, dass gleiche Benutzerkonten mit gleichem Namen durch den Java- und ABAP-Stack auf den gleichen Benutzerstammsatz abgebildet werden.

Verwaltung mehrerer SAP Systeme

Müssen mehrere SAP Systeme verwaltet werden, so wird durch das Konzept zur Benutzerverwaltung der mit der Benutzerverwaltung einhergehende Administrationsaufwand maßgeblich bestimmt. Es muss entschieden werden, ob eine dezentrale oder zentrale Benutzerverwaltung eingesetzt wird. Die Entscheidung ist dabei abhängig vom Einsatzszenario für das SAP System und den Anforderungen der dabei insgesamt eingesetzten Systeme.

Neben den oben beschriebenen Aspekten sind dann außerdem durch das Benutzerverwaltungskonzept folgende Aspekte zu behandeln:

- Auf welchem System werden welche Benutzerkonten verwaltet (Definition des führenden Systems)?
- Wie erfolgt die Verteilung der Benutzerkonten auf die einzelnen Systeme?
- Welche Systeme benötigen oder verlangen eine separate Benutzerverwaltung?

Zentrale Benutzerverwaltung

Eine zentrale Benutzerverwaltung ist sinnvoll, wenn es sich um eine möglichst homogene Art von Benutzern (z. B. behörden- oder unternehmensinterne Benutzer) handelt, die auf mehrere SAP Systeme zugreifen. Dabei sollten die Sicherheitsanforderungen in den Zugriffsszenarien nicht stark differieren. Ist die Benutzermenge inhomogen (z. B. behörden- oder unternehmensinterne Benutzer, Benutzer von Partnerunternehmen oder -behörden, Kunden mit loser Behörden- bzw. Unternehmensbindung), so kann es sinnvoll sein, mehrere Verwaltungsinseln (d. h. Systeme mit jeweils einer zentralen Benutzerverwaltung) einzurichten, die die Benutzer der unterschiedlichen Einsatzszenarien verwalten.

Bei der Entscheidung für oder gegen eine zentrale Benutzerverwaltung müssen auch technische Randbedingungen bedacht werden. Soll beispielsweise die Zentrale Benutzer Verwaltung (ZBV, Central User Administration, CUA) eines SAP Systems verwendet werden, wird eine funktionierende ALE-Landschaft vorausgesetzt (siehe auch M 5.128 *Absicherung der SAP ALE (IDoc/BAPI) Schnittstelle*).

Dann ist es auch möglich die Zuordnung von Berechtigungen zu Benutzern zentral zu verwalten und in andere SAP Systeme zu transportieren.

Weitere Hinweise zur Sicherheit bei der Benutzerverwaltung finden sich in , M 4.259 *Sicherer Einsatz der ABAP-Stack Benutzerverwaltung* und M 4.267 *Sicherer Einsatz der SAP Java-Stack Benutzerverwaltung*.

Hinweise auf weitere Dokumentationen zur Benutzerverwaltung in SAP Systemen finden sich in M 2.346 *Nutzung der SAP Dokumentation*. **SAP Informationsquellen**

Berechtigungskonzept

Berechtigungen steuern, wer auf Funktionen und Daten zugreifen darf. Das Berechtigungskonzept ist daher wichtig für die Sicherheit beim Zugriff auf Funktionen und Daten eines SAP Systems. Eine bedarfsgerechte Planung der Berechtigungen durch ein ausgereiftes Berechtigungskonzept ist darum unerlässlich. Maßnahme M 2.342 *Planung von SAP Berechtigungen* enthält die Informationen, die dabei zu beachten sind.

Ressourcen-Planung

Ein SAP System kann ein Unternehmen oder eine Behörde nur dann optimal unterstützen, wenn die Rechner-Ressourcen auf das Einsatzszenario und auf die dabei benötigte SAP Software und deren Ressourcen-Anforderungen abgestimmt sind.

Im Ressourcen-Plan ist daher die Hardware-Ausstattung genau zu planen. Themen sind unter anderem:

- Anzahl der benötigten Rechner
- CPU- und Speicher-Ausstattung der Rechner
- benötigte Festplattenkapazitäten
- erforderliche Netz-Bandbreite
- notwendige Netzsegmente und Netzkoppelelemente

Die relevante SAP Dokumentation zur Ressourcen-Planung wird in M 2.346 *Nutzung der SAP Dokumentation* genannt. **SAP Informationsquellen**

Planen der SAP Systemlandschaft

Ein SAP System besteht immer aus mehreren Komponenten mit unterschiedlichen Aufgaben, die miteinander über die Netzinfrastruktur kommunizieren. Die Sicherheit eines SAP Systems kann schon durch die genutzte Architektur der Systemlandschaft positiv beeinflusst werden. Umgekehrt kann eine nicht hinreichend geplante und aufgebaute Systemlandschaft zu Sicherheitsproblemen führen.

Da die aus Sicherheitssicht günstigste Systemlandschaft sehr vom Einsatzszenario eines SAP Systems und dem Schutzbedarf der gespeicherten Daten abhängt, können in einem IT-Grundschutz-Baustein nur grundsätzliche Empfehlungen gegeben werden. SAP bietet jedoch in der Regel für verschiedene Produkte und Einsatzszenarien Empfehlungen für den günstigsten Systemaufbau an.

Allgemein sollte die Planung so erfolgen, dass nur die unbedingt benötigten Zugriffe auf und zwischen Komponenten möglich sind. Insbesondere ist eine Trennung von Produktiv-System, Test- und Abnahme-System sowie

Entwicklungs-System vorzusehen. Durch entsprechende Planung ist sicherzustellen, dass Produktivdaten eines SAP Systems nicht unverändert in Systeme für Tests und Abnahmen oder für die Entwicklung übertragen und dort genutzt werden. Kann dies nicht sichergestellt werden, müssen die Test- und Abnahme-Systeme so geschützt sein, dass auch dort die Vertraulichkeit der Daten gewährleistet ist.

Durch die Definition der Systemlandschaft muss unter anderem Folgendes festgelegt werden:

- Auf welchen Rechnern sind die einzelnen Komponenten zu installieren?
- Wo sind die einzelnen Rechner und Komponenten netztechnisch angesiedelt?
- Welche Komponenten müssen vor Zugriffen (intern, extern) durch entsprechende Firewalls oder Router geschützt werden?
- Auf welche Komponenten müssen Benutzer (intern, extern) direkt zugreifen? (Die entsprechenden Komponenten können daher nicht vollständig durch Firewalls oder Router geschützt werden.)
- Welche Komponenten müssen aufgrund des Zugriffsverhaltens in der DMZ (De-Militarisierte Zone) angesiedelt werden?
- Wie kann die Verfügbarkeit des gesamten SAP Systems gewährleistet werden?

Weitere Hinweise für spezielle Einsatzszenarien finden sich M 2.343 *Absicherung eines SAP Systems im Portal-Szenario* und M 2.344 *Sicherer Betrieb von SAP Systemen im Internet*.

SAP Informationsquellen

SAP Dokumentationen mit detaillierten Hinweisen zur empfohlenen Systemlandschaft finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Audit- und Logging-Konzept

Das Audit- und Logging-Konzept muss festlegen, welche Aktivitäten des SAP Systems und welche Aktivitäten der Benutzer zu protokollieren sind. Außerdem müssen folgende Aspekte berücksichtigt werden:

- Wer hat die Berechtigung, die Audit- und Protokoll-Einstellungen zu verändern?
- Wo werden die Protokolldaten abgelegt?
- Wer hat Zugriff auf die erstellen Protokolldaten?
- Wie erfolgt die Auswertung der erstellten Protokolldaten?
- Durch wen und in welchem Umfang erfolgen Sicherheitsprüfungen (Audits) und in welchen Abständen?

Ein SAP System besitzt umfangreiche Möglichkeiten, um interne Abläufe und Benutzeraktivitäten zu protokollieren. Die hier wichtigen Aspekte werden in *M 4.270* SAP Protokollierung thematisiert.

Neben der reinen Systemüberwachung, die durch die Protokollierung erreicht werden soll, ist im Rahmen von Audits die Sicherheit des SAP Systems regelmäßig zu prüfen. Audits können dabei sowohl durch Administratoren (Selbstkontrolle) als auch durch andere Prüfer erfolgen. Die Prüfer können dabei aus anderen Abteilungen stammen (IT-Sicherheit, Revision) oder aber von externen Dritten (IT-Auditoren, Wirtschaftsprüfer,

Aufsichtsorganisationen). Weitere Informationen dazu finden sich in M 2.347 *Regelmäßige Sicherheitsprüfungen für SAP Systeme*. Es ist zu beachten, dass Selbstkontrollen durch Administratoren nicht ausreichen, um die Sicherheit von SAP Systemen zu beurteilen.

Änderungsmanagement-Konzept

Die Aktualisierung eines SAP Systems durch Patches, Hot-Fixes und Updates ist wichtig, um die Sicherheit des Systems zu erhalten. Fehler in der Programmierung können nur behoben werden, wenn das System regelmäßig aktualisiert wird. Da sich die Änderungsmanagement-Prozesse von ABAP- und Java-Stack technisch unterscheiden, sind zwei separate Konzepte zu entwerfen. Folgende Fragestellungen sind jeweils durch das Konzept zu klären:

- Nach welchem Prozess erfolgt die Systemaktualisierung über die Systemvarianten Entwicklung, Test und Abnahme, Produktion?
- Wie wird sichergestellt, dass die eingespielten Updates den Betrieb nicht negativ beeinflussen?
- In welchen Zeitabständen erfolgt die Aktualisierung?
- Wer besitzt die Berechtigung, Aktualisierungen im Produktivsystem durchzuführen?
- An welchen Stellen des Änderungsmanagement-Prozesses müssen Kontrollschritte erfolgen?
- Wie wird sichergestellt, dass Aktualisierungen nicht durch eine einzelne Person durchgeführt werden können?
- Wie ist der Zugriff auf die Werkzeuge und Funktionen einzuschränken, die für die Aktualisierung benötigt werden?
- Wie werden Veränderungen protokolliert und dadurch nachvollziehbar gemacht?

Transportsystem

Änderungen werden in den ABAP-Stack über das so genannte Transportsystem eingespielt. Dabei können mehrere SAP Systeme zu einem Transportverbund (Transportdomäne genannt) zusammengeschaltet werden. Im Rahmen der Planung des Änderungsmanagement-Konzeptes ist daher ein Transportkonzept zu erstellen. Hier sind unter anderem folgende Fragestellungen und Aspekte zu klären:

- Wer darf Transporte erzeugen?
- Der Freigabeprozess für Transporte muss klar definiert werden, es müssen Qualitätsziele definiert sein, die eingehalten werden, bevor neue Transporte oder Patches eingespielt werden.
- Wer darf Transporte einspielen?
- Wie kommen die Transporte (technisch) von einem System zum anderen?
- Wie ist die Prozessreihenfolge zu definieren, so dass unterschiedliche Personen involviert werden, damit die benötigten Kontrollschritte durchgeführt werden?
- Es dürfen keine direkten Transporte durch Entwickler von der Entwicklung in Test und Abnahme oder die Produktion möglich sein.
- Welcher Integritätsschutz von Transportdateien soll eingesetzt werden?

- Wie ist die Nachvollziehbarkeit sicherzustellen? (Frage: Wer hat wann was gemacht?)
- Die Transportlandschaft muss geplant werden: Welche Instanzen und Mandanten sind jeweils involviert? Von welcher Quelle darf in welches Ziel transportiert werden?

Weitere Informationen und Empfehlungen finden sich in M 2.221 *Änderungsmanagement*, M 4.272 *Sichere Nutzung des SAP Transportsystems* und M 4.273 *Sichere Nutzung der SAP Java-Stack Software-Verteilung*.

SAP Informationsquellen

Hinweise aus SAP Dokumentationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Backup-Konzept

Bezüglich des Backup-Konzeptes bestehen keine außergewöhnlichen Anforderungen für ein SAP System. Im Backup-Konzept muss unter anderem Folgendes festgelegt werden:

- Wann werden welche Komponenten und Daten gesichert?
- Wer besitzt die Berechtigung dazu?
- Wer besitzt die Berechtigung zum Wiederherstellen von Daten?
- Wer besitzt Zugriff auf die archivierten Backup-Daten?
- Wo werden die Backup-Daten sicher gelagert? Hier ist besonders darauf zu achten, dass Backup-Daten räumlich getrennt von Produktivdaten gelagert werden.

Die Verantwortlichkeiten und Prozessabläufe sind zu definieren und umzusetzen. Das SAP Backup-Konzept sollte sich in ein bestehendes Backup-Verfahren integrieren, so dass keine speziellen Ausnahmeprozeduren notwendig werden.

Ein funktionierendes Backup-Konzept ist insbesondere im Rahmen der Notfallvorsorge (siehe M 6.97 *Notfallvorsorge für SAP Systeme*) wichtig.

Notfallvorsorge-Konzept

Das Notfallvorsorge-Konzept für SAP Systeme muss geschäftskritische Notfälle und zugehörige Notfall-Prozeduren definieren. Folgende Notfälle sollten mindestens berücksichtigt werden:

- Ausfall eines SAP Servers
- Ausfall der Datenbank eines SAP Systems
- Kompromittierung eines SAP Systems
- Ausfall des Transportsystems (ABAP) oder der Software-Verteilung (JAVA)
- Ausfall eines kompletten Rechenzentrums

Die Verantwortlichkeiten im Rahmen der Notfallvorsorge (siehe auch M 6.97 *Notfallvorsorge für SAP Systeme*) und für die definierten Notfall-Prozeduren müssen eindeutig Personen zugeordnet werden. Es empfiehlt sich, regelmäßig Notfallübungen durchzuführen und die Prozesse anhand der dabei gemachten Erfahrungen anzupassen.

Ergänzende Kontrollfragen:

- Ist der SAP Einsatz umfassend geplant worden?

- Sind alle Einsatzszenarien bekannt und bedacht?
- Stehen die erstellten SAP Sicherheitsteilkonzepte im Einklang mit bestehenden Sicherheitskonzepten?
- Wurden der Personal- oder Betriebsrat, der Datenschutzbeauftragte und die IT-Sicherheitsverantwortlichen in die Planungen mit einbezogen?
- Sind die Produktivsysteme von Entwicklungs-, Test- und Abnahmesystemen isoliert?
- Sind regelmäßige Notfallübungen geplant?

M 2.342 Planung von SAP Berechtigungen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Leiter IT

Erklärung der wichtigsten Begriffe

Berechtigungen in einem SAP System steuern die Zugriffsmöglichkeiten seiner Benutzer. Die Sicherheit der Geschäftsdaten hängt daher direkt von den eingestellten Berechtigungen ab. Aus diesem Grund muss die Vergabe von Berechtigungen sorgfältig geplant und durchgeführt werden, um die gewünschte Sicherheit zu erreichen.

Berechtigungen

Die Funktionen eines SAP Systems (z. B. Programme oder Reports, generell Applikationen im SAP System) werden über Transaktionen aufgerufen, die dabei unterschiedliche Operationen oder Aktivitäten (z. B. Schreiben, Lesen, Löschen) auf Daten ausführen können. Die über Transaktionen gestarteten Applikationen prüfen beim Aufruf, ob der aufrufende Benutzer über die notwendigen Berechtigungen verfügt, die angeforderte Operation auf den durch die Applikation angesprochenen Daten auszuführen.

Berechtigungsobjekte

Der Prüfmechanismus baut auf so genannten Berechtigungsobjekten auf, die Autorisierungsfelder besitzen. Eine konkrete Berechtigung kann als Ausprägung eines Berechtigungsobjektes mit ausgefüllten Autorisierungsfeldern verstanden werden. Beim Start einer Transaktion prüft der SAP Kern zunächst, ob der Benutzer die Berechtigung zum Start der Transaktion besitzt. Nach dem Start kann die Transaktion auch weitere Berechtigungsprüfungen durchführen. Geprüft wird, ob der zugreifende Benutzer eine Berechtigung besitzt, die vom benötigten Berechtigungsobjekt abgeleitet ist. Ist dies der Fall, werden die Autorisierungsfelder der Berechtigung daraufhin geprüft, ob sie die benötigten Werte oder Wertekombinationen enthalten. Eine Transaktion kann dabei auf mehrere Berechtigungen prüfen. Welche dies sind, wird im Programm-Code festgelegt. Beim Start einer Transaktion wird vom SAP Kern immer auf das Berechtigungsobjekt S_TCODE geprüft. Beim Start von Applikationen wird auf das Berechtigungsobjekt S_PROGRAM geprüft. Die eigentliche Prüfung erfolgt also immer durch den Kern des SAP Systems, auch wenn diese durch den Programm-Code der Transaktion angestoßen wird.

Organisationsebenen

Aus Applikationssicht sind insbesondere diejenigen Autorisierungsfelder von Berechtigungsobjekten wichtig, die als so genannte Organisationsebenen ausgeprägt werden müssen. Sie berechtigen dann eine Rolle, eine bestimmte Transaktion, beispielsweise für den angegeben Buchungskreis (oftmals eine zusammenhängende Geschäftseinheit eines Unternehmens, z. B. Tochterunternehmen) durchzuführen.

Rollen und Profilgenerator

Berechtigungen werden Benutzern dadurch zugeordnet, dass ihnen so genannte Rollen zugeordnet werden. Rollen geben an, welche Transaktionen durch den Benutzer ausgeführt werden sollen, dem eine Rolle zugeordnet wurde. Da jede Transaktion auf bestimmte, durch den Programm-Code festgelegte Berechtigungsobjekte prüft, kann für jede Rolle ein Berechtigungsprofil (d. h. Menge von Berechtigungen) abgeleitet werden, in dem alle Berechtigungsobjekte enthalten sind, die zur Ausführung der

Transaktionen generell benötigt werden. Der Prozess, das Berechtigungsprofil für eine Rolle und die darin enthaltenen Transaktionen zu erstellen, wird über den Profilgenerator (Transaktion PFCG) automatisiert.

Prüfkennzeichen für Transaktionen

Über Prüfkennzeichen für Transaktionen kann gesteuert werden, für welche Berechtigungsobjekte, auf die eine Transaktion prüft, der SAP Kern tatsächlich eine Prüfung ausführt. Über die Prüfkennzeichen können folglich Berechtigungsobjekte beim Aufruf einer Transaktion von der Prüfung ausgeschlossen werden. In diesem Fall wird durch den Profilgenerator auch keine Berechtigung im generierten Berechtigungsprofil erzeugt. Die Prüfkennzeichen werden über die Transaktion SU24 gepflegt, hier werden auch für die einzelnen Autorisierungsfelder der Berechtigungsobjekte die Werte gepflegt, die durch den Profilgenerator in die generierten Berechtigungen der Profile eingetragen werden. Es handelt sich dabei um Vorschlagswerte. Die Profile, die durch den Profilgenerator erzeugt werden, müssen unter Umständen noch manuell nachbearbeitet werden.

Planungsschritte bei der Vergabe von Berechtigungen

Definition von Rollen

Die Vergabe von Berechtigungen in einem SAP System ist also ein mehrstufiger Prozess. Zunächst müssen die benötigten Rollen definiert werden. Wichtig ist dabei, dass die Rollen letztendlich Arbeitsplätze oder Positionen im Unternehmen oder der Behörde beschreiben. Sie sollten nicht auf einzelne Mitarbeiter bezogen sein, sonst wird die Anzahl an Rollen unübersichtlich und unbeherrschbar. Ein gutes Berechtigungskonzept steht und fällt damit, ob die definierten Rollen sorgfältig spezifiziert wurden.

Erzeugung von Berechtigungsprofilen

Sind die Rollen definiert, müssen die zugehörigen Berechtigungsprofile durch den Profilgenerator erzeugt werden. Der Umfang der erzeugten Berechtigungen in den Rollenprofilen wird durch die Konfiguration der Prüfkennzeichen beeinflusst. Auch dies muss sorgfältig geplant werden, da abgeschaltete Prüfungen immer auch einen gewissen Grad an Sicherheitsverlust bedeuten. Die erzeugten Profile und enthaltenen Berechtigungen sind zu prüfen und gegebenenfalls anzupassen.

Zuweisung der Rollen

Abschließend werden die Berechtigungen Benutzern dadurch zugewiesen, dass einem Benutzer eine Rolle zugeordnet und der so genannte Benutzerabgleich angestoßen wird. Dadurch werden im Benutzerstammsatz die im Berechtigungsprofil der Rolle enthaltenen Berechtigungen gespeichert.

Berechtigungskonzept

Das Berechtigungskonzept für ein SAP System muss in zwei Ausprägungen erstellt werden: für den ABAP-Stack und für den Java-Stack. Es gilt dabei zu beachten, dass sich das Berechtigungssystem des Java-Stacks fundamental von dem des ABAP-Stacks unterscheidet. Konzeptionell sind jedoch die gleichen Fragestellungen zu betrachten. Dies sind unter anderem:

- Welche Rollen werden benötigt?
- Welche Rolle darf welche Funktionen des SAP Systems aufrufen (z. B. Transaktionen, Programme oder Reports)?
- Welche Rolle darf auf welche Daten des SAP Systems zugreifen?

- Welche administrativen Rollen mit welchen Berechtigungen werden benötigt, um das geplante Administrationskonzept umzusetzen?
- Nutzen Applikationen neben dem SAP Standardberechtigungssystem noch weitere Berechtigungen? Diese sind entsprechend im Konzept zu berücksichtigen und zu planen.
- Welche Prozesse für die Berechtigungsverwaltung sind mit den zugehörigen Verantwortlichkeiten zu definieren (z. B. Beantragung, Genehmigung, Anlegen, Verändern, Löschen)?
- Sind Funktionstrennungsaspekte im Berechtigungskonzept ausreichend beachtet? Hier spielen insbesondere auch rechtliche Anforderungen eine Rolle.
- Wird beim Änderungsmanagement auch das Risikopotential betrachtet, welches durch eine Berechtigungshäufung entstehen kann?

Es ist darauf zu achten, dass für alle anfallenden Vorgänge im Kontext von Berechtigungen Prozesse definiert werden und die Prozesse vollständig spezifiziert sind. Zusätzlich sind die jeweiligen Verantwortlichkeiten vollständig festzulegen. So wird verhindert, dass sich durch unklare Verantwortlichkeiten oder unvollständig definierte Prozesse Sicherheitslücken einschleichen.

Rahmenbedingungen bei der Planung von Berechtigungen

Die Definition der Rollen und der zugeordneten Berechtigungen muss sich einerseits an den Erfordernissen der Institution orientieren, andererseits müssen hier auch die Anforderungen einbezogen werden, die sich aus den rechtlichen Rahmenbedingungen ergeben, wie beispielsweise dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KontrAG), der Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) oder dem Bundesdatenschutzgesetz (BDSG). Eine ausführliche Planung ist daher unumgänglich. Je detaillierter die Erfordernisse der Rollen bekannt sind, desto besser können später die Berechtigungen vergeben werden. Dabei ist auf die notwendige Trennung zwischen Rollen zu achten. Es ist empfehlenswert, die Rollen, und damit die Berechtigungen, an die interne Organisationshierarchie und die darin existierenden Positionen und Stellen anzupassen. So kann beispielsweise erreicht werden, dass bei Positionswechseln von Mitarbeitern deren alte Berechtigungen nicht mehr verfügbar sind.

Beteiligung von verantwortlichen Stellen

Wichtig ist außerdem, dass im Unternehmen oder in der Behörde Verantwortliche für Informationen und Prozesse ernannt werden (Informationseigentümer bzw. Verfahrensverantwortliche), die einen bestimmten Datenbestand der Organisation verantworten. Beispielsweise ist der Leiter der Finanzabteilung (Chief Financial Officer, CFO) für den Finanz- und Controllingbereich verantwortlich. Die Verantwortlichen aller Bereiche sind unbedingt in die Planung der benötigten Rollen, Berechtigungen und Prozesse einzubeziehen, da nur sie die dazu notwendigen Kenntnisse auf fachlicher Ebene besitzen. Administratoren sind in der Regel nicht in der Lage, die Rollen und Berechtigungen auf Applikationsebene alleine zu planen.

Im Rahmen der Berechtigungsplanung ist auch Folgendes festzulegen:

- Welche Berechtigungen sind als kritisch zu betrachten (d. h. erlauben kritische Operationen im SAP System unter administrativen, rechtlichen oder betriebswirtschaftlichen Aspekten)?
- Welche Rollen dürfen welche kritischen Berechtigungen, Profile oder Rollen erhalten?
- Welche Rollen dürfen welche Werte für kritische Berechtigungsfelder erhalten?

Weitere Hinweise zur Definition von kritischen Berechtigungen finden sich in M 4.261 *Sicherer Umgang mit kritischen SAP Berechtigungen.*

ABAP-Stack

Im Detail unterscheiden sich die Konzepte für den ABAP- und Java-Stack sehr. Für den ABAP-Stack muss die Berechtigungsverwaltung über den Profilgenerator und nicht manuell erfolgen. Generell muss von der manuellen Verwaltung dringend abgeraten werden, da dies häufig zu Fehlkonfigurationen der Berechtigungen führt. Durch den Profilgenerator wird sichergestellt, dass die Benutzer nur die Berechtigungen erhalten, die zum Ausführen derjenigen Transaktionen notwendig sind, die ihnen über die Rollen zugeordnet wurden. Daher ist wichtig, dass insbesondere die Konzepte, Prozesse und Abläufe auf die Verwendung des Profilgenerators abgestimmt sind.

JAVA-Stack

Für den JAVA-Stack besteht hingegen keine Wahlmöglichkeit, da der Berechtigungsmechanismus der Spezifikation der Java 2 Enterprise Edition (J2EE) genutzt werden muss. Es ist dabei zu beachten, dass die "User Management Engine" (UME) über diesen Standard hinausgehende Optionen anbietet.

Weitere Informationen finden sich in M 4.260 *Berechtigungsverwaltung für SAP Systeme*, in M 4.262 *Konfiguration zusätzlicher SAP Berechtigungsprüfungen* sowie in M 4.268 *Sichere Konfiguration der SAP Java-Stack Berechtigungen*.

SAP Informationsquellen

Hinweise auf SAP Dokumentationen, die bei der Planung des Berechtigungskonzeptes genutzt werden können, finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Planen der Berechtigungsverwaltung

Die Verwaltung der Berechtigung muss geplant und das gewünschte Verwaltungskonzept muss definiert werden. Im Wesentlichen ist dabei zu berücksichtigen, welche Aufgaben in der Berechtigungsverwaltung durch wen erledigt werden. Hier empfiehlt sich ein rollenbasierter Ansatz (siehe auch M 4.260 *Berechtigungsverwaltung für SAP Systeme)*, so dass den definierten Rollen später konkrete Benutzer und damit Personen zugeordnet werden können. Dabei ist zu beachten, dass unvereinbare Rollen (Funktionstrennung) nicht derselben Person zugeordnet werden. Da in einer Organisation auch für die Berechtigungsverwaltung schon eine Vielzahl an Rollen impliziert sind, müssen diese entsprechend abgebildet werden.

So gibt es beispielsweise in der Regel keine einzelne Administrator-Rolle, vielmehr sind Rollen wie Benutzer-Administrator, Rollen-Administrator, Berechtigungs-Administrator, Entwickler, Help-Desk-Mitarbeiter oder Transport-Manager zu betrachten. Folglich sind die von SAP vordefinierten Rollen in der Regel nicht ohne Anpassungen zu benutzen.

Ergänzende Kontrollfragen:

- Sind die Rollen und Berechtigungen adäquat geplant worden?
- Wurden applikationsspezifische Berechtigungen und Berechtigungs-mechanismen bei der Planung berücksichtigt?
- Wurden die Verantwortlichen auf geschäftlicher Ebene in die Planung einbezogen?
- Ist die Verwaltung der Berechtigungen mit allen Prozessen geplant und wurden die Verantwortlichkeiten vollständig definiert

M 2.343 Absicherung eines SAP Systems im Portal-Szenario

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Leiter Entwicklung

Verantwortlich für Umsetzung: Administrator, Entwickler

SAP Systeme werden immer häufiger auch in Portal-Szenarien eingesetzt. Im Folgenden wird davon ausgegangen, dass es sich um ein internes Behörden- oder Unternehmensportal handelt, über welches auf ein SAP System zugegriffen wird. Diese Maßnahme behandelt nicht die Sicherheit des Behörden- oder Unternehmensportals, sondern die Sicherheit eines SAP Systems im Umfeld des Portales. Für SAP Systeme in Internetszenarien finden sich entsprechende Maßnahmen in M 2.344 *Sicherer Betrieb von SAP Systemen im Internet*. Der Zugriff in Portal-Szenarien erfolgt in der Regel über HTTP, und Benutzer setzen dafür einen Browser ein.

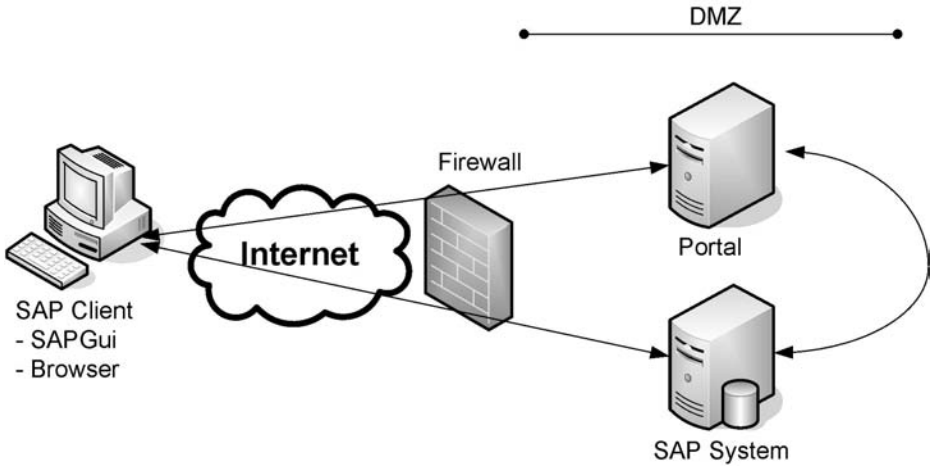


Abbildung: SAP System im Portal-Szenario

In Portalszenarien wird oft fälschlich angenommen, dass das eingesetzte Portal auf das "nachgelagerte" SAP System zugreift. Ein direkter Benutzerzugriff auf das SAP System wäre dann nicht notwendig. In der Regel erfolgt jedoch im Portal nur eine Umleitung auf das SAP System, so dass die Benutzeranfragen direkt an das SAP System erfolgen. Dies ist oft sogar transparent für den Benutzer, da die im Browser angezeigten Daten innerhalb der aufgerufenen Portalseite in einem Rahmen eingeblendet werden. Insofern ist auch in Portal-Szenarien die Maßnahme M 2.344 *Sicherer Betrieb von SAP Systemen im Internet* relevant.

Grundsätzliche Aspekte

Generell sind für SAP Systeme in Portal-Szenarien folgende grundsätzliche Aspekte wichtig:

- Architektur des Netz- und Systemaufbaus (siehe auch M 2.341 *Planung des SAP Einsatzes*)
- Kommunikationsabsicherung (siehe auch M 5.125 *Absicherung der Kommunikation von und zu SAP Systemen*)
- Sicherheit von Anwendungen im Internet-Einsatz

- Erkennen von Angriffen (Intrusion Detection Systeme)
- Schutz vor Viren beim Hoch- oder Herunterladen von Dateien (siehe auch M 4.271 *Virenschutz für SAP Systeme*)

Folgende Aspekte, die sich direkt aus dem Portal-Szenario ableiten, sind besonders zu berücksichtigen:

Systemzugriff einschränken

Alle SAP Systeme, die durch Browser-Umleitungen angesprochen werden, müssen für Benutzer zugreifbar sein. Dieser Umstand ist in der Risikobetrachtung zu berücksichtigen und hat Auswirkungen auf die Position des SAP Systems im Netz, da es beispielsweise in der DMZ (Demilitarisierte Zone) angesiedelt werden muss.

Der Zugriff auf die betroffenen SAP Systeme muss durch eine Firewall auf die Ports beschränkt werden, über die HTTP bzw. HTTPS abgewickelt wird. Je nach Szenario sollte der Zugriff auf das SAP System über einen Reverse Proxy geleitet werden, so dass auf das SAP System nicht direkt zugegriffen wird.

Dialogzugriff einschränken

In der Regel darf der SAPGui-Zugang für die über das Portal angesprochenen SAP Systeme nur eingeschränkt zugelassen werden. Insbesondere für Benutzer, die nur über das Portal mittels Browser zugreifen, muss der SAPGui-Zugang unterbunden werden. Hier können beispielsweise Benutzer vom Typ "Internetbenutzer" eingesetzt werden, wenn der Port-Zugang nicht durch die Firewall beschränkbar ist. Es ist generell zu bedenken, dass der SAPGui-Zugang für Administratoren möglich sein muss, so dass die Firewall entsprechend zu konfigurieren ist. Alternativ kann auch eine separates Administrationsnetz genutzt werden.

Internet Transaction Server (ITS)

Wird der Internet Transaction Server (ITS) zum Zugriff auf das SAP System nicht genutzt, sollte der ITS Zugang deaktiviert werden, da dieser einen SAPGui-ähnlichen Zugang zum SAP System bietet. Die ITS Komponente muss vor der Version 6.40 des SAP Web Application Servers als separate Komponente (WGate, AGate) installiert werden. In diesem Fall sollten diese Komponenten nicht installiert oder aber deinstalliert werden.

Ab Version 6.40 ist der ITS integriert, so dass die entsprechenden Dienste im ABAP-Stack (z. B. webgui) und Java-Stack (z. B. mi oder me) deaktiviert werden müssen. Dies erfolgt im ABAP-Stack dadurch, dass der ICF-Dienst "webgui" deaktiviert ist (siehe auch M 5.127 *Absicherung des SAP Internet Connection Framework (ICF)*). Im Java-Stack (siehe auch *Systeme*M 4.266 Sichere Konfiguration des SAP Java-Stacks) sind die Applikationen "mi" und "me" über den Deploy-Dienst zu deaktivieren.

Authentisierung/Single Sign-On

In der Regel ist Single Sign-On zwischen dem Portal und dem SAP System konfiguriert. Daher ist sicherzustellen, dass Konten mit gleichen Namen in beiden Systemen der gleichen Person zugeordnet sind. Kann dies nicht sichergestellt werden, so muss der so genannte Benutzer-Mapping-Mechanismus des Portals genutzt werden. Beim Zugriff auf das SAP System

werden dann die hinterlegten Konten-Informationen genutzt. In diesem Fall ist dann auf die Konsistenz der Benutzer-Mapping-Informationen zu achten.

Berechtigungen

In Portal-Szenarien kann der Fall auftreten, dass Applikationen, die im Portal ablaufen (Frontend-Applikation), selbst direkt auf das SAP System zugreifen. Je nach Applikationsdesign wird dann ein technisches Konto oder das Konto des angemeldeten Benutzers zum Zugriff genutzt. Für dieses Konto darf im SAP System dann nur der Aufruf derjenigen ABAP-Funktionsgruppen erlaubt sein, die für die Portalanwendung benötigt werden.

Generell ist darauf zu achten, dass die Berechtigungen der im SAP System gehaltenen Benutzer minimal gestaltet werden. Bei den Planungen sollte davon ausgegangen werden, dass die Berechtigungsprüfung der Frontend-Applikation auch unterlaufen werden kann. Wird der Benutzer vom Portal lediglich umgeleitet, so greift er direkt auf das SAP System zu. Daher sollten die Berechtigungen im SAP System immer so eingerichtet sein, dass nur die Funktionen aufgerufen werden können, die durch die Portal-Applikation möglich sind. Dies ist insbesondere dann wichtig, wenn der Dialog-Zugriff von Portal-Benutzern nicht ausgeschlossen ist.

Sitzungsmanagement der Applikationen

Alle Applikationen des ABAP- und des Java-Stacks, die über das Portal genutzt werden, sollten ein sicheres Sitzungsmanagement implementieren. Insbesondere ist durch die Programmierung der Applikationen sicherzustellen, dass Sitzungsinformationen bei der Benutzerabmeldung vom Portal ungültig werden.

Es ist zu bedenken, dass die Abmeldung vom Portal nicht automatisch zur Abmeldung am SAP System führt. Dies ist immer dann ein Problem, wenn ein Client-Rechner von mehreren Personen genutzt wird, da dann ein nachfolgender Benutzer unter Umständen auf die Daten des vorherigen Benutzers im SAP System zugreifen kann.

SAP Informationsquellen

SAP stellt Programmier-Frameworks (z. B. Business Server Pages, BSP) zur Verfügung, die eine automatisierte Abmeldung am SAP System anbieten. Bei Eigenentwicklungen sollte dies bei der Entscheidung, welche Technologie bzw. Framework zur Implementierung genutzt wird, berücksichtigt werden.

Ergänzende Kontrollfragen:

- Wurde eine Risikobetrachtung basierend auf den tatsächlichen Zugriffsanforderungen für das SAP System durchgeführt?
- Ist der mögliche Systemzugriff auf das notwendige Minimum beschränkt?
- Ist der Dialogzugriff unterbunden, wenn dieser nicht benötigt wird?
- Sind die eingesetzten Applikationen mit einem sicheren Sitzungsmanagement ausgerüstet, das auch in Portal-Szenarien funktioniert?

M 2.344 Sicherer Betrieb von SAP Systemen im Internet

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Leiter Entwicklung

Verantwortlich für Umsetzung: Administrator, Entwickler

SAP Systeme werden immer häufiger auch in Internet-Szenarien eingesetzt. In der Regel sind dann entsprechende Zusatzapplikationen installiert, oder sie werden im Rahmen von Internet-Portal-Szenarien (siehe auch M 2.343 *Absicherung eines SAP Systems im Portal-Szenario*) als "Backend-Systeme" eingesetzt. Der Zugriff in Internet-Szenarien erfolgt in der Regel über HTTP, und Benutzer setzen dafür einen Browser ein.

Daher sind in Internet-Szenarien folgende Aspekte zu berücksichtigen:

Systemzugriff nach Risikobetrachtung einschränken

Alle SAP Systeme, die direkt aus dem Internet angesprochen werden, sind einem erhöhten Risiko ausgesetzt. Dies ist in der Risikobetrachtung zu berücksichtigen. Der Zugriff auf die betroffenen SAP Systeme muss durch eine Firewall auf die Ports beschränkt werden, über die HTTP bzw. HTTPS abgewickelt wird.

Generell gelten für den Zugriff auf ein SAP System aus dem Internet die gleichen Anforderungen, wie für jedes andere System, beispielsweise einen Web-Server (siehe auch B 5.4 *Webserver*). Daher sind die allgemeinen, relevanten Maßnahmen für vernetzte Systeme mit Internetanschluss zu berücksichtigen. So kann es beispielsweise sinnvoll sein, auf das SAP System über einen Reverse Proxy oder eine Applikationsfirewall (siehe auch Baustein B 3.301 *Sicherheitsgateway (Firewall)*) zuzugreifen.

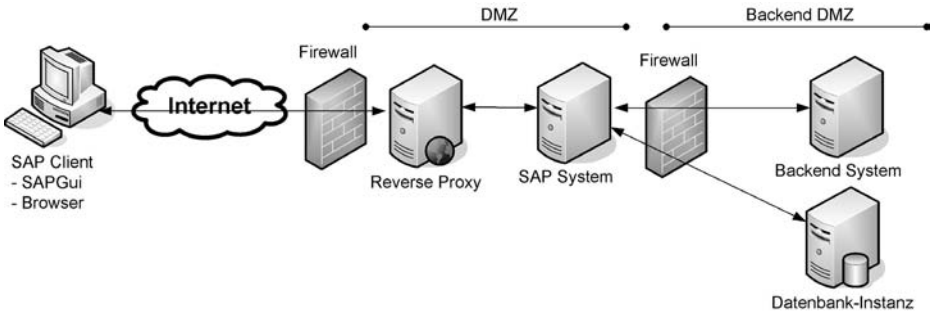


Abbildung: SAP System im Internet

Kommunikationsschnittstelle prüfen und absichern

Über die HTTP-basierten Schnittstellen werden Applikationen angeboten. Sowohl für die System-Applikationen als auch für normale Applikationen muss eine Risikobetrachtung erfolgen. Weiterhin ist eine Sicherheitsprüfung der Web-Schnittstelle sinnvoll, um die Gefährdung gegenüber typischen Web-basierten Angriffen einschätzen zu können.

Generell ist zu bedenken, dass über die HTTP-Schnittstelle auch RFC-Zugriffe möglich sind. Daher dürfen nur die Dienste aktiviert werden, die benötigt werden und die sorgfältig auf ihre Eignung zum Betrieb im Internet hin geprüft wurden.

Dialogzugriff einschränken

Der direkte SAPGui-Zugriff auf SAP Systeme über das Internet sollte ausgeschlossen werden und durch eine Firewall auf die Protokolle HTTP und HTTPS beschränkt sein.

Internet Transaction Server

Wird der Internet Transaction Server (ITS) zum Zugriff auf das SAP System nicht genutzt, so sollte der ITS Zugang deaktiviert werden, da dieser einen SAPGui-ähnlichen Zugang zum SAP System bietet.

Die ITS Komponente muss vor der Version 6.40 des SAP Web Application Servers als separate Komponente (WGate, AGate) installiert werden. In diesem Fall sollten diese einfach nicht installiert sein. Ab Version 6.40 ist der ITS integriert, so dass die entsprechenden Dienste im ABAP-Stack (z. B. Webgui, siehe M 5.127 *Absicherung des SAP Internet Connection Framework (ICF)*) und Java-Stack (z. B. mi oder me, siehe M 4.266 *Sichere Konfiguration des SAP Java-Stacks*) deaktiviert werden müssen.

Wird der ITS genutzt, so muss in Hinblick auf die Berechtigungen im SAP System sorgfältig geprüft werden, ob nur die jeweils erlaubten Funktionen aufgerufen werden können. Stichprobenprüfungen reichen in diesem Fall nicht aus. Die Prüfung ist unter Umständen mit erheblichem Aufwand verbunden. Insbesondere sollten alle Transaktionen, auf die nicht zugegriffen werden soll, deaktiviert werden, um auszuschließen, dass diese durch kritische Berechtigungskombinationen aufgerufen werden können. Da ein SAP System mehrere tausend Transaktionen enthalten kann, ist dies ein zeitintensiver Konfigurationsprozess, der in der Regel nicht geleistet werden kann. Daher muss die Gefährdung durch ein sorgfältig durchdachtes Berechtigungskonzept möglichst gering gehalten werden.

Authentisierung/Single Sign-On

Single Sign-On Zugriffe aus dem Internet sollten nur zwischen den für den Internet-Zugriff freigegebenen Systemen aktiviert sein.

Für externe Systeme sollten keine Vertrauensstellungen konfiguriert werden, da die Sicherheit für diese nicht kontrolliert werden kann.

Berechtigungen

Es ist darauf zu achten, dass die Berechtigungen der im SAP System gehaltenen Benutzer minimal gestaltet werden. Es empfiehlt sich, für Benutzer, die keinen SAPGui-Zugriff benötigen, Konten vom Typ Kommunikations- oder Internet-Benutzer einzusetzen.

Validieren von Daten aus SAP Systemen mit Internet-Zugriff

Daten, die von SAP Systemen mit Internetzugriff an Systeme ohne Internetzugriff weitergegeben werden - etwa durch Anfragen oder durch Datentransport - müssen validiert werden, bevor sie an das Backend-System weitergesendet werden.

Verfügbare Daten

Werden Daten aus internen SAP Systemen über SAP Systeme mit Internet-Zugriff bereitgestellt, so sollte Folgendes geprüft werden:

- Es sollte geprüft werden, ob es tatsächlich erforderlich ist, dass die Daten über direkte Zugriffe auf die internen Systeme bereitgestellt werden oder ob periodische Datenexporte und -importe möglich sind. Dies verhindert den Zugriff auf interne Systeme von außen.
- Beim Exportieren von Daten sollte geprüft werden, ob alle Informationen exportiert werden müssen oder ob tatsächlich nur ein Teil der Informationen benötigt wird. Dies beschränkt die auf dem SAP System mit Internetzugriff gespeicherten Daten.

Bei Export-/Import-Lösungen ist zu beachten, dass dies die direkte Applikationsintegration (etwa für CRM oder SRM Systeme) unterbindet, so dass die Vorteile der direkten Integration nicht mehr genutzt werden können. Zusätzlich muss der Datentransport konfiguriert und verwaltet werden. Daher bietet sich diese Lösung in der Regel nur für einfache Szenarien an.

Ergänzende Kontrollfragen:

- Wurde eine Risikobetrachtung für das SAP System durchgeführt, die die Internet-Anbindung angemessen berücksichtigt?
- Ist der mögliche Systemzugriff auf das notwendige Minimum beschränkt?
- Werden nur die benötigten Dienste angeboten?
- Sind die angebotenen Dienste einer erfolgreichen Sicherheitsprüfung unterzogen worden?

M 2.345 Outsourcing eines SAP Systems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Beim Outsourcing von SAP Systemen ist Folgendes zu beachten:

- Die Maßnahmen des Bausteines B 1.11 Outsourcing sind beim Outsourcing-Partner umzusetzen.
- Besonderes Augenmerk verdient die reibungslose Prozessintegration, damit beispielsweise auch Rückmeldungen vom Outsourcing-Partner zum Outsourcing-Auftraggeber erfolgen. Dies trifft auch auf die Prozesse im Kontext der Benutzer- und Berechtigungsverwaltung zu.
- Es empfiehlt sich, eine Tabelle mit allen Aufgaben, die für ein SAP System anfallen, aufzustellen. In dieser Tabelle sollte vermerkt werden, welche Aufgaben durch Mitarbeiter des Outsourcing-Partners und welche durch eigene Mitarbeiter durchgeführt werden. Die verantwortlichen Personen sind zu dokumentieren. Die nachfolgende Tabelle ist als unvollständiges Beispiel zu verstehen und muss auf die lokalen Gegebenheiten angepasst werden. Die Aufgaben müssen in der Regel in Unteraufgaben verfeinert werden.

Aufgabe	Verantwortlich
Planung des SAP Systems	Unternehmen/Behörde (Outsourcing-Partner jedoch einbeziehen)
Definition des Berechtigungskonzeptes	Unternehmen/Behörde
Installation des SAP Systems	Outsourcing-Partner
Basis-Konfiguration des SAP Systems	Outsourcing-Partner (mit Vorgaben durch das Unternehmen bzw. der Behörde aus der Planungsphase)
Konfiguration auf Ebene von Modulen oder Applikationen	Unternehmen/Behörde (entsprechend der Vorgaben aus der Planungsphase)
Basis-Administration - Anlegen von Benutzern	Outsourcing-Partner (nach Auftrag durch Unternehmen bzw. Behörde, bei Rollentrennung beim Outsourcing-Partner)
Basis-Administration - Verwalten von Berechtigungen	Outsourcing-Partner (nach Auftrag durch Unternehmen bzw. Behörde, bei Rollentrennung beim Outsourcing-Partner)

Applikationsadministration - Anlegen von Benutzern	Unternehmen/Behörde (nach internem Genehmigungsprozess)
Applikationsadministration - Verwalten von Berechtigungen	Unternehmen/Behörde (nach internem Genehmigungsprozess)
Einspielen von Updates und Patches	Outsourcing-Partner

Erläuterungen:

- In der Regel erfolgt der Betrieb der Rechner und die Basis-Administration des SAP Systems durch den Outsourcing-Partner. Die Applikationsverwaltung und -administration erfolgt in der Regel durch den Outsourcing-Auftraggeber. Es ist zu beachten, dass der Outsourcing-Partner über die applikationsspezifischen (Sicherheits-) Anforderungen informiert wird. Nur so kann eine adäquate Basis-Administration erfolgen.
- Es sollten regelmäßige Abstimmungen für den Bereich Sicherheit erfolgen. Dabei können geänderte Anforderungen des Outsourcing-Auftraggebers und Vorschläge des Outsourcing-Partners zum Erhöhen der Sicherheit diskutiert werden.
- Im Rahmen der Risikobetrachtung ist zu bedenken, dass der Outsourcing-Partner volle Kontrolle über die Daten des betriebenen SAP Systems hat. Dies ist aus Sicherheitssicht für alle Behörden und Unternehmen kritisch zu betrachten. Die Verfügbarkeit entsprechender Kontrollen wird beispielsweise auch im Sarbanes Oxley Umfeld geprüft.
- Werden sensitive Daten verarbeitet, die eine besondere Sorgfaltspflicht implizieren, die sich auch aus gesetzlichen Vorgaben ableiten oder explizit gefordert sind, so muss auch der Outsourcing-Partner entsprechend in die Pflicht genommen werden. Der Outsourcing-Partner muss dann durch eine entsprechende Geheimhaltungsverpflichtung rechtlich gebunden werden.
- Für die Benutzer- und Berechtigungsverwaltung ist es sinnvoll, dass ein Mitarbeiter des Outsourcing-Auftragnehmers in den Prozess der Berechtigungsplanung eingebunden ist, denn nur so kann der Outsourcing-Partner beispielsweise den applikationsbezogenen Sicherheitsansprüchen Rechnung tragen.

Ergänzende Kontrollfragen:

- Liegt ein adäquates Outsourcing-Konzept für das SAP System vor?
- Ist die Aufgabenverteilung unter Sicherheitsgesichtspunkten sinnvoll und sind die Verantwortlichkeiten für alle Aufgaben geregelt und dokumentiert?
- Stellen die Prozesse für die Benutzer- und Berechtigungsverwaltung sicher, dass auch im Outsourcing-Szenario keine Berechtigungen angesammelt werden können?

M 2.346 Nutzung der SAP Dokumentation

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Leiter IT, Entwickler

SAP stellt eine Vielzahl von Dokumenten und Informationen zur Verfügung. Die verfügbare Dokumentation muss insbesondere Administratoren bekannt sein und regelmäßig auf Aktualisierungen geprüft werden.

SAP stellt Informationen zentral über den SAP Service Marketplace (http://service.sap.com) zur Verfügung. Es ist zu beachten, dass zum Zugriff JavaScript im Browser aktiviert sein muss und meist eine Authentisierung erfolgen muss. Eine Ausnahme bildet das SAP Help Portal, über das die Produkt-Dokumentationen erhältlich sind.

Der SAP Service Marktplatz verweist auf weitere Informationsquellen. Im Folgenden werden einige Beispiele genannt:

- Über den SAP Service Marktplatz werden SAP Hinweise oder zusätzliche Software angeboten. Wichtig sind hier auch die sicherheitsrelevanten Informationen, die unter dem Quicklink "/security" zu finden sind. Hier kann auch der SAP Security Newsletter abonniert werden, über den sicherheitsrelevante Informationen per E-Mail verteilt werden. Wichtig sind außerdem die SAP Produkt-Sicherheitsleitfäden, die unter dem Quicklink "/securityguide" angeboten werden. Im vorliegenden Kontext ist insbesondere der SAP NetWeaver Sicherheitsleitfaden relevant.
- Über das SAP Help Portal (http://help.sap.com) sind für alle Produkte Anleitungen und umfangreiche Dokumentationen verfügbar.
- Das SAP Developer Network (http://sdn.sap.com) ist als Informationsquelle für Entwickler gedacht. Hier ist eine kostenfreie Registrierung notwendig.

Im Folgenden sind die relevanten SAP Dokumente für die einzelnen Maßnahmen des vorliegenden Bausteines angegeben. Die Dokumente finden sich, wenn nicht anders angegeben, im SAP Help Portal.

M 2.341 Planung des SAP Einsatzes

Benutzerverwaltung

Detailinformationen zur Benutzerverwaltung in SAP Systemen finden sich im SAP Dokument "Identity Management", Kapitel "Benutzer und Rollen (BC-Sec-USR)", in den Abschnitten "Benutzerpflege" und "Zentrale Benutzerverwaltung" sowie im Abschnitt "User Management Engine".

Ressourcen-Planung

SAP bietet zum Thema Ressourcen-Planung (auch "Sizing" genannt) umfangreiche Informationen auf dem Service Marktplatz an. Unter dem Stichwort "Solution Life-Cycle Management" finden sich unter anderem die Themen "Quick Sizer Tool" und "Sizing Guidelines". Diese Informationen helfen, die Ressourcen-Planung durchzuführen.

SystemlandschaftDetaillierte Hinweise zur empfohlenen Systemlandschaft finden sich in der Regel in den Sicherheitsleitfäden zu den einzelnen SAP Produkten, die auf dem SAP Service Marktplatz unter dem Kürzel "securityguide" zu finden sind.

Detailinformationen zum Transportsystem finden sich im SAP Dokument "SAP Netweaver Technical Operations Manual" in den Abschnitten "Software Change Management" der ABAP- und Java-Stack-Beschreibungen.

M 2.347 Regelmäßige Sicherheitsprüfungen für SAP Systeme

Detaillierte Informationen zum Audit Information System (AIS) finden sich im SAP Hinweis 451960.

M 2.342 Planung von SAP Berechtigungen

Detailinformationen, die bei der Planung des Berechtigungskonzeptes genutzt werden können, finden sich im SAP Dokument "Identity Management", Kapitel "Benutzer und Rollen (BC-Sec-USR)", im Abschnitt "SAP Berechtigungskonzept".

M 2.349 Sicherheit bei der Software-Entwicklung für SAP Systeme

Weitere Hinweise zu Debugging-Berechtigungen finden sich in den SAP Hinweisen 13202 und 65968.

M 4.256 Sichere Installation von SAP Systemen

Weitere Detail-Informationen zur Betriebssystemabsicherung sind im SAP Dokument "SAP NetWeaver Security Guide" in den Abschnitten "SAP System Security Under UNIX/LINUX" und "SAP System Security Under Windows" enthalten.

M 4.258 Sichere Konfiguration des SAP ABAP-Stacks

IMG

Im SAP Dokument "Customizing (BC-CUS)" findet sich im Abschnitt "Einführungsleitfaden (IMG)" die IMG Dokumentation, die beim Einführungsleitfaden zu beachten ist.

Profile

Detailinformationen zum Umgang mit Profilen finden sich im SAP Dokument "Konfiguration" im Abschnitt "Profile".

Systemänderbarkeit

Detaillierte Informationen zum Thema Systemänderbarkeit finden sich im SAP Dokument "Transport Organizer (BC-CTS-ORG)" im Abschnitt "Systemänderbarkeit einstellen".

Mandanten

Administratoren müssen sich mit den Auswirkungen der Mandanten-Konfiguration sehr genau vertraut machen. Entsprechende Detail-Dokumentation findet sich im SAP Dokument "Transport Organizer (BC-CTS-ORG)" im Abschnitt "Mandantensteuerung".

Betriebssystem-kommandos

Detailbeschreibungen zum Absichern der Betriebssystemkommandos finden sich im SAP Dokument "SAP NetWeaver Security Guide" im Abschnitt "Logical Operating System Commands" sowie im Dokument "Konfiguration" im Abschnitt "Externe Betriebssystem-Kommandos: Inhalt".

Single Sign-On

Weitere Detailinformationen zu Single Sign-On finden sich im SAP Dokument "SAP NetWeaver Security Guide" im Abschnitt "User Authentication and Single Sign-On" sowie im Dokument "Verwendung von Anmeldetickets".

SNC

Weitere Informationen zu SNC finden sich im SAP Dokument "SAP NetWeaver Security Guide" im Abschnitt "Transport Layer Security".

M 4.259 Sicherer Einsatz der ABAP-Stack Benutzerverwaltung

Benutzerverwaltung

Weitere Hinweise zur Benutzerverwaltung in SAP Systemen finden sich im SAP Dokument "Identity-Management" im Abschnitt "Vorgehen bei der Erstinstallation".

Standardbenutzer

Detailhinweise zum Umgang mit Standardbenutzern finden sich im SAP Dokument "SAP NetWeaver Security Guide" im Abschnitt "Protecting Standard Users".

M 4.260 Berechtigungsverwaltung für SAP Systeme

Berechtigungs-verwaltung

Detailhinweise zum Aufbau der Berechtigungsverwaltung und zu relevanten Berechtigungen finden sich im SAP Dokument "Identitymanagement" im Abschnitt "Organisation der Berechtigungsverwaltung".

Profilgenerator

Detailhinweise zur Berechtigungsverwaltung mit dem Profilgenerator finden sich im SAP Dokument "Identitymanagement" im Abschnitt "Rollenpflege".

M 4.261 Sicherer Umgang mit kritischen SAP Berechtigungen

Berechtigungsprüfungen

Allgemeine Hinweise zu Berechtigungsprüfungen finden sich im SAP Dokument "Identity-Management" im Abschnitt "Berechtigungsprüfungen". Bei der Identifikation kritischer Berechtigungen ist entsprechendes Wissen über die zugrunde liegenden Berechtigungsprüfungen notwendig.

Systemberechtigungen

Weitere Informationen zu SAP Systemberechtigungen finden sich im SAP Dokument "Identity-Management" im Abschnitt "Schutzmaßnahmen für besondere Profile".

M 4.262 Konfiguration zusätzlicher SAP Berechtigungsprüfungen

Deaktivieren von Berechtigungsprüfungen

Weitere Informationen zum Deaktivieren von Berechtigungsprüfungen finden sich im SAP Dokument "Identity-Management" in den Abschnitten "Berechtigungsprüfungen" und "Umfang der Berechtigungsprüfungen verringern".

Berechtigungsgruppen

Weitere Informationen zur Konfiguration von Berechtigungsgruppen finden sich im SAP Dokument "ALV Grid Control (BC-SRV-ALV)" im Abschnitt "Berechtigungsgruppen pflegen und zuordnen".

M 4.263 Absicherung von SAP Destinationen

Weitere Detailinformationen zur Zugriffssteuerung auf Destinationen finden sich im SAP Dokument "RCF/ICF Security Guide" im Abschnitt "Controlling Access to RFC Destinations".

M 4.264 Einschränkung von direkten Tabellenveränderungen in SAP Systemen

Detailinformationen zu Parameter-Transaktionen finden sich an folgenden Stellen:

- SAP Dokument "RFC Security Guide", Abschnitt "Authorization Object S_TABU_DIS (Table Maintenance)"
- Dokumentation des Einführungsleitfadens (IMG, Transaktion SPRO) unter "SAP Web Application Server/ Systemadministration/ Benutzer und Berechtigungen/ Zeilenbezogene Berechtigungen"

- SAP Dokument "Berechtigungen in mySAP HR" im Abschnitt "Anwendungsübergreifende Berechtigungsobjekte"

Weitere Informationen zu Parametertransaktionen und Berechtigungen im Zusammenhang mit Transaktion SE93 finden sich in folgenden SAP Dokumenten:

- SAP Dokument "ABAP-Programmierung (BC-ABA)", Abschnitt "Parametertransaktion"
- SAP Dokument "Identity-Management", Abschnitt "Berechtigungsprüfungen"

M 4.265 Sichere Konfiguration der Batch-Verarbeitung im SAP System

Weitere Details zur Batch-Verarbeitung finden sich im SAP Dokument "Hintergrundverarbeitung" im Abschnitt "Berechtigungen für die Hintergrundverarbeitung".

M 4.266 Sichere Konfiguration des SAP Java-Stacks

Java-Stack-Dienste

Hinweise zu den Java-Stack-Diensten und deren Funktion finden sich in den jeweiligen Handbüchern, wie etwa dem SAP Dokument "Technisches Betriebshandbuch für SAP NetWeaver" im Abschnitt "Administration des SAP Web Application Server (JAVA)" sowie in den zugehörigen Dokumenten "Architekturhandbuch", "Administrationshandbuch" und "Entwicklerhandbuch".

HTTP PUT

Der SAP Hinweis 606733 bietet zur HTTP PUT Problematik weitere Detailinformationen an.

M 4.269 Sichere Konfiguration der SAP System Datenbank

Die SAP Empfehlungen zur Absicherung der Datenbank finden sich im SAP Dokument "Operating System and Database Platform Security Guides" im Abschnitt " Database Access Protection". Die Empfehlungen erfolgen für die unterschiedlichen Datenbankprodukte.

M 4.270 SAP Protokollierung

Systemüberwachungsfunktionen

Detailbeschreibungen zu den Systemüberwachungsfunktionen finden sich im SAP Dokument "Werkzeuge zur Systemüberwachung".

Änderungsverfolgung

Weitere Informationen zur Änderungsverfolgung sind im SAP Hinweis 1916 und den darin referenzierten Hinweisen zu finden.

M 4.271 Virenschutz für SAP Systeme

Weitere Detailinformationen zur Schnittstelle für Computer-Viren-Schutzprogramme finden sich im SAP Dokument "Viren-Scan-Schnittstelle". Hinweise zu Produkten, die über die Schnittstelle angebunden werden können, finden sich auf dem SAP Service Marktplatz unter dem Quicklink "securitypartners" unter "Partners for Virus Scan interface (NW-VSI)".

M 4.272 Sichere Nutzung des SAP Transportsystems

Detailinformationen zum Transportmanagementsystem finden sich im SAP Dokument "Change and Transport System - Überblick (BC-CTS)" und "Transport Management System (BC-CTS-TMS)".

M 4.273 Sichere Nutzung der SAP Java-Stack Software-Verteilung

Weitere Detailinformationen zur Software-Verteilung im SAP Java-Stack finden sich im SAP Dokument "SAP NetWeaver Java Development Infrastructure".

M 5.125 Absicherung der Kommunikation von und zu SAP Systemen

SNC

Detailhinweise zur SNC-Konfiguration finden sich in den SAP Dokumenten "Administration Manual" im Abschnitt "Configuring SNC (SAP J2EE Engine to ABAP Engine)". Weitere Hinweise finden sich im SAP Dokument "Network and Transport Layer Security" im Abschnitt "Secure Network Communications (SNC)".

SSL

Detaillierte Anleitung zur Installation und Konfiguration von SSL finden sich im SAP Dokument "Systemsicherheit" im Abschnitt "SAP Web AS für SSL-Unterstützung konfigurieren" und im SAP Dokument "Administration Manual" im Abschnitt "Configuring the Use of SSL on the SAP J2EE Engine". Informationen über den SSL-Schutz bei internen LDAP Zugriffen des Java-Stacks sind im Dokument "Configuring SSL Between UME and LDAP Directory (SAP NW`04)" beschrieben.

M 5.126 Absicherung der SAP RFC-Schnittstelle

allgemeine Dokumentation

Detailhinweise zur RFC-Kommunikation finden sich im SAP Dokument "RFC/ICF Security Guide" im Abschnitt "RFC Scenarios".

Trusted Systems

Weitere Informationen zum Thema "Trusted Systems" finden sich in den SAP Dokumenten "RFC/ICF Security Guide" im Abschnitt "Authorization Object S_RFCACL" und im Dokument "Komponenten der SAP Kommunikationstechnologie" im Kapitel "RFC" im Abschnitt "Trusted System: Vertrauensbeziehungen zwischen SAP Systemen".

sideinfo Datei

Weitere Detailinformationen zur sideinfo Datei finden sich im SAP Dokument "Komponenten der SAP Kommunikationstechnologie" im Abschnitt "Introduction to RFC Client Programs" und im Dokument "SAP Gateway" im Abschnitt "Side-Information-Tabellen".

externe RFC-Server

Detailinformationen zu externen RFC-Servern finden sich im SAP Dokument "RFC/ICF Security Guide" in den Abschnitten "Security Measures - Overview (RFC)" und "RFC Communication between SAP Systems and External (Non-SAP) Systems". Informationen zum RFC SDK finden sich im Dokument "Komponenten der SAP Kommunikationstechnologie" im Abschnitt "The RFC API" und im Abschnitt "Contents of the RFC SDK".

SAP Gateway

Nähere Informationen zum SAP Gateway finden sich im SAP Dokument "SAP Gateway" im Abschnitt "Sicherheitseinstellungen beim SAP Gateway".

M 5.127 SAP Internet Connection Framework (ICF) absichern

Weitere Detailinformationen zum ICF finden sich im SAP Dokument "Komponenten der SAP-Kommunikationstechnologie" im Kapitel "Internet Communication Framework" im Abschnitt "Administration: HTTP Kommunikation mit dem SAP-System als Server" und im SAP Dokument "RFC/ICF Security Guide" im Abschnitt "ICF Scenarios".

M 5.128 Absicherung der SAP ALE (IDoc/BAPI) Schnittstelle

Weitere Informationen zur Absicherung der ALE-Schnittstelle finden sich im SAP Dokument "Security Guide ALE (ALE Applications)".

M 5.129 Sichere Konfiguration der HTTP-basierten Dienste von SAP Systemen

SOAP

Weitere Detailinformationen zur SOAP-Schnittstelle finden sich im SAP Dokument "Komponenten der SAP-Kommunikationstechnologie" im Abschnitt "SOAP Framework" des Kapitels "Internet Communication Framework".

Content-Server-Schnittstelle

Weitere Hinweise zur Content-Server-Schnittstelle finden sich im SAP Dokument "SAP Content-Server Security Guide" und im Dokument "Knowledge Provider (BC-SRV_KPR)" im Abschnitt "SAP Content Server HTTP 4.5 Schnittstelle".

M 6.97 Notfallvorsorge für SAP Systeme

Detaillierte Hinweise zum Backup finden sich im "SAP NetWeaver Technical Operations Manual". Für den ABAP-Stack in den Abschnitten "Sicherung und Wiederherstellung" sowie "Erstellen einer homogenen Systemkopie", für den Java-Stack im Abschnitt "Sicherung und Wiederherstellung des SAP Web Application Server (Java)".

Ergänzende Kontrollfragen:

- Ist die verfügbare SAP Dokumentation genutzt worden?
- Wird die verfügbare SAP Dokumentation regelmäßig auf Aktualisierungen geprüft?

M 2.347 Regelmäßige Sicherheitsprüfungen für SAP Systeme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, IT-Sicherheitsmanagement, Revisor

Die Sicherheit eines SAP Systems kann nur dann auf Dauer gewährleistet werden, wenn dieses regelmäßig geprüft wird. Auf diese Weise können Fehlkonfigurationen und Schwachstellen aufgedeckt und behoben werden.

Sicherheitsprüfungen sollten in regelmäßigen Abständen durch unterschiedliche Personen erfolgen. So sollten beispielsweise Administratoren in relativ kurzen Abständen (etwa monatlich) Kurzprüfungen durchführen. Es empfiehlt sich dabei, eine Prüfliste aufzubauen, damit ein definierter Prüfumfang gewährleistet ist. Festgestellte kleinere Probleme können meist sofort durch die Administratoren korrigiert werden, größere Probleme sind entsprechend der Prozessvorgaben weiterzumelden. In mittleren Zeitabständen (mehrere Monate) sollten Sicherheitsprüfungen durch andere, interne Rollen (z. B. IT-Sicherheit, IT-Revision) erfolgen. In längeren Zeitabständen können dann auch Prüfungen durch externe Prüfer sinnvoll sein. Folgende Aspekte sind bei Prüfungen zu berücksichtigen:

Regelmäßige Recherche von sicherheitsrelevanten Informationen

Generell müssen sich Administratoren und für die IT-Sicherheit verantwortliche Personen regelmäßig über Neuerungen und Änderungen informieren, die die verantworteten Systeme betreffen. Dazu sind insbesondere die SAP Informationsquellen regelmäßig zu sichten.

SAP Informationsquellen

Siehe dazu auch M 2.346 *Nutzung der SAP Dokumentation*.

Berechtigungen für Revisionsbenutzer

Für das SAP Benutzerkonto, das zur Prüfung der Systemkonfiguration durch externe Personen genutzt wird, sollten nur lesende Berechtigungen vergeben sein. Veränderungen dürfen durch den Revisionsbenutzer nicht durchgeführt werden. Im ABAP-Stack darf dem Revisionsbenutzer nicht das Profil SAP_ALL zugeordnet werden.

Können die Berechtigungen des Revisionsbenutzers nicht auf den lesenden Zugriff beschränkt werden, so darf der Zugriff nur im 4-Augen-Prinzip erfolgen.

SAP Informationsquellen

SAP bietet ein eigenes Audit System (Audit Information System, AIS) an, das es Revisoren ermöglicht, ein SAP System zu untersuchen. Dabei sind bereits unterschiedliche Rollen und Berechtigungen verfügbar, die dem Benutzerkonto des Revisionsbenutzers zugeordnet werden können. Die verfügbaren Rollen sind in der Regel so gestaltet, dass nur lesender Zugriff besteht. Die Rollen können im Profilgenerator (Transaktion PFCG) über die Suche "SAP*AUDITOR*" eingesehen werden.

Zugriff auf AIS konfigurieren

Für die Prüfung kann das Audit Information System (AIS) eingesetzt werden. Das AIS liegt in unterschiedlichen Versionen vor: als Transaktion SECR und in der rollenbasierten Version

Über die Transaktion SECR können Prüfungen teilweise automatisiert erfolgen. Das AIS erlaubt es außerdem, das Prüfergebnis zu dokumentieren und den Prüfstatus (Ampel-Status: rot, gelb, grün) vorzuhalten.

Es empfiehlt sich, eine Untermenge der angebotenen Prüfmöglichkeiten zu definieren (Top 10 Security Reports) und diese abzuarbeiten. Dabei ist die festgestellte Ist-Konfiguration gegen die Soll-Konfiguration zu prüfen.

Es ist zu bedenken, dass das AIS kritische Systeminformationen preisgibt. Der Zugriff muss daher auf die berechtigten Prüfer eingeschränkt werden (S_TCODE, Transaktion SECR).

Im Gegensatz zur Transaktion SECR besteht das rollenbasierte AIS aus vorgefertigten Rollen, Berechtigungen und Programmen, die es ermöglichen, einem Benutzer die für ein Audit notwendigen Berechtigungen auf System- und Modul-Ebene zu erteilen. Im Fokus stehen dabei vornehmlich kaufmännische Audits. Das rollenbasierte AIS muss entsprechend eingerichtet und konfiguriert werden.

SAP Informationsquellen

Detaillierte Informationen dazu finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Prüfen der Veränderungen der Systemänderbarkeit

Die Einstellungen zur Systemveränderbarkeit sind regelmäßig zu prüfen. Dazu kann die Transaktion SE03 "Administration/Systemänderbarkeit" genutzt werden. Zu prüfen sind die globalen Einstellungen und die Einstellungen für jeden Mandanten. Informationen zur Systemänderbarkeit finden sich auch in M 4.258 *Sichere Konfiguration des SAP ABAP-Stacks*.

Für den Java-Stack besteht nicht die Möglichkeit, die Systemänderbarkeit durch Systemeinstellungen zu konfigurieren.

Security Auditlog

Das Security Auditlog enthält sicherheitsrelevante Protokoll-Einträge. Eine regelmäßige Auswertung muss daher erfolgen. Für die Auswertung können die Transaktionen SM20, SM20N oder RZ27_Security eingesetzt werden, wobei die Transaktion SM20N aufgrund der besseren Benutzungsschnittstelle zu bevorzugen ist. Um die Transaktionen SM20 und SM20N verwenden zu können, muss vorher mit der Transaktion SM19 der Auswerteumfang definiert und das Auditlog aktiviert werden (siehe auch M 4.270 *SAP Protokollierung*).

Profilparameter

Die eingestellten Profilparameter sind gegen die geplanten Soll-Werte zu prüfen (siehe auch M 4.258 *Sichere Konfiguration des SAP ABAP-Stacks)*. Die gültigen Profilparameter lassen sich auch direkt über die Transaktion SM20N anzeigen. Alternativ kann der Report RSPARAM über die Transaktion SE38 ausgeführt werden.

Benutzerinformationssystem

Über das Benutzerinformationssystem (Transaktion SUIM) sollten regelmäßig Prüfungen erfolgen. Folgende Informationen sind dabei sicherheitsrelevant:

- Benutzer mit Falschanmeldungen
  Dies kann auf Angriffsversuche hindeuten.
- Benutzer mit Anmeldedaten und Kennwortänderungen
  So lassen sich Benutzer identifizieren, die nie angemeldet sind oder ihr Passwort nicht geändert haben, sofern dies nicht automatisch erzwungen wird.
- Benutzer mit kritischen Kombinationen von Berechtigungen für den Transaktionsstart
  Es sollte ein Abgleich mit dem Berechtigungskonzept erfolgen.
- Benutzer mit kritischen Berechtigungen
  Es sollte ein Abgleich mit dem Berechtigungskonzept erfolgen.
- Änderungsbelege für Benutzer, Rollenzuordnungen, Rollen, Profile und Berechtigungen
  Hierbei ist insbesondere auf Änderungen an administrativen Objekten zu prüfen.

Erreichbare SAP Gateways

Über die Transaktion RSGWLST können die von einem SAP System erreichbaren SAP Gateways anderer SAP Systeme bestimmt werden. Dies zeigt die Verbindungs- und Zugriffsmöglichkeiten auf. Es können die Einstellungen der Datei "secinfo" der entfernten Gateways eingesehen werden, über die die Autorisierungen zum Ansprechen und Registrieren des entfernten SAP Gateways definiert werden. Zusätzlich können die Destinationen und die registrierten RFC-Server-Programme der ansprechbaren entfernten SAP Gateways abgeprüft werden.

Die Auswertung erfordert jedoch entsprechende technische Kenntnisse. Da über die Transaktion RSGWLST auch sensitive Systeminformationen erlangt werden können, muss die Transaktion zugriffsbeschränkt werden.

Der Status des SAP Gateways des lokalen Systems kann über die Transaktion SMGW (Gateway Monitor) geprüft werden.

Prüfen der Single Sign-On (SSO) Möglichkeiten

Benutzer können sich an einem SAP System zunächst mit gültigen Authentisierungsinformationen (z. B. Benutzername/Passwort, Zertifikat) anmelden und dann über den SSO Mechanismus ohne erneute Eingabe von Authentisierungsinformationen auf andere SAP Systeme zugreifen.

Über die Transaktion STRUST können die Zertifikate anderer SAP Systeme eingesehen werden, die das lokale SAP System bei SSO-Zugriffen akzeptiert. Hier sollten nur vertrauenswürdige Systeme eingetragen sein. Alternativ kann die Prüfung auch über die Transaktionen SSO2 oder SSO2_ADMIN erfolgen.

Regelmäßige Prüfung der Berechtigungen

Das vollständige Prüfen von Berechtigungen ist in der Regel aufgrund des Mengengerüstes nicht manuell möglich. Daher ist ein gutes Berechtigungskonzept unbedingt notwendig. Aber auch dann müssen die Berechtigungen regelmäßig auf Konsistenz mit dem Berechtigungskonzept geprüft werden. Hier können Stichproben (siehe auch "Benutzerinformationssystem" oben) für wichtige Benutzergruppen durchgeführt werden. Das Berechtigungskonzept muss sicherstellen, dass Prozesse aufgesetzt sind, die verhindern, dass Berechtigungen angesammelt werden.

SAP Informationsquellen

Zusätzlich können Werkzeuge zum Einsatz kommen, die ein integriertes Änderungs- und Risikomanagement anbieten, so dass beispielsweise die Möglichkeit des Betrugs durch Benutzer aufgrund von Berechtigungsproblemen verringert werden kann. SAP bietet dazu den so genannten "Compliance Calibrator" an, der die konfigurierten Berechtigungen dahingehend prüft, ob Benutzer Berechtigungen besitzen, die aus Sicherheitssicht als kritisch zu betrachten sind. Solche Prüfungen finden typischerweise auch im Sarbanes-Oxley-Umfeld statt, sind generell jedoch für jede Behörde oder jedes Unternehmen sinnvoll. Die Prüfung muss die unter diesen Gesichtspunkten kritischen Berechtigungen für Transaktionen (wie etwa SE80, SE16, SQVI oder kritische Autorisierungsobjekte für Benutzer, beispielsweise S_PROGRAM, S_USER_GRP, S_TABU_DIS, S_RFC, S_USR_RFC) erkennen und anzeigen.

Aktualität der Updates prüfen

Für das SAP System ist die Aktualität der installierten Updates zu prüfen. Dazu kann die Transaktion SPAM eingesetzt werden. Der aktuelle Patch-Stand des Systems muss dann mit den verfügbaren Patches verglichen werden. Dies erfordert, dass dem Prüfer die von SAP verfügbaren Patches bekannt sind.

Die Prüfung muss auch auf Fehler oder Warnungen bei Updates erfolgen. Dabei ist zu beachten, dass Warnungen auch dann existieren können, wenn der Update-Status auf "grün" steht.

Sicherheit der Kommunikationsschnittstellen prüfen

Die Sicherheit der unterschiedlichen Kommunikationsschnittstellen (siehe auch M 5.125 *Absicherung der Kommunikation von und zu SAP Systemen*) sollte geprüft werden. Dies betrifft beispielsweise die RFC-, ICF- und ALE-Schnittstellen des ABAP-Stack und die Schnittstellen des Java-Stacks.

Hier ist insbesondere zu prüfen, wer administrative Berechtigungen besitzt und welche Dienste und Funktionen verfügbar sind.

Ergänzende Kontrollfragen:

- Wird das SAP System regelmäßig einer Sicherheitsprüfung unterzogen?
- Werden die Berechtigungen regelmäßig mindestens stichprobenartig geprüft?
- Ist das SAP System auf einem aktuellen Patch-Stand?

M 2.348 Sicherheit beim Customizing von SAP Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement,

Verantwortlich für Umsetzung: Administrator

Im Rahmen des Customizings wird ein SAP System so konfiguriert und angepasst, dass es die gewünschte Unterstützung für die Institution anbieten kann. Diese Aufgabe ist in der Regel zeitaufwendig. Folgendes ist daher zu bedenken:

- Für das Customizing ist ein entsprechendes Konzept zu erstellen, das den gewünschten Soll-Zustand des SAP Systems möglichst genau beschreibt und auch die Prozesse definiert, nach denen das Customizing durchgeführt wird.
- Für das Konzept ist eine Anforderungsanalyse notwendig. Dabei muss festgelegt werden, welche Anpassungen durch das Customizing erfolgen müssen, damit das gewünschte System-Verhalten erreicht wird (siehe auch M 2.341 *Planung des SAP Einsatzes*.
- Im Rahmen des Customizing-Prozesses sind Rückmelde-Prozesse einzusetzen, die Anpassungen des Konzeptes während der Umsetzung (siehe auch M 4.258 *Sichere Konfiguration des SAP ABAP-Stacks*) erlauben.
- Das Customizing darf nur von sachkundigen und vertrauenswürdigen Personen durchgeführt werden.
- Anpassungen der Konfigurationen sollten nicht im Produktiv-System erfolgen, sondern über das Transportsystem kontrolliert eingespielt werden.

Ergänzende Kontrollfragen:

- Ist ein Customizing-Konzept erstellt worden?
- Wird das Customizing durch vertrauenswürdiges Personal durchgeführt?

M 2.349 Sicherheit bei der Software-Entwicklung für SAP Systeme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Entwickler

Um ein SAP System an die spezifischen Bedürfnisse eines Unternehmens oder einer Behörde anzupassen, kann die Funktion des Systems durch Eigenentwicklungen verändert oder erweitert werden. Folgendes muss aus Sicherheitssicht bei der Software-Entwicklung für SAP Systeme beachtet werden:

Entwickler in Produktiv-Systemen

Da Produktiv-Systeme schützenswerte System- und Geschäftsdaten enthalten, dürfen Entwickler keinen Zugriff auf die Produktiv-Systeme erhalten. Insbesondere darf kein Debugging im Produktiv-System erfolgen. Fehleranalysen müssen im Entwicklungssystem durchgeführt werden. Dies bedeutet für den ABAP-Stack, dass kein Benutzer mit der Berechtigung S_DEVELOP ausgestattet werden darf. Die Werkzeuge CATT und eCATT (ABAP-Stack) oder Remote-Debugging der Engine (Java-Stack) dürfen in Produktiv-Systemen nicht genutzt werden. Dies ist durch die Mandanten- bzw. Java-Stack-Konfiguration auszuschließen.

In besonders begründeten Ausnahmefällen, in denen Entwickler Fehleranalysen nur in Produktiv-Systemen durchführen können, dürfen diesen temporär Anzeigeberechtigungen und Debugging-Berechtigungen ohne Modifikationsmöglichkeiten eingeräumt werden. Die Sicherheit ist durch zusätzliche organisatorische Maßnahmen entsprechend zu unterstützen.

SAP Informationsquellen

Weitere Hinweise zu diesem Thema finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Direktes Einspielen neuer Software in das Produktiv-System durch Entwickler muss durch ein mehrstufiges Software-Freigabe-Konzept unterbunden werden (siehe M 4.272 *Sichere Nutzung des SAP Transportsystems* und M 4.273 *Sichere Nutzung der SAP Java-Stack Software-Verteilung*).

Sicherheitsvorgaben bei Eigenentwicklungen

Die Entwickler sollten durch geeignete Sicherheitsvorgaben unterstützt werden. Nur wenn konkrete Anforderungen oder Rahmenbedingen bekannt sind, kann ein Entwickler diese in der Programmierung berücksichtigen. Empfehlenswert sind unter anderem die folgenden Vorgaben:

- ABAP-Code muss immer Berechtigungen prüfen.
- Die eigenen und verwendeten Berechtigungsobjekte im ABAP-Code sind zu dokumentieren und müssen über die Transaktion SU24 für den Profilgenerator eingepflegt werden (siehe auch M 2.342 *Planung von SAP Berechtigungen)*.

- Für Java-Code sind die benutzten Dienste zu dokumentieren.
- Die verwendeten Rollen und Vorgaben an die so genannten "Security Constraints" (d. h. welche Rollen für den Zugriff auf Applikationsfunktionen notwendig sind) sind für Java-Applikationen zu dokumentieren.
- Für ABAP-Programme sollte der ABAP Code Inspector (Transaktion SCI) eingesetzt werden, um eigene Programme unter anderem auf Sicherheit und das Einhalten der SAP Namenskonventionen zu prüfen. Dies gilt insbesondere dann, wenn keine anderen Werkzeuge genutzt werden, um sicherheitsrelevante Kontrollen von ABAP-Programmen durchzuführen.

Sicherheit bei Fremdanwendungen

Software, die durch Dritte entwickelt wurde, darf nur nach einem sorgfältigen Abnahmeprozess im SAP System installiert werden. Im Abnahmeprozess sind auch Sicherheitsprüfungen durchzuführen. Die Sicherheitsanforderungen sind im Pflichtenheft detailliert zu beschreiben. Nur so kann die gewünschte Sicherheit der Anwendung umgesetzt werden.

Ergänzende Kontrollfragen:

- Sind Sicherheitsaspekte in den Software-Entwicklungsprozess integriert?
- Erhalten die Software-Entwickler Sicherheitsvorgaben?
- Wird Software nur nach einem Abnahmeverfahren installiert, in dem auch Sicherheitsaspekte geprüft werden?

M 2.350 Aussonderung von SAP Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Wird entschieden, ein SAP System nicht weiter zu betreiben, weil es beispielsweise durch eine neuere Systemversion auf neuer Hardware abgelöst wird, so sind die nachfolgend beschriebenen Punkte zu beachten. Die Maßnahmen sollen verhindern, dass ein Angreifer die freigewordene Identität des SAP Systems missbrauchen kann. Der Aussonderungsprozess muss also dafür Sorge tragen, dass die Identität des SAP Systems gelöscht und unbrauchbar wird.

Löschen/Entsorgen der Speichermedien

Die Speichermedien aller betroffenen Rechner sind vor der Wiederverwendung sicher zu löschen (siehe M 2.167 *Sicheres Löschen von Datenträgern*). Wird die Hardware entsorgt, so muss dies ebenfalls auf sichere Weise geschehen (siehe M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln)*.

System aus dem SAP Verbund löschen

In der Regel ist ein SAP System in einen SAP Verbund eingebunden. Andere Systeme besitzen daher Referenzen auf das auszusondernde System.

Alle Referenzen auf das ausgesonderte System in anderen SAP Systemen oder Komponenten müssen gelöscht werden. Dies betrifft unter anderem

- Identitäten (d. h. technische Benutzer), unter denen das ausgesonderte System zugreift,
- Vertrauensstellungen,
- Destinationen,
- Konfigurationen des Transportsystems,
- Konfigurationen der zentralen Benutzerverwaltung,
- Konfigurationen der Systemüberwachung (Monitoring).

Es muss beachtet werden, dass dabei auch Referenzen in Systemen externer Partner betroffen sein können. Der Aussonderungsprozess muss daher auch dafür sorgen, dass entsprechende Prozesse bei betroffenen externen Partnern angestoßen werden.

System aus dem Netzverbund löschen

Alle Referenzen auf Netz- und Betriebssystem-Ebene sind zu löschen. Dies betrifft unter anderem

- DNS-Einträge,
- Firewall-Regeln,
- SAPGui/SAPLogon-Konfiguration (Systemlisten),
- Einträge in "host" und "services" Dateien.

Für die Listen verfügbarer Systeme für das SAP Logon - diese werden in der Datei saplogon.ini gespeichert - empfiehlt es sich, eine zentrale Verwaltung zu nutzen und die Datei auf die Clients zu verteilen.

Ergänzende Kontrollfragen:

- Sind alle aktuellen Referenzen eines SAP Systems dokumentiert?
- Sind alle Daten auf den verwendeten Datenträgern sicher gelöscht worden?
- Sind externe Partner darüber informiert, dass das SAP System ausgesondert wurde?

M 2.351 Planung von Speichersystemen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Die grundsätzliche Entscheidung, welche Art von Speichersystem angemessen für die Institution ist, muss durch eine Anforderungsanalyse festgestellt werden. Zunächst ist festzustellen, welche Anwendungen vom Speichersystem zukünfig unterstützt werden sollen und welche vorhandene Hardware durch ein Speichersystem unterstützt oder abgelöst werden soll.

Maßgebliche Kenngrößen sind die Anforderungen an die Verfügbarkeit, Performance, Kapazität. Bei normalen Verfügbarkeitsanforderungen sollte zudem geprüft werden, welche Komplexität für die Institution tragbar ist. Die Einführung von SAN-Systemen bedeutet, dass eine neue Basistechnik eingeführt wird. Damit ist ein entsprechender Aufwand zur Planung und Einführung dieser Technik zu kalkulieren.

NAS-Systeme sind auf die einfache Integration in etablierte IT Umgebungen und auf den Datei-orientierten Zugriff besonders ausgerichtet. Ihr Einsatz ist also dann angezeigt, wenn Dateien und Datei-orientierte Anwendungen auf hochwertigere aber dennoch eher einfach zu administrierende Speichersysteme konsolidiert werden sollen.

Wenn kurzfristig Speicherplatz auf Servern durch zentralen Speicher ersetzt werden soll, langfristig jedoch höhere Verfügbarkeitsanforderungen zu erwarten sind, kann auch der Einsatz von Speichersystemen erwogen werden, die ein Mischform von SAN und NAS darstellen. Solche Speichersysteme lassen sich in erster Ausbaustufe als (sehr hochwertige) NAS-Systeme betreiben. Durch Aufrüstung interner Komponenten können sie zu SAN-Systemen für weitere Server und bei Bedarf zu redundanten Speichernetzen ausgebaut werden.

Wenn die Schutzbedarfsfeststellung für eines dieser betrachteten Systeme sofort oder in absehbarer Zukunft ergibt, dass hoher oder sogar sehr hoher Schutzbedarf in Bezug auf die Verfügbarkeit vorliegt, so dass eine redundante Datenspeichrung an verschiedenen Standorten erforderlich ist, dann sollte SAN-Technologie eingesetzt werden (das Speichersystem sollte SAN-Protokolle unterstützen). Nur mit dieser Technik lassen sich vollständig redundante und hoch-verfügbare Speichersysteme aufbauen.

Auswahl der Hardware

Anforderungen an Speicherkapazität

Entscheidende Kenngrößen bei der Auswahl des Speichersystems sind

- der derzeitige und der prognostizierte Bedarf an Speicherplatz der Anwendungen,
- die Anforderungen der Anwendung an die Geschwindigkeit der Speicherzugriffe,
- die Anforderungen an die Ausfallsicherheit für die Anwendungen.

Es ist für die Planung von Speichersystemen und Speichernetzen zu erfassen, welche Geschäftsprozesse und Anwendungen in der Institution das Speichersystem sofort und in Zukunft nutzen werden und welche Anforderungen bezüglich des Wachstums des Speicherbedarfs, der Performance und der Ausfallsicherheit dadurch gestellt werden. Bei einer solche Prognose sollte beachtet werden, dass eine solche Schätzung stets sehr großzügig erfolgen sollte. Es zeigt sich immer wieder, dass auch großzügige Schätzungen des zukünftigen Speicherbedarfs in kurzer Zeit von den tatsächlichen Anforderungen übertroffen wurden.

Bei der Planung von Speichersystemen muss auch die erforderliche Datensicherung mit einbezogen werden, denn die Abschätzung des Speicherbedarfs bestimmt auch die Auslegung der Datensicherungsgeräte. Hierbei muss sichergestellt werden, dass auch nach Ausbau des Speichersystems mit den angeschlossenen Datensicherungsgeräten Zeiten für Datensicherung und auch für das Wiedereinspielen einer Datensicherung erzielt werden können, die den Verfügbarkeitsanforderungen der betroffenen Organisationseinheiten genügen.

Anforderung der Anwendungen

Speichersysteme dienen üblicherweise einer Vielzahl von Servern und damit von Anwendungen der Speicherung ihrer Daten. Das gilt vor allem für SAN-Systeme. Die Anforderungen an das Speichersystem in Bezug auf Verfügbarkeit, Integrität und Vertraulichkeit werden durch die Anwendung mit dem höchsten Schutzbedarf definiert.

Verfügbarkeitsanforderungen

Bei der internen technischen Auslegung eines SAN ist zu prüfen, ob die Verfügbarkeitsanforderungen der Institution an das SAN nahe legen, eine desaster-tolerante Auslegung (M 2.354 *Einsatz einer hochverfügbaren SAN-Konfiguration*) zumindest in die Planungen einzubeziehen.

Vertraulichkeitsanforderungen

Wenn die Institution Anwendungen betreibt, die besonders hohe Anforderungen an die Vertraulichkeit der Daten stellt, so ist in die Planungen einzubeziehen, dass die Daten sowohl während des Transports im SAN als auch auf den Speichermedien durch Verschlüsselung geschützt werden. Dazu ist eine besondere Sicherheitsanalyse vorzunehmen.

Auswahl von Produkten / Herstellern / Lieferanten

Der Einsatz von Produkten verschiedener Generationen oder von verschiedenen Herstellern erhöht im Allgemeinen die Komplexität des Gesamtsystems und kann unter Umständen zu Problemen führen. Daher kann es ratsam sein, eine Homogenität der Systeme anzustreben. Auch bei der Auswahl der Vertragspartner sollte bedacht werden, dass Probleme, die beim Aufbau, Test und Betrieb entstehen können, in der Regel schneller und effektiver beseitigt werden, wenn nur ein Anbieter involviert ist.

Auf der anderen Seite kann eine starke Abhängigkeit von bestimmten Herstellern oder Lieferanten auch Probleme verursachen. Meistens spielen außerdem auch wirtschaftliche Aspekte bei der Auswahl der Produkte eine wichtige Rolle. Alle diese Faktoren sollten bei der Planung von Neubeschaffungen berücksichtigt werden. Als weiterer Punkt muss beachtet werden, dass Hersteller meistens die einwandfreie Funktion ihrer Lösungen nur für bestimmte Zusammenstellungen von Hard- und Software garantieren

und durch Support-Leistung unterstützen. Daher ist es ratsam, auf die Zertifizierung von Produkten im Hinblick auf ihrer Einsatzumgebung undauf die verbindlichen Aussagen der Hersteller zur Kompatibilität und Interoperabilität von Produkten zu achten.

Verwendung eines zentralen Verwaltungssystems

Der Einsatz einer gemeinsamen Management Applikation für die zentrale und einfache Überwachung und Verwaltung von Ressourcen vereinfacht die Administration der Speichersysteme. Insbesondere für größere Speichersysteme ist der Einsatz eines zentralen Verwaltungssystems für eine effiziente Speicherverwaltung unumgänglich. Der Einsatz von proprietären Verwaltungsmechanismen bei den verschiedenen Produkten machte es bisher schwierig, ein zentrales Management in heterogenen Speicherumgebungen zu implementieren. Die Verabschiedung des SMI-S (Storage Management Initiative Specification) Standards von der SNIA (Storage Network Industry Association) bietet jetzt Herstellern die Möglichkeit, die Anbindung ihrer Produkte an zentralen Verwaltungssystemen viel einfacher zu gestalten.

Planung des Netzanschlusses

Die interne Vernetzung der SAN-Komponenten erfolgt üblicherweise durch ein eigenes Fibre Channel Netz. Auch wenn intern iSCSI genutzt wird, ist aus Gründen der Betriebssicherheit ein eigenes Netz zu schaffen.

Wenn zur Verwaltung und Kontrolle von NAS-Systemen oder SAN-Komponenten (Speichergeräte, SAN-Switches, etc) der Anschluß dieser Geräte an ein LAN erforderlich ist, sollte dieses LAN als separates Administrationsnetz betrieben werden. Damit werden folgende Schutzziele verfolgt:

- Administrative Daten und Aktionen können nicht von beliebigen Benutzern belauscht werden.
- Es können Protokolle (insbesondere SNMP Version1) eingesetzt werden, die bekannt unsicher sind, aber mangels verfügbarer Alternativlösungen zur Überwachung des Betriebs eingesetzt werden müssen.
- Die Rechteverwaltung innerhalb eines solchen Netzes wird übersichtlicher.
- Besondere Kontrollmaßnahmen wie Intrusion Detection Systeme können übersichtlicher und effizienter gestaltet werden.

Infrastruktur

Vor der Anschaffung und Inbetriebnahme eines SAN müssen verschiedene planerische Tätigkeiten durchgeführt werden.

Der Standort der Komponenten eines SAN muss in einem zutrittsgeschützten Serverraum oder einem Rechenzentrum geplant werden. Empfehlungen für die Infrastruktursicherheit von Serverräumen finden sich in Baustein B 2.4 *Serverraum*, die Anforderungen an Rechenzentren in Baustein B 2.9 *Rechenzentrum*.

Neben der allgemein geschützten Aufstellung sollte auch überprüft werden, ob die Klimatisierung des gewählten Standortes und die Stromversorgung dort

den technischen Anforderungen und der angestrebten Verfügbarkeit des Speichersystems entsprechen. Die Stationierung der einzelnen Komponenten des SAN-Systems ist sorgfältig zu planen. So sollte sorgfältig geprüft werden, wo Sicherungsgeräte, die regelmäßige oder gelegentlichen manuellen Eingriff erfordern (z. B. Entnahme oder Wechsel von Bandkassetten) zweckmäßig und unter Beachtung aller Sicherheitsanforderungen aufgestellt werden können.

Ebenso ist bei räumlich verteilten SAN-Konfigurationen zu prüfen, ob alle Geräte permanent mit Strom versorgt werden können. Es kann nötig sein, einen SAN Switch in einem normalen Verteilerraum zu installieren, um extern stationierte Server anzuschließen. Dieser Raum ist dann ebenso wie die Server in die Energieversorgung über USV und Netzersatzanlage einzubinden.

Prozesse

Das Speichersystem ist als zentrale IT-Komponente in alle Steuerungsprozesse der IT zu integrieren. Insbesondere Überwachungs- und Eskalationsverfahren sind innerhalb der vorhandenen Betriebsabläufe auf den NAS- oder SAN-Betrieb anzupassen. Leistungen des Herstellers zur Überwachung und zur Betriebssicherung sind in eigene Abläufe einzubeziehen. Dabei sind stets die Vorgaben der Sicherheitsleitlinie und von Ausführungsbestimmungen der Institution zu beachten.

Personal

Es ist zu überprüfen, wie viele Mitarbeiter mit welcher Ausbildung für den Betrieb des Speichersystems benötigt werden. Stehen nicht genügend ausgebildete Mitarbeiter zur Verfügung, müssen die erforderlichen Schulungsmaßnahmen rechtzeitig initiiert werden.

Ergänzende Kontrollfragen:

- Wurde die Infrastruktur für die Stationierung von Speichersystemen geprüft und angepasst?
- Wurde eine Sicherheitsrichtlinie für den Betrieb von SAN-Systemen erstellt?
- Wann wurde die Sicherheitsrichtlinie zum letzten Mal aktualisiert?
- Wurden in der Sicherheitsrichtlinie Vorgaben zur Einrichtung, zum Betrieb und zur Störungsbehandlung von Speichersystemen beschrieben?

M 2.352 Erstellung einer Sicherheitsrichtlinie für NAS-Systeme

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Ein NAS-System ist als zentraler Datenspeicher für Abläufe und Geschäftsprozesse in der Institution essentiell. Der sichere und ordnungsgemäße Betrieb kann nur sichergestellt werden, wenn Stationierung, Administration und Betrieb in die bestehenden sicherheitstechnischen Vorgaben integriert sind.

Die zentralen sicherheitstechnischen Anforderungen und das zu erreichende Sicherheitsniveau ergeben sich aus der organisationsweiten Sicherheitsleitlinie und sollten in einer spezifischen Sicherheitsrichtlinie für NAS-Systeme formuliert werden. Damit wird die übergeordnete und allgemein formulierte Sicherheitsleitlinie in ihrer Anwendung auf NAS-Systeme konkretisiert.

Für die Erstellung einer Sicherheitsrichtlinie für NAS-Systeme ist zuerst die Maßnahme M 2.316 *Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server* zu beachten. Dort werden die allgemeinen Sicherheitsvorkehrungen für IT-Systeme mit einer Server-Funktion vorgestellt. Für die Erstellung einer Sicherheitsrichtlinie für NAS müssen dann Festlegungen gemäß des Einsatzgebietes des NAS-Systems spezifiziert werden.

Die allgemeine Administrations- und Konfigurationsstrategie für das NAS ("Liberal" oder "Restriktiv") sollte entsprechend des Schutzbedarfs der damit verarbeiteten Informationen und den darauf zugreifenden Anwendungen entwickelt werden.

Zusätzlich sind bei den einzelnen Bereichen der NAS-Sicherheitsrichtlinie folgende Punkte zu beachten:

- Die Vorgaben für die Installation und Konfiguration gemäß M 4.274 *Sichere Grundkonfiguration von Speichersystemen*) müssen eingehalten werden. Weitere Vorgehensweisen und Regelungen müssen diesbezüglich definiert werden:
  - Das Vorgehen bei der Erstinstallation ist zu definieren und zu dokumentieren. Wenn diese vom Hersteller oder Lieferanten vorgenommen wird, ist die entsprechende Dokumentation einzufordern.
  - Wenn eine Fernwartung durch den Hersteller oder einen Dienstleister vorgesehen ist, müssen entsprechende organisatorische und technische Regelungen zur Fernwartung definiert werden.
- Ein Konzept für die Zugriffskontrolle muss erstellt werden. In NAS-Systemen wird dies hauptsächlich mit Hilfe von Access Control Lists erreicht. Auch sogenannten "Storage Security Appliances" können als transparente Proxies zwischen Clients und dem NAS geschaltet werden und somit einen zusätzlichen Zugriffsschutz bieten.

- Wenn ein NAS-System einen integrierten Webserver nicht nur als internes Konfigurationswerkzeug enthält, so muss vermieden werden, dass Netzzonen unterschiedlichen Vertrauens bedient werden. So ist es zulässig das NAS-System gleichzeitig als Dateiserver im Intranet und als Intranet-Webserver zu betreiben. Es ist nicht zulässig, das NAS-System als Dateiserver im Intranet und gleichzeitig als Webserver zu betreiben.
- Die Sicherheitsrichtlinie für NAS-Systeme muss Vorgaben für die sichere Administration und den sicheren Betrieb definieren (siehe auch M 4.275 *Sicherer Betrieb eines Speichersystems*).
- Je nach Einsatzbereich ist der Einsatz von Verschlüsselung (Standards, Schlüsselstärken) zu definieren.
- Der Einsatz von geeigneten Werkzeugen für Betrieb und Wartung und die Integration in ein bestehendes Netzmanagement sind zu untersuchen (siehe M 2.359 *Überwachung und Verwaltung von Speichersystemen*).
- Berechtigungen und Vorgehensweisen bei Softwareupdates und Konfigurationsänderungen müssen definiert werden. Änderungen müssen dokumentiert werden.
- Das NAS-System ist in das Virenschutzkonzept der Institution einzubinden, die Installation und Konfiguration von Anti-Viren-Software sowie die Versorgung mit Signatur-Updates muss geplant werden.
- Ein angemessenes Datensicherungskonzept (siehe dazu Baustein B 1.4 *Datensicherungskonzept*) ist auf das festgestellte Schutzniveau des NAS-Systems abzustimmen und mit dem organisationsweite Datensicherungskonzept abzustimmen.
- Für die Definition von Regelungen für Sicherheitsvorfälle ist der Baustein B 1.8 *Behandlung von Sicherheitsvorfällen* zu berücksichtigen. Darüber hinaus müssen
  - Richtlinien für die Reaktion auf Betriebsstörungen und technische Fehler (lokaler Support, Fernwartung), sowie
  - Regelungen für spezielle Sicherheitsvorfälle wie Schadprogramme, Eindringen von Unbefugten oder einen unerwartet hohen Verbrauch von CPU-Ressourcen definiert werden.
- Für die Notfallvorsorge für NAS-Systeme ist neben der Einbindung in das organisationsweite Notfallvorsorgekonzept auch M 6.98 *Notfallvorsorge für Speichersysteme* zu beachten.

Die Sicherheitsrichtlinie für NAS-Systeme muss für alle Beteiligten zugreifbar sein. Sie muss regelmäßig aktualisiert werden.

Ergänzende Kontrollfragen:

- Wurde eine Sicherheitsrichtlinie für den Betrieb von NAS-Systemen erstellt?
- Wann wurde die Sicherheitsrichtlinie zum letzten Mal aktualisiert?
- Wurden in der Sicherheitsrichtlinie Vorgaben zur Einrichtung, zum Betrieb und zur Störungsbehandlung von NAS-Systemen beschrieben?

M 2.353 Erstellung einer Sicherheitsrichtlinie für SAN-Systeme

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Ein SAN ist als zentrale Instanz zur Datenspeicherung für einige oder viele Abläufe und Geschäftsprozesse in der Institution essentiell. Der sichere und ordnungsgemäße Betrieb kann nur sichergestellt werden, wenn Planung, Stationierung, Administration und Betrieb von SAN-Systemen in die bestehenden sicherheitstechnischen Vorgaben integriert sind.

Die zentralen sicherheitstechnischen Anforderungen und das zu erreichende Sicherheitsniveau ergeben sich aus der organisationsweiten Sicherheitsleitlinie und sollten in einer spezifischen Sicherheitsrichtlinie für Speichersysteme formuliert werden, um die übergeordnet und allgemein formulierte Sicherheitsleitlinie im gegebenen Kontext zu konkretisieren und umzusetzen.

Grundlage für eine angemessene Definition von Forderungen, die in der Sicherheitsrichtlinie ausgedrückt werden, ist die Dokumentation der Schutzbedarfsfeststellung aller Daten, die im SAN gespeichert werden sollen. Nur hieraus lässt sich ableiten, welche Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit der Daten gestellt werden und entsprechend, welcher technische und organisatorische Aufwand angemessen ist.

Da SAN-Systeme ein dediziertes Netz enthalten, ist für die Erstellung einer Sicherheitsrichtlinie für SAN-Systeme zuerst die Maßnahme M 2.279 *Erstellung einer Sicherheitsrichtlinie für Router und Switches* zu beachten. Dort werden die allgemeinen Sicherheitsvorkehrungen für IT-Komponenten, die in einem internen Netz den Zugang zu Informationen oder anderen Systemen ermöglichen, vorgestellt.

Weitere Aspekte, die in der Sicherheitsrichtlinie eines SAN-Systems behandelt werden müssen sind:

Vorgaben für die Planung eines SAN:

- Es sind Vorgaben für die technische Infrastruktur zu entwickeln, in der SAN-Komponenten aufgestellt werden. Die Infrastruktur der Räume, in denen SAN Komponenten stationiert werden, muss geeignet sein, um die Verfügbarkeitsanforderungen des SAN-Systems zu erfüllen.
- Es sind Vorgaben zu machen, die den Zugriff Externer (zu Wartungszwecken) regeln. Da Überwachungs- und Wartungsverträge von Lieferanten von SAN Komponenten oftmals direkte Anbindung des Speichersystems an Überwachungssysteme des Herstellers oder Lieferanten fordern, ist festzulegen, wie solche Zugriffe kontrolliert und protokolliert werden.
- Wenn in Bezug auf die Verfügbarkeit ein sehr hoher Schutzbedarf festgestellt wird, ist der Einsatz einer desaster-toleranten SAN-Konfiguration einzufordern. Ist eine sehr hohe Verfügbarkeit des

SANs gefordert, sind SPoF (Single Points of Failure), die bei einem Ausfall den Komplettausfall des Systems mit sich ziehen, zu vermeiden. Der Betrieb einer solchen Konfiguration ist durch besondere Testsysteme zu unterstützen, auf denen Änderungen und Software-Updates geprüft werden können.

Vorgaben für der Arbeit von Administratoren:

- Es ist zu dokumentieren, nach welchem Schema Administrationsrechte für SAN-Komponenten oder das Gesamtsystem vergeben werden. Wenn möglich, ist ein Rollenkonzept zu entwickeln.
- Es sollten Administrator-Rollen definiert werden, denen aufgabenbezogen die nötige Rechte eingeräumt werden. Insbesondere sollte die routinemäßige Systemverwaltung (zum Beispiel Backup) nur mit den unbedingt nötigen Rechten durchgeführt werden können. Die Administrator-Kennungen werden dann den Rollen zugeordnet. Um die Auswirkungen von Fehlern zu reduzieren, darf unter einer Administrator-Kennung nur gearbeitet werden, wenn es zwingend notwendig ist.
- Der administrative Zugriff ist mindestens durch Einsatz starker Passwörter, gegebenenfalls auch durch besondere Maßnahmen zur Benutzerauthentisierung, abzusichern.
- Die Verwaltung und Kontrolle von SAN-Ressourcen durch die Administratoren und der Zugriff für Revisoren auf die Systeme ist entweder nur lokal über eine direkt angeschlossene Konsole, ein eigenes Administrationsnetz oder über verschlüsselte Verbindungen zulässig. Der Zugriff auf SAN-Ressourcen ist auf definierte Systeme zu beschränken und z. B.durch Sicherheitsgateways zu kontrollieren.
- IT-Systeme, die als Management-Konsole oder zur Revision eingesetzt werden, sind auf stärkstmögliche Weise vor Viren und Schadprogrammen zu schützen.
- Durch die vorgegebene Aufgabenteilung, durch Vorgaben und Regelungen und eine stets aktuelle Dokumentation der Einstellungen aller SAN-Komponenten ist sicherzustellen, dass Administratoren keine Aktionen ausführen oder Einstellungen am SAN vornehmen, die zu Inkonsistenzen, Ausfällen oder Datenverlust führen können. Relevante Änderungen müssen dokumentiert werden. Es ist dazu empfehlenswert, ein Änderungsmanagement-Verfahren, z. B. in Anlehnung an die ITIL (IT Infrastructure Library) zu betreiben.
- Es ist festzulegen, ob für bestimmte Änderungen das Vieraugenprinzip anzuwenden ist.

Vorgaben für die Installation und Konfiguration des SAN:

- Das Vorgehen bei der Erstinstallation ist zu dokumentieren. Da diese in den meisten Fällen vom Hersteller oder Lieferanten vorgenommen wird, ist die entsprechende Dokumentation einzufordern.

- Nach der Installation sind die Default-Einstellungen in Bezug auf Sicherheitsgefährdungen zu überprüfen, unsichere Dienste auf LAN-Schnittstellen von SAN-Switches und Speichergeräten zu deaktivieren und die Änderungen von Standardkennungen und -Passwörtern zu prüfen.
- Die Funktion "Systemkonsole für das SAN" ist auf möglichst wenige Geräte zu beschränken. Zugriffe dieser Geräte auf SAN-Komponenten über das LAN sollten ausschließlich über verschlüsselte Verbindungen ermöglicht werden. Der Kreis der Zugriffsberechtigten Anwender auf die Geräte ist möglichst klein zu halten. Regeln zur Verwendung und Konfiguration von Konsole und Restriktion der Zugriffsarten sind zu dokumentieren.
- Es sind Regelungen zu Erstellung und Pflege von Dokumentation, und die Form der Dokumentation (z. B. Verfahrensanweisungen für die Einrichtung administrativer Kennungen, Betriebshandbücher für Abläufe und Kontrollen im Normalbetrieb) vorzugeben.
- Auch innerhalb des SANs sollten spezifische Methoden der Segmentierung (siehe M 5.130 *Absicherung des SANs durch Segmentierung*)genutzt werden. Damit wird im SAN ein besserer Schutz von Teilbereichen - sowohl bezüglich der Vertraulichkeit als auch bezüglich der Integrität der Konfiguration und der Verfügbarkeit des SANs erreicht.

Vorgaben für den sicheren Betrieb:

- Die SAN-Administration ist abzusichern, indem Zugriffe nur über besondere Verbindungen (ein separates Administrationsnetz, gegebenenfalls auch das Speichernetz selbst) zugelassen werden.
- Es sind gegebenenfalls Werkzeuge für Betrieb und Wartung und die Integration der SAN Komponenten in ein bestehendes Netzmanagement auszuwählen. Vorgaben für eine sichere Konfiguration dieser Werkzeuge müssen definiert werden. Wenn möglich, sollten nur verschlüsselte Verbindungen genutzt und nicht benötigte Schnittstellen und Dienst gesperrt werden.
- Falls eine Fernwartung oder Überwachung durch den Hersteller genutzt werden soll, müssen Vorgaben für die Absicherung der Zugänge definiert werden. Beispielsweise ist die Anbindung per VPN oder exklusiv genutzte Verbindungen zur realisieren und eine für die Institution nachvollziehbare Protokollierung dieser Aktivitäten einzufordern.
- Die Berechtigungen für die Initiierung von Software-Updates und Konfigurationsänderungen sind eindeutig festzulegen. Die Vorgehensweise ist zu dokumentieren. Sobald sehr hohe Anforderungen an die Verfügbarkeit bestehen, ist zu fordern, dass Änderungen und Updates stets vor dem Wirkbetrieb an baugleichen Testsystemen zu erproben und zu bewerten sind.
- Während des SAN-Betriebes sind alle administrativen Tätigkeiten zu protokollieren. Darüber hinaus muss ein Konzept für die Verwaltung und Überwachung der Speichersysteme erstellt werden. Informationen zu diesem Thema finden sich in M 2.359 *Überwachung und Verwaltung von Speichersystemen*.

- Die Regelungen für die Datensicherung des SANs sind mit dem übergreifenden Datensicherungskonzepts der Institution (siehe dazu Baustein B 1.4 *Datensicherungskonzept*) und mit den Schutzbedarfsanforderungen des SAN abzustimmen.Bei besonderen Anforderungen an die Vertraulichkeit ist hier die Rechteverwaltung auf Backups vorzugeben.
- Wegen der zentralen Bedeutung des SANs ist dessen Notfallvorsorge (siehe auch M 6.98 *Notfallvorsorge für Speichersysteme*) in das organisationsweite Notfallvorsorgekonzept einzubinden.
- Auch für Revision und Audit sind Verantwortlichkeiten und Vorgehen zu beschreiben. Die SAN-Revision ist in ein übergreifendes Revisionskonzept zu integrieren.

Ergänzende Kontrollfragen:

- Wurde eine Sicherheitsrichtlinie für den Betrieb von SAN-Systemen erstellt?
- Wann wurde die SAN-Sicherheitsrichtlinie zum letzten Mal aktualisiert?
- Wurde ein Sicherheitsniveau in der Sicherheitsrichtlinie definiert?
- Wurden in der Sicherheitsrichtlinie Vorgaben zur Einrichtung, zum Betrieb und zur Störungsbehandlung von SAN-Systemen beschrieben?

M 2.354 Einsatz einer hochverfügbaren SAN-Konfiguration

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Leiter IT

Haben Systeme und Anwendungen, deren Daten im SAN gespeichert werden sollen, einen sehr hoher Schutzbedarf in Bezug auf die Verfügbarkeit aufzuweisen, so muss der Einsatz einer hochverfügbaren SAN-Konfiguration in Betracht gezogen werden.

Der Begriff "hochverfügbar" bezeichnet hier eine hohe Widerstandsfähigkeit gegen Schadensereignisse und wird auch als "Desaster-tolerant" bezeichnet. Bezogen auf die gespeicherten Daten einer Institution bedeutet das, dass mit Hilfe von SAN-Komponenten ein Speichersystem derart aufgebaut wird, dass

- alle Daten an zwei Standorten vorgehalten werden,
- die SAN-Komponenten in den beiden Standorten gekoppelt, aber nicht abhängig voneinander sind
- ein Schadenereignis an einem Standort die Funktionalität der Komponenten am zweiten Standort nicht gravierend beeinträchtigt.

Kenngrößen, die anzeigen, ob eine solche Architektur nötig und angemessen ist, sind:

- Die **maximale Wiederanlaufzeit** (engl. oft RTO: recovery time objective) gibt die Zeitspanne an, die vergehen darf, bis nach einem Schadensereignis IT-Systeme wieder in hinreihender Funktionalität zur Unterstützung von Geschäftsabläufen zur Verfügung stehen.
- Der **maximal tolerierbare Datenverlust** (engl. oft RPO: recovery point objective): Aus dem Alter des letzten verfügbaren konsistenten Datenbestandes lässt sich die Menge an "verloren gegangener Arbeit" nach dem Eintritt eines Schadensereignisses bemessen. Der maximal tolerierbare Datenverlust beschreibt im Grunde die Menge oder auch Komplexität an Arbeit, die mit einem für die Institution noch tragbaren Aufwand aufgeholt werden kann.
- Das **betroffene Umfeld** umfasst den räumlichen Umfang des Schadensereignisses. Nur wenn ein Standort mit seinen Systemen außerhalb der Wirkung des Ereignisses liegt, bleibt er nützlich.

SAN-Speichersysteme sind eine Schlüsseltechnik, um sehr hohe Anforderungen an die Verfügbarkeit der IT zu erfüllen:

Sie können bei Erhalt einer leistungsfähigen Koppelung so weit räumlich getrennt werden, dass auch gegen umfassend wirkende Ereignisse Vorsorge möglich ist.

Die mögliche leistungsfähige Koppelung kann genutzt werden, um den maximalen Datenverlust klein zu halten.

Die maximale Ausfallzeit einer Anwendung kann jedoch nur in geringem Umfang durch die SAN-Konfiguration gesteuert werden. Da die Ausfallzeit ausschließlich aus Sicht der Anwender gemessen werden darf, hängt sie nicht nur von der Verfügbarkeit der gespeicherten Daten ab, sondern genauso von der Verfügbarkeit der übrigen IT-Infrastruktur (Server, Netz, PCs,...), die von SAN-Komponenten mit Daten versorgt werden.

Möglichkeit der Konfiguration

Es existieren verschiedene Möglichkeiten, ein SAN-System hochverfügbar zu konfigurieren.

Spiegelung durch den Server

Die einfachste Möglichkeit des hochverfügbaren SAN-Einsatzes ist dann gegeben, wenn ein Server, der seine Daten auf einem SAN-Speicher ablegt, an ein zweites, räumlich abgesetztes Speichersystem angeschlossen wird.

Jeder Schreibzugriff des Servers wird auf beiden Speichersystemen durchgeführt. Nachteilig an dieser Lösung ist, dass die Konfiguration der Instanz "Speicher" wiederum teilweise auf dem Server stattfindet.

Damit findet wieder Administration am einzelnen Server statt. Ein Vorteil eines zentralen Speichersystems an dem auch zentral administriert werden kann, wird so verschenkt. Zudem muss die Verkabelung komplexer angelegt werden, da jeder Server mit beiden Speichersystemen verbunden wird. Vereinfacht darstellt muss in Ergänzung der Verbindung zwischen Server und Speichersystem eine zweite Leitung von Server direkt zum abgesetzt stationierten zweiten Speichersystem verlegt werden.

Replikation

Replikation kann durch den Server oder durch das Speichersystem erfolgen.

Server-basierte Replikation wird in der Regel über eine eigene Software, die Applikation oder das Betriebssystem realisiert. Allerdings geht dieser Ansatz meistens mit einer hohen Belastung von CPU, Hauptspeicher und Bandbreite einher.

Bei der Replikation durch das Speichersystem werden die Server mit einem Speichersystem verbunden, dieses Speichersystem gleicht seinen Datenbestand komplett oder entsprechend seiner Konfiguration mit einem weiteren Speichersystem in einem abgesetzten Standort ab.

Synchrone Replikation

Wenn die Standorte nah genug beieinander liegen, ist synchrone Datenreplikation möglich. "Synchrone Datenreplikation" bedeutet, dass jeder Schreibzugriff des Servers von seiner direkt angeschlossenen Speicherplatte erst dann als fertig gemeldet wird, wenn das zweite, abgesetzte Speichersystem dem ersten Speichersystem das erfolgreiche Schreiben bestätigt hat.

Damit werden Festplattenzugriffe aus Sicht des Servers langsamer, da zwei Plattensysteme schreiben und weil die Signallaufzeit zwischen dem Speichersystem in Standort A und dem in Standort B hinzukommt.

Asynchrone Replikation

Bei der asynchronen Datenreplikation sorgt besondere Replikationssoftware auf den Speichersystemen dafür, dass das Speichersystem in Standort A seine

veränderten Daten regelmäßig an das Speichersystem in Standort B übermittelt.

Damit hat der Server ein ungebremstes Speichersystem zugeordnet. Ein weiterer Vorteil an der Stelle ist, dass eine Behörde bzw. ein Unternehmen nicht mehr gezwungen ist, die exakt identischen Speichersysteme für die Notfallvorsorge an zwei Orten bereit zu halten. Am Hauptstandort kommt dann ein hochleistungsfähiges System zum Einsatz. Am zweiten Standort kann dagegen ein günstigeres System installiert werden, so dass dennoch die Hauptaufgaben in einem Notfallszenario gewährleistet werden.

Der Nachteil bei der asynchronen Replikation ist, dass das zweite Speichersystem stets einen älteren Datenbestand hat. Wie groß der Datenverlust bei Ausfall des primären Systems ist, hängt von der eingesetzten Technik ab.

Synchrone Datenreplikation von Speichersystemen ist nur dann sinnvoll, wenn auch redundante Serversysteme bereitstehen, die den Betrieb direkt weiterführen können. Ein Szenario, bei dem an einem Standort das Speichersystem komplett ausfällt, die angeschlossenen Server und Netzkomponenten aber nicht (z. B. die des SAN), ist eher selten.

Bei der Planung einer hochverfügbaren SAN-Konfiguration muss zunächst das gesamte Notfallvorsorge-Konzept für die IT der Institution geprüft werden. Die Verfügbarkeitsanforderungen an das SAN und die angeschlossenen Server schriftlich müssen schriftlich festgelegt werden.

Angepasst an die Anforderungen und Risikopolitik der Institution ist die Planung eines hochverfügbaren SANs nur der erste Schritt in Richtung Hochverfügbarkeit. Gleichzeitig muss eine passende Planung der Weiterentwicklung der gesamten IT-Umgebung und der Notfallplanung für die Institution erfolgen.

Ein hochverfügbares SAN ist nur dann sinnvoll, wenn auch Server für den Wiederanlauf bereitstehen und wenn die Anwender an intakten Arbeitsplätzen über ein funktionierendes Netz auf die Daten zugreifen können.

Es ist zu beachten, dass ein hochverfügbares SAN um ein Test- und Konsolidierungssystem ergänzt werden muss. Konfigurationsänderungen und Software-Updates dürfen bei Aufbau einer hochverfügbaren Konfiguration nie direkt am produktiven System vorgenommen werden. Von der Institution sind Systeme vorzuhalten, an denen sämtliche Änderungen getestet werden können. Nur so lässt sich sicherstellen, dass der Betrieb nicht durch administrative Eingriffe gefährdet wird.

Ergänzende Kontrollfragen:

- Hat die Institution ein aktuelles IT-Notfallkonzept?
- Sind die Anforderungen an das SAN und die angeschlossenen Serversysteme dokumentiert?

M 2.355 Auswahl von Lieferanten für ein Speichersystem

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement, Leiter IT

Nachdem die Anforderungen für ein Speichersystem spezifiziert wurden ist ein geeigneter Lieferant zu identifizieren. Die Auswahl möglicher Lieferanten muss dabei mehr Kriterien berücksichtigen als die reine Hardwarelösung und deren Preis.

Es ist davon auszugehen, dass die Unterstützung des Lieferanten mindestens bei der Lösung von Problemen im Betrieb und erst recht bei Hardwareausfällen benötigt wird.

Entsprechend sind neben Preisen und Konditionen für das Speichersystem und dessen Inbetriebnahmen auch die Konditionen der Unterstützung zu bewerten.

Die Aspekte der Wartung und Instandhaltung werden schriftlich im Vertrag im Rahmen von so genannten Service Level Agreements (SLAs) definiert.

Entsprechend sollte das Angebot eines möglichen Lieferanten neben den Hardware und Softwarepreisen auch die Preise für die denkbaren SLAs beinhalten, so dass der Kunde die Gesamtpakete vergleichen kann, wenn verschiedene Hersteller oder Lieferanten in Betracht kommen.

Wenn ein Speichersystem nicht gekauft, sondern z. B. geleast wird, muss auch vertraglich festgehalten werden, wie bei Vertragsende der Datentransfer auf Nachfolgesysteme und andere technische und organisatorische Fragen zu welchen Kosten gehandhabt werden.

Generell ist festzustellen, dass gerade bei komplexen Systemen eine Lösung aus einer Hand Vorteile haben kann: in der Regel können Probleme, die beim Aufbau, Test und Betrieb entstehen, schneller und effektiver beseitigt werden, wenn nur ein Anbieter involviert ist.

Bei Lösungen aus Komponenten verschiedener Anbieter können in der Anschaffung preisliche Vorteile erzielt werden, es ist aber wichtig zu prüfen, ob dieser Vorteil auch bei Betrachtung der Kosten der Umsetzung (Grundkonfiguration, Probebetrieb, Datenmigration) und des Betriebs (Wartung, Unterstützung bei Problemen) bestehen bleibt.

Ergänzende Kontrollfragen:

- Sind alle Vereinbarungen schriftlich fixiert?
- Enthält der Vertrag eindeutige und quantifizierbare Leistungsbeschreibungen?
- Sind genaue Regelungen für das Laufzeitende des Vertrages getroffen worden?

M 2.356 Vertragsgestaltung mit SAN-Dienstleistern

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement, Leiter IT

Nur wenige Institutionen werden die technische Betreuung der SAN-Komponenten in Normalbetrieb und in Notfallsituation selbst leisten können und wollen. Daher müssen diese dann auf geeignete Hersteller und Lieferanten zugreifen, im weiteren kurz als Dienstleister bezeichnet.

Die Aspekte, die im Folgenden beschrieben werden, sind als Hilfsmittel und Checkliste bei der Vertragsgestaltung zu sehen. Art, Umfang und Detaillierungsgrad der vertraglichen Regelungen hängen von den Verfügbarkeitsanforderungen des Auftraggebers und auch von der Komplexität des konkreten SANs ab.

Grundsätzlich sollte der Dienstleister auf die Einhaltung aller relevanten Gesetze und Vorgaben, vor allem aber des Datenschutzes nach dem Bundesdatenschutzgesetz (BDSG) und auf den Einsatz von organisatorischen und technischen Maßnahmen zur IT-Sicherheit verpflichtet werden. Diese sollten mindestens dem Niveau des IT-Grundschutzes entsprechen und gegebenenfalls auf weitere vom Auftraggeber vorgegebene Sicherheitsanforderungen verpflichtet werden.

Neben diesen allgemeinen Verpflichtungen empfiehlt es sich, alle vereinbarten Leistungen messbar und prüfbar im Vertrag schriftlich zu fixieren. So kann es z. B. angemessen sein, zu vereinbaren, dass ein qualifizierter Mitarbeiter des Dienstleisters bei bestimmten Problemfällen innerhalb von 4 Stunden vor Ort sein muss. Eine solche konkrete, an den Anforderungen der Institution festgemachte Aussage kann eventuell sinnvoller sein als ein Pauschalangebot ("Gold-Support"), das möglicherweise ungünstige Ausnahmen (Sonntags nur telefonische Unterstützung) von der geforderten Qualität beinhaltet.

Auch die Erstellung des Notfallvorsorgekonzeptes für das SAN sollte Vertragsbestandteil sein. Insbesondere ist zu klären, wer für die fachlichen Inhalte verantwortlich ist und welche Mitwirkungspflichten dem Auftraggeber obliegen.

Es ist dringend anzuraten, dass der Auftraggeber genügend Vorbereitung in die Zusammenstellung der eigenen Anforderungen investiert. Nachträgliche Konkretisierungen und Ergänzungen des Vertrages, die aufgrund unterschiedlicher Interpretation von ungenau beschriebenen Leistungen notwendig werden, sind oftmals mit deutlichen Kostenerhöhungen für den Auftraggeber verbunden.

Im Folgenden findet sich eine Themenliste, die bei der Herstellung oder Prüfung eines Vertragsentwurfes herangezogen werden kann:

Organisatorische Regelungen und Prozesse

- Festlegung von Kommunikationswegen und Ansprechpartnern

- Festschreibung von Zeiten (z. B. Tagbetrieb, Nachtbetrieb, was zählt als Wochenende, Feiertage)
- Festlegung von Prozessen, Arbeitsabläufen und Zuständigkeiten
- Verfahren bei Problemen und Krisen, Benennung von Ansprechpartnern mit den nötigen Befugnissen
- Zugriffsmöglichkeiten des Dienstleisters auf IT-Ressourcen des Auftraggebers
- Zutritts- und Zugriffsberechtigungen für Mitarbeiter des Dienstleisters zu den Räumlichkeiten und IT-Systemen des Auftraggeber
- Übergabe von Datenbeständen bei Beendigung des Vertragsverhältnisses, Datenlöschung bei Rücknahme von Speichermedien durch den Auftragnehmer

Personal

- Gegebenenfalls Gestaltung der Arbeitsplätze von externen Mitarbeitern
- Festlegung und Abstimmung von Vertretungsregelungen
- Planung von Fortbildungsmaßnahmen

Notfallvorsorge

- erforderliche Handlungen beim Eintreten eines Störfalls
- Reaktionszeiten und Eskalationsstufen
- Mitwirkungspflicht des Auftraggebers bei der Behebung von Notfällen
- Vereinbarung zur Bereitstellung von Ersatz- oder Ausweichsystemen
- Von besonderer Bedeutung können Regelungen im Fall höherer Gewalt sein. Es sollte beispielsweise geklärt sein, wie bei einem Streik des Personals des Dienstleisters die Verfügbarkeit dieses durch z. B. weiteres externes Personal sichergestellt werden kann.

Haftung, juristische Rahmenbedingungen

- Eine Verpflichtung der einzelnen Mitarbeiter des Auftragnehmers auf die Einhaltung von geltenden Normen und Gesetzen sowie besonderer vereinbarter Sicherheitsmaßnahmen ist vertraglich zu regeln. Gegebenenfalls sind besondere Geheimhaltungsvereinbarungen vertraglich zu fixieren.
- Die Einbindung Dritter, Subunternehmer und Unterauftragnehmer des Dienstleisters ist zu regeln. In der Regel empfiehlt es sich nicht, diese grundsätzlich auszuschließen, sondern sinnvolle Regelungen festzulegen.
- Die Eigentums- und Urheberrechte an Systemen, Software und Schnittstellen sind festzulegen. Es ist zu klären, ob der Dienstleister bereits bestehende Verträge mit Dritten (Hardwareausstattung, Serviceverträge, Softwarelizenzen etc.) übernimmt.

- Die Weiterverwendung der vom Dienstleister eingesetzten Tools, Prozeduren, Skripte, Batchprogramme ist für den Fall der Beendigung des Dienstleistungsvertrags zu regeln.
- Regelungen für das Ende des Vertragsverhältnisses, z. B. für einen Wechsel oder bei Insolvenz des Dienstleisters, sollten spezifiziert werden.
- Auf ein ausreichend flexibles Kündigungsrecht ist zu achten.
- Der Auftragnehmer ist zu verpflichten, nach Beendigung des Auftrags alle vom Auftraggeber im Rahmen des Vertragsverhältnisses angeschaffte Hard- und Software inklusive gespeicherter Daten zurückzugebens sowie alle gespeicherten Informationen sicher zu löschen.
- Haftungsfragen im Schadensfall sind zu klären. Sanktionen oder Schadensersatz bei Nichteinhaltung der Dienstleistungsqualität dürfen aus Sicht des Auftraggebers dabei nicht überschätzt werden.
    - Zunächst ist stets zu fragen, wie ein Schaden nachgewiesen bzw. der Verursacher überführt werden kann
    - Wie wird beispielsweise ein Imageschaden quantifiziert?
    - Wie ist es zu bewerten, wenn gravierende Pflichtverletzungen aufgedeckt werden, die nur zufällig nicht zu einem größeren Schaden geführt haben?
    - Das Recht auf Schadensersatzzahlungen ist wertlos, wenn diese die Zahlungsfähigkeit des Dienstleisters übersteigen und dieser Insolvenz anmeldet.

Änderungsmanagement und Testverfahren

- Es müssen Regelungen gefunden werden, die es ermöglichen, dass der Auftraggeber in der Lage ist, sich neuen Anforderungen anzupassen. Es ist festzulegen, wie geänderte Anforderungen des Auftraggebers behandelt werden.
- Testverfahren für neue Soft- und Hardware sind zu vereinbaren. Dabei sind folgende Punkte einzubeziehen:
    - Regelungen für Updates und Systemanpassungen
    - Zuständigkeiten bei Auftraggeber und Dienstleister bei der Erstellung von Testkonzepten und bei der Durchführung von Tests
    - Abnahme- und Freigabeprozeduren. Es ist immer wieder zu beobachten, dass der Auftragnehmer explizit oder implizit eine Freigabe von Änderungen für den produktiven Betrieb vornimmt, obwohl gegebenenfalls beachtlichen Risiken und Verantwortung bei Auftraggeber liegen.

Kontrolle des Auftragnehmers

- Die Dienstleistungsqualität muss regelmäßig kontrolliert werden. Der Auftraggeber muss die dazu notwendigen Auskunfts-, Einsichts- und Zugangsrechte besitzen. Wenn unabhängige Dritte Audits oder Benchmark-Tests

durchführen sollen, muss dies bereits im Vertrag geregelt sein.

Ergänzende Kontrollfragen:

- Sind alle Vereinbarungen schriftlich fixiert?
- Enthält der Vertrag eindeutige und quantifizierbare Leistungsbeschreibungen?

M 2.357 Aufbau eines Administrationsnetzes für Speichersysteme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Verwaltung und Überwachung von Ressourcen wie SAN- oder NAS-Komponenten, an die hohe Sicherheitsanforderungen gestellt werden, muss angemessen umgesetzt werden. Der Aufbau eines eigenen LANs, das ausschließlich administrativen Aufgaben dient, ist oft der übersichtlichste, effektivste und wirtschaftlichste Weg, um diesen Anforderungen zu genügen. In diesem Administrationsnetz werden PCs stationiert, die ausschließlich zur Verwaltung kritischer Komponenten dienen.

Grundsätzlich sollen auch innerhalb dieses Netzes nur sichere Protokolle (ssh statt telnet, https statt http) zur Administration genutzt werden. Die zumindest logische, wenn nicht gar physische Abtrennung dieses Administrationsnetzes von Produktionsnetz macht jedoch den Einsatz unsicherer Protokolle, insbesondere des in vielen Produktionsumgebungen immer noch fast unvermeidlichen SNMP Version1, tolerierbar.

Konzeption/Planung

- Ein sehr einfacher Aufbau eines solchen Netzes kann damit starten, dass ein separater Switch in Betrieb genommen wird.
- Alle Clients der Administratoren werden mit ihrem Netzanschluss an das Administrationsnetz gebunden.
- Alle Server und Systeme mit erhöhtem Sicherheitsbedarf (aktive Netzkomponenten, Speichersysteme) erhalten einen zusätzlichen Netzanschluß und werden damit an das Administrationsnetz gebunden.
- Auf den Servern wird der Administrationszugang der Betriebs- und Anwendungssoftware wo immer das möglich ist, exklusiv an die Netzadresse im Administrationsnetz gebunden.

Im Administrationsnetz sollten private (wie in RFC-Standard 1918 beschrieben) Adressen benutzt werden. Solche Adressen werden in "offiziellen" Netzen nicht geroutet, so dass ein Anschluss an offizielle Netze, wenn er denn nötig werden sollte, stets NAT (Network Address Translation) und weitere Schutzmaßnahmen, die durch eine Firewall realisiert werden, erfordert.

Im Administrationsnetz sollte auf allen IT-Komponenten durch Nutzung oder Einsatz eines NTP-Servers eine einheitliche Uhrzeit sichergestellt werden. Damit wird die Auswertung von Protokollen erleichtert und die Bewertung von Vorfällen, die Wirkung auf mehreren Komponenten zeigen, ermöglicht.

Die verfügbaren Ressourcen für den gesamten Aufbau eines Speichersystems sind zu ermitteln. Hierzu gehören sowohl Personalressourcen, die erforderlich sind, um ein Konzept zu erstellen und umzusetzen bzw. um das Netz zu betreiben, als auch die hierfür notwendigen finanziellen Ressourcen.

Die Ergebnisse sind entsprechend zu dokumentieren.

Es ist zudem zu prüfen, ob im Administrationsnetz zusätzliche Überwachungsmaßnahmen etabliert werden sollten. Zum Beispiel kann durch Einsatz von Netz-IDS zusätzlich überwacht werden, ob unzulässige Aktivitäten im Netz zu beobachten sind.

Ebenso könnte in einem solchen Netz auch eine zentrale Protokollierung etabliert werden, in der eine zentrale Instanz als Protokollserver die Logdaten aller Server und Speichersysteme verwaltet. Es ist zu beachten, dass solche besonderen Maßnahmen gegebenenfalls mit der Personalvertretung abgestimmt werden müssen.

Falls das Administrationsnetz einen komplexen Aufbau aufweist, sollte der Baustein B 4.1 *Heterogene Netze* für Aufbau und Prüfung herangezogen werden.

Umsetzung

Zunächst ist zu untersuchen, wie ein produktives Netz und die darin stationierten Server und sonstigen Geräte (aktive Netzkomponenten, Speichersysteme) um ein Administrationsnetz erweitert werden können.

Zunächst sind die Maßnahmen M 2.139 *Ist-Aufnahme der aktuellen Netzsituation* und M 2.140 *Analyse der aktuellen Netzsituation* zu bearbeiten. Anschließend sind die Anforderungen an die Netzkommunikation des neu aufzubauenden Administrationsnetzes zu ermitteln sowie eine Schutzbedarfsfeststellung des zukünftigen Netzes durchzuführen.

Die Schutzbedarfsanforderungen des Administrationsnetzes sind aus den bestehenden IT-Verfahren, die über dieses Netz administriert werden sollen, abzuleiten.

Betrieb

Mit Aufnahme des Testbetriebes muss eine Prüfung stattfinden, die die Sicherheitsvorkehrungen testet und zur Grundlage der Betriebsdokumentation dieses Netzes wird. Typische Prüffragen sind:

- Ist eine durchgängige Trennung des Administrationsnetzes vom Produktionsnetz gegeben?
- Werden wo immer möglich sichere Dienste (secure shell, https) genutzt? Sind die unsicheren Varianten dieser Dienste (telnet, http) auf den administrierten Geräten deaktiviert?
- Ist überschaubar und dokumentiert, wo auf den Einsatz unsicherer Dienste nicht verzichtet werden kann?
- Sind alle Default-Kennungen und -Passwörter auf PC, Servern und aktiven Netzkomponenten etc. geändert?

Anschließend kann der produktive Betrieb gestartet werden.

Aussonderung

Wenn PCs oder andere Hardware ausgesondert oder auch nur zu Reparatur zeitweise aus dem Netz genommen werden, ist sicherzustellen, dass keine internen Informationen (Passwörter, Protokolldateien, Dokumente zu Interna etc.) darauf gespeichert sind.

Notfallvorsorge

Es muss eine Notfallplanung geben, so dass Betrieb des produktiven Netzes sichergestellt wird, wenn das Administrationsnetz ausfällt.

Ergänzende Kontrollfragen:

- Ist das Administrationsnetz von produktiven IT-Netzen physisch oder durch Firewalls kontrolliert abgetrennt?
- Ist der Umfang besonderer Überwachungs- oder Protokollierungsmaßnahmen mit der Personalvertretung abgestimmt?

M 2.358 Dokumentation der Systemeinstellungen von Speichersystemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Dokumentation der Systemeinstellungen zum Speichersystem weist die Umsetzung von technischen und organisatorischen Vorgaben nach und beschreibt die individuelle Konfiguration der Institution. Die Dokumentation ist Grundlage für die Administration im Normalbetrieb und für die Planung und Durchführung von Änderungen. Zudem ist eine aktuelle und korrekte Dokumentation Grundlage der Notfallvorsorge.

Daten, die im Notfall relevant sind, müssen in allen Notfallszenarien zugreifbar sein. Dabei muss jedoch beachtet werden, dass Informationen zu den Systemeinstellungen vertraulich sind und daher ausreichend vor unberechtigtem Zugriff geschützt werden müssen.

Umfang der Dokumentation

Dokumentiert werden sollten insbesondere folgende Informationen:

Zur Organisation:

- Eine Beschreibung der definierten Rollen und der zugehörigen Rechteprofile
- Die administrativen Benutzer des Speichersystems mit zugeteilter Rolle
- Den Zeitpunkt der Einrichtung von Benutzertkennungen und -rechten und gegebenenfalls die Befristung und weitere Erläuterungen
- Die Kontaktdaten des Benutzers und dessen organisatorische Einbindung
- Vorgaben zu Datensicherung und Notfallvorsorge

Zur Technik:

- Die Aufstellung aller Speichergeräte mit Angaben zu Typ, Zweck und Anwenderkreis
- Die logischen und physischen Zuordnungen der Speichergeräte zu den Servern
- Sämtliche Anbindungen der Speichergeräte an die Netze (SAN, LAN, gegebenenfalls WAN zur Fernüberwachung)
- Eine Aufstellung, welche Geräte über eine NAS-Schnittstelle Daten exportieren
- Eine Aufstellung aller Management-Schnittstellen (In-Band und Out-Band). Diese sollte auch eine Übersicht enthalten, welche Schnittstellen aktiv sind und welche Dienste darüber erreichbar sind.

Zur Administration:

- Eine grafische Darstellung der Netze (SAN, LAN, gegebenenfalls WAN) und der konfigurierten Verbindungen zwischen Speichersystemen, Servern und Administrations-PC.
- Alle erforderlichen Angaben zur Aktivierung und Deaktivierung von Schnittstellen und Diensten.

- Die notwendigen Einstellung für die Datensicherung
- Die Einstellungen zur Protokollierung
- Empfehlenswert ist eine kurze Darstellung ("Kochbuch") der Handhabung von wichtigen oder regelmäßig durchzuführenden Administrationstätigkeiten.

regelmäßige Prüfung der Dokumentation

Die Dokumentation zur Organisation sollte regelmäßig (mindestens alle 6 Monate) daraufhin überprüft werden, ob sie den tatsächlichen Stand der Rechtevergabe widerspiegelt und ob die Rechtevergabe noch den Sicherheitsanforderungen und den aktuellen Aufgaben der Benutzer entspricht.

Die technische Dokumentation sollte noch häufiger zumindest stichprobenartig überprüft werden, da sie die Grundlage der Notfallvorsorge ist.

Ergänzende Kontrollfragen:

- Sind Aufzeichnungen über die zugelassenen Benutzer und Gruppen und deren Rechteprofile vorhanden?
- Sind die Aufzeichnungen aktuell?
- Wann wurden die Aufzeichnungen das letzte Mal überprüft?
- Ist die Dokumentation (auch die Papierdokumentation) vor unberechtigten Zugriffen ausreichend geschützt?

M 2.359 Überwachung und Verwaltung von Speichersystemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um Fehlersituationen und Sicherheitsprobleme zeitnah erkennen und beheben zu können, ist es notwendig, den laufenden Betrieb von Speichersystemen zu überwachen. Während bei einem Server punktuell der Server zu überwachen ist, müssen beim Einsatz eines Speichersystems sowohl der Server als auch der Speicher überwacht werden.

Um die Auswertung von Daten verschiedener Quellen praktikabel zu machen, sollte durch Einsatz oder Nutzung eines NTP-Servers eine einheitliche Datum-/Uhrzeiteinstellung auf allen Geräten erzwungen werden.

Ein Speichersystem selbst kann wiederum aus einer Vielzahl von Komponenten bestehen. Zu überwachen sind Daten über den Zustand der Hardware des Speichersystems, Daten zur Auslastung des Speichersystems und Daten über die Transportwege.

Diese Daten können effizient nur automatisiert durch Programme analysiert werden. Dabei muss eine Vielzahl von Daten gesammelt und ausgewertet werden. Wichtige Nachrichten können durch den Einsatz von Nachrichten-Filtern herausgefiltert und somit schneller erkannt werden.

In diesem Zusammenhang müssen folgende Komponenten überwacht werden:

- Die Anwendungen, die in einem Speichersystem Daten verarbeiten oder eine Hilfsfunktion haben. Dazu gehören die Sicherungssoftware und auch Anti-Viren-Software.
- Die Nutzdaten, die von Anwendungen verarbeitet werden und dann über das Speichernetz vom Server auf Speichersysteme transportiert werden.
- Die Netzhardware, die für den Transport der Daten benötigt wird.
- Die Speicherhardware (Plattensysteme, Bandlaufwerke), die zur Speicherung der Daten benötigt wird.
- Das Netz. Bei einem NAS-System ist das TCP/IP-Netz zu überwachen, bei einem SAN das Speicher-interne Netz und zudem das zusätzlich zur Steuerung und Verwaltung genutzte lokale Netz.

Neben der Überwachung der Ressourcen sollte auch die Verwaltung einzelner Komponenten und des Gesamtsystems von zentraler Stelle aus möglich sein. Systeme, die für die Steuerung und Kontrolle von Speichersystemen eingesetzt werden können, werden oft als Speicher-Managementsysteme bezeichnet.

NAS-Management

Die Überwachung von reinen NAS-Systemen ist häufig besonders einfach gestaltet. Auch wenn das System scheinbar "wartungsfrei" erscheint, ist es nötig, technische und oder organisatorische Überwachungsmaßnahmen zu etablieren. Nach Möglichkeit sollte das NAS-System in ein einfaches Netz-

Managementsystem eingebunden werden, um mindestens zu kontrollieren, ob das NAS-System verfügbar ist und hinreichend Speicherkapazität aufweist.

SAN-Management

Bei der Überwachung von SAN-Systemen stehen die Mechanismen des In-Band-Managements und des Out-Band-Managements zur Verfügung.

In-Band Management findet auf den Schnittstellen und Netzen statt, die dem Datentransport zwischen den SAN-Geräten dienen. Die Möglichkeiten der Konfiguration und der Überwachung sind beim In-Band-Management häufig weiter reichend und komfortabler, da die zugrunde liegende Software produktnah ist und Hersteller hier Alleinstellungsmerkmale suchen.

Das Out-Band Management benutzt zusätzliche Schnittstellen, üblicherweise TCP/IP-Netzanschlüsse. Als Protokoll zur Informationsgewinnung ist SMNP weit verbreitet. Out-Band-Management bietet (auch) die üblichen Standards und erleichtert die Kombination von Produkten unterschiedlicher Hersteller.

Da als Protokoll beim Out-Band-Management oft noch die wenig sichere SNMP Version 1 genutzt wird, ist ein separates Management-LAN zu betreiben (siehe M 2.357 *Aufbau eines Administrationsnetzes für Speichersysteme*).

Bei höherem Anspruch an die Verfügbarkeit sollte die Kombination gewählt werden. Wenn sowohl In-Band- als auch Out-Band-Management und Überwachung im Einsatz sind, erleichtert und beschleunigt die zusätzliche Netzanbindung die Überwachung und Diagnose von Problemen.

Zentrale Kontrolle

In größeren Installationen, vor allem bei SANs mit verschiedenen Standorten der Komponenten, sollte eine zentrale Stelle existieren, an die alle für den Betrieb wichtigen Informationen gemeldet werden. Der Einsatz von Programmen, die das Geschehen übersichtlich grafisch darstellen können, ist ratsam.

Ein solches Managementsystem stellt die Schnittstelle zu einem komplexen System dar. Es kann nur von hinreichend geschultem Personal effizient genutzt werden.

Ergänzende Kontrollfragen:

- Gibt es eine zentrale Stelle, an die Informationen unterschiedlicher Speichersysteme gemeldet werden?
- Welche Indikatoren, die Probleme oder Störungen ankündigen werden überwacht?
- Sind Nachrichten-Filter im Einsatz, um die wesentlichen Nachrichten herauszufiltern und besser darzustellen?
- Sind die Mitarbeiter, die das Speichersystem überwachen, ausreichend geschult, um Meldungen korrekt zu interpretieren und Probleme frühzeitig zu erkennen?

M 2.360 Sicherheits-Audits und Berichtswesen bei Speichersystemen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement,

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator, Revisor

Umfang und Häufigkeit von Sicherheitsüberprüfungen auf Speichersystemen werden durch die Daten, die auf dem jeweiligen Speichersystem verarbeitet werden, bestimmt. Bei komplexen Systemen, auf denen eine Vielzahl von Anwendungen ihre Daten auf dem Speichersystem ablegen, muss eine Analyse der Geschäftsprozesse und eine darauf abgestimmte Feststellung des Schutzbedarfs vorgenommen werden. Dabei ist für Anwendungen und Daten, die die wesentlichen Geschäftsprozesse unterstützen, der Schutzbedarf festzustellen, um Anforderungen an die Häufigkeit und Tiefe von Sicherheits-audits zu erhalten. Wie üblich geben die strengsten Anforderungen einer einzelnen Anwendung die Vorgabe für das Gesamtsystem.

Zur Überwachung aller sicherheitsrelevanten Tätigkeiten muss ein Prozess eingerichtet werden. In diesem muss festgelegt sein, welche Sicherheitsreports regelmäßig erstellt werden. Da Speichersysteme komplex zusammengesetzt sein können, müssen Sicherheitsreports relevante Beobachtungen aus verschiedenen Quellen zusammenstellen und bewerten. Zudem muss festgelegt werden, wie mit Abweichungen von den Vorgaben umgegangen wird. Die Sicherheitsreports sollten als Information für den Auditor verwendet werden.

Inhalt eines Audits

Ein Audit gleich die Sicherheitsvorgaben mit den aktuellen Einstellungen und Daten ab. Durch ein solches Audit wird überprüft, ob die geforderten Sicherheitseinstellungen und Abläufe eingehalten werden.

Ziel des Sicherheitsaudits

Wichtig ist, dass ein Audit nur zur Feststellung von Tatsachen und nicht zur Ermittlung von Schuldigen dient, siehe auch M 2.182 *Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen.*

Sicherheits-Berichtswesen

Das Resultat eines Audit kann als eine einfache Soll-Ist-Gegenüberstellung gehalten werden. Der Bericht soll in gebotener Kürze die Vorgaben z. B. aus der Sicherheitsrichtlinie darstellen und die Feststellungen des Audits zu den einzelnen Vorgaben darstellen. Wenn Abweichungen vom Soll gefunden werden und Maßnahmen zur Besserung bekannt sind, so sollten diese direkt in den Report geschrieben werden.

Unabhängigkeit der Auditoren

Die Durchführung der Audits muss durch unabhängige Auditoren erfolgen, d. h. das durchführende Personal darf sich und seine Arbeit nicht selbst auditieren.

Auch wenn die Tätigkeit der Auditoren durch die Administratoren des Speichersystems unterstützt wird, benötigen sie tiefere Kenntnisse über das Speichersystem zur Durchführung ihrer Tätigkeit. Diese Kenntnisse sind durch regelmäßige Schulungen zu erwerben bzw. zu aktualisieren.

Autorisierung der Auditoren

Wenn die Auditoren selbstständig und ohne Unterstützung durch die Administratoren tätig werden sollen, so ist eine Rolle "Auditor" für alle Komponenten des Speichersystems zu definieren. Die Rechte zu dieser Rolle sollten als "Nur Lesen" aller Einstellungen und Logdateien des Speichersystems definiert werden.

Wenn keine konkreten Vorgaben der Institution vorliegen, so sollte der Auditor mindestens die folgenden Bereiche prüfen:

- Es gibt ein Sicherheitskonzept für die technische Ausgestaltung und organisatorische Regelungen des Speichersystems.
- Der Schutzbedarf der gespeicherten Daten in Bezug auf Verfügbarkeit und Vertraulichkeit wurde nach Vorgaben der Anwender festgelegt und dokumentiert.
- Bei Inbetriebnahme wurden in allen Komponenten (Speicher, Sicherungsgeräte, gegebenenfalls SAN-Switche), Administrations-PC und zusätzlicher Software die Standardpasswörter ersetzt.
- Alle Komponenten (Speicher, Sicherungsgeräte, gegebenenfalls SAN-Switche) sind in zutrittsgeschützten Räumen mit angemessener Infrastruktur (Stromversorgung, Klimatisierung) stationiert.
- Administrative Zugriffe auf Speichersysteme erfolgen ausschließlich über ein separates Administrationsnetz.
- Das Administrationsnetz ist durch Firewall, Anti-Viren-Software und gegebenenfalls einem IDS abgesichert.
- Zur Administration werden nur gesicherte Verbindungen (z. B. über https, ssh) genutzt.
- Der Zugriff auf die Speichersysteme und ihre Daten ist ausreichend geschützt und vom restlichen Organisationsnetz geeignet abgetrennt.
- Die Daten werden verschlüsselt transportiert bzw. gespeichert, wenn dies aufgrund ihres Schutzbedarfs erforderlich ist.
- Das Logging ist so eingestellt, dass Fehlersituationen und Missbrauchsversuche protokolliert werden. Die Protokolldateien werden regelmäßig kontrolliert.
- Grundkonfiguration und folgende relevante Änderungen der Konfiguration sind schriftlich dokumentiert. Ein Netzplan der Topologie der Speichersysteme und ihrer Verbindungen zum LAN ist vorhanden und aktuell. Diese Dokumentation ist auch im Notfall verfügbar.
- Nach Änderungen werden sicherheitsrelevante Einstellungen des Speichersystems erneut überprüft.

- Der störungsfreie Ablauf von Datensicherungen und die Brauchbarkeit von Sicherungsmedien werden regelmäßig kontrolliert.

Ergänzende Kontrollfragen:

- Findet eine regelmäßige Überprüfung der Speichersysteme statt?
- Sind die Vorgaben der Institution den Auditoren bekannt?
- Werden regelmäßig Sicherheitsberichte für die Speichersysteme erstellt?

M 2.361 Deinstallation von Speichersystemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Werden ein Speichersystem oder einzelne Festplatten aus einem Speichersystem nicht mehr benötigt, so ist zunächst sicherzustellen, dass alle Daten, die auf diesem System gespeichert werden, in geeigneter Weise auf andere Systeme übertragen werden.

Anschließend ist sicherzustellen, dass alle Nutzdaten und Konfigurationsdaten sicher gelöscht werden.

Austausch einzelner Datenträger

Sind Festplatten, auch einzelne, defekt und müssen deshalb ausgetauscht werden, ist sicherzustellen, dass die ausgetauschten Festplatten durch Externe wie z.B. durch den Hersteller so behandelt werden, dass die Daten nicht reproduziert werden können. Auch wenn Platten vom Speichersystem als defekt gemeldet werden, muss sichergestellt werden, dass die Daten auf diesem Medium nicht an Dritte gelangen können.

Wenn hoher oder sehr hoher Schutzbedarf der Daten festgestellt wurde, sollte mit dem Hersteller oder Händler vereinbart werden, dass die betreffenden Platten physisch vernichtet werden. Ein Nachweis des Herstellers oder des Lieferanten ist gegenüber der Institution zu führen.

Festplatten löschen

Wenn intakte Festplatten ausgetauscht werden, die gegebenenfalls weiterverwendet werden können oder sollen, müssen die darauf gespeicherten Daten so gelöscht werden, dass ihr Inhalt nicht mehr reproduziert werden kann (siehe auch M 2.167 *Sicheres Löschen von Datenträgern*).

Für SAN- und NAS-Festplatten in komplexen Speichersystemen sind spezielle Löschprogramme des Herstellers erforderlich. Das Löschen kann dann durch das mit der Wartung beauftragte Unternehmen durchgeführt werden. Dazu muss eine vertragliche Vereinbarung mit einer entsprechenden Verpflichtung des Dienstleisters vorgenommen werden. Auch hierzu ist gegenüber der Institution ein Nachweis zu führen.

Abbau eines Speichersystems

Wenn ein Speichersystem außer Betrieb genommen werden soll, ist zunächst ein Vorgehen zur Migration der Daten zu entwerfen. Es muss sichergestellt sein, dass alle Daten auf dem Speichersystem in geeigneter Form auf andere Speichersysteme überführt werden.

In geeigneter Form heißt, dass alle Anforderungen, die sich aus der Tätigkeit der Institution ergeben, aber auch gesetzliche Anforderungen zu Aufbewahrungsfristen und dergleichen, erfüllt werden.

Es empfiehlt sich, eine Transitionsphase einzuplanen, während der die auf das neue Speichersystem übertragenen Daten im Nutzbetrieb verwendet werden, das alte Speichersystem aber noch derart zugreifbar ist, dass spät erkannte Probleme noch gelöst werden können.

Erst wenn die Transitionsphase als abgeschlossen erklärt wird, können die Nutzdaten gelöscht werden. Dazu sollte mit dem Hersteller bzw. Lieferanten ein effizientes, an den Schutzbedarf der Daten angepasstes Verfahren, ausgewählt werden. Im Zweifel ist für alle Platten des Speichersystems das Verfahren wie bei Austausch einzelner Platten zu wählen.

Verwaltungsinformationen entfernen

Die IP-Adressen bei NAS-Systemen bzw. LUN und ähnliche Angaben bei SAN-Komponenten müssen aus der Konfiguration entfernt werden. Ebenso ist sicherzustellen, dass sonstige Verwaltungsinformationen zuverlässig entfernt werden. Dazu gehören beispielsweise Informationen, die z. B. von einem Webserver, der als Administrationswerkzeug auf dem System läuft, gespeichert werden.

Lizenzschlüsselverwaltung

Es muss geprüft werden, ob Software-Lizenzen (z. B. für Anti-Viren-Software) nicht mehr benötigt werden und daher abbestellt werden können.

Dokumentation

Eine Abschlussdokumentation über die Datenmigration und die Datenlöschung ist anzulegen.

Die Dokumentation zur Notfallplanung ist zu kontrollieren. Auch funktionale Abhängigkeiten in Planungen zum Wiederanlauf nach Störungen müssen an die neue Konfiguration angepasst werden. In der Notfall-Dokumentation und der Betriebsdokumentation dürfen keine Verweise mehr auf das deinstallierte Speichersystem Bezug nehmen.

Ergänzende Kontrollfragen:

- Werden sensitive Daten auf frei werdenden Festplatten vollständig gelöscht?
- Trägt das Löschverfahren dem Schutzbedarf der gespeicherten Informationen Rechnung?
- Werden Verweise auf das deinstallierte System aus allen relevanten Dokumenten entfernt?

M 2.362 Auswahl eines geeigneten Speichersystems

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Um zu einer fundierten Entscheidung über die im jeweiligen Anwendungsfall angemessene Speichertechnik zu kommen, sind die technischen Grundlagen der NAS- und SAN-Technologien detailliert zu beleuchten und deren Auswirkungen auf den möglichen Einsatz in der Institution zu prüfen. Die Entscheidungsgrundlagen müssen dabei dokumentiert werden.

Network Attached Storage

NAS-Systeme sind spezielle Server, die Speicherplatz als einsatzbereites Dateisystem zur Verfügung stellen. Als Dateisystem werden hierfür meistens Windows (SMB/CIFS) oder Unix (NFS) zur Auswahl gestellt. NAS-Systeme sind sehr einfach in eine bestehende Netz-Infrastruktur zu integrieren. Sie können wie Clients oder Server an das Netz der Institution angeschlossen werden. Entsprechend sind NAS-Systeme oft als "Appliance" ausgeführt. Sie werden betriebsfertig ausgeliefert und können nach einigen elementaren Eingaben z. B. der Netzeinstellungen in Betrieb genommen werden. Basissoftware eines NAS-Systems ist üblicherweise eine für diesen Einsatzfall minimierte und optimierte Version eines Standard-Betriebssystems (häufig Unix oder Linux, gegebenenfalls auch Windows).

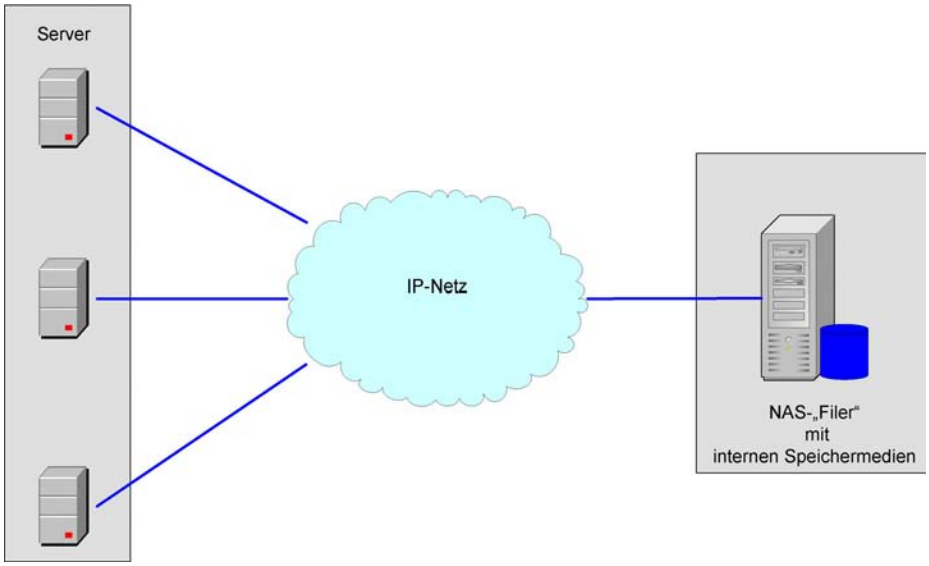


Abbildung: NAS - Network Attached Storage

Diese einfache Anbindung ist gleichzeitig ein Nachteil von NAS, da die Network Attached Storage-Systeme über Ethernet Technik mit den Servern beziehungsweise mit den Clients verbunden sind. Die darunter liegenden TCP/IP-Protokolle haben einen relativ geringen Durchsatz und verwenden dabei einen relativ großen Protokoll-Overhead. So sind sie im Grunde nicht

für den schnellen Zugriff auf Massenspeicher ausgelegt. Der Einsatz von NAS-Systemen kann eine hohe Belastung des LANs zur Folge haben. In vielen Anwendungsfällen ist jedoch festzustellen, dass eine Gigabit-Ethernet-Anbindung im Realbetrieb hinreichend schnell ist und durch eine geeignete Architektur des LANs Engpässe de facto nicht zu beobachten sind.

Durch die Verwendung von Standardnetzen und Standardprotokollen besitzen NAS-Systeme die gleichen Schwachstellen, die auch Unix oder Windows Server betreffen.

Weniger geeignet sind Standard-NAS-Lösungen als Speichersysteme für Anwendungen, die nicht dateiorientiert sind. Darunter fallen alle größeren Datenbanken und zum Beispiel auch Microsoft Exchange-Server. Wenn eine solche Anwendung auf einem NAS-System betrieben werden soll, ist zu überprüfen, ob Produkte am Markt verfügbar sind, die spezifisch für den Betrieb des Produktes und das Einsatzszenario optimiert sind.

Ein NAS-System kann oft eine Reihe von Servern ersetzen. Obwohl die reinen Hardwarekosten meistens deutlich höher sind als der Ausbau der einzelnen Server mit mehr und/oder größeren Festplatten, kann es eine erhebliche Verbesserung der Verfügbarkeit bringen. Deutliche Vorteile liegen in der oft vorhandenen Möglichkeit durch Konfiguration des Geräts oder Hardwareerweiterungen im laufenden Betrieb Kapazitätsanforderungen ohne Stillstand zu erfüllen. Verbesserungen sind auch bei der Datensicherung zu erzielen. Mit direkt angeschlossenen Datensicherungsgeräten (Bandlaufwerken, "JukeBoxen" zur Archivierung) ausgestattet, kann eine Vereinfachung, Beschleunigung und Stabilisierung bei der Sicherung von Datenbeständen, die über gewachsene Serverlandschaften verteilt sind, erzielt werden.

Ein Nachteil von einfachen NAS-Systemen ist, dass ein Ausfall oft weiterreichende Folgen hat als der Ausfall eines einzelnen Servers und dass ein Ausfall nicht einfach durch ein in der Institution kurzfristig verfügbares Ersatzsystem kompensiert werden kann.

Storage Area Networks

SANs bestehen aus Plattensubsystemen, Datensicherungssystemen und einer eigenen Netz-Infrastruktur. Plattensubsysteme fassen intern eine Menge von Festplatten zusammen. Hier wird unterschieden, ob diese Zusammenfassung lediglich durch ein gemeinsames Gehäuse und gemeinsame Stromversorgung geschieht (JBOD = Just a Bunch of Disks) oder ob ein spezielles Schaltgerät, der so genannte RAID-Controller mit Hilfe der RAID-Technik (RAID = Redundant Array of Independent Discs) die physikalischen Festplatten zu virtuellen Festplatten zusammenfasst. Darüber hinaus gibt es intelligente RAID-Controller, die weitere Dienste zur Verfügung stellen können.

Durch die Zusammenfassung mehrerer physikalischer Festplatten zu virtuellen Einheiten, auch "Speichervirtualisierung durch RAID" genannt, kann durch ein geschicktes Kombinieren von physikalischen Festplatten die Ausfallsicherheit oder die Performance des Gesamtsystems oder beides erhöht werden. Der RAID-Controller zeigt nach außen nur die zusammengefassten Festplatten (virtuelle Festplatte oder logisches "Volume") und verteilt die Daten, die er auf einer solchen Festplatte schreiben soll, auf die einzelnen physikalischen Festplatten.

Diese Funktionalität kann auch im Server mit Hilfe einer speziellen Applikation, des "Volume Managers", implementiert werden, wobei dann der Server stärker belastet wird.

Es existieren verschiedene Systeme, nach denen die Datenverteilung geregelt wird, die so genannten RAID-Levels. Wenn das RAID-Level die Speicherung von redundanten Informationen unterstützt, dann bleiben die gespeicherten Informationen selbst nach dem Ausfall einer Festplatte intakt und können rekonstruiert werden. Oft können einzelne Festplatten des Plattensubsystems im laufenden Betrieb ausgetauscht werden ("hot swap").

Plattensubsysteme bieten die Möglichkeit, alle Teilkomponenten redundant auszulegen und können somit zur Erhöhung der Verfügbarkeit eingesetzt werden. Ein weiterer Vorteil ist, dass durch passende Konfigurationsmechanismen der einer Anwendung zugeordnete Speicherplatz an ihren Platzbedarf angepasst werden kann.

Ein Plattensubsystem stellt lediglich Speicher für die Anwendungen zur Verfügung. Selbst bei redundanter Speicherung der Daten ist eine zusätzliche Datensicherung notwendig, da z. B. logische Defekte beim Datenbestand durch Redundanz im Speichersystem nicht korrigiert werden können. Als Systeme zur Datensicherung sind Bandlaufwerke, optische Medien, aber auch wiederum spezielle Festplattensysteme nutzbar. Auch diese Geräte werden direkt in das Speichernetz integriert.

SANs verwenden eine eigene Netz-Hardware und eigene für den Anwendungsfall geeignete schnelle Netzprotokolle. Meistens sind Glasfaserkabel im Einsatz (Systembezeichnung: Fibre Channel, FC). Ein einfaches Storage Area Network besteht aus einem Fibre Channel Switch oder Director (größere Switche, die mit mehr Funktionalitäten ausgestattet sind, werden oft als Director bezeichnet), einem oder mehreren Plattensubsystemen und den Servern, die über so genannte Host Bus Adapter, kurz HBA, mit dem Fibre Channel Switch verbunden werden.

Fibre Channel Netze verwenden ein spezielles, an die Anforderung von Massenspeichernutzung angepasstes Protokoll, das hohe Übertragungsraten ermöglicht und deshalb für Speichersysteme sehr geeignet ist. Ebenfalls möglich ist der Einsatz von iSCSI Geräten. iSCSI "verpackt" Speicherprotokolle, also Steuerbefehle für Massenspeicher und zugehörige Daten, in IP-Pakete. iSCSI wird eingesetzt, um über eine virtuelle Ende-zu-Ende-Verbindung den Zugriff von Servern mittels iSCSI Host-Bus-Adapter auf das Speichernetz zu ermöglichen, ohne dass eigene Speichernetze betrieben werden müssen. Vorhandene Netzkomponenten (LAN-Switch) können genutzt werden, es muss keine neue oder von der vorhandenen Netztechnik verschiedene Hardware für die Verbindungen zwischen Servern und Speichergeräten eingesetzt werden. Der Begriff SAN wird im Folgenden für beide Technologien verwendet. Wenn eine Unterscheidung notwendig ist wird "Fibre Channel SAN" oder FC-SAN und entsprechend iSCSI-SAN oder IP-SAN verwendet.

Ein großer Vorteil von SANs ist ihre Desaster-Toleranz. Das Konzept des Multi-Pathing, das im SAN konsequent verfolgt wird, spielt dabei eine wesentliche Rolle: Falls es einem Server möglich ist über mehrere Host Bus Adapter und über unterschiedliche Netzverbindungen ein Plattensubsystem zu erreichen, so kann der Datentransfer zwischen beiden Systemen auf mehrere Datenwege verteilt werden. Durch den Einsatz mehrerer Host Bus Adapter in den Servern und die Präsentation der virtuellen Festplatten auf mehreren Schnittstellen eines Plattensubsystems lassen sich somit die mögliche Übertragungsgeschwindigkeit und Verfügbarkeit des Speichersystems effektiv steigern. Wenn zwei oder mehr Host Bus Adapter in einem Server genutzt werden, so wird bei Ausfall eines Adapters die Last auf den oder die verbleibenden HBA verlagern. Dieses für Betriebssystem und Anwendungen transparente "Failover" verbessert somit die Verfügbarkeit des Servers. Entsprechend kann durch eine redundante Auslegung aller Teilkomponenten eines SANs eine sehr hohe Ausfallsicherheit erreicht werden. Die Maßnahme M 2.354 *Einsatz einer hochverfügbaren SAN-Konfiguration* beschreibt dieses Thema ausführlicher.

So wäre es in einem kleinen Storage Area Network denkbar, dass sich an zwei möglichst weit auseinander liegenden Orten auf dem Betriebsgelände jeweils ein baugleiches Plattensubsystem befindet, jedes dieser Plattensubsysteme ist mit einem von zwei auch wieder getrennt installierten Switchen verbunden. Um eine redundante Verbindung zum SAN zu gewährleisten, verfügen die Server zumindest über zwei Host Bus Adapter, so dass jeder Host Bus Adapter mit einem der beiden SAN-Switche verbunden ist.

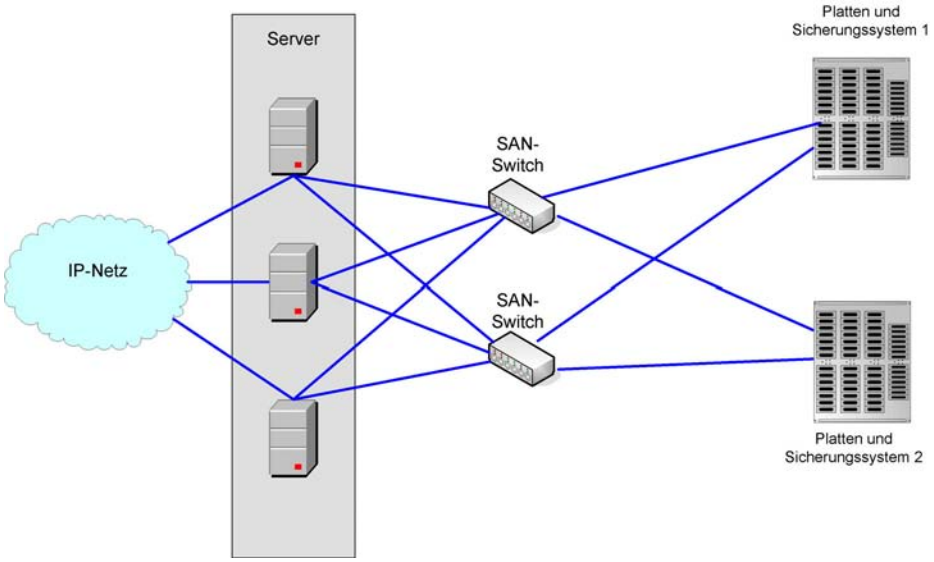


Abbildung: SAN - Storage Area Network

Somit wäre ein Ausfall einzelner Leitungen, eines Switches oder sogar eines Plattensubsystems ohne Beeinträchtigung der Gesamtsystemleistung denkbar.

Beim Design eines SANs ist es leicht möglich, Redundanzen zu schaffen, so dass ein Ausfall einzelner Komponenten wie Kommunikationsleitungen, Switches oder sogar eines Plattensubsystems keine Beeinträchtigung der Gesamtsystemleistung bewirkt.

Bei höchsten Anforderungen an die Verfügbarkeit kann dieser Ausbau so erweitert werden, dass in zwei oder mehr räumlich weit auseinander liegenden (bis zu 100 km) und technisch autarken Rechenzentren jeweils in allen Komponenten redundante SANs aufgebaut werden. So kann im Extremfall der Ausfall eines kompletten Rechenzentrums ohne Betriebsunterbrechung oder Kapazitätsverlust für die Anwender kompensiert werden.

Weitere Redundanz lässt sich durch "Cluster"-Server erreichen, die eine logische Maschine auf zwei oder mehr physische Server verteilen. Dabei wird eine Anwendung auf zwei oder mehr Servern installiert. Diese Server arbeiten mit denselben Anwendungsdaten. Falls ein Server eine Störung erleidet, übernimmt der zweite Server automatisch die Arbeit des ausgefallenen Kollegen.

Erkauft werden die positiven Eigenschaften einer SAN-Lösung durch Preis und Komplexität. Die gleiche Menge Speicher ist in der Realisierung durch ein SAN um ein Vielfaches teuerer als in der Ausführung als Direct Attached Storage.

Zudem ist auch die Planung und der Aufbau eines SANs so komplex, dass es für die Institution sehr ratsam ist, externe Unterstützung hinzuzuziehen.

Zusammenfassung

Kurz dargestellt ist NAS ein Speichersystem mit Datei-basiertem Zugriff, SAN ein Speichersystem mit Block-basiertem Zugriff. SAN setzt also "tiefer" an und bietet alle technischen Möglichkeiten, die für die Datenspeicherung angeboten werden. NAS ist eine Erweiterung der Serverlandschaft der Institution.

Kombinierte Geräte

Mittlerweile werden auch Speichersysteme angeboten, die eine Mischform zwischen NAS und SAN darstellen. Der interne Aufbau solcher Systeme erfüllt alle Kriterien eines SANs. Nach außen können sie jedoch als NAS-System betrieben werden. Durch Aufrüstung und entsprechende Konfiguration können solche Speichersysteme auch im Mischbetrieb genutzt werden. So kann sich ein Gerät sowohl für einige Anwendungen per Ethernet-Anschluss als "Filer" präsentieren, also als intelligenter Netzknoten zur Bereitstellung von Datei-Diensten, zugleich aber für andere Server als "purer Speicher" per Fibre Channel oder iSCSI dienen.

Ergänzende Kontrollfragen:

- Sind bei der Planung der Speichersysteme und Speichernetze die Möglichkeiten und Grenzen der verschiedenen Arten von Speichersystemen für die Verantwortlichen der Institution transparent gemacht worden?
- Ist die Entscheidungsgrundlage für die Auswahl eines geeigneten Speichersystems dokumentiert worden?

M 2.363 Schutz gegen SQL-Injection

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator, Anwendungsentwickler

Um die Ausnutzung von SQL-Injections (siehe G 5.131 *SQL-Injection*) zu verhindern oder zumindest zu erschweren, sind eine Reihe von Maßnahmen zu ergreifen. Diese erstrecken sich über alle Komponenten einer Anwendung, von der Applikation selbst über den Server bis hin zum Datenbank-Managementsystem (DBMS).

Maßnahmen bei der Programmierung von Applikationen

Eine der wichtigsten Maßnahmen zur Vermeidung von SQL-Injection ist die sorgfältige Überprüfung und Filterung von Eingaben und Parametern durch die Applikation. Überprüft werden sollte, ob die übergebenen Daten dem erwarteten Datentyp entsprechen. Wird z. B. ein numerischer Parameter erwartet, kann man diesen in PHP ("PHP: Hypertext Preprocessor") mit der Funktion *is_numeric()* prüfen. Die Filterung hingegen muss dafür sorgen, dass Sonderzeichen wie das Quote-Zeichen (‘), das Semikolon (;) und doppelte Bindestriche (--) ignoriert werden.

Sicherer ist der Einsatz von *Stored Procedures* beziehungsweise *Prepared SQL-Statements* (Java = PreparedStatement-Klasse, PHP-MySQL = mysql_real_escape_string()-Funktion). Diese werden von vielen Datenbank-Managementsystemen (DBMS) angeboten und sind ursprünglich dazu gedacht, häufiger auftretende Abfragen zu optimieren. Der Vorteil dieser parametrisierten Statements ist, dass Parameter nicht mehr direkt in ein SQL-Statement eingebunden werden. Vielmehr werden diese getrennt vom SQL-Statement separat an die Datenbank übergeben. Das Zusammenführen von Statement und Parametern erfolgt durch das DBMS selbst, wobei die oben genannten Sonderzeichen automatisch maskiert werden.

Um potentiellen Angreifern keine Anhaltspunkte für Angriffe zu liefern, sollte besonderes Augenmerk darauf gelegt werden, dass Applikationen möglichst keine Fehlermeldungen nach außen ausgeben, die Rückschlüsse auf das verwendete System oder auf die Struktur der dahinterliegenden Datenbank zulassen.

Serverseitige Maßnahmen

Die wichtigste Sicherheitsmaßname auf dem Server ist das Härten des Betriebssystems. Um so wenig Angriffspunkte wie möglich zu bieten, werden dabei Maßnahmen ergriffen wie:

- das Deaktivieren nicht benötigter Dienste,
- das Löschen nicht benötigter Benutzerkonten,
- das Einspielen relevanter Patches und
- das Löschen aller für die Funktion des Servers unnötigen Bestandteile.

Darüber hinaus sollte der Einsatz eines Application-Level-Gateways (ALG) (siehe M 5.117 *Integration eines Datenbank-Servers in ein Sicherheitsgateway*) erwogen werden. ALGs können auf Applikationsebene die Daten überwachen, die zwischen Webbrowser und Anwendung ausgetauscht werden, und verhindern, dass schädliche Daten den Server erreichen.

Eine weitere zusätzliche Sicherheitsmaßnahme stellt der Einsatz von Intrusion-Detection-Systemen (IDS) und Intrusion-Prevention-Systemen (IPS) dar. IDS analysieren den über ein Netz übertragenen Datenverkehr und erkennen potentiell gefährliche Daten. Die dazu eingesetzten Analysetechniken unterteilen sich in *Misuse* und *Anomaly Detection*. Die Misuse Detection versucht, bereits bekannte Angriffsmuster zu erkennen. Die Anomaly Detection verfolgt den Ansatz, die zulässigen Verhaltensmuster zu lernen und Abweichungen davon als Angriff zu identifizieren. Während ein IDS in der Lage ist, Angriffe zu erkennen und Warnungen auszugeben, ist ein IPS in der Lage, entsprechende Reaktionen auszuführen. Die Reaktion kann beispielsweise darin bestehen, die Verbindung zu blockieren, Daten zu verwerfen oder zu ändern.

Bei erhöhten Sicherheitsanforderungen sollte geprüft werden, ob der Einsatz von IDS beziehungsweise IPS zweckmäßig ist.

Datenbankseitige Maßnahmen

Ebenso wie beim Betriebssystem sollte auch eine Härtung der Datenbank erfolgen. Im Falle der Datenbank bedeutet dies z. B.:

- das Entfernen nicht benötigter Stored Procedures,
- das Deaktivieren nicht benötigter Dienste,
- das Löschen nicht benötigter Benutzerkonten und Default Accounts und
- das Einspielen relevanter Patches.

In diesem Zusammenhang sollte auch ein speziell für den Datenbankzugriff vorgesehener Account angelegt werden, der mit möglichst eingeschränkten Zugriffsrechten auskommen sollte.

Darüber hinaus sollten sensitive Daten, wie z. B. Passwörter, in der Datenbank soweit möglich nur verschlüsselt gespeichert werden.

Von vielen Herstellern werden mittlerweile sogenannte Schwachstellen-Scanner angeboten, die sowohl Applikationen als auch Datenbanken auf Sicherheitslücken, wie beispielsweise mögliche SQL-Injections, überprüfen können.

Beispiel für prinzipielles Vorgehen zur Erstellung von sicherem Code bei Verwendung von PHP und MySQL:

In PHP verhindert die Funktion mysql_real_escape_sting() die Übergabe von Sonderzeichen an eine MySQL-Datenbank. Die Funktion maskiert die in dem übergebenen String enthaltenen Sonderzeichen wie z. B. Quotes und verhindert so SQL-Injections.

Anstatt der folgenden Syntax:

```
$query = "SELECT * FROM users
WHERE username=
‘" . $_POST[‘username’] . "‘
AND password=
‘" . $_POST[‘password’] . "‘";
```

sollte also diese Syntax verwendet werden:

```
$query = "SELECT * FROM users
WHERE username=
‘" . mysql_real_escape_string($_POST[‘username’]) . "‘
AND password=
‘" . mysql_real_escape_string($_POST[‘password’]) . "‘";
```

Beispiel für sicheren Code bei Verwendung von ASP mit ADO und SQL-Server:

Die Verwendung eines prepared Statements für das obige Beispiel sieht in diesem Fall folgendermaßen aus:

```
$query = "SELECT * FROM users WHERE username=?
AND password=?"
Set cmd = Server.CreateObject("ADODB.Command")
cmd.CommandText = query
cmd.CommandType = adCmdText
Set param = cmd.CreateParameter("",adVarChar, adParamInput,
nMaxUsernameLength, strUsername)
cmd.Parameters.Append
Set param = cmd.CreateParameter("",adVarChar, adParamInput,
nMaxUsernameLength, strPassword)
cmd.Parameters.Append
Set rs = cmd.Execute()
```

Hierbei ist zu beachten, dass die oben aufgeführten Code-Beispiele nur den grundsätzlichen Ansatz zur Vermeidung von SQL-Injection veranschaulichen sollen.

M 2.364 Planung der Administration für Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Organisatorische Maßnahmen

Vor der Einführung eines Windows Server 2003 sind umfangreiche Planungen durchzuführen, damit eine geregelte und auch sichere Einführung sowie anschließend ein sicherer Betrieb ermöglicht werden. Aus der Beschreibung des Einsatzszenarios und der Definition des Einsatzzwecks ergeben sich Anforderungen an die Planung der Administration des Windows Server 2003. Administrative Änderungen, die im laufenden Betrieb durchgeführt werden, können sicherheitsrelevante Nebeneffekte hervorrufen. Die Planung der Administration muss anhand der Vorgaben der Sicherheitsrichtlinie erfolgen (siehe M 2.316 *Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server*). Darin sollte unter anderem darauf hingewiesen werden, dass die Verwendung des Servers in der Rolle einer Arbeitsstation eines Benutzers zu unterlassen ist.

Zutritt und Zugang

Die Administration kann vor Ort mit dem Zugang zur Konsole des Servers, von einem anderen Computer innerhalb des LAN oder von außerhalb z. B. über VPN erfolgen. Bei der Planung der Aufgaben und Berechtigungen der Administratoren sind Regelungen der Zutrittsberechtigung zu treffen (siehe M 2.6 *Vergabe von Zutrittsberechtigungen*). Dabei ist die vorher erarbeitete Funktionstrennung (siehe M 2.5 *Aufgabenverteilung und Funktionstrennung*) zu beachten. Unnötige Zutrittsrechte zum Server sind zu vermeiden.

Typische administrative Aufgaben

Aufgabenliste

- Ereignisanzeige überwachen
- Software installieren, warten und deinstallieren
- Windows Komponenten hinzufügen/ändern/entfernen
- Aktualisierungen (Windows Update)
- Auslastung kontrollieren
- Funktion der Hardware überwachen
- Funktion von Applikationen und Diensten überwachen
- Dateisystem warten
- Rechte entsprechend neuer Anforderungen anpassen
- Benutzer/Gruppenverwaltung, neue Benutzer/Gruppen anlegen, verschieben oder löschen
- Anpassungen am OU Design vornehmen
- Änderungen oder Anpassungen am Active Directory vornehmen
- Daten sichern
- Netzwerkkonnektivität prüfen
- Virenschutz prüfen und warten
- Registrierdatenbank warten
- Datum/Uhrzeit/Zeitzonen administrieren

Eingebaute Standardgruppen für die Administration

Lokale Sicherheitsgruppen

Die Administration von Windows Server 2003 erfordert weitreichende Berechtigungen und somit ein geeignetes Berechtigungskonzept. Folgende lokale Sicherheitsgruppen für die Administration sind nach einer Standardinstallation vorhanden:

Systemdefinierte Sicherheitsgruppe	**Administratives Zugriffsniveau**	**Bedeutung für die Administration**
Administratoren	Voll	Vollzugriff auf alle Bereiche, sehr sicherheitskritisch
Hauptbenutzer	Hoch	Umfangreicher Zugriff auf Systemeinstellungen, mit einigen Einschränkungen: Hauptbenutzer können z. B. nicht den Besitz von Dateien übernehmen, Gerätetreiber laden oder entladen, Sicherheits- und protokolle verwalten, Dienste installieren
Sicherungs-Operatoren	Hoch	Lese- und Schreibzugriff auf alle Dateien
Remoteunterstützungsanbieter	Hoch	nur in Active-Directory-Umgebung vorhanden, dürfen von Ferne an einer Konsolensitzung teilnehmen ("Shared Desktop"), erhalten somit die Rechte des angemeldeten Benutzers. Für Fernadministration ungeeignet, besser geeignet ist *Remotedesktop*
Hilfedienstgruppe	Kein bis hoch	mit Hilfe dieser Gruppe können Administratoren gemeinsame Rechte für alle Supportanwendungen festlegen, kann hohes Sicherheitsrisiko verursachen
Netzwerkkonfigurations-Operatoren	Mittel	Eigenschaften von Verbindungen im Ordner *Netzwerkverbindungen* administrieren

Druck-Operatoren	Mittel	Administration von Druckern und Druckerwarteschlangen
Leistungsprotokollbenutzer	Gering	Administration der Konsole *Leistung* (perfmon.exe)
Distributed COM-Benutzer	Gering	Administration der Konsole *Komponentendienste*
Systemmonitorbenutzer	Gering	lesender Zugriff auf Leistungszähler und -protokolle
Benutzer	Sehr gering	erlaubt Anmeldung an Mitgliedsservern und alleinstehenden Servern
Remotedesktopbenutzer	Kein	Gruppe zur Steuerung der Remote-Desktop-Einwahlmöglichkeit
TelnetClients	Kein	Gruppe zur Steuerung der Telnet-Einwahlmöglichkeit
Replikations-Operator	Kein	vom Betriebssystem verwendete Gruppe, darf nicht für Benutzer verwendet werden
Gäste	Kein	Steuerung des Ressourcenzugriffs für Benutzer ohne Anmeldung, darf nicht für Benutzer verwendet werden

Hinweis:

Die Standardgruppen auf einem Domänencontroller unterscheiden sich zum Teil von den hier genannten.

Prinzip der minimal nötigen Berechtigungskombination

Für die Aufgabenerfüllung der Administration gibt es im Betriebssystem Windows Server 2003 Sicherheitsgruppen, z. B. die Gruppe *Administratoren*, die vollen administrativen Zugriff auf alle Bereiche des Servers haben und somit die Sicherheit des Windows Server 2003 erheblich beeinflussen können. Für definierte Einsatzzwecke von Windows Server 2003, z. B. *Dateiserver*, sind Sicherheitsgruppen mit nicht vollen administrativen Rechten einzuplanen. So können administrative Aufgaben, z. B. das Erstellen einer Datensicherung unter Verwendung der Gruppe *Sicherungsoperatoren*, sowie die damit einhergehenden Gefährdungen auf ihre Teilbereiche im Windows Server 2003 beschränkt werden. Es ist immer das Prinzip der minimal nötigen Berechtigungskombination einzuhalten. Z. B. sollte betrachtet werden, ob es ausreicht, die Administrationsaufgaben mit den geringeren Rechten der Sicherheitsgruppe *Hauptbenutzer* durchzuführen (siehe M 5.10 *Restriktive Rechtevergabe*). Bei einem bestehenden Netz ist zu berücksichtigen, ob für die festgelegten Aufgaben mit den vorhandenen Sicherheitsgruppen aus dem Active Directory oder dem lokalen Server gearbeitet werden kann (zu berücksichtigen ist hierbei G 2.115 *Ungeeigneter Umgang mit den Standard-Sicherheitsgruppen von Windows Server 2003*). Die Installation von

zusätzlichen Komponenten erweitert die Auswahl von Standardgruppen, die für die Administration in Frage kommen. Ein Beispiel hierfür ist die Sicherheitsgruppe *Terminalserverbenutzer* bei installierten Terminalserverdiensten oder *DHCP-Administratoren* bei installiertem DHCP-Dienst. Die Festlegung auf vorhandene Sicherheitsgruppen ist jedoch nicht immer geeignet, da deren Rechte nicht administriert werden können. Daher ist eine für die festgelegten Administrationsaufgaben angepasste Sicherheitsgruppe zu empfehlen.

Um Fehler zu vermeiden, ist genau festzulegen, für welche administrativen Aufgaben die Berechtigungen der Gruppe *Administratoren* wirklich erforderlich sind. Zum Beispiel können Änderungen des Vollzugriffs im Dateisystem standardmäßig nur durch die Gruppe *Administratoren* erfolgen (für weitere Informationen siehe M 4.149 *Datei- und Freigabeberechtigungen unter Windows 2000/XP*), andererseits hat die Gruppe *Administratoren* immer Zugriff via Remotedesktop auf jedem Server, unabhängig von der Gruppe *Remotedesktopbenutzer*. In größeren Umgebungen sollten immer die Gruppen mit dem niedrigsten administrativen Zugriffsniveau bevorzugt werden. Bei Bedarf können Berechtigungen um Gruppen mit höherem Zugriffsniveau ergänzt werden.

Selbstdefinierte Gruppen

Auswirkungen von selbstdefinierten Gruppen beachten

Weiterhin können selbstdefinierte Sicherheitsgruppen entworfen werden, welche die Berechtigungen für eine definierte administrative Aufgabe enthalten. Eigene Gruppen können entsprechend ihres Zugriffsniveaus in der oben genannten Auflistung ergänzt werden.

Durch die Planung muss vermieden werden, dass Programme ungewollt mit zu weitreichenden administrativen Berechtigungen aufgerufen werden, weil die Programme dadurch Zugriff auf kritische Bereiche des Servers erhalten und die Sicherheit des Servers gefährden können.

Benutzerkonten für die Administration

Abgrenzung zwischen Nutzung und Administration

Bei der Betrachtung der Arbeitsaufgaben, die eine Person mit einem autorisierten Benutzerkonto in einer IT-Umgebung durchführt, muss für Administratoren eine grundlegende Abgrenzung gefunden werden:

- Welche Aufgaben betreffen die Nutzung des IT-Systems?
- Welche Aufgaben betreffen die Administration des IT-Systems?

Zwei separate Konten

Es ist sehr zu empfehlen, diese Betrachtungsweise in zwei separaten Konten für eine Person abzubilden. Da die eingebauten Standardgruppen von Windows Server 2003 keine spezielle Nutzung als Administrator bzw. Benutzer erzwingen, sollte ein normales Benutzerkonto für das tägliche Arbeiten und ein administratives Konto für administrative Aufgaben vorhanden sein und dementsprechend genutzt werden.

Ansätze für möglichst geringe Berechtigungen

Es ist wichtig, einen definierten und dokumentierten Prozess für die Einrichtung und Entfernung von Benutzerkonten zu implementieren. Dies ist besonders wichtig für administrative Konten.

Das Ziel ist immer, die Anmeldung einer Benutzersitzung auf einem Windows-Server-2003- oder Windows-Verwaltungscomputer mit so geringen Berechtigungen wie möglich durchzuführen, am besten mit normalen Benutzerrechten. Mehrere grundlegende Ansätze sind hierfür denkbar:

- **Sekundäre Anmeldung auf dem Server**

  Sekundäre Anmeldung auf dem Server

  Auf dem zu administrierenden Server wird eine normale Benutzersitzung mit eingeschränkten Rechten angemeldet, Administrationswerkzeuge werden mit Hilfe der sekundären Anmeldung (*Ausführen als...* oder *runas*) mit dem entsprechenden administrativen Benutzerkonto auf dem Server ausgeführt. In diesem Fall ist zu überlegen, ob normalen Benutzern die lokale Anmeldung auf einem Server erlaubt wird (Standardeinstellung) oder ob hierfür eine separate Sicherheitsgruppe entworfen wird.

- **Einrichten einer Verwaltungsstation**

  Einrichten einer Verwaltungsstation

  Für den Betrieb einer Verwaltungsstation ist *Active Directory* zu empfehlen (M 2.229 *Planung des Active Directory*). Die Anmeldung an der Verwaltungsstation erfolgt mit einem Benutzerkonto, das auf diesem Computer nur geringe Berechtigungen besitzt (z. B. Benutzer). Von der Verwaltungsstation aus wird auf die zu administrierenden Server mit entsprechenden Werkzeugen (siehe unten) zugegriffen. Entweder hat das Benutzerkonto dort die erforderlichen Berechtigungen, oder der Zugriff erfolgt mit Hilfe der sekundären Anmeldung. Dadurch ist in den meisten Fällen keine komplette Anmeldung mit administrativen Berechtigungen nötig.

- **Lokales Anmelden mit erweiterten Berechtigungen**

  Lokales Anmelden mit erweiterten Berechtigungen

  In diesem Szenario sollte das lokale Anmelden an Servern generell unterbunden und nur für ausgewählte administrative Benutzerkonten freigeschaltet werden. Diese Benutzerkonten sollten genau für die vorgesehene Aufgabe angepasst sein. Weitere Einschränkungen dieser Konten, z. B. Anmeldezeiten, sind zu empfehlen.

Es empfiehlt sich, die jeweiligen Strategien in einer Richtlinie für die Windows Server 2003 Umgebung zu vermerken.

Konfigurationsänderungen

Während des laufenden Betriebs und in Wartungsfenstern

Es muss bei der Planung beachtet werden, dass administrative Änderungen im laufenden Betrieb hinsichtlich Verfügbarkeit und Zuverlässigkeit als kritisch zu betrachten sind (siehe M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen*). Bei der Planung der administrativen Aufgaben muss also unterschieden werden, welche Aufgaben während des laufenden Betriebs und welche Aufgaben nur in speziellen Wartungsfenstern durchgeführt werden können. Dies ist stark von der Konfiguration von Windows Server 2003, den zusätzlichen Serverapplikationen und den Verfügbarkeitsanforderungen abhängig. Konfigurationsänderungen sollten vorzugsweise nur in speziellen Wartungsfenstern durchgeführt werden, da unter Umständen Neustarts des Servers im laufenden Betrieb provoziert werden können.

Administrationswerkzeuge

Ein wichtiger Aspekt ist die Auswahl der geeigneten Administrationswerkzeuge für den jeweiligen Server. Die mitgelieferten Werkzeuge von Windows Server 2003 bieten eine sehr gute Integration in die Sicherheitsmechanismen des Betriebssystems und ein einheitliches Bedienkonzept.

Die zentralen mitgelieferten Komponenten für die Administration sind:

- ***Microsoft Management Console* (MMC)**

  Microsoft Management Console (MMC)

  Fast alle Komponenten sind über ein eigenes MMC-Snap-In zu administrieren. Mit der MMC können Komponenten auf entfernten Servern von einer Verwaltungsstation aus administriert werden. Viele Werkzeuge von Drittherstellern benutzen die MMC als Administrationsoberfläche.

- **Fernadministration per Remotedesktop**

  Fernadministration per Remotedesktop

  Die Verwendung von Remotedesktops kann die Sicherheit des Servers hinsichtlich Integrität und Vertraulichkeit verringern, siehe G 5.132 *Kompromittierung einer RDP-Benutzersitzung unter Windows Server 2003*. Außerdem entstehen erhöhte organisatorische Anforderungen.

- **Konsolen, die *Internet Information Services* (IIS) erfordern**

  Diese werden für die Administration des Anwendungsservers sowie zum Teil für die Zertifizierungsdienste benötigt. Außerdem setzen viele Werkzeuge von Drittherstellern auf Web-basierte Konsolen. Hierbei entstehen zusätzliche Risiken, so dass gegebenenfalls weitere Maßnahmen umzusetzen sind (siehe M 4.282 *Sichere Konfiguration der IIS-Basis-Komponente unter Windows Server 2003*).

- **Kommandozeilenbefehle**

  Kommandozeilenbefehle

  Viele Komponenten von Windows Server 2003 können mit Kommandozeilenbefehlen administriert werden. Sie stellen ein mächtiges Werkzeug dar. Die Syntax der Kommandos ist teilweise kompliziert, so dass ein erhebliches Risiko für falsche Bedienung und Fehlkonfiguration besteht. Die Verwendung sollte sich auf Fälle konzentrieren, bei denen GUI-basierte Werkzeuge nicht im erforderlichen Maß zur Verfügung stehen.

  Einige Einstellungen sind jedoch tatsächlich nur durch entsprechende Kommandozeilenbefehle zu realisieren. Meist ist der konkrete Anwendungsfall explizit dokumentiert, z. B. in Artikeln der *Microsoft Knowledge Base*, in der Windows-Hilfe oder in anderen vom Hersteller online bereitgestellten Dokumenten. Es wird empfohlen, die Gewährleistung und der Umfang der Herstellerunterstützung für den konkreten Anwendungsfall vorab mit dem Hersteller zu klären.

  Die Verwendung von Kommandozeilenwerkzeugen ist geeignet, wenn eine sehr flexible Automation von Vorgängen erforderlich ist, zum Beispiel mit Hilfe von Skripten. Die Skripte müssen vor Verwendung auf einem Testsystem erprobt werden (siehe M 2.367 *Einsatz von Kommandos und Skripten unter Windows Server 2003*).

Bestimmte Konfigurationsroutinen und Administrationsprogramme von Drittherstellern können weitere Konfigurationsänderungen an Windows Server 2003 erfordern, z. B. wenn diese IIS-Komponenten oder das .NET-Framework voraussetzen. Dadurch kann die Sicherheit des Servers beeinträchtigt werden. Bei der Festlegung ihrer Verwendung ist auf ihre Eignung zu achten (siehe B 1.10 *Standardsoftware*).

Die Verwendung von 16-bit-Programmen für Administrationszwecke ist generell zu vermeiden.

- **Fernadministration**

  - **Zugriff aus dem LAN**

Zugriff aus dem LAN

Die mitgelieferten Remote-Werkzeuge bieten innerhalb des LAN einen effizienten Zugriff auf Windows Server 2003. Sofern die IT-Sicherheitsrichtlinie für Windows Server 2003 erfüllt ist, sind für ein normales Sicherheitsniveau keine weiteren Maßnahmen erforderlich. Die Nutzung der im LAN zugelassenen Remote-Werkzeuge, z. B. von Remote-Desktop-Verbindungen, sollten in einer Sicherheitsrichtlinie definiert sein.

  - **Zugriff über Sicherheits-Gateways**

Zugriff über Sicherheits-Gateways

Der Zugriff über Sicherheits-Gateways sollte auf Grundlage der RAS-Sicherheitsrichtlinie (siehe M 2.187 *Festlegen einer RAS-Sicherheitsrichtlinie*) erfolgen. Remote-Werkzeuge können von einem anderen Computer innerhalb des LAN, aber auch von außerhalb, z. B. über das Internet, verwendet werden. Für einen Fernzugriff von außerhalb der durch Sicherheits-Gateways geschützten IT-Umgebung muss der Authentisierungsvorgang und die Datenübertragung verschlüsselt werden. Hierfür ist HTTPS oder VPN zu empfehlen. Weiterhin ist zu beachten, dass der Zugriff von externen Clients auf wenige Computer beschränkt wird. Hierfür müssen jedoch alle beteiligten Komponenten in das Administrationskonzept mit einbezogen werden (z. B. Sicherheits-gateways, VPN-Gateways, Windows-Server-2003-Zertifizierungsdienste).

Im Rahmen der Planung der Fernadministration zu Windows Server 2003 muss auch für den entfernten Zugang eine Sicherheitsrichtlinie festgelegt werden. Die durch die organisationsweiten IT-Sicherheitsrichtlinien geltenden Vorschriften sind dazu entsprechend anzupassen und zu erweitern.

Externe Dienstleister

Separate Sicherheitsgruppen

Die speziellen Anforderungen an Outsourcing (siehe B 1.11 *Outsourcing*) sowie vertragliche Vereinbarungen mit externen Dienstleistern müssen in das Berechtigungskonzept (siehe oben) einfließen. Für externe Dienstleister sollten separate Sicherheitsgruppen entworfen werden, die nur in den notwendigen Bereichen von Windows Server 2003 über Berechtigungen verfügen. Die vorhandenen Standardgruppen sind meist nicht geeignet. Beispielsweise ist zu überlegen, ob für einen reinen Datensicherungsdienstleister die Berechtigungen der Gruppe *Sicherungsoperatoren* schon zu weitreichend sind.

Die Übergabe von Anmeldedaten von administrativen Konten sowie die Durchsetzung von Kennwortrichtlinien gestaltet sich besonders schwierig, wenn die jeweils beauftragte Person des Dienstleisters nicht vor Ort arbeitet (siehe auch G 2.111 *Kompromittierung von Anmeldedaten bei Dienstleisterwechsel*). Kommt außerdem Active Directory zum Einsatz, ist es nicht möglich, innerhalb einer Domäne unterschiedliche Kennwortrichtlinien für externe Dienstleister zu erzwingen. Dies muss daher auf organisatorischer Ebene geregelt und in einer IT-Richtlinie definiert werden.

Einspielen von Patches und Updates

Windows Server 2003 ermöglicht das regelmäßige automatische Einspielen von Aktualisierungen. Das Risiko von automatischen Neustarts und von Inkompatibilitäten mit installierten Programmen ist hierbei abzuwägen.

Für Server mit hohem Schutzbedarf sollte diese Funktion deaktiviert werden. Bei Servern mit normalem Schutzbedarf ist die Entscheidung für automatisches Update im Einzelfall zu treffen.

Automatische Updates sollten nicht direkt aus dem Internet bezogen werden, sondern über ein Software-Verteilungssystem (z. B. *Windows Server Update Service*, WSUS) verwaltet und zum Installieren freigegeben werden. Hier sind Regeln zu definieren, welche Arten von Updates und Patches automatisch installiert werden und welche der Freigabe durch einen Administrator bedürfen. In jedem Fall ist M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates* umzusetzen und zu gewährleisten.

Vor dem Einspielen von Service Packs in der Windows-Server-2003-Umgebung sollte eine Ausroll-Strategie (Reihenfolge der Server, mögliches Rollback) festgelegt werden. Hierbei ist auch zu berücksichtigen, dass Service Packs bestimmte neue Funktionen enthalten können, die auf Servern mit bestimmten Rollen vorrangig installiert werden müssen. Ein Beispiel hierfür ist die neue Sicherheitsgruppe *Distributed COM-Benutzer* im Service Pack 1.

Dokumentation

Dokumentationskonzept

Zur Planung der Administration gehört auch der Entwurf eines geeigneten Dokumentationskonzeptes. Es sollte eng an das Änderungsmanagement (M 2.221 *Änderungsmanagement*) angelehnt sein.

Aufgaben, Berechtigungen und Werkzeuge der Administratoren

Die definierten Aufgaben der Administratoren des Windows Server 2003, die entsprechenden Berechtigungen (auch Ressourcenberechtigungen) und die verwendeten Administrator-Werkzeuge sind in die Dokumentation aufzunehmen, um bei Personalausfall den weiteren Betrieb zu ermöglichen (siehe G 1.1 *Personalausfall* und M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*).

Kennwörter von Dienstkonten

Es ist ein geeignetes Konzept zur Dokumentation der Kennwörter von Dienstkonten zu entwickeln. Diese Kennwörter sind hochkritisch und müssen einer strikten Zugriffskontrolle unterliegen (z. B. Tresor, Mehrfachverschlüsselung und Vier-Augen-Prinzip).

Bei der Verwendung von administrativen Skripten muss eine erweiterte Dokumentation angefertigt werden. Die zu dokumentierenden Konfigurationen und Einsatzszenarien können aus der Dokumentation der Testumgebung für Skripte verwendet werden (siehe M 4.240 *Einrichten einer Testumgebung für einen Server*).

Ergänzende Kontrollfragen:

- Haben die Mitarbeiter der IT-Abteilung normale und administrative Benutzerkonten?
- Ist die Fernadministration sicherheitsverträglich organisiert worden?
- Ist eine sicherheitsverträgliche Regelung für das Einspielen von Updates getroffen worden?
- Ist ein Wartungsfenster definiert worden?

M 2.365 Planung der Systemüberwachung unter Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Fachverantwortliche, Revisor

Ereignisprotokolle

Beim Betrieb von Windows Server 2003 werden vielfältige und umfangreiche Ereignisprotokolle erzeugt. Diese Protokolle dienen vorrangig dem Nachweis und der Aufrechterhaltung eines ordnungsgemäßen Betriebes, aber auch der Fehleranalyse. Sie sind oft auch Grundlage von Revisionen oder weiteren Auswertungen.

Grundsätze zur Protokollierung

Aus den Inhalten der Protokolle ergeben sich Aufbewahrungsfristen und zu berücksichtigende datenschutzrechtliche Aspekte. Die Grundsätze zur Protokollierung sollten den gesetzlichen Anforderungen entsprechen und den Missbrauch von Protokolldaten sowie damit verbundene Gefährdungen und Risiken minimieren. (siehe M 5.9 *Protokollierung am Server*, M 2.64 *Kontrolle der Protokolldateien*, M 2.110 *Datenschutzaspekte bei der Protokollierung*).

Grundsätze der Überwachung und Protokollierung

- Protokolle sind nur im notwendigen Umfang zu erzeugen. Ihre Erzeugung verursacht Ressourcen- und Speicherplatzverbrauch. Es gilt das Vermeidungsprinzip.
- Höhere Sicherheitsanforderungen erfordern allgemein eine umfangreichere Überwachung.
- Protokolle werden für begründete, festgeschriebene Zwecke erzeugt und unterliegen dieser Zweckbindung.
- Die Überwachung und Protokollierung unterliegt den Interessen der Organisation und muss mit der Personalvertretung und dem Datenschutzbeauftragten abgestimmt sein.
- Protokolle sind vor unberechtigtem Zugriff, vor Manipulation und nachträglicher Änderung zu schützen.
- Protokolle sind regelmäßig und ausreichend zeitnah auszuwerten.
- Für die korrekte Auswertung von Protokollen sind exakte und synchrone Zeiteinträge sowie definierte Formate, Schnittstellen und Verfahren erforderlich.
- Bei der Auswertung von Protokollen sind die Grundsätze des Bausteins B 1.8 *Behandlung von Sicherheitsvorfällen* zu berücksichtigen.
- Protokolle sind nach Überschreiten ihrer maximalen Aufbewahrungsfrist zu löschen.

Überwachungsrichtlinie

Überwachungsrichtlinie einrichten

Auf Grundlage der Sicherheitsrichtlinie für den zu überwachenden Windows Server 2003 muss eine Überwachungsrichtlinie für den Server abgeleitet und umgesetzt werden. In der Überwachungsrichtlinie wird definiert, welche Ereignisse durch wen zu überwachen sind, welche Aktionen auf bestimmte

Ereignisse innerhalb einer festgelegten Reaktionszeit erfolgen müssen und wie mit den Protokolldaten umzugehen ist. Die bei Windows Server 2003 mitgelieferten Sicherheitsvorlagendateien befinden sich im Ordner *%SystemRoot%\Security\Templates*. Sie können mit der Managementkonsole MMC (Snap-In *Sicherheitsvorlagen*) eingesehen werden und dienen der Übersicht und Orientierung.

Welche Benutzer und Ereignisse überwacht werden sollen, wird im *Gruppenrichtlinien*-Snap-In festgelegt. Es sollte dokumentiert sein, ob und - wenn ja - aus welchem Grund zu folgenden Kategorien Erfolgs- und/oder Fehlerereignisse protokolliert werden:

- Anmeldeversuche
- Anmeldeereignisse
- Kontenverwaltungsereignisse
- Active Directory-Zugriffe
- Objektzugriffe
- Rechteverwendungen
- Prozessnachverfolgungen
- Systemereignisse
- Richtlinienänderungen

Objektüberwachung

Überwachung aktivieren

Für die Überwachung der Objektzugriffe (z. B. Dateien) ist zu beachten, dass diese sowohl in der Überwachungsrichtlinie des Servers als auch in den Eigenschaften der ausgewählten Objekte aktiviert sein muss. Zum Beispiel erlaubt Windows Server 2003 für Administratoren sowohl die Übernahme des Besitzes von Dateien als auch deren Übergabe an Dritte und damit auch an den ursprünglichen Besitzer. Dieser ist somit nur eingeschränkt in der Lage, eine solche Aktion zu erkennen. Deshalb sollten solche Ereignisse für überwachte Objekte zuverlässig ausgewertet werden.

Ereignisprotokolle

Mit der *Ereignisanzeige* können die Protokolle manuell eingesehen und verwaltet werden. Jeder einzelne Eintrag besitzt ergänzende Details und eine eindeutige Ereignis-ID, zu der ausführliche Beschreibungen existieren. Die Konfiguration der Ereignisanzeige muss definiert sein. Dazu sind die folgenden Aspekte zu beachten:

- **Rollentrennung**

  Rollentrennung

  Der Speicherort für die Ereignisprotokolle kann gegebenenfalls vom Standard *%SystemRoot%\system32\config* abweichen, wenn z. B. deren Auswertung nicht von der Administration beeinflusst werden darf. In diesem Ordner befindet sich auch die Registry. Daher ist es nicht sinnvoll, dem Administrator den Zugriff auf diesen Ordner zu entziehen. Seit Windows Server 2003 ist eine Beschränkung der Berechtigungen auf die Protokolle der Ereignisanzeige

möglich. Die gewünschten Zugriffsberechtigungen (*Access Control List*, ACL) werden mittels einer Sicherheitsbeschreibungssprache (*Security Descriptor Definition Language*, SDDL) im Registry-Wert *CustomSD* für die separaten Protokolle definiert.

Alternativ kann eine gewünschte Trennung von Administration und Überwachung mit einem Systemmanagementwerkzeug realisiert werden, auf das der betreffende Administrator keinen Einfluss besitzt.

- **Protokollgröße und -aufbewahrung**

  Die maximale Größe der Protokolldateien muss mit dem Verhalten beim Überschreiben, der erwarteten Anzahl möglicher Ereignisse und dem zu protokollierenden Überwachungszeitraum harmonieren. Falls "*Ereignis nie überschreiben*" konfiguriert wird, ist zu gewährleisten, dass die Protokolldatei nicht zu groß wird und so das System beeinträchtigt. Ansonsten könnte der Server stoppen und herunterfahren, sofern die Sicherheitseinstellungen so konfiguriert sind. Die geforderte Verfügbarkeit wäre unter Umständen nicht gegeben.

- **Relevante Protokolle**

  Die Ereignisprotokolle umfassen mindestens die Protokolle
  - System,
  - Anwendung und
  - Sicherheit.

  Abhängig von der Rolle und Funktion des Servers und können zusätzlich die Protokolle
  - Verzeichnisdienst,
  - DNS-Server und
  - Dateireplikationsdienst

  geführt werden.

  Weitere dateibasierte Protokolle, die in Abhängigkeit der Rolle und Funktion des Servers berücksichtigt werden sollten, sind:
  - IIS-Protokolle
  - RRAS-Protokolle
  - RADIUS-Protokolle

- **Ereignistypen**

  In den Protokollen können folgende Ereignistypen enthalten sein:
  - Fehler
  - Warnung
  - Information
  - Erfolgsüberwachung
  - Fehlversuchsüberwachung

Instrumente zur Überwachung protokollierter Ereignisse

Überwachungs-instrumente

Protokolle können je nach Bedarf manuell (z. B. über die Ereignisanzeige), mittels benutzerdefinierter Skripte (z. B. *Eventlg.pl*, *Eventquery.vbs*), mit speziellen Werkzeugen (z. B. *Dumpel.exe*, *Auditusr.exe*, *EventCombMT*) oder mit vollautomatisierten Managementwerkzeugen (z. B. *Microsoft Operations*

Manager 2005, MOM 2005) ausgewertet werden. Darüber hinaus existieren auch Produkte von Drittanbietern.

Quellenhinweise:

Werkzeug	Quelle
Eventlg.pl	Windows 2000 Resource Kit, Supplement 1
Eventquery.vbs	Windows 2000 Resource Kit, Supplement 1
Dumpel.exe	Windows 2000 Server Resource Kit, Supplement 1
Auditusr.exe	Bestandteil Windows Server 2003 mit SP1
EventCombMT	Microsoft Windows Server 2003 Resource Kit Tools

Diese Produkte decken auch Anforderungen an eine Überwachung ab, welche mit den Bordmitteln eines Windows Server 2003 nicht ausreichend realisiert werden können. Dazu zählt z. B. die Benachrichtigung per SMTP, echtzeitnahe Reaktion auf Ereignisse oder ansatzweise eine forensische Analyse, zur Feststellung verdächtiger Vorfälle und Ermittlung der Verursacher.

Überwachung der Verfügbarkeit

Bei der Überwachung der Verfügbarkeit eines Windows Server 2003 oder seiner Dienste ist zu berücksichtigen, dass eine zuverlässige Überwachung und automatische Eskalation nur von einem unabhängigen Drittsystem gewährleistet werden kann.

Die Art der Überwachung sollte ebenfalls in der Überwachungsrichtlinie dokumentiert sein.

- **Automatisierte Überwachung**

  Manuelle Überwachungen und Auswertungen nicht empfehlenswert

  Manuelle Überwachungen und Auswertungen sind potenziell fehlerbehaftet und subjektiv, unterliegen individuellen Schwankungen und sind nur eingeschränkt verfügbar. Die automatisierte Überwachung und Auswertung ist manuellen Verfahren vorzuziehen. Der Grundsatz der Angemessenheit ist zu berücksichtigen.

  Details zur empfohlenen Vorgehensweise sind von Microsoft im Planungshandbuch für die Sicherheitsüberwachung und Angriffserkennung beschrieben.

  Auch wenn für die Sicherheitsüberwachung eines Windows Server 2003 das Sicherheitsprotokoll der Ereignisanzeige höchste Priorität besitzt, darf nicht übersehen werden, dass weitere Ereignisse und somit deren Aufzeichnung sicherheitsrelevant sind. Eine regelmäßige Korrelation der Daten der Ereignisprotokolle mit anderen Daten wie beispielsweise Urlaubstagen, Feiertagen, Uhrzeiten etc. sollte durchgeführt werden, um Abweichungen von "normaler" Nutzung festzustellen.

- **Systemmonitor**

  Systemmonitor nutzen

  Der Systemmonitor mit seinen Leistungsprotokollen und Warnungen liefert zuverlässig Informationen über die aktuelle Verfügbarkeit von Ressourcen wie Hauptspeicher, Prozessor, Netzwerk und Festplattenplatz. Er kann automatisch beim Überschreiten definierter Grenzwerte warnen. Damit kann die Sicherstellung der Verfügbarkeit eines Servers unterstützt

werden. Die statistischen Auswertungen der Leistungsprotokolle über einen längeren Zeitraum gestatten Trendanalysen und eine rechtzeitige bedarfsgerechte Erweiterung oder Modernisierung erforderlicher Hardware. Auch Druckerwarteschlangen lassen sich mit dem Systemmonitor überwachen.

- **Hardware**

  Informationen von Hardwarekomponenten

  Hardwarekomponenten, welche speziell zur Verbesserung der Verfügbarkeit beschafft wurden (z. B. Unterbrechungsfreie Stromversorgung, Temperaturüberwachung), produzieren Ereignisse oder Protokollinformationen, die in die Überwachung einzubeziehen sind.

- **Anwendungen**

  Informationen aus Anwendungen

  Anwendungen können sicherheitsrelevante Informationen im Anwendungs-Protokoll der Ereignisanzeige oder in eigenen Protokollen dokumentieren. Diese Informationen und/oder Protokolle sollten ebenfalls in die Überwachung einbezogen werden.

Dokumentation

Überwachungsrichtlinie als Dokumentation

Als Dokumentation dient die Überwachungsrichtlinie. Weiterhin sollten Sicherheitsvorlagen (.inf-Dateien) für die effektive Überwachungsrichtlinie des Windows-Server-2003 Systems erstellt werden. Bei zusätzlichen Tools sind die überwachten Objekte und die protokollierten Ereignis-Typen zu dokumentieren.

Ergänzende Kontrollfragen

- Werden die Grundsätze der Überwachung und Protokollierung angewendet?
- Wurde aus der Sicherheitsrichtlinie eine Überwachungsrichtlinie für den Windows Server 2003 abgeleitet?
- Werden neben dem Sicherheitsprotokoll der Ereignisanzeige weitere Protokolle ausgewertet?
- Werden die Ergebnisse der Überwachung auch zur Identifikation von unerkannten Schwachstellen und Schulungsbedarf genutzt?
- Werden Dienstkonten regelmäßig auf potenziellen Missbrauch überwacht, z. B. durch Fehlversuchsüberwachung?

M 2.366 Nutzung von Sicherheitsvorlagen unter Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Sicherheitsrelevante Einstellungen können in Windows Server 2003 durch *Sicherheitsvorlagen* festgelegt werden. Da die meisten Bereiche des Systems sicherheitsrelevante Aspekte aufweisen, sind Vorlagen ein wichtiges und mächtiges Administrationswerkzeug. Mit ihrer Hilfe können Einstellungen standardisiert und zentral administriert werden. Die wichtigsten Werkzeuge für Vorlagen sind Sicherheitskonfigurationseditor (englisch Security Configuration Editor, SCE) und Sicherheitskonfigurations-Assistent (englsich Security Configuration Wizard, SCW, erst ab Service Pack 1 enthalten). Eine kurze Beschreibung ist unter den Hilfsmitteln zum IT-Grundschutz zu finden (siehe *Nutzung von Sicherheitsvorlagen unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Sicherheitsvorlagen

Im Unterschied zu administrativen Vorlagen (M 2.368 *Umgang mit administrativen Vorlagen unter Windows Server 2003*) enthalten Sicherheitsvorlagen für alle Einstellungsoptionen konkrete Werte. Das Aktivieren einer Sicherheitsvorlage in der lokalen Sicherheitsrichtlinie verändert unmittelbar die Systemkonfiguration. Sämtliche Einstellungen der Vorlage werden sofort aktiviert und mit dem konkreten Wert konfiguriert.

Windows-NT-4.0-Vorlagen migrieren

Der Vorlagentyp von Windows NT 4.0 (Dateien mit der Erweiterung *.pol*) sollte auf Windows Server 2003 nicht mehr angewendet werden. Vorhandene Sicherheitsvorlagen mit diesem Typ sollten als Gruppenrichtlinienobjekte neu erstellt werden. Das Programm *Gpolmig.exe* aus dem *Windows Server 2003 Ressource Kit* kann den Aufwand hierfür verringern.

Allgemeine Vorsichtsmaßnahmen für Sicherheitsvorlagen

In G 3.81 *Unsachgemäßer Einsatz von Sicherheitsvorlagen für Windows Server 2003* sind einige Gefährdungen aufgezählt. Durch eine sorgfältige Planung und Umsetzung und durch Beachtung von Grundregeln kann sichergestellt werden, dass Sicherheitsvorlagen die gewünschte Wirkung auf dem Zielsystem haben.

Anforderungsanalyse

Zu Beginn sollte der Aufwand für das Entwickeln und Testen abgeschätzt werden. Dies ist abhängig von der Anzahl der unterschiedlich konfigurierten Zielsysteme, Art und Anzahl der Einstellungen in einer Vorlage sowie der vorgesehenen Verteilungsstrategie von Vorlagen auf die Zielsysteme. Dies sollte vorab in einer Anforderungsanalyse geklärt werden, in welcher auch vorhandene Sicherheitsrichtlinien für den IT-Verbund zu berücksichtigen sind.

Testumgebung

Eine Test- und Entwicklungsumgebung oder zumindest ein vorübergehend isolierter Testserver ist in jedem Fall zu empfehlen. Je höher die Anzahl von Einstellungen und Zielkonfigurationen ist, desto größer der Aufwand für die Testumgebung. Je mehr sich die Konfiguration eines Testservers in einem bestimmten Bereich der tatsächlichen Konfiguration von potenziellen Zielservern annähert, desto besser kann die Wirkung der Vorlage für diesen Bereich vorhergesagt werden.

Der technische Aufwand für einzelne Einstellungen, wie beispielsweise die Kennwortlänge, ist klein und mit geringerem Risiko verbunden (eine Testumgebung ist hier nicht unbedingt nötig). Dies gilt insbesondere, wenn sie als Gruppenrichtlinie automatisch auf alle relevanten Server und Clients übertragen werden.

Ausrollstrategie

Das Verteilen und Aktivieren der Sicherheitsvorlagen in der Produktivumgebung (nachfolgend *Ausrollen* genannt) stellt ein nicht unerhebliches Risiko dar, insbesondere, wenn sich beim Test nicht hinreichend nachvollziehen lässt, wie sich kritische Einstellungen auf dem Zielserver auswirken werden. Dann ist es erforderlich, das Ausrollen zunächst auf einzelne, weniger kritische Server zu beschränken und erst bei entsprechendem Erfolg weiter auszudehnen. Des Weiteren sollten so genannte Rollback-Szenarien eingeplant und getestet werden. Rollback bedeutet, dass die Konfiguration des Servers bei Problemen wieder in den vorherigen Zustand zurückversetzt werden kann. Die Sicherung des Systemstatus und die zuverlässige Wiederherstellung sollten bei den Rollout- und Rollback-Szenarien berücksichtigt werden.

In vielen Fällen ist es sicherer, eine große Anzahl von Einstellungen auf mehrere Sicherheitsvorlagen zu verteilen und dann stufenweise auszurollen. Es kann zum Beispiel Vorlagen für bestimmte Windows Server 2003 Komponenten, für bestimmte Behörden- oder Unternehmensbereiche oder für bestimmte Sicherheitsstufen (z. B. Basissicherheit und hohe Sicherheit) geben. Dieses Vorgehen ist deutlich flexibler für die Entwicklung weiterer Vorlagen, da gezielt spezifische Vorlagen ersetzt werden können, während bewährte Grundeinstellungen erhalten bleiben. Beim stufenweisen Ausrollen kann es zu Konflikten kommen, wenn zwei Vorlagen dieselbe Einstellung definieren. Die Ausrollstrategie entscheidet darüber, welche Vorlage dominiert.

Sicherheitsvorlagen können manuell auf einem Server oder automatisiert auf mehreren Servern ausgerollt werden. Das manuelle Ausrollen erfolgt mittels der Konsolen des SCE bzw. des SCW und empfiehlt sich für einzelne Server mit sehr hohem Schutzbedarf, da mögliche unerwünschte Effekte so am schnellsten erkannt und behoben werden können. Die Automatisierung erfolgt mittels Skripten oder durch Active Directory. Letzteres ist für das stufenweise Ausrollen am besten geeignet, da mit geringem Aufwand eine Reihe von Vorlagen zugewiesen und die jeweils dominierende Vorlage festgelegt werden kann.

Es wird deutlich, dass eine geeignete Strategie für den jeweiligen IT-Bereich konzeptionell festgelegt werden muss, bevor Sicherheitsvorlagen produktiv eingesetzt werden. Sicherheitsvorlagen können den Freigabeprozess für Konfigurationsänderungen in Windows Server 2003 sowie die Bereitstellungskonzepte (M 4.281 *Sichere Installation und Bereitstellung von Windows Server 2003*) deutlich transparenter gestalten. Sie sollten in einen Freigabeprozess im Rahmen von M 2.221 *Änderungsmanagement* eingebunden sein.

Sicherheitskonfigurations-Editor (SCE)

Der SCE besteht nach einer Standardinstallation aus den Konsolen:

- *Lokale Sicherheitsrichtlinie* (unter *Start* | *Systemsteuerung* | *Verwaltung*): führt Sicherheitseinstellungen direkt auf lokalem Server durch
- *Sicherheitsvorlagen*: erstellt und verwaltet Sicherheitsvorlagen (*.inf*-Dateien) führt keine Konfigurationsänderungen am Server durch
- *Sicherheitskonfiguration und -analyse:* Modellierung von Sicherheitseinstellungen und Analyse des Systems mit Hilfe einer zwischengeschalteten Konfigurationsdatenbank, Export und Import von Sicherheitsvorlagen, Überprüfen der Richtlinienkonformität, Aktivieren einer modellierten Sicherheitskonfiguration

Die Konsolen *Sicherheitsvorlagen* und *Sicherheitskonfiguration und -analyse* werden über die *Microsoft Management Console* (MMC) aufgerufen.

SCE umfasst zentrale Sicherheitseinstellungen

Mittels der Werkzeuggruppe SCE werden alle Aspekte der Authentisierung und Signierung von Netzverkehr zwischen Windows-Computern eingestellt. Außerdem werden hier alle zentralen Sicherheitseinstellungen für einen Server eingestellt, unter anderem die Überwachungsrichtlinien und Berechtigungen im Dateisystem und in der Registrierdatenbank. In Domänen enthalten die SCE-Konsolen zusätzliche Einstellungen für Kerberos und andere domänenweite Einstellungen. Alle diese Einstellungen können in Sicherheitsvorlagen gespeichert werden. Es ist zu empfehlen, immer die aktuellsten vom Hersteller angebotenen Einstellungen einzuspielen (siehe Hilfsmittel zum IT-Grundschutz, *Nutzung von Sicherheitsvorlagen unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Beispielvorlagen

Bei Windows Server 2003 werden einige Sicherheitsvorlagen für unterschiedliche Sicherheitsanforderungen mitgeliefert. Sie befinden sich im Verzeichnis *C:\WINDOWS\security\templates*. Vom Hersteller sind weitere dokumentierte Vorlagen erhältlich.

Rollback

Die Einstellungen unter *Eingeschränkte Gruppen*, *Systemdienste*, *Registrierung* und *Dateisystem* können nicht mittels Rollback rückgängig gemacht werden. Solche Einstellungen können durch das Anwenden einer anderen Sicherheitsvorlage neu gesetzt werden. Eine Rollback-Variante stellt das parallele Entwickeln von Rollback-Vorlagen dar, welche die Einstellungen aus den eigentlichen Sicherheitsvorlagen im Notfall mit unkritischeren Werten überschreibt. Besonders kritisch sind Ressourcenberechtigungen (ACL) und Objekt-Überwachungseinstellungen (SACL). Berechtigungskonzepte, die in Sicherheitsvorlagen abgebildet werden, können vorhandene Berechtigungsstrukturen durch Anwenden der Vorlage unwiederbringlich zerstören. Hier muss M 2.370 *Administration der Berechtigungen unter Windows Server 2003* berücksichtigt werden.

Jedem Server sollte eine Sicherheitsvorlage zugewiesen sein

Für jeden Server sollte eine verbindliche Festlegung aller Einstellungen unter *Kontorichtlinien*, *Lokale Richtlinien* und *Ereignisprotokoll* getroffen werden. Hierzu sind die IT-Sicherheitsrichtlinien und Sicherheitskonzepte für den betrachteten IT-Verbund und die Maßnahmen des IT-Grundschutzes heranzuziehen. Ferner können die Standardeinstellungen von Windows Server 2003 sowie die mitgelieferten Sicherheitsvorlagen als Referenz verwendet werden. Es sollte für jeden Server eine gültige Sicherheitsvorlage bzw. ein Satz Sicherheitsvorlagen existieren. Die Sicherheitskonfiguration des Servers sollte dem letzten dokumentierten Stand der Sicherheitsvorlagen entsprechen.

Die Konformitätsanforderungen sollten in einer IT-Sicherheitsrichtlinie für den betrachteten IT-Verbund vorgeschrieben werden.

Der Sicherheitskonfigurationsassistent (SCW) stellt eine Erweiterung und zum Teil eine Vereinfachung des SCE dar. Es gelten dieselben Grundsätze. Hinweise und Empfehlungen zur Bedienung des SCW finden sich in den Hilfsmitteln zum IT-Grundschutz (siehe *Nutzung von Sicherheitsvorlagen unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Dokumentation

Für eine minimale Dokumentation von Sicherheitsvorlagen genügt es, für jeden Server die verwendeten Vorlagendateien (Dateien mit der Erweiterung *.inf* oder *.xml*), deren Version und bei selbsterstellten Vorlagen auch deren Inhalt in die Systemdokumentation aufzunehmen. Durch entsprechendes Versionsmanagement und Zugriffskontrolle auf die Vorlagen sollte nachvollziehbar sein, wer wann welche Vorlagen editiert hat. Wird die Vorlage über Active Directoy bereitgestellt, sind alle weiteren Faktoren zu dokumentieren, welche die Wirksamkeit der Einstellungen für den oder die Server bestimmen, z. B. *Organizational Unit* (OU), Sicherheits- und WMI-Filter. Es muss immer nachvollziehbar sein, woher eine einzelne Sicherheitseinstellung stammt.

Auf dieser Basis sollten Dokumentationen und gegebenenfalls Konzepte für Tests, eigene Skripte sowie Bereitstellungs- und Rollbackszenarien im Zusammenhang mit Sicherheitsvorlagen erstellt werden. Die Dokumentation sollte ebenfalls zur Planung der regelmäßigen Auswertung von System- und Sicherheitsprotokollen herangezogen werden.

Vorlagen als Basis für Systemdokumentation geeignet

Für die Sicherheitsvorlagen des SCW werden Transformations- und Stylesheet-Dateien für Anzeige und Ausdruck der Vorlagen mitgeliefert (*C:\WINDOWS\security\msscw\transformfiles*). Für die Basisdokumentation der Serverrollen im Rahmen einer Systemdokumentation ist dies ausreichend.

Zur Dokumentation von aktiven Einstellungen ist die GPMC-Konsole (*Group Policy Management Console*) gut geeignet, sofern Active Directory zum Einsatz kommt. Für die Gruppenrichtlinienobjekte, Richtlinienergebnissätze und Gruppenrichtlinienmodellierungen können Berichte in druckbarem Format in eine HTML-Datei exportiert werden (gewünschtes Objekt markieren | Menü *Aktion* | *Bericht speichern...*).

Ergänzende Kontrollfragen:

- Werden Sicherheitsvorlagen verwendet und in den Test- und Freigabeprozess des Änderungsmanagements eingebunden?
- Basieren die Einstellungen in den Sicherheitsvorlagen auf aktuellen Sicherheitsempfehlungen des Herstellers?
- Wurden Rollout- und Rollback-Strategien bzw. Rollbackvorlagen geplant und getestet?
- Unterliegen die Sicherheitsvorlagendateien einer Versions- und Zugriffskontrolle?
- Befinden sich veraltete Vorlagen aus Windows NT 4.0 im Einsatz?

M 2.367 Einsatz von Kommandos und Skripten unter Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

In der Praxis werden häufig Kommandos und Skripte für kleine Aufgaben wie z. B. das Setzen oder Anzeigen eines bestimmten Parameters eingesetzt. Skripte ermöglichen den automatisierten Ablauf von Kommandos und werden so zu machtvollen Werkzeugen. Das Schadenspotenzial durch Fehlbedienung und Unkenntnis bei einem einzelnen Kommando kann sich in einem Skript potenzieren. Deshalb müssen Skripte mit Bedacht eingesetzt werden, damit ihre Auswirkungen kontrollierbar und nachvollziehbar bleiben. Wird der Aufwand für Planung, Entwurf und Wartung in Kauf genommen, können administrative Aufgaben mittels Skripten vereinheitlicht und standardisiert werden.

Kommando

Unter Kommandos versteht man den Aufruf von Programmen mittels des Feldes *Ausführen...* oder über die Befehlszeile der Eingabeaufforderung. Diese wird herkömmlich auch als "DOS-Box" bezeichnet. Während unter DOS der Befehlszeileninterpreter *command.com* agierte, steht unter Windows Server 2003 die wesentlich leistungsfähigere *CMD.exe* zur Verfügung. Alles, was in dieser CMD-Shell aufgerufen werden kann, wird als Kommando bezeichnet. Es muss dabei unterschieden werden zwischen den impliziten Kommandos und Steuerungskonstrukten der CMD-Shell, Kommandos des Betriebssystems und Kommandos von Drittherstellern. Kommandos können in einer lesbaren Datei (Batch-Datei, spezielle Skript-Datei) zusammengestellt werden.

Skript

Klartext-Datei

Ein Skript ist eine Klartext-Datei, welche mit einem beliebigen Editor (z. B. *notepad.exe*) erstellt werden kann. Die in einem Skript enthaltenen Anweisungen werden beim Aufruf durch einen entsprechenden Interpreter ausgeführt. Skripte werden unter Windows hauptsächlich für die Automatisierung der Administration eingesetzt. Sie können vor allem die Ausführung sich ständig wiederholender Administrationsaufgaben sehr erleichtern. Werden sie automatisch ausgeführt, z. B. über *Geplante Tasks*, arbeiten sie auch in Abwesenheit eines Administrators. Die Wiederverwendung von Skripten gewährleistet die Nachvollziehbarkeit und einheitliche Qualität der durchgeführten Aufgaben.

Anforderungen

Anforderungen wie bei Standardsoftware

Für Skript-Interpreter, mitgelieferte Skripte und Skripte aus Zusatzpaketen des Herstellers (z. B. *MBSA*, *Support Tools*, *Ressource Kit*) sowie eigenentwickelter Skripte sollten die gleichen Anforderungen gelten wie für eine Standardsoftware (siehe B 1.10 *Standardsoftware*). Es handelt sich letztlich um Standardsoftware für die Administration unter Windows Server 2003. Die Anforderungen und Bedingungen für die Erstellung und Anwendung von Skripten sind zu analysieren und daraus verbindliche

Festlegungen zu treffen (siehe M 2.83 *Testen von Standardsoftware*).

Erstellen und Warten von Skripten nur durch qualifiziertes Personal

Skripte im Umfeld eines betriebskritischen IT-Systems dürfen nicht von administrativem Personal geschrieben und gepflegt werden, das für die Programmierung von Skripten nicht ausreichend geschult ist und über wenig Erfahrung verfügt (siehe G 2.67 *Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten*). Es muss ganz besonders im Umfeld der Administration und deren Automatisierung sichergestellt werden, dass keine unerlaubte bzw. nicht freigegebene Software in Form von Werkzeugen oder komplexen Skripten angewendet wird. Auf den Einsatz von Software ohne nachvollziehbare Herkunft ist zu verzichten.

Sicherheitsrichtlinie

Der Rahmen für den Einsatz von Skripten sollte in einer Sicherheitsrichtlinie festgelegt werden. Es ist mindestens festzulegen, für welchen Einsatzzweck und aus welcher Herkunft Skripte verwendet und welche Skriptumgebungen bzw. Skriptsprachen benutzt werden dürfen. Weiterhin ist festzulegen, welche Anforderungen an die Entwicklung und Freigabe für Skripte in bestimmten Einsatzbereichen gelten sollen. Wenn nichts anderes festgelegt wird, sind immer die Maßnahmen aus B 1.10 *Standardsoftware* anzuwenden. Es ist allerdings zu berücksichtigen, dass diese unter Umständen nicht für jeden Einsatzbereich effektiv und praktikabel sind, z. B. bei Anmeldeskripten.

Es sollte überlegt werden, generell keine unsignierten Skripte zuzulassen. Die Signaturen basieren auf Sicherheitszertifikaten. Skripte des Herstellers sind bereits signiert. Es empfiehlt sich, die eigenen Zertifikate aus Vorlagen einer Windows-Server-2003 Zertifizierungsstelle zu erstellen. Zum Signieren werden spezielle Programmier-Objekte der Crypto-API von Windows Server 2003 verwendet, auf die mittels Skripten zugegriffen werden kann. Nähere Informationen sind dem *Platform Software Developement Kit* (Platform SDK) für Windows Server 2003 zu entnehmen. Die Richtlinie kann ab Windows XP/Server 2003 mit Hilfe einer Softwareeinschränkungsrichtlinie administrativ umgesetzt werden.

Grundsätze

Problem Abwärtskompatibilität

Für alle Skripte sollte beachtet werden, dass sie in der Regel zwar aufwärts, aber oft wegen ihrer Weiterentwicklung bei der Nutzung neuer Funktionen nicht abwärts kompatibel sind.

Sicherheitskontext während der Ausführung

Skripte werden immer im Sicherheitskontext der aufrufenden Benutzersitzung ausgeführt, d. h. sie verfügen während des Ablaufs über die Berechtigungen dieses Sicherheitskontextes. Wird ein Skript durch einen Dienst oder einen laufenden Prozess gestartet, dann gilt der Sicherheitskontext dieses Dienstes oder Prozesses auch für das Skript. Für viele Funktionen, auf die mittels Skript zugegriffen wird, werden administrative Berechtigungen auf einzelnen Objekten oder auf dem gesamten Server benötigt.

Keine Kennwörter im Quelltext verwenden

Werden Skripte für Benutzer (z. B. An-/Abmeldeskripte) oder Dienste (z. B. im Zusammenhang mit Datensicherung) bereitgestellt, dürfen innerhalb des Skriptablaufs keine unerlaubten erweiterten Berechtigungen vergeben oder administrative Kennungen kompromittiert werden.

Häufig werden Skripte bei Domänenanmeldungen oder über Gruppenrichtlinien des Active Directory automatisch verteilt und ausgeführt.

Es sollte dafür gesorgt werden, dass Quelltexte von administrativen Skripten den Benutzern verborgen bleiben und dass die Skriptausführung den Betrieb nicht beeinträchtigt. Entsprechende Einstellungen befinden sich z. B. in den mitgelieferten administrativen Vorlagen unter *Administrative Vorlagen | System | Skripts*.

Systemeigene Mittel für Skripts:

Unter Windows Server 2003 stehen nach einer Standardinstallation umfangreiche Möglichkeiten zum Erstellen und Ausführen von Skripten zur Verfügung:

- *Eingabeaufforderung*/CMD-Shell und Batch-Dateien (.BAT, .CMD)

  Eingabeaufforderung

  Es handelt sich um eine Skriptumgebung des Herstellers, die auch eine Dokumentation beinhaltet. Die Möglichkeiten der Batch-Programmierung waren in älteren Versionen eingeschränkt, sind aber inzwischen sehr mächtig (z. B. steht eine *FOR*-Anweisung zur Verfügung). Es ist keine Installation erforderlich.

- *Microsoft Visual Basic Scripting* (VBScript) und *JScript*

  Microsoft Visual Basic Scripting

  VBscript ist eine einfache Skriptsprache. Sie besitzt keine eingebauten Funktionen zur Administration. Diese werden erst in der Kombination mit *Windows Scripting Host* (WSH) und den Schnittstellen zur *Windows Management Instrumentation* (WMI), *Active Directory Service Interface* (ADSI) und anderen Schnittstellen des Betriebssystems erschlossen. Dazu müssen Objekte in das Skript eingebunden werden, die über diese Schnittstellen bereitgestellt werden. Ohne gute Kenntnisse der entsprechenden Objektmodelle ist deren Nutzung zwar mit Hilfe von umfangreichen Vorlagen und Beispielen möglich, jedoch nicht zu empfehlen (z. B. wegen ähnlicher Methoden wie GetObject versus CreateObject). JScript ist mit VBScript hinsichtlich des Einsatzzwecks gleichzusetzen. Der Unterschied besteht in der an die Programmiersprache Java angelehnten Syntax. VBScript und JScript werden seit dem Erscheinen von Windows Server 2003 nicht mehr weiterentwickelt und sind daher unter dem Aspekt der Zukunftssicherheit kritisch zu bewerten.

- *Windows Scripting Host* (WSH)

  Windows Scripting Host

  Skripte (z. B. in Form von .vbs- oder .js-Dateien) werden über *CScript.exe* (Kommandozeilenausgabe) oder *WScript.exe* (grafisches Ausgabefenster) aufgerufen und abgearbeitet. Durch diese beiden Programme wird der WSH in Ausführung gebracht. WSH ist die standardmäßige Umgebung zur Skriptverarbeitung. Er besitzt eigene Programmfunktionen und kann Erweiterungen für WSH-kompatible Sprachen nachladen (VBScript, JScript). Der WSH ist ein Interpreter. Er kann COM-Objekte verwenden und hat somit Zugriff auf eine Reihe von Systemschnittstellen (siehe oben). *WScript.exe* und *CSript.exe* enthalten einen rudimentären Debugger zum Testen von Skripten.

  Im Zusammenhang mit WSH sind eine Reihe von Aktualisierungen und Fehlerkorrekturen für Windows NT/2000/XP/2003 erschienen, die Sicherheitsprobleme behoben und z. T. die Überarbeitung bestehender

Skripte erforderlich gemacht haben. Dies sollte bei der Entwicklung von Skripten für den WSH berücksichtigt werden.

- Scripting mit *Windows Management Instrumentation* (WMI)

  Windows Management Instrumentation

  WMI (*Windows-Verwaltungsinstrumentation*) ist als zentrale Verwaltungstechnologie in Windows Server 2003 integriert. WMI enthält für einen einheitlichen Zugriff auf die Konfiguration, Verwaltung und Überwachung fast aller Windows-Ressourcen. WMI gibt es bereits seit 1998 (Windows NT 4.0 SP4). Die WMI-Architektur ist komplex, sie besteht aus drei Schichten (Ressourcen, Infrastruktur, Nutzer) und ist objektorientiert aufgebaut. Sie wurde über DLLs für die Anbieterbeschreibungen (*%SystemRoot%\system32\wbem*) und den WMI-Dienst (*winmgmt.exe*) implementiert. Für den Zugriff mittels Windows-Skripten werden kompatible Skriptumgebungen wie WSH oder ActivePerl verwendet. Mit dem Snap-In *wmimgmt.msc*, dem WMI-Testprogramm *wbemtest.exe* oder dem Befehlszeilen-Werkzeug *wmic.exe* können WMI-Konfigurationen vorgenommen bzw. verfügbare Klassendefinitionen untersucht werden.

- Scripting mit *Active Directory Service Interface* (ADSI)

  Active Directory Service Interface

  Mit ADSI wird eine scriptbasierte Verwaltung des Verzeichnisdienstes Active Directory analog der WMI-Technologie ermöglicht.

Microsoft-Werkzeuge, die nicht Standardbestandteil von Windows Server 2003 sind:

- Werkzeug *Scriptomatic*

  Scriptomatic

  Mit Scriptomatic wird ein Werkzeug zum Generieren von Skripten bereitgestellt. Das Werkzeug unterstützt WMI und ADSI.

- Windows *PowerShell*

  Windows PowerShell

  Mit Windows PowerShell wird eine weiterentwickelte Kommandozeilen- und Skriptingumgebung für die Windows-Plattform angeboten, welche VBScript, JScript und den WSH ablöst.

Für viele Werkzeuge und Skripte, die von Microsoft bereitgestellt werden, gibt es keine generelle Produktunterstützung. Dies ist im Einzelfall mit dem Hersteller zu klären. Teilweise wurden die Werkzeuge zu Lehrzwecken bereitgestellt, besitzen keine oder nur unzureichende Fehlerbehandlungen und sind nicht leistungsoptimiert.

WSH abschalten

WSH blockieren, um Missbrauch vorzubeugen

Die Skript-Fähigkeiten von Windows werden leider auch zur Verbreitung von Schadsoftware (G 5.23 *Computer-Viren*) missbraucht. Auf Clients werden Skripte daher häufig eingeschränkt oder unterbunden. In einer Client/Server-Umgebung kann der administrative und organisatorische Nutzen von Skripten das erhöhte Risiko und den entsprechenden Sicherheitsaufwand rechtfertigen. Werden nur Kommandozeilenskripte benötigt, sollte der WSH auf dem Server blockiert werden, um die Sicherheit zu erhöhen.

Der WSH kann auf verschiedene Weise blockiert werden:

1. Erstellen des Registrierschlüssels (Windows 2000/XP/Server 2003)

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\Enabled
(Format Reg_DWORD)

Der Wert wird auf Null gesetzt. Die geänderte Registrierungseinstellung sollte in einer administrativen Vorlage abgebildet werden.

2. Softwareeinschränkungsrichtlinie (Windows XP/Server 2003)

   Mit entsprechenden Regeln können die Dateien Wscript.exe und Cscript.exe oder Skriptdateien selbst an der Ausführung gehindert werden (siehe Maßnahme M 4.286 *Verwendung der Softwareeinschränkungsrichtlinie unter Windows Server 2003*).

Alternative Skriptumgebungen

Skriptalternativen nicht unbedingt vorteilhaft

Alternative Skriptumgebungen wie Perl, KiXtart und andere verringern die Angriffsfläche von Windows Server 2003 nicht automatisch. Sie greifen genauso auf Betriebssystemfunktionen zu und können eigene Sicherheitslücken enthalten. Es gelten die oben genannten Anforderungen und Grundsätze.

Dokumentation

Dokumentation nach Maßstäben der Software-Entwicklung

Für die Entwicklung von Skripten empfehlen sich die in der Software-Entwicklung gängigen Dokumentationsgrundsätze. Mindestens sollten ein Anforderungskatalog, eine Funktionsbeschreibung und Benutzerhilfe, die Ausführungsbedingungen sowie eine Versionskontrolle vorliegen. In der Dokumentation der jeweiligen Windows-Komponente oder des jeweiligen Betriebskonzeptes muss anhand von Skriptname und Versionsnummer erkennbar sein, welches Skript eingesetzt wird.

Ergänzende Kontrollfragen

- Gibt es Festlegungen zur Benutzung von Skripten auf organisationskritischen Servern?
- Sind alle eigenentwickelten Skripte sowie Werkzeuge oder Skripte von Drittherstellern angemessen dokumentiert und getestet?
- Wurde der Einsatz der Skripte und Werkzeuge formell freigegeben?
- Ist die Umgebung, in der Skripte ausgeführt werden dürfen, ausreichend gegen Missbrauch und Schadsoftware geschützt?

M 2.368 Umgang mit administrativen Vorlagen unter Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Windows-Gruppenrichtlinien sind ein effektives und vielseitiges Mittel zur Konfiguration von diversen Windows-Systemen, unter anderem Windows Server 2003. Notwendige Vorüberlegungen für den Einsatz von Gruppenrichtlinien sind den Maßnahmen M 2.326 *Planung der Windows XP Gruppenrichtlinien* und M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000* zu entnehmen.

Zusammenhang von Gruppenrichtlinien und der Registrierdatenbank

Einstellungen in Gruppenrichtlinien wirken sich auf die Registrierdatenbank aus

Die meisten Einstellungen in den Gruppenrichtlinien führen zu Änderungen in der Registrierdatenbank eines Windows-Systems. Die Registrierdatenbank gehört zu den kritischen Kernkomponenten eines Windows-Servers und benötigt besonderen Schutz und besondere Sorgfalt. Die Aspekte "Test", "Sicherheitsüberwachung", "Rückführung" und "Dokumentation" sollten immer berücksichtigt werden. Hierzu müssen geeignete Werkzeuge verwendet werden - der Registrierungseditor von Windows allein deckt die genannten Aspekte nicht ab.

Änderung der Registrierdatenbank über administrative Vorlagen

Gruppenrichtlinien können durch Vorlagen von Microsoft und durch benutzerdefinierte Vorlagen, z. B. von anderen Softwareherstellern, erweitert werden. Diese so genannten administrativen Vorlagen stellen einen Satz von Einstellungsoptionen bereit, die gezielt und automatisiert Registrierungsschlüssel in die Registrierdatenbank schreiben. Im Zusammenspiel mit der in Windows Server 2003 mitgelieferten Gruppenrichtlinienverwaltung (*Group Policy Management Console*, GPMC) und den umfangreichen netzbasierten Bereitstellungsmechanismen (Active Directory) von Gruppenrichtlinien sind administrative Vorlagen ein geeignetes Mittel zum sicheren Umgang mit der Registrierdatenbank von Windows-Server-2003 Systemen.

Ausschließlicher Einsatz von administrativen Vorlagen empfohlen

Es wird empfohlen, Änderungen an Schlüsseln in der Registrierungsdatenbank ausschließlich über administrative Vorlagen vorzunehmen und auf manuelle Änderungen vollständig zu verzichten. Im Rahmen des Änderungsmanagements sollten zumindest manuell durchgeführte Änderungen an Registrierungsschlüsseln zeitnah in einer benutzerdefinierten administrativen Vorlage implementiert werden.

Kompatibilität von administrativen Vorlagen

Kompatibilität zwischen Vorlagen verschiedener Windows-Versionen

Jede Version von Windows-Betriebsystemen ab Windows 2000 und fast jedes Service Pack enthält administrative Vorlagen des Herstellers, die um neue Einstellungsoptionen erweitert worden sind und alle Optionen der Vorgänger-Versionen beinhalten. Dies gilt auch für Windows Server 2003. Die Abwärtskompatibilität der neuen Einstellungsoptionen ist in den Vorlagen dokumentiert und wird in der GPMC-Konsole angezeigt. Die meisten

Einstellungsoptionen haben auf einer inkompatiblen Windows-Version keine Wirkung. Beim Öffnen einer in Windows Server 2003 enthaltenen Vorlage auf einem Windows 2000 Server-System bleiben die inkompatiblen Einstellungsoptionen unsichtbar.

Gruppenrichtlinie an der neuesten Windows-Version ausrichten

Eine Gruppenrichtlinie sollte immer basierend auf der administrativen Vorlage der neusten Windows-Version erstellt werden, auf welcher die Richtlinie voraussichtlich verwendet wird. Die jeweiligen Vorlagen sind auf den Internetseiten von Microsoft in der Datei 'adminpak.msi' verfügbar. Wenn eine benutzerdefinierte administrative Vorlage für Windows Server 2003 erstellt wird, so sind Kompatibilität und Wirkung auf frühere Windows-Versionen ausreichend zu testen und in der Vorlage zu dokumentieren.

Aktualisierung des Betriebssystems

Einstellungen aus Vorlagen bleiben bei der Systemaktualisierung erhalten

Nach einer Aktualisierung des Betriebssystems bleiben alle Einstellungen erhalten und können mit den gegebenenfalls erneuerten administrativen Vorlagen des Betriebssystems verwaltet werden. Benutzerdefinierte Vorlagen samt aktivierten Einstellungen bleiben unverändert erhalten und können in den zugehörigen Gruppenrichtlinienobjekten ("Group Policy Objects", GPO) verwaltet werden.

Anwenden benutzerdefinierter administrativer Vorlagen

Registry Tattooing

Das Anwenden einer benutzerdefinierten administrativen Vorlage schreibt für jede aktivierte Einstellungsoption den entsprechenden Registrierungsschlüssel dauerhaft - wie bei den Windows NT 4-Systemrichtlinien - in die Registrierdatenbank. Zum Entfernen ist dann manuelles Editieren der Registry erforderlich. Der Effekt heißt in Windows 2000 Server und Windows Server 2003 "nicht verwaltbare Richtlinieneinstellung" und wird auch "Registry Tattooing" genannt. Danach kann in der GPMC-Konsole nur noch der Wert des Schlüssels geändert werden, z. B. von 1 auf 0 für "ja″ oder "nein" oder von 0x000D auf 0x0020 für die Veränderung einer Warteperiode, jedoch nicht mehr der Schlüssel selbst.

Kein Tattooing bei voll verwaltbaren Vorlagen

Der "Tattooing-Effekt" tritt nicht bei mitgelieferten administrativen Vorlagen einiger Microsoft-Produkte auf, z. B. Windows 2000/XP/2003 und Office XP/2003. Sie heißen in Windows XP/2003 "voll verwaltbare Vorlagen", die resultierenden Einstellungen heißen kurz "Richtlinien" (engl. "True Policies"). Diese Richtlinieneinstellungen werden zusätzlich in den Registrierschlüsseln

HKEY_LOCAL_MACHINE\Software\Policies

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies

HKEY_CURRENT_USER\Software\Policies

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

verwaltet und als .pol-Dateien im Dateisystem abgelegt. Die Policies-Schlüssel sollten nicht durch benutzerdefinierte administrative Vorlagen manipuliert werden.

Vor der Anwendung sollte der Systemstatus (englisch "Systemstate") gesichert werden (siehe M 6.99 *Regelmäßige Sicherung wichtiger Systemkomponenten für Windows Server 2003*). Das Sichern der Registrierung allein genügt nicht, um bei Komplikationen mit einer Vorlage den Ursprungszustand wiederherstellen zu können. Außerdem müssen Funktionalität und Wirkung der Einstellungen unbedingt auf einem isolierten Testsystem erprobt werden. Hierbei sind alle Windows-Versionen zu berücksichtigen, mit denen die Vorlage verwendet werden soll.

Ausroll-Strategie

Werden die Einstellungen auf mehrere Server angewendet, so ist der Ausroll-Prozess in einem unkritischen Bereich der Produktivumgebung zu beginnen. Der Bereich ist unter ständiger Beobachtung und Erfolgskontrolle sukzessive auf kritischere Schichten der Produktivumgebung auszuweiten. Zur Erfolgskontrolle dient in einer Active-Directory-Umgebung die GPMC-Konsole oder auf einem allein stehenden Server die Richtlinienergebnissatz-Konsole (RSOP-Konsole).

Sicherheitsüberwachung für benutzerdefinierte Schlüssel

Für jeden so erstellten Schlüssel sind im Sicherheitsprotokoll mindestens Schreibzugriffe zu erfassen. Die Einstellung der Objektüberwachung mittels Sicherheitsprotokoll wird in der Maßnahme M 2.365 *Planung der Systemüberwachung unter Windows Server 2003* beschrieben. Die Schreibberechtigung für normale Benutzerkonten ist zu deaktivieren. Beides kann manuell mit dem Registrierungseditor, skriptgesteuert (siehe M 2.367 *Einsatz von Kommandos und Skripten unter Windows Server 2003*) oder mittels einer Windows-Sicherheitsvorlage (siehe M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003*) geschehen.

Entfernen benutzerdefinierter administrativer Vorlagen

Maßnahmen vor dem Entfernen administrativer Vorlagen

Das Entfernen administrativer Vorlagen erfordert einen ähnlich hohen administrativen Aufwand wie das Einspielen. Wenn einige oder alle Einstellungsoptionen einer administrativen Vorlage nicht mehr verwendet werden sollen, dann wird sie üblicherweise aus der GPMC-Konsole entfernt und gegebenenfalls durch eine modifizierte Version ersetzt. Jedoch werden dadurch Registrierungsschlüssel weder entfernt noch wenigstens zurückgesetzt. Daher müssen vor dem Entfernen der Vorlage aus der GPMC-Konsole alle aktiven Einstellungen, die in der GPMC-Konsole sichtbar sind, dokumentiert und anschließend auf einen unkritischen Wert gesetzt werden. Unkritisch sind solche Werte, die zur Unwirksamkeit eines Registrierungsschlüssels führen. Die Vorlage sollte erst nach entsprechender Erfolgskontrolle mittels GPMC- oder RSOP-Konsole entfernt werden. Das erneute Hinzufügen einer versehentlich entfernten Vorlage zeigt in der GPMC-Konsole nicht die vorhandenen Registriereinstellungen an, auch wenn der oder die Registrierungsschlüssel noch gesetzt und wirksam sind.

Unbenutzte Schlüssel löschen

Um die Gefahr des Missbrauchs solcher verwaisten Registrierungsschlüssel auszuschließen, müssen anschließend alle nicht mehr verwendeten Registrierungsschlüssel vor ungewollter Verwendung geschützt werden. Dies ist im Normalfall nur durch Löschung möglich. Die Löschung kann manuell mit dem Registrierungseditor oder skriptgesteuert erfolgen. Alternativ können durch eine

Windows-Sicherheitsvorlage der Zugriff auf die Schlüssel verweigert und die Überwachungseinstellungen verschärft werden, wodurch sich allerdings die Eintragungshäufigkeit im Sicherheitsprotokoll erhöht und der Aufwand für die Auswertung steigt.

Dokumentation

Aktuellen Zustand der eingesetzten administrativen Vorlagen dokumentieren

Für eine minimale Dokumentation von administrativen Vorlagen genügt es, für jeden Server die verwendeten Vorlagendateien (Dateien mit der Erweiterung ".adm"), deren Version und bei benutzerdefinierten Vorlagen auch deren Inhalt in die Systemdokumentation aufzunehmen. Durch entsprechendes Versionsmanagement und Zugriffskontrolle auf die Vorlagen sollte nachvollziehbar sein, wer wann welche Vorlagen editiert hat. Weiterhin müssen jede aktivierte Einstellungsoption, ihr aktueller Wert und die zugrunde liegende Vorlage erfasst werden. Wird die Vorlage über Active Directoy bereitgestellt, sind alle weiteren Faktoren zu dokumentieren, welche die Wirksamkeit der Einstellungen für den oder die Server bestimmen (z. B. OU, Sicherheits- und WMI-Filter). Es muss immer nachvollziehbar sein, woher der einzelne Registrierungsschlüssel stammt.

Auf dieser Basis sollten Dokumentationen und gegebenenfalls Konzepte für Tests, eigene Skripte und Bereitstellungs- und Rückführungsszenarien im Zusammenhang mit administrativen Vorlagen erstellt werden. Die Dokumentation sollte ebenfalls zur Planung der regelmäßigen Auswertung von System- und Sicherheitsprotokollen herangezogen werden.

Zur Dokumentation von aktiven Einstellungen ist die GPMC-Konsole gut geeignet, sofern Active Directory zum Einsatz kommt. Für die Gruppenrichtlinienobjekte, Richtlinienergebnissätze und Gruppenrichtlinienmodellierungen können Berichte in druckbarem Format in eine HTML-Datei exportiert werden (gewünschtes Objekt markieren | Menü *Aktion* | *Bericht speichern*...).

Ergänzende Kontrollfragen:

- Gibt es manuell hinzugefügte Schlüssel in der Registrierdatenbank, die nicht durch eine administrative Vorlage oder ein geeignetes Werkzeug verwaltet werden?
- Werden Schreibzugriffe für alle durch benutzerdefinierte administrative Vorlagen erstellten Registrierungsschlüssel überwacht und für normale Nutzer gesperrt?
- Wurde die Wirksamkeit der mit administrativen Vorlagen konfigurierten Registrierungsschlüssel getestet?
- Sind alle aktivierten Einstellungen der administrativen Vorlagen in die Systemdokumentation des Servers aufgenommen worden?

M 2.369 Regelmäßige sicherheitsrelevante Wartungsmaßnahmen eines Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Grundlagen für eine geregelte Wartung

Die Wartung dient der Werterhaltung eines Windows Server 2003 bzw. der Aufrechterhaltung seiner Funktionen und vorgesehenen Verwendbarkeit. Sie darf nur von fachkundigem sowie autorisiertem Personal ausgeführt werden und kann Bestandteil einer Gewährleistung sein. Bei der Durchführung von Wartungen sind insbesondere beim Einsatz von externem Personal die Forderungen der Maßnahme M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten* zu berücksichtigen.

Eine Wartung wird regelmäßig und geplant auf Grundlage eines Wartungsplanes, in der Regel außerhalb des Normalbetriebes durchgeführt. Werden Cluster für den Netzwerklastenausgleich eingesetzt (*Network Load Balancing,* NLB), ist auch eine Wartung ohne Unterbrechung des Normalbetriebs möglich. Die Wartung umfasst Konfigurationsarbeiten, Reinigungen, die Begutachtung und Erneuerung von Verschleißteilen, Hardware-Erweiterungen sowie das Beheben kleiner Defekte. Herstellerangaben sind dabei zu beachten (siehe M 2.213 *Wartung der technischen Infrastruktur*).

Somit werden erkannte Fehler behoben, Anpassungen und Aktualisierungen umgesetzt und gegebenenfalls über Erweiterungen neue Funktionen und Anwendungen bereitgestellt. Die Erweiterungen dürfen nur nach ausreichendem Testen und vorliegender Genehmigung vorgenommen werden. Änderungen am Server sind zu dokumentieren.

Wartungsanforderungen und deren Durchführung sind vom Verantwortlichen für die Wartung, meist der zuständige Administrator, zu koordinieren (siehe Baustein B 1.9 *Hard- und Software-Management*) und zu dokumentieren (Maßnahme M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*).

Vorbereitung der Wartung

Prüfen, ob der sichere Betrieb gefährdet wird

Anhand der Teilkonzepte für die Rollen und Komponenten des Servers sollten die bei der Wartung abzuarbeitenden Bereiche identifiziert werden. Für wartungsrelevante Aspekte können die spezifischen Grundschutzmaßnahmen konsultiert werden. Anhaltspunkte für weitere wartungsrelevante Aspekte in verschiedenen Anwendungsszenarien sind in der Dokumentationsbibliothek *Microsoft Operations Framework* (MOF) für Windows Server 2003 zu finden.

Bestimmte wartungsrelevante Systemeigenschaften lassen sich nur im Normalbetrieb feststellen. Deshalb sind entsprechende Informationen aus dem *Systemmonitor, Netzwerkmonitor,* Taskmanager und rollenspezifischen Konsolen rechtzeitig zu ermitteln und zu berücksichtigen. Besonderes Augenmerk ist dabei auf die Seitenfehler in Verbindung mit der Auslagerungsdatei und auf den Ressourcenverbrauch von Prozessen zu richten (siehe M 2.365 *Planung der Systemüberwachung unter Windows Server 2003*). Mit dem *Windows Systemressourcen Manager* (WSRM) besteht für

Enterprise- oder Datacenter-Editionen die Möglichkeit, den Ressourcenverbrauch für Anwendungen, Prozesse und Dienste mittels Richtlinien zu definieren und zu steuern.

Es sollte ein Protokoll zu den während der Wartung abzuarbeitenden Schritten geführt werden, das auch Datum und einen Verantwortlichen enthält. Nach der Wartung sollte es aufbewahrt werden, um später eventuelle Unregelmäßigkeiten nachvollziehen zu können, z. B. bei der Auswertung der Ereignisanzeige.

Das Systemprotokoll aus der Ereignisanzeige ist auf Fehler und Warnungen zu prüfen. Es ist auf jeden Fall zu beurteilen, in wie weit der sichere Betrieb des Server durch diese Ereignisse gefährdet ist.

Wenn durch Wartungsarbeiten ein stark erhöhtes Aufkommen von bestimmten Ereignistypen zu erwarten ist, dann sollte dies vorher angekündigt werden, um Fehlalarme zu vermeiden. Unter Umständen kann dies auch für andere Protokolle sinnvoll sein, soweit sie betroffen sind.

Darüber hinaus kann die Serverhardware mit anderen Werkzeugen überwacht werden. Viele Hersteller bieten für ihre Hardware eigene Überwachungssoftware an, die auch Warnmeldungen senden und verarbeiten kann. Je nach Ausstattung werden z. B. die Festplatten, die Lüfterdrehzahl, die Spannungen des Netzteiles und die unterbrechungsfreie Stromversorgung überwacht. Häufig bieten hochwertige Festplatten eine so genannte Fehlerfrüherkennung. Dadurch ist es möglich, rechtzeitig vor dem Ausfall der Festplatte diese zu wechseln. Es ist zu gewährleisten, dass diese Informationen bei der Wartung berücksichtigt werden, siehe hierzu auch M 2.365 *Planung der Systemüberwachung unter Windows Server 2003*.

Regelmäßige Wartungsarbeiten

Hardwarekomponenten prüfen

Es ist zu prüfen und zu gewährleisten, dass die Serverhardware vollständig ist und keine in der Organisation nicht zugelassenen Komponenten beinhaltet. Für den sicheren Betrieb des Servers müssen alle Geräte und Dienste ohne Störung in Betrieb sein. Deshalb ist ihr ordnungsgemäßer Betrieb in der *Computerverwaltung (Gerätemanager* und *Dienste)* zu kontrollieren.

Die aktuellen *Systemeigenschaften* des Servers sind mit den dokumentierten Konfigurationsvorgaben abzugleichen. Dabei sind besonders die Einstellungen unter *Erweitert*, *Systemwiederherstellung* und *Automatische Updates* zu beachten. Falls Sicherheitsvorlagen verwendet werden, ist die Konformität des Servers zur aktuellen Version der Vorlagen zu prüfen.

Patches

Patchlevel überprüfen

Bei einer Wartung ist zu überprüfen, ob aktuell verfügbare Sicherheits-Patches eingepflegt sind. Für diese Aufgabe kann der Microsoft Security Baseline Analyser (MBSA) genutzt werden. Zuvor sollte jedoch geprüft werden, ob der MBSA alle relevanten Patches detektieren kann und welche der verfügbaren Patches tatsächlich für den Server relevant sind. Normalerweise werden erforderliche Sicherheitsaktualisierungen zeitnah ausgeführt. Da unter Umständen einzelne Patches für deren Wirksamkeit einen Neustart von Geräten, Diensten oder gar des Servers erforderlich machen, können diese

Aktualisierungen nur während einer Wartung ausgeführt werden. Abweichungen sind zu begründen.

Konten und Passwörter

Die Organisationsrichtlinien für den Umgang mit Konten und Passwörtern gelten auch für lokale Konten des Servers und die Dienstkonten (siehe M 4.48 *Passwortschutz unter NT-basierten Windows-Systemen*). Im Rahmen von Wartungs- und Integritätsprüfungen des Windows-Server-2003-Systems sollte geprüft werden, ob die Organisationsrichtlinien für den Umgang mit Konten und Passwörtern bzw. die Regelungen des Berechtigungskonzeptes eingehalten werden. Insbesondere sollte hierbei geprüft werden, ob unbenutzte lokale Konten vorhanden sind oder leere Passwörter bzw. Passwörter, die nicht den Organisationsrichtlinien entsprechen, vergeben wurden. Hierbei können Tools bzw. Scripte des MBSA genutzt werden. Besonderes Augenmerk ist auch auf temporäre Konten zu richten, also solche, die nur für einen begrenzten Zeitraum vorgesehen waren oder sind.

Dienstkonten verfügen häufig über erweiterte Rechte und bedürfen deshalb eines besonderen Schutzes. Bei der Kennwortänderung der Dienstkonten muss das neu vergebene Kennwort zusätzlich in den Eigenschaften des betroffenen Dienstes auf dem Reiter *Anmelden* eingetragen werden. Anschließend ist ein Neustart der betroffenen Dienste notwendig. Werden diese Dienste während des Normalbetriebes benötigt, können solche Maßnahmen nur während der Wartung durchgeführt werden, siehe auch Maßnahme M 4.284 *Umgang mit Diensten unter Windows Server 2003*.

Datenträger und Datenbestände

Nicht erlaubte Datentypen und Software

Die Datenbestände des Servers sind auf nicht erlaubte Datentypen und Software zu prüfen. Abweichungen sind gemäß Vorgaben der Organisation zu behandeln. Dabei sind auch verschlüsselte Datenbestände zu erfassen, welche den Vorgaben der Verschlüsselungsrichtlinie der Organisation nicht entsprechen. Unerwünschte EFS-Verschlüsselungen können z. B. mit dem Werkzeug *EFSInfo* lokalisiert werden (siehe auch M 4.278 *Sichere Nutzung von EFS unter Windows Server 2003*).

Vorgaben für Speicherplatznutzung

Vorgaben für die Speicherplatznutzung (z. B. maximale Verzeichnisgröße oder Auslagerung alter Daten) sind auf deren Einhaltung zu kontrollieren und gegebenenfalls umzusetzen. Datenträgerkontingente unterstützen diese Aufgabe, erlauben jedoch für Windows Server 2003 (bis einschließlich SP1) nur eine Beschränkung pro Benutzer und Partition. Mit dem Windows Server 2003 R2 stehen mit der erweiterten Kontingentverwaltung und der Dateiprüfung umfangreiche und komfortable Werkzeuge mit Berichtsfunktion zur Verfügung.

Aktuelle Berechtigungen

Die aktuellen Berechtigungen für Daten, Freigaben, Registrierung und Drucker sind auf Unregelmäßigkeiten sowie Abweichungen von Vorgaben zu prüfen. Für relativ statische Datenbestände und für Systemdaten wird die Dokumentation und Überprüfung der vergebenen Berechtigungen mittels *.inf*-Dateien (*Sicherheitsvorlagen*) und *Sicherheitskonfiguration und -analyse* empfohlen.

Die Wartung für Datenträger umfasst die Überwachung des freien Speicherplatzes auf der Partition, die Datenträgerbereinigung und die Defragmentierung. Für deren Durchführung ist ausreichend Zeit einzuplanen.

Versteckte Datenströme

Erhebliche Inkonsistenzen zwischen der Summe der gespeicherten Dateien, dem erwarteten und dem noch verfügbaren Speicherplatz auf der Festplatte können auf unerwünschte versteckte Datenströme (*Alternate Data Streams*, ADS) auf NTFS-Partitionen hinweisen. Falls es Hinweise auf versteckte Datenströme gibt, sollte darauf geachtet werden, dass die eingesetzte Antivirensoftware versteckte Datenströme untersucht (siehe M 2.157 *Auswahl eines geeigneten Computer-Viren-Suchprogramms*). Ist die Festplattenbelegung durch vermutete versteckte Datenströme erheblich, sollte eine Analyse mit geeigneten Werkzeugen von Drittherstellern erfolgen (siehe G 2.116 *Verlust von Daten beim Kopieren oder Verschieben in komplexen Datenstrukturen*).

Visuelle Kontrolle

Sichtprüfung der Server-Hardware

Durch die visuelle Kontrolle ist das äußere Umfeld des Servers zu begutachten. Dabei sind Kabel und Verbindungen, sowie die Befestigung von Baugruppen zu kontrollieren. Weiterhin ist eine Überprüfung der Sauberkeit und gegebenenfalls eine Reinigung der Lüftungskanäle, der Ventilatoren und der Kühlkörper durchzuführen.

Spezielle Wartungsarbeiten

Daten löschen

Sollen Datenträger im Zuge von Wartungsarbeiten zuverlässig gelöscht werden, kann das nur mit Werkzeugen von Drittanbietern durchgeführt werden (z. B. VS-Clean, siehe unter *Produkte und Tools* auf der BSI Webseite).

Ist Hardware redundant ausgelegt, wie z. B. durch RAID 5, doppelte Netzteile und Cluster, muss beim Ausfall einer redundanten Komponente diese umgehend ersetzt werden, da ansonsten die Ausfallsicherheit nicht mehr gegeben ist.

Alle Hardware-Hersteller bieten aktuelle Informationen, Firmware und Treiber für ihre Produkte an. Es wird empfohlen, diese Angebote regelmäßig zu prüfen und bei wesentlichen Änderungen deren Umsetzung innerhalb der Wartung zu berücksichtigen.

Garantie- und Wartungsverträge

Die Einhaltung von Garantie- und Wartungsverträgen ist zu überwachen, damit erforderliche Wartungen durch Vertragspartner durchgeführt werden und keine unnötigen Ausfälle oder Kosten entstehen. Die Beschaffung ist rechtzeitig über notwendige Aktivitäten zu unterrichten.

Ergänzende Kontrollfragen:

- Gibt es einen angemessenen Wartungsplan für den Server?
- Wie werden durchgeführte Wartungsarbeiten nachgewiesen?
- Wurde eine Datenträgerbereinigung mit anschließender Defragmentierung durchgeführt?

- Sind die erforderlichen Garantie- und Wartungsverträge noch gültig und entsprechen den aktuellen Anforderungen?

M 2.370 Administration der Berechtigungen unter Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator, Fachverantwortliche

Übersicht der zur Verfügung stehenden Berechtigungskonzepte

Das Sicherheitsmodell mit Konten, Gruppen und Zugriffsberechtigungen beschränkt sich keineswegs auf Objekte im Dateisystem NTFS. Vielmehr können in fast allen Bereichen des Betriebssystems Berechtigungen auf eine Vielzahl von Objekten vergeben werden. Somit können die Berechtigungen für jede Art von authentisierbaren Konten fein granuliert werden.

Aspekte des Berechtigungsmodells von Windows Server 2003 sind:

- Benutzerkonten und Computerkonten
- Systemkonten
- vordefinierte Standardgruppen
- Gruppenmitgliedschaften
- Verschachtelung von Gruppen (nur Active Directory)
- Zugriffsberechtigungen am Objekt (*Access Control List*, ACL)
- Systemzugriffskontrollen-Einstellung am Objekt (*System Access Control List*, SACL)
- Vererbung

Folgende Berechtigungseinstellungen sind nicht Teil des oben genannten Berechtigungsmodells:

- ressourcenbasierte Berechtigungsmechanismen in den *Internet Information Services* (IIS)
- Systemrechte (engl. rights/privileges)
- rollenbasiertes Zugriffsmanagement (*Role Based Access Control,* RBAC)

Die Möglichkeiten dieser Berechtigungseinstellungen werden unter den Hilfsmitteln zum IT-Grundschutz (siehe *Administration der Berechtigungen unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*) erläutert.

Schulung

Das Verständnis der oben aufgezählten Mechanismen und der dahinter stehenden Philosophien muss den Administratoren durch Schulungen und Bereitstellung von Fachbüchern vermittelt werden. Ansonsten ist ein sicherer Betrieb der jeweils eingesetzten Mechanismen und damit von Windows Server 2003 insgesamt nicht zu gewährleisten.

Je nach Aufgabenbereich der Administratoren sollten sie auch zu den entsprechenden Komponenten geschult werden, um die Auswirkung von Berechtigungskonfigurationen einschätzen und vorausplanen zu können.

Details zu einzelnen Berechtigungen in den verschiedenen Bereichen des Betriebssystems können aus der Online-Hilfe von Windows und der Microsoft Technet Dokumentation für Administratoren entnommen werden.

Grundregeln

Die Administration von Berechtigungen für Benutzerkonten und administrative Konten erfordert ein Grundverständnis der Berechtigungs- und Sicherheitsmechanismen und die Einhaltung gewisser Grundregeln. Vor allem scheinbar kleine Berechtigungsänderungen im laufenden Betrieb ohne vorherige Tests müssen besonders sorgfältig durchgeführt werden, um die Verfügbarkeit des IT-Systems nicht zu gefährden.

Least Privileges

Bei allen Tätigkeiten und Planungen im Zusammenhang mit dem Einräumen von Berechtigungen sollte immer das Prinzip der geringsten Berechtigungen (englisch *Least Privileges*) gelten. Das müssen nicht immer die absolut minimalen Berechtigungen zum Erfüllen einer spezifischen Aufgabe sein. Vielmehr sollten einem Konto nicht "vorsorglich" weit reichende Berechtigungen eingeräumt werden, sondern es soll nur solche Berechtigungen erhalten, die zur Abdeckung der für das Konto definierten Anforderungen notwendig sind. Berechtigungen können Schritt für Schritt auf ein höheres Niveau angehoben werden, wenn die Anforderungen dies rechtfertigen. Ein Konto sollte z. B. nicht Vollzugriff auf eine Ressource bekommen, wenn der Benutzer des Kontos keine administrativen Tätigkeiten auf der Ressource auszuführen braucht.

Simulationswerkzeuge

Eine generelle Schwierigkeit besteht in der Vorhersage der Auswirkungen einer bestimmten Berechtigungskonfiguration. Windows Server 2003 bietet verschiedene Simulationswerkzeuge zur Vorhersage der Auswirkungen von Berechtigungskonfigurationen an:

- **Die Registerkarte *Effektive Berechtigungen***

  In den Sicherheitseinstellungen eines Objektes, z. B. einer Datei, ist die Option zur Simulation unter *Erweitert* | *Effektive Berechtigungen* | *Auswählen* zu erreichen. Simulationen sollten sowohl mit der konfigurierten Sicherheitsgruppe als auch stichprobenartig mit Benutzerkonten durchgeführt werden, welche die Rechte ausüben sollen.

- **Die Konsole *Richtlinienergebnissatz* (Resultant Set of Policies, RSOP)**

  Start | *Ausführen* | *rsop.msc* eintippen

  Kommt Active Directory zum Einsatz, kann dieser Prozess über die Gruppenrichtlinienverwaltungs-Konsole auch auf entfernten Computern im Netz gestartet und ausgewertet werden.

Von den Simulationswerkzeugen sollte bei der Modellierung von Berechtigungen und bei der Administration im laufenden Betrieb intensiv Gebrauch gemacht werden. Es ist zu empfehlen, dies beim Freigabeprozess für Konfigurationsänderungen in einer entsprechenden IT-Sicherheitsrichtlinie zu formulieren.

Account Sharing, vergessene Kennwörter

Benutzerkonten dürfen nicht von mehreren Personen verwendet werden (so genanntes *Account Sharing*). Dies gilt für administrative wie für normale Benutzerkonten. Falls der Administrator aus zwingenden organisatorischen Gründen ein geteiltes Konto zur Verfügung stellen muss, ist dies für den Einzelfall zu begründen und zu dokumentieren. Das verwendete Konto, das Verfahren für die Durchsetzung der Kennwortrichtlinie, die Berechtigungen (ACL) und Überwachungseinstellungen (SACL) sowie der berechtigte Personenkreis sind zu dokumentieren. Der Missbrauch kann hier nur auf organisatorischem Wege vermieden werden. Geteilte Benutzerkonten sind ähnlich administrativen Konten als kritische Konten einzustufen und bei der Systemüberwachung zu berücksichtigen.

Password-Reset-Disketten

Der *Forgotten Password Wizard* von Windows XP/2003 dient zum Zurücksetzen vergessener lokaler Kennwörter, ohne dass lokal gespeicherte private Schlüssel dabei gelöscht werden. In einer Umgebung mit zentralisierter Authentisierung sollte dieser Wizard nicht verwendet werden, da er die Sicherheit eines solchen Konzeptes unterläuft. *Password-Reset-Disketten* dürfen nicht erstellt werden. Dies muss in der IT-Sicherheitsrichtlinie festgehalten werden und kann z. B. mittels Gruppenrichtlinien durchgesetzt werden.

Ergänzende Kontrollfragen:

- Gibt es ein eigenes Berechtigungskonzept?
- Werden dem Administrator die Berechtigungskonzepte von Windows Server 2003 durch Schulungen und Fachbücher vermittelt?
- Wird das Verweigern von Zugriffsrechten auf ein Objekt mit den jeweiligen Fachverantwortlichen abgestimmt?
- Werden vorsorglich Simulationswerkzeuge bei der Modellierung von Berechtigungen und bei der Administration im laufenden Betrieb benutzt?
- Wird Account Sharing im betrachteten IT-Verbund unterbunden bzw. auf ein Mindestmaß begrenzt?

M 2.371 Geregelte Deaktivierung und Löschung ungenutzter Konten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Personalabteilung

Verantwortlich für Umsetzung: Administrator, Fachverantwortliche

Soll ein Benutzerkonto deaktiviert oder gelöscht werden, muss anhand der Dokumentation der Zugriffsberechtigungen überprüft werden, welche Berechtigungen das Konto in der IT-Umgebung hat und für welche Authentisierungsvorgänge es benötigt wird.

Konten deaktivieren

Ungenutzte Benutzerkonten sind ein Sicherheitsrisiko und sofort zu deaktivieren

Ungenutzte Benutzerkonten können ein Sicherheitsrisiko darstellen. Aus diesem Grunde ist eine Empfehlung, die Angriffsoberfläche zu reduzieren und diese ungenutzten Konten zu deaktivieren. Dies ist umso wichtiger, je höher die Privilegien dieser Konten sind (administrative Konten). Aus diesem Grunde ist die Infrastruktur regelmäßig auf aktive Benutzer- und administrative Konten zu untersuchen, die nicht mehr verwendet werden. Es ist ebenfalls wichtig, dass solche Konten nicht von verschiedenen Personen verwendet werden. Es muss immer nachvollziehbar sein, wer wann welches Konto verwendet hat.

Konten löschen

Zugriffsrechte prüfen und Konto aus ACL löschen

Muss ein Benutzerkonto gelöscht werden, ist anhand der Dokumentation zu überprüfen, welche Zugriffsrechte das Benutzerkonto hat. Vor dem Löschen des Kontos muss geprüft werden, auf welche Objekte (zum Beispiel Dateifreigaben) die Berechtigungen gesetzt sind. Nach dem Löschen ist sicherzustellen, dass die Konten bzw. deren Sicherheitskennung aus den Zugriffsberechtigungslisten (Access Control List, ACL) entfernt worden sind.

Vorsicht bei administrativen Konten

Dabei darf Windows Server 2003 in seiner Lauffähigkeit nicht eingeschränkt werden, z. B. durch gelöschte Dienstkonten. Bei der Löschung administrativer Konten sollte eine Stellvertreterregelung greifen, sofern die administrativen Aufgaben bestehen bleiben. Hierfür muss bereits vor der Löschung ein entsprechendes Ersatzkonto existieren und in Betrieb genommen worden sein. Wird hierbei nicht sorgfältig vorgegangen, dann kann es sehr schwierig werden, die Administrierbarkeit einer Ressource bzw. den Zugriff auf Ressourcen wiederherzustellen. Daher kann es sich als notwendig erweisen, das Konto zunächst zu deaktivieren und erst nach einem Test zu löschen. Beim Löschen von Benutzerkonten sollte vorher ein Verfahren definiert sein, das den Verbleib und gegebenenfalls die Weiterverwendung der vom Benutzer erzeugten Daten regelt. Ansonsten können die Daten unter Umständen nur mit erhöhtem Aufwand (Objektbesitz übernehmen durch Administratoren) oder gar nicht mehr lesbar gemacht werden. Dies gilt in besonderem Maße für hochvertrauliche bzw. verschlüsselte Daten (siehe Maßnahme M 4.278 *Sichere Nutzung von EFS unter Windows Server 2003*). Es sollte dementsprechend vor der Löschung auch ermittelt werden, in welchen Gruppen der Benutzer Mitglied war, um zu prüfen, ob er möglicherweise bislang das einzige Mitglied einer Gruppe mit administrativen Rechten oder Ressourcenberechtigungen war.

Dies genannten Schritte stellen auch eine Herausforderung an die zugrunde liegenden organisatorischen Prozesse dar. Dies ist unter anderem in der Maßnahme M 3.10 *Auswahl eines vertrauenswürdigen Administrators und Vertreters* beschrieben.

Dokumentation

Die geregelte Deaktivierung oder Löschung von Benutzerkonten sowie damit verbundene Fristen sollte in einer Sicherheitsrichtlinie für den IT-Verbund dokumentieren werden.

Ergänzende Kontrollfragen:

- Wird das System regelmäßig auf ungenutzte administrative und Benutzerkonten überprüft?
- Werden ungenutzte Benutzerkonten sofort deaktiviert?
- Wird vor dem Löschen von Benutzerkonten überprüft, auf welche Objekte die Berechtigungen gesetzt sind?
- Existieren Verfahren für den Verbleib bzw. die Weiterverwendung von Daten, nach der Löschung von Benutzerkonten?
- Besteht ein administratives Ersatzkonto?

M 2.372 Planung des VoIP-Einsatzes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Eine grundlegende Voraussetzung für den sicheren Einsatz von VoIP ist eine angemessene Planung im Vorfeld. Die Planung für den Einsatz von VoIP kann in mehreren Schritten nach dem Prinzip des Top-Down-Entwurfs erfolgen: Ausgehend von einem Grobkonzept für das Gesamtsystem werden konkrete Planungen für Teilkomponenten in spezifische Teilkonzepten festgelegt. Die Planung betrifft dabei nicht nur Aspekte, die klassischerweise mit dem Begriff Sicherheit verknüpft werden, sondern auch normale betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen können.

Im Grobkonzept sollten beispielsweise folgende typische Fragestellungen behandelt werden:

- Soll vollständig oder partiell auf VoIP umgestiegen werden? Soll VoIP nur für die Kommunikation der leitungsvermittelnden TK-Anlagen untereinander eingesetzt?
- Gibt es besondere Anforderungen an die Verfügbarkeit von VoIP oder an die Vertraulichkeit und Integrität der Telefonate bzw. der Signalisierungsinformationen?
- Welche Signalisierungs- und Medientransportprotokolle sollen eingesetzt werden?
- Wie vielen Benutzern soll die Kommunikation über VoIP ermöglicht werden?
- Wie soll die Anbindung ans öffentliche Telefonnetz erfolgen? Sollen VoIP-basierte Kommunikationsverbindungen direkt aus dem öffentlichen Datennetz gestattet werden?
- Kann die Sicherheit des vorhandenen LANs durch VoIP beeinträchtigt werden? Ist das vorhandene LAN für die Nutzung von VoIP ausreichend dimensioniert? Müssen Änderungen an der Netzarchitektur vorgenommen werden?

Die folgenden Teilkonzepte sollten bei der Planung des VoIP-Einsatzes berücksichtigt werden:

- **Umfang der Verschlüsselung:** Es muss festgelegt werden, was verschlüsselt werden soll. Beispielsweise kann entschieden werden, dass die gesamte Kommunikation im LAN nicht verschlüsselt, aber alle externen Gespräche vor der Einsicht und Manipulation durch Dritter geschützt werden sollen (siehe Maßnahme M 2.374 *Umfang der Verschlüsselung von VoIP*). Im Weiterem muss entschieden werden, ob die Multimediadaten und/oder die Signalisierung verschlüsselt werden sollen.
- **Verschlüsselungsmechanismen:** Wenn für einzelne Kommunikationsstrecken die Verschlüsselung festgelegt wurde, muss entschieden werden, wie der Schutz integriert werden kann. Die Verschlüsselung kann sowohl

auf der Anwendungsschicht, wie beispielsweise über H.235 oder SRTP (siehe M 5.134 *Sichere Signalisierung bei VoIP* und M 5.135 *Sicherer Medientransport mit SRTP*), als auch auf tieferen Schichten, wie über SSL/TLS, IPSec oder VPNs, erfolgen.

- **Komponentenauswahl:** Um die getroffenen Entscheidungen umsetzen zu können, müssen die einzusetzenden Geräte diese auch unterstützen. Können keine entsprechenden Geräte beschafft werden, weil beispielsweise nicht alle Anforderungen erfüllt werden können, muss die Planung korrigiert werden. Hierdurch entstehende Änderungen müssen mit dem IT-Sicherheitsmanagement abgestimmt und dokumentiert werden.
- **Notfallvorsorge:** Nicht nur für die Geschäftsprozesse ist die Verfügbarkeit der Telefonie eine wichtige Voraussetzung. Bei einem Ausfall der Telefonie kann keine Hilfe in Notfällen gerufen werden. Daher müssen entsprechende Vorkehrungen getroffen werden. Weitere Informationen hierzu sind in der Maßnahme M 6.100 *Erstellung eines Notfallplans für den Ausfall von VoIP* zu finden.
- **Netztrennung:** In einigen Fällen kann die logische oder physikalische Trennung des VoIP-Netzes vom Datennetz sinnvoll sein (siehe Maßnahme M 2.376 *Trennung des Daten- und VoIP-Netzes*). In der Planungsphase ist zu entscheiden, ob eine Segmentierung notwendig ist.
- **Leistungsmerkmale:** Sehr oft bieten VoIP-Komponenten zusätzliche Leistungsmerkmale. Diese können den Betrieb einer zusätzlichen Middleware-Komponente erfordern oder besitzen andere sicherheitsrelevante Nachteile. Zu den sicherheitskritischen Leistungsmerkmalen gehören beispielsweise das Aufschalten auf ein bestehendes Gespräch, Raumüberwachungsfunktionen und das Wechselsprechen. Während der Planung ist zu entscheiden, welche Leistungsmerkmale verwendet werden soll.
- **Administration und Konfiguration:** Es ist frühzeitig festzulegen, wer die Administration und Konfiguration vornehmen soll. Hierfür sollte ein für VoIP zuständiger Administrator benannt werden. Im weiterem ist zu entscheiden, wie die Administration erfolgen soll (siehe M 4.287 *Sichere Administration der VoIP-Middleware* und M 4.288 *Sichere Administration von VoIP-Endgeräten*).
- **Protokollierung:** Die Protokollierung von Meldungen der einzelnen VoIP-Komponenten spielt eine wichtige Rolle, beispielsweise bei der Diagnose und Behebung von Störungen oder bei der Erkennung und Aufklärung von Angriffen. In der Planungsphase sollte entschieden werden, welche Informationen mindestens protokolliert werden sollen und wie lange die Protokolldaten aufbewahrt werden sollen. Außerdem muss festgelegt werden, ob die Protokolldaten lokal auf dem System oder auf einem zentralen Logserver im Netz gespeichert werden sollen.

Alle Entscheidungen, die in der Planungsphase getroffen wurden, müssen so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Dabei ist zu beachten, dass diese Informationen meist von anderen Personen als dem Autor ausgewertet werden müssen. Daher ist auf passende Strukturierung und Verständlichkeit zu achten.

Ergänzende Kontrollfragen:

- Welche Dokumentation existiert über die Planung des VoIP-Einsatzes?

M 2.373 Erstellung einer Sicherheitsrichtlinie für VoIP

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Bei der Telefonie werden hohe Erwartungen in deren Verfügbarkeit gesetzt. Ebenso wichtig ist aber deren Vertraulichkeit. Daher ist der sichere und ordnungsgemäße Betrieb von Telekommunikationseinrichtungen besonders wichtig. Dieser kann nur sichergestellt werden, wenn das Vorgehen in die bestehenden sicherheitstechnischen Vorgaben integriert ist.

Die zentralen sicherheitstechnischen Anforderungen an VoIP sowie das zu erreichende Sicherheitsniveau ergeben sich aus der organisationsweiten Sicherheitsleitlinie. Sie sollten in einer spezifischen Sicherheitsrichtlinie für VoIP formuliert werden, um die übergeordnete und allgemein formulierte Sicherheitsleitlinie zu konkretisieren und umzusetzen. In diesem Zusammenhang ist zu prüfen, ob neben der organisationsweiten Sicherheitsleitlinie weitere übergeordnete Vorgaben wie beispielsweise IT-Richtlinien, Passwortrichtlinien, Richtlinien zu den IT-Systemen, auf denen die VoIP-Komponenten betrieben werden, oder Vorgaben zur Internetnutzung zu berücksichtigen sind.

Die VoIP-Sicherheitsrichtlinie muss allen Personen und Gruppen, die an Planung, Beschaffung und Betrieb der VoIP-Komponenten beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Wie bei allen Richtlinien sind ihre Inhalte und ihre Umsetzung im Rahmen einer übergeordneten Revision regelmäßig zu prüfen.

Die Sicherheitsrichtlinie sollte zunächst das generell zu erreichende Sicherheitsniveau spezifizieren und grundlegende Aussagen zum Betrieb von VoIP treffen. Nachfolgend sind einige Punkte aufgeführt, die berücksichtigt werden sollten.

Allgemeine Regelungen für die VoIP-Nutzung

Alle VoIP-Benutzer sollten über potentielle Risiken und Probleme bei der VoIP-Nutzung sowie über den Nutzen, aber auch die Grenzen der eingesetzten Sicherheitsmaßnahmen aufgeklärt sein.

Da für die VoIP-Komponenten immer wieder neue Sicherheitslücken offen gelegt werden, sollte sich das IT-Sicherheitsmanagement regelmäßig über aktuelle Risiken informieren. Gegebenenfalls ist es angebracht, die Mitarbeiter regelmäßig über die neu bekannt gewordenen Gefahren zu informieren und damit auch zu sensibilisieren.

Bei der Erstellung einer Sicherheitsrichtlinie ist es empfehlenswert, so vorzugehen, dass zunächst ein Maximum an Forderungen und Vorgaben für die Sicherheit der Systeme aufgestellt wird. Diese sollten anschließend zwischen allen Beteiligten abgestimmt werden und auf Machbarkeit überprüft werden. Idealerweise wird so erreicht, dass alle notwendigen Aspekte berücksichtigt werden. Für jede im zweiten Schritt verworfene oder abgeschwächte Vorgabe sollte der Grund für die Nicht-Berücksichtigung dokumentiert werden.

In der Sicherheitsrichtlinie muss klar geregelt sein,
- ob und wo VoIP-Komponenten eingesetzt werden dürfen,
- unter welchen technischen Einsatzbedingungen VoIP eingesetzt wird. Hierzu gehören vor allem die Festlegung von Sicherheitsmaßnahmen, die Auswahl und Installation der erforderlichen Sicherheitshard- und -software sowie Vorgaben für die sichere Konfiguration der betroffenen IT-Systeme,
- welche Informationen nicht über VoIP kommuniziert werden dürfen und
- welche Leistungsmerkmale und Funktionen unterstützt werden sollen.

Mitarbeiter müssen darüber informiert sein, unter welchen Bedingungen sie VoIP außerhalb der eigenen Institution benutzen dürfen, da hier unter Umständen andere Sicherheitsregelungen gelten.

VoIP-Middleware

Für den Betrieb von VoIP-Middleware muss unter anderem folgendes geregelt werden:

- Die Vorgaben für Beschaffung von Geräten anhand eines Anforderungsprofils (siehe auch M 2.375 *Geeignete Auswahl von VoIP-Systemen*) müssen erstellt werden.
- Es müssen Regelungen für die Arbeit der Administratoren und Revisoren getroffen werden. Folgende Fragen sollten hierfür beantwortet werden:
  - Über welche Zugangswege dürfen Administratoren und Revisoren auf die Systeme zugreifen (beispielsweise nur lokal an der Konsole, über ein eigenes Administrationsnetz oder über verschlüsselte Verbindungen)?
  - Welche Vorgänge müssen dokumentiert werden? In welcher Form wird die Dokumentation erstellt und gepflegt?
  - Gilt für bestimmte Änderungen das Vier-Augen-Prinzip?
  - Kann der Aufgabenbereich des Administrators für die IT-Systeme von dem Verantwortlichen für die VoIP-Applikation getrennt werden?
- Die Verantwortlichkeiten müssen festgelegt und geregelt werden.
- Vorgaben für die Installation und Konfiguration, wie
  - das Vorgehen bei der Erstinstallation,
  - die Überprüfung der Default-Einstellungen hinsichtlich ihrer Sicherheitsgefährdungen und
  - die Verwendung und Konfiguration

  müssen festgelegt und dokumentiert werden.
- Eine Benutzer- und Rollenverwaltung muss eingeführt, beziehungsweise erweitert werden. Hierzu gehören:
  - Regelungen zur Benutzer- und Rollenverwaltung, Berechtigungsstrukturen (Ablauf und Methoden der Authentisierung und Autorisierung, Berechtigungen für Installation, Updates, Konfigurationsänderungen etc.),
  - ein Rollenkonzept für die Administration und
  - eine Konzeption der Benutzerverwaltung. Die Benutzer müssen angelegt und Telefonnummern zugewiesen werden. Den Benutzern können bestimmte Privilegien, wie der Möglichkeit kostenpflichtige Servicenummern anzurufen, zuwiesen werden.

- Ein sicherer Betrieb erfordert Regelungen
  - zur Erstellung und Pflege von Dokumentation, Form und Umfang der Dokumentation, z. B. Verfahrensanweisungen, Betriebshandbücher,
  - dazu, welche Dienste und Protokolle zugelassen bzw. nicht zugelassen werden,
  - zu den erlaubten Kommunikationsverbindungen, wie zum Beispiel sollte ein direkter Verbindungsaufbau von internen VoIP-Systemen in öffentliche Netzen vermieden werden,
  - für die Durchführung von Softwareaktualisierungen und
  - zu den Vorgaben in der Sicherheitsrichtlinie der IT-Systeme, auf denen die VoIP-Middleware betrieben wird.
- Die Vorgaben für den sicheren Betrieb sollten Informationen dazu beinhalten, wie
  - die Administration abzusichern ist (beispielsweise sollte ein Administrationszugriff nur über abgesicherte Verbindungen erfolgen),
  - verschlüsselnde Signalisierungs- und Medientransport-Protokollen einzusetzen sind,
  - welche Werkzeuge für Betrieb und Wartung einzusetzen sind,
  - Berechtigungen zu vergeben sind und welche Vorgehensweisen bei Software-Updates und Konfigurationsänderungen zu beachten sind und
  - welche Sicherheitsmaßnahmen auf dem Betriebssystem umzusetzen sind, auf dem die Middleware betrieben wird.
- Für die Protokollierung ist zu entscheiden,
  - welche Ereignisse protokolliert,
  - wo die Protokolldateien gespeichert und
  - wie und in welchen Abständen die Protokolle ausgewertet werden sollen.
- Für die Datensicherung und Wiederherstellung bei VoIP-Komponenten muss das organisationsweite Datensicherungskonzept erweitert werden.
- Es müssen Regelungen für die Reaktion auf Betriebsstörungen, technische Fehler (lokaler Support, Fernwartung) und Sicherheitsvorfälle getroffen werden.

VoIP-Endgeräte

Im Folgenden werden Vorgaben für den Betrieb von VoIP-Endgeräten vorgestellt, die in der Sicherheitsrichtlinie ergänzt werden sollten.

- Es müssen Vorgaben für Beschaffung von Geräten anhand eines Anforderungsprofils gemacht werden.
- Es müssen Regelungen für die Arbeit der Administratoren und Revisoren getroffen werden. Ein Beispiel hierfür wäre die Trennung der Administration des einzusetzenden Softphones von der Administration des IT-Systems.

- Vorgaben für die Installation und Konfiguration müssen in der Sicherheitsrichtlinie aufgenommen werden. Hierzu sollten folgende Fragen beantwortet werden:
  - Ist eine Konfiguration bei der Auslieferung der Hardphones ausreichend oder soll im Betrieb eine Konfiguration möglich sein?
  - Wie werden bei einer hohen Anzahl von Endgeräten die Änderungen der Konfiguration im Betrieb durchgeführt?
  - Über welche Zugangswege dürfen Administratoren auf die Endgeräte zugreifen?
  - Welche Arten von Konfigurationen der Leistungsmerkmale, wie beispielsweise Weiterleitungen, dürfen die Benutzer durchführen?
- Vorgaben für den sicheren Betrieb spielen eine wichtige Rolle. Hierzu gehören
  - die Absicherung der Administration (beispielsweise Zugriff nur über abgesicherte Verbindungen),
  - der Einsatz von verschlüsselnden Signalisierungs- und Medientransport-Protokollen,
  - Werkzeuge für Betrieb und Wartung, Integration in ein bestehendes Netzmanagement,
  - Berechtigungen und Vorgehensweisen bei Software-Updates und Konfigurationsänderungen,
  - Vorgaben für Maßnahmen bei der Abwesenheit des Benutzers, wie beispielsweise Rufumleitungen und Sperren des Telefons und
  - der sichere Betrieb des Betriebssystems, auf dem ein Softphone betrieben wird.
- Für die Notfallvorsorge müssen in der Sicherheitsrichtlinie Regelungen für die Bereitstellung von alternativen Kommunikationswegen aufgenommen werden.

Die Verantwortung für die Umsetzung der VoIP-Sicherheitsrichtlinie liegt beim IT-Betrieb, Änderungen und Abweichungen hiervon dürfen nur in Abstimmung mit dem IT-Sicherheitsmanagement erfolgen.

Ergänzende Kontrollfragen:

- Wurde eine Sicherheitsrichtlinie für die Nutzung und den Betrieb von VoIP erstellt?
- Wann wurde die VoIP-Sicherheitsrichtlinie zum letzten Mal aktualisiert?
- Wurden in der VoIP-Sicherheitsrichtlinie unterschiedliche Einsatzzwecke der Komponenten, wie Endgeräte, Gateways, Gatekeeper und Proxies, berücksichtigt?

M 2.374 Umfang der Verschlüsselung von VoIP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Gelingt es einem Angreifer, sich an einer geeigneten Stelle Zugang zu einem internen Netz zu verschaffen, kann er die gesamte Netzkommunikation im LAN protokollieren. Falls die VoIP-Nutzlast nicht verschlüsselt ist, kann der Angreifer sämtliche Informationen mitlesen. Beispielsweise kann er durch die Auswertung der Signalisierungsinformationen ermitteln, wer wie lange mit wem telefoniert hat. Allerdings könnte ein Angreifer auch die Nachrichten auswerten, die über das Medientransport-Protokoll ausgetauscht werden und dadurch die Telefongespräche mithören. Daher sollte überlegt werden, dass die VoIP-Nutzdaten verschlüsselt werden. Eine Verschlüsselung müssen aber alle beteiligten TK-Systeme unterstützen.

Schutz vor Innentätern

Bei der Überlegung, ob die Kommunikation über VoIP verschlüsselt werden soll, ist es häufig zweckmäßig, zwischen interner und externer Kommunikation zu unterscheiden.

Für VoIP-Telefonate innerhalb eines LANs kann überlegt werden, ob auf eine Verschlüsselung verzichtet werden kann. Dabei muss sichergestellt werden, dass auf diese Informationen nicht über einen unsicheren Netzbereich, wie einem WLAN, durch einen Außentäter zugegriffen werden kann. Um die internen Gespräche vor dem Zugriff durch Innentätern zu schützen, kann der Einsatz einer Verschlüsselung aber sinnvoll sein. Hierfür ist der Betrieb der VoIP-Endgeräte als VPN-Endpunkte oder die Nutzung eines verschlüsselten Medientransportprotokolls, wie SRTP, denkbar.

Wenn alle eingesetzten VoIP-Geräte verschlüsselte Signalisierungsprotokolle unterstützen, wird empfohlen, diese zu nutzen. Hierdurch wird unter anderem verhindert, dass ein Angreifer Passwörter mitlesen und sich als ein anderer Benutzer beispielsweise am SIP-Registrar anmelden kann.

Schutz vor Außentätern

Verlassen Pakete mit VoIP-Inhalten das gesicherte LAN, müssen sie mit entsprechenden Verfahren geschützt werden. Für den Schutz der VoIP-Kommunikation ist eines oder mehrere der folgenden Verfahren auszuwählen:

- Nutzung verschlüsselnder Medientransportprotokolle, wie SRTP (Secure Realtime Transport Protocol).
- Verschlüsselung der Signalisierungsprotokolle, beispielsweise mit TLS (Transport Layer Security)
- Virtual Private Networks (VPNs):

  Durch den Einsatz von VPN-Gateways können Informationen verschlüsselt zwischen entfernten LANs übertragen werden. Einzelne Geräte können als VPN-Endpunkte betrieben werden. Dies hat den weiteren Vorteil, dass ein Innentäter ebenfalls keinen Zugriff auf die Informationen erhält. Ohne eine direkte Unterstützung von verschlüsselnden Signalisierungs- und Medientransportprotokollen kann auf dieser Weise eine protokollunabhängige Verschlüsselung eingesetzt werden.

  Werden, beispielsweise für eine Kommunikation zwischen verschiedenen Liegenschaften, mehrere VoIP-Vermittlungseinheiten (Middleware) benö-

tigt, sollten diese ebenfalls in einen VPN zusammengefasst werden, wenn keine anderen Verschlüsselungsmechanismen aktiviert werden können. Wird die Verbindung, beispielsweise zwischen mehreren Middleware-Komponenten in unterschiedlichen Liegenschaften, nicht ausreichend geschützt, könnte ein Angreifer unter Umständen alle Gespräche zwischen den Liegenschaften abhören. Wird die Middleware auf einem IT-System betrieben, kann in der Regel eine VoIP-protokollunabhängige VPN-Unterstützung problemlos nachinstalliert werden.

- Verschlüsselung des Funknetzes:

  Auf ein ungesichertes Funknetz innerhalb einer Institution könnte auch von außerhalb der Liegenschaft auf das Netz zugegriffen werden. Sind die VoIP-Gesprächsteilnehmer über ein WLAN miteinander verbunden, muss ein qualifizierter Schutz für das WLAN, wie WPA2, genutzt werden (siehe hierzu Baustein B 4.6 *WLAN*). Da sich diese Verschlüsselung auf das Funknetz beschränkt, ist zu beachten, dass die Informationen im restlichen LAN ungeschützt übertragen werden. Verlassen die VoIP-Informationen nicht über andere Wege das LAN, gelten bei einer qualifizierten Verschlüsselung die gleichen Bedingungen wie bei einer internen Kommunikation, bei der unter Umständen auf eine Verschlüsselung verzichtet werden kann.

Soll ein Gespräch zu einem Telefonteilnehmer über ein öffentliches Telefonnetz aufgebaut werden, kann die Verbindung zwischen dem VoIP-Endgerät und dem Gateway, der zwischen dem IP-Netz und dem öffentlichen leitungsvermittelnden Netz eingesetzt wird, gegebenenfalls mit VPNs oder verschlüsselnden Signalisierung- und Medientransportprotokollen geschützt werden. Da nur sehr wenige Telefone für leitungsvermittelnde Netze Schutzmechanismen bereitstellen und deren Einsatz vom jeweiligen Empfänger abhängig ist, ist eine Verschlüsselung zwischen VoIP-Gateway und dem Gesprächspartner meist nicht realistisch.

Ist eine verschlüsselte Kommunikation, beispielsweise zu externen Gesprächspartnern, nicht möglich, müssen die Benutzer hierüber informiert und sensibilisiert werden. Vertrauliche Gespräche sollten bei einer fehlenden Verschlüsselung nicht über das Telefon geführt werden.

Bei der Beschaffung von VoIP-Komponenten muss darauf geachtet werden, dass diese verschlüsselnde Signalisierungs- und Medientransportprotokolle wie z. B. TLS und SRTP unterstützen (siehe M 2.375 *Geeignete Auswahl von VoIP-Systemen*).

Ergänzende Kontrollfragen:

- Werden zwischen den VoIP-Komponenten verschlüsselnde Signalisierungs- und Medientransportprotokolle eingesetzt?
- Kann ein VPN für die Kommunikation der VoIP-Middleware eingesetzt werden?

M 2.375 Geeignete Auswahl von VoIP-Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Beschaffungsstelle, Administrator

Die verschiedenen Hersteller von TK-Produkten bieten zahlreiche Lösungen zur Telefonie an. Neben reinen Geräte für VoIP und für analoge und digitale Telefonie können auch Produkte, die beide Architekturen unterstützen, erworben werden. Beispiele sind TK-Anlagen für leitungsvermittelnde Netze, die über einen IP-Anschluss verfügen und Gateways, die zwischen eine VoIP-Architektur und ein öffentliches, leitungsvermittelndes Telefonnetz geschalten werden können. Für die Auswahl sind neben der Grundfunktionalität, wie der Unterstützung der benötigten Signalisierungs- und Medientransportprotokolle, zahlreiche sicherheitstechnische Aspekte zu berücksichtigen.

Bevor VoIP-Komponenten beschafft werden, muss eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Aufgrund der Bewertung kann dann eine fundierte Kaufentscheidung erfolgen, die sicherstellt, dass das zu beschaffende Produkt im praktischen Betrieb den Anforderungen genügt.

Allgemeine Anforderungen

Nachfolgend werden einige allgemeine Anforderungen aufgelistet, die bei der Beschaffung von VoIP-Endgeräten und der Middleware berücksichtigt werden sollten:

1. Allgemeine Kriterien
   - Soll eine VoIP-Appliance oder eine Lösung, die auf einem Standard-PC betrieben werden kann, beschafft werden?

     In jedem Fall muss das meist komplexe Betriebssystem so konfiguriert werden, dass nur die wirklich benötigten Funktionen aktiviert sind, die Zugriffsrechte restriktiv vergeben und Schwachstellen systematisch beseitigt werden.
   - Unterstützt das Produkt alle benötigten Protokolle?
   - Werden Schulungen von dem Hersteller oder einem unabhängigen Anbieter zu dem Produkt angeboten?
   - Gibt es verlässliche Informationen zur Zuverlässigkeit und Ausfallsicherheit von Hard- und Software?
   - Können die VoIP-Komponenten den Ansprüchen an die Performance gerecht werden?
   - Ist das Produkt nach formalen Methoden, wie den Common Criteria, evaluiert?
   - Ist die VoIP-Komponente interoperabel zu bestehenden Produkten?
   - Unterstützen die VoIP-Komponenten eine sichere Anmeldung und eine sichere Benutzerverwaltung?
   - Enthält die mitgelieferte Produktdokumentation eine genaue Beschreibung aller technischen und administrativen Details?

- Wird für die VoIP-Komponenten die Möglichkeit des Abschlusses von Wartungsverträgen angeboten? Oft ist der Zugriff auf Updates und Unterstützungsleistungen vom Hersteller nur in Verbindung mit einem gültigen Wartungsvertrag möglich. Können im Rahmen der Wartungsverträge maximale Reaktionszeiten für die Problembehebung festgelegt werden? Bietet der Hersteller einen technischen Kundendienst (Hotline) an, der in der Lage ist, sofort bei Problemen zu helfen?
- Lässt sich das Produkt einfach installieren, konfigurieren, und administrieren?

2. Protokollierung

Die angebotenen Möglichkeiten zur Protokollierung müssen mindestens die in der Sicherheitsrichtlinie festgelegten Anforderungen erfüllen. Insbesondere sind die folgenden Punkte relevant:

- Ist der Detailgrad der Protokollierung konfigurierbar?
- Werden durch die Protokollierung alle relevanten Daten erfasst?
- Ist der Zugriff auf die Protokolldaten mit einem Zugriffsschutz versehen?
- Unterstützt das System zentrale Protokollierung? Eine zentrale Protokollierung erleichtert eine gezielte Auswertung der Protokolldaten.
- Kann die Protokollierung so erfolgen, dass die Bestimmungen des Datenschutzes erfüllt werden können?

3. Updates

- Werden regelmäßig Updates und Patches für das Produkt angeboten? Werden Sicherheitspatches zeitnah nach Bekanntwerden einer Sicherheitslücke angeboten?
- Können durch eine Aktualisierung der Software auch neuere Versionen der Signalisierungs- und Medientransportprotokolle, in denen Sicherheitsprobleme beseitigt wurden und die zusätzliche Sicherheitsmechanismen bereitstellen, verwendet werden?
- Berücksichtigen die Updates tiefere Schichten der VoIP-Komponente, wie Updates im Betriebssystem oder Dienste, die nicht in unmittelbaren Zusammenhang zu VoIP stehen? Um bestehende Schwachstellen im Betriebssystem der Appliance oder im IT-System zu beseitigen, sollten diese Bestandteile ebenfalls aktualisiert werden.
- Werden Updates und Patches so abgesichert, dass ausgeschlossen werden kann, dass bei der Übertragung der Updates diese gegen manipulierte Versionen ausgetauscht werden können?

4. Administration

   - Unterstützen die VoIP-Komponenten sichere Protokolle zur Administration?
   - Können die VoIP-Komponenten so konfiguriert werden, dass die vorgegebenen Sicherheitsziele erreicht werden können?
   - Können wichtige Konfigurationsparameter vor Veränderungen durch Benutzer geschützt werden?
   - Können die VoIP-Komponenten über eine zentral gesteuerte Management-Software administriert werden? Ist die administrative Schnittstelle so gestaltet, dass auf fehlerhafte, unsichere oder inkonsistente Konfigurationen hingewiesen wird oder diese verhindert werden?

5. Verschlüsselung

Um über VoIP verschlüsselt kommunizieren zu können, müssen die beteiligten Geräte entsprechende Funktionalitäten beinhalten. Je nach Schutzbedarf kann aber während der Planung entschieden worden sein, auf eine Verschlüsselung der internen VoIP-Kommunikation zu verzichten. Dennoch sollten auch dann VoIP-Komponenten angeschafft werden, die über die Möglichkeit zur Verschlüsselung verfügen oder bei denen diese nachgerüstet werden kann. Folgende Aspekte sollten berücksichtigt werden:

- Unterstützen die VoIP-Komponenten die Verschlüsselung der Medientransport- und Signalisierungsinformationen oder kann die Unterstützung nachträglich eingebunden werden?
- Können die VoIP-Komponenten als VPN-Endpunkte betrieben werden?

Auswahl von Vermittlungssystemen (Middleware)

Telefonie stellt oft einen essentiellen Geschäftsprozess dar. Daher werden unter anderem hohe Anforderungen an die Verfügbarkeit gestellt. Folgende Kriterien sollten bei der Beschaffung berücksichtigt werden:

- Kann die VoIP-Middleware redundant ausgelegt werden?
- Bietet der Hersteller gegebenenfalls Hochverfügbarkeitslösungen an?
- Sollen ein oder mehrere, zentrale Geräte die VoIP-Gesamtfunktionalität bereitstellen oder sollen mehrere einzelne, von einander abhängige Geräte beschafft werden?

  Einzelne, voneinander abhängige Geräte sind zum Beispiel SIP-Registrare, Proxy-Server und Location Server. Systeme, die alle VoIP-Funktionalitäten in einer Gesamtlösung bereitstellen, lassen sich oft leichter konfigurieren. Mehrere, verteilte Systeme können dagegen besser skaliert werden. Da die Administration bei mehreren Geräten oft aufwendiger ist, sind dadurch Fehlkonfigurationen wahrscheinlicher.

Auswahl der aktiven Netzkomponenten

Falls für den Umstieg auf VoIP neue Netzkomponenten wie Switches beschafft werden, müssen diese ebenfalls besondere Voraussetzungen erfüllen. Soll VoIP über ein bestehendes Datennetz genutzt werden, müssen die Geräte VoIP-Pakete erkennen und bevorzugt weiterleiten können. Soll zwischen zwei lokalen Netzen über ein unsicheres Datennetz, wie dem Internet, telefoniert werden können, müssen weitere Anforderungen gestellt werden. Wenn bisher keine Maßnahmen zur Verschlüsselung ergriffen wurden, sollten beispielsweise die am unsicheren Netz angeschlossenen Gateways als VPN-Endpunkte eingesetzt werden können.

Ergänzende Kontrollfragen:

- Sind die Anforderungen an VoIP-Komponenten ausreichend spezifiziert und dokumentiert?

M 2.376 Trennung des Daten- und VoIP-Netzes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Leiter Haustechnik

Verantwortlich für Umsetzung: Leiter IT, Administrator, Haustechnik

IP-Telefonie ermöglicht das Telefonieren über existierende IP-Datennetze. Jedoch können zur Erhöhung von Skalierbarkeit, Dienstqualität (QoS), Administrierbarkeit und Sicherheit die Datennetze von den Sprachnetzen auch logisch getrennt werden. Es muss überprüft werden, ob eine Trennung von Daten- und VoIP-Netz erforderlich ist. Eine Trennung ist sinnvoll, wenn Daten- und VoIP-Netz einen unterschiedlichen Schutzbedarf haben.

Trennung der Netze über VLANs

Lokale Netze können physikalisch durch aktive Netzkomponenten oder logisch durch eine entsprechende VLAN-Konfiguration, also über virtuelle lokale Netze (Virtual Local Area Networks), segmentiert werden. Eine logische Trennung kann mit VLAN-Technologie auf der Ebene 2 mit VLAN-fähigen Switches aufgebaut werden (siehe auch M 2.277 *Funktionsweise eines Switches*). VLANs alleine bieten jedoch keinen Schutz vor Angreifern, die sich mit ihrem IT-System (PC, Laptop oder Server) physikalisch an ein VLAN anschließen. Da die Netzdose, also der VLAN-Port, des Telefons jedem unmittelbar zugänglich ist, könnte ein Angreifer direkt die Telefone im VLAN angreifen, indem er z. B. anstatt eines Telefons seinen PC mit dem VLAN verbindet.

Aus diesem Grunde sollten weitere, über die logische Netztrennung hinausgehende Maßnahmen getroffen werden, um derartigen Angriffe zu begegnen.

Physikalische Trennung der Netze

Bei erhöhten Sicherheitsanforderungen kann eine komplette physikalische Trennung des Sprachnetzes vom Datennetz sinnvoll sein. Die physikalische Trennung von Daten- und Sprachnetzen verringert deutlich die Angriffsmöglichkeiten. Außerdem kann bei dem Ausfall eines Netzes, beispielsweise durch den Ausfall der aktiven Netzkomponenten oder einem Kabelbruch, weiterhin über das verbleibende Netz kommuniziert werden. Durch die Trennung hat die Auslastung des Datennetzes keinen Einfluss auf die Auslastung des Sprachnetzes.

Probleme einer Trennung

Bei einer konsequenten Trennung des VoIP-Netzes vom IP-Datennetz können in der Praxis allerdings anderswo zusätzliche Aufwände entstehen:

- Die VoIP-Komponenten benötigen Zugriff auf Benutzerdatenbanken, wie LDAP-Verzeichnisse, die sich typischerweise bereits im Datennetz befinden, aber bei einer Netztrennung eventuell doppelt gepflegt werden müssten.
- Die Verwaltung des VoIP-Netzes, wie die Namensauflösung über DNS, erfordert in der Regel den Zugriff auf das Datennetz.
- Die Administration der VoIP-Komponenten kann bei einer konsequenten Trennung der Netze aufwendiger sein, beispielsweise da Software-Aktuali-

sierungen der VoIP-Komponenten dann nicht mehr über ein Datennetz übertragen werden können, beispielsweise über SFTP, sondern vor Ort eingespielt werden müssen. Auch eine Remote-Konfiguration von VoIP-Komponenten, beispielsweise über SSH oder SHTTP, setzt einen Anschluss an ein Datennetz oder separate IT-Systeme zur Konfiguration voraus.

Diese Probleme können aber durch entsprechende Gateways zwischen dem Daten- und Sprachnetz gelöst werden. Für viele Dienste könnte ein Proxy-Server im Sprachnetz betrieben werden, von dem die Anfragen aus dem Sprachnetz in das Datennetz weitergeleitet werden.

- Weitere Probleme bei der Netztrennung stellen die Nutzung von Multifunktionsgeräten, wie VoIP-Telefone mit integrierten Mail-Client, oder die weit verbreiteten Softphones dar. Diese Endgeräte benötigen sowohl Zugriff auf das Sprach- als auch auf das Datennetz.

  Ein Ansatz zur Lösung wäre, diese Geräte in einem dafür angelegten logischen Netz zu betreiben. Eine physikalische Trennung ist hier nicht möglich.

- Um den Aufwand der Verkabelung zu verringern, besitzen viele Hardphones einen integrierten "Miniswitch". Dabei wird das Telefon direkt an die Netzdose angeschlossen und ein weiteres IT-System, wie der Arbeitsplatzrechner, wird mit dem Telefon verbunden.

  Diese Anordnung verhindert die physikalische Trennung des Sprach- vom Datennetz. Für eine logischen Trennung muss der Access-Switch die beiden an einem Switchport angeschlossenen Geräte unterscheiden können. Dies ist beispielsweise über die MAC-Adresse oder durch eine IEEE 802.1X-Anmeldung möglich.

Schutz der Ports

Sollen Hardphones oder andere VoIP-Endgeräte, über die nur telefoniert werden soll, eingesetzt werden, ist darauf zu achten, dass von den Netzanschlüssen, mit denen diese Geräte verbunden sind, ausschließlich die vorgesehen VoIP-Verbindungen aufgebaut werden können. Anderenfalls könnte ein Angreifer ein mobiles IT-System an die Netzdose für das TK-Endgerät anschließen und Zugriff auf nicht für ihn bestimmte Informationen und Dienste erhalten. Ein Beispiel hierfür ist ein Telefon in einer nicht dauerhaft beaufsichtigten Umgebung, wie einer Tiefgarage. Dieser Schutz kann durch entsprechende Filterregeln an den aktiven Netzkomponenten erfolgen

Je nach Schutzbedarf können zusätzliche Maßnahmen, wie Authentisierung nach IEEE 802.1X, eingesetzt werden, um einen sichereren Betrieb zu gewährleisten. Es muss aber berücksichtigt werden, dass eine dynamische oder statische Zuordnung der MAC-Adresse zu einem (Switch) Port oder einer VLAN-Zugriffsliste keinen ausreichenden Schutz darstellt, da MAC-Adressen leicht gefälscht werden können.

Ergänzende Kontrollfragen:

- Gibt es eine physikalische oder logische Trennung zwischen Daten- und Sprachnetz?

M 2.377 Sichere Außerbetriebnahme von VoIP-Komponenten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Sollen VoIP-Komponenten, beispielsweise Endgeräte oder Middleware, außer Betrieb genommen oder ersetzt werden, so müssen von den Geräten alle sicherheitsrelevanten Informationen gelöscht werden. Dies gilt nicht nur, wenn Geräte an Hersteller, Service-Unternehmen, Entsorgungsunternehmen oder sonstige Dritte weitergegeben werden. Auch bei Verschrottung, Umzug oder Weitergabe an andere Benutzer müssen entsprechende Maßnahmen ergriffen werden. Neben der endgültigen Außerbetriebnahme betrifft dies insbesondere auch Reparaturen, Wartung und Garantieaustausch.

In vielen Fällen ist es erforderlich, frühzeitig mit Herstellern, Händlern beziehungsweise Service-Unternehmen zu klären, welche Maßnahmen zur Löschung sicherheitsrelevanter Informationen mit den Vertrags- und Garantiebedingungen vereinbar sind. Oft können hier gemeinsam sinnvolle Vorgehensweisen festgelegt werden.

Je nach Einsatzzweck der Komponenten können beispielsweise folgende Informationen auf den Geräten gespeichert sein:

- Auflistungen, wer mit wem telefoniert hat,
- Zeitpunkt und Dauer der Anrufe,
- Benutzernamen und Passwörter für die Anmeldung an der VoIP-Infrastruktur,
- Rechte und Privilegien der einzelnen Benutzer,
- E-Mail-Adressen der einzelnen Benutzer für Voice-Mails,
- Ansagen für den Anrufbeantworter,
- hinterlassene Nachrichten für die Benutzer,
- IP-Adressen und weitere Informationen, die auf den Netzaufbau schließen lassen,
- Protokolldateien,
- Zertifikate und Schlüssel,
- Konfigurationsdateien,
- persönliche Telefonbücher,
- organisationsweite Telefonverzeichnisse mit allen Mitarbeitern,
- Passwörter, um private Gespräche abzurechnen,
- Informationen über weitere Dienste für die Benutzer, wie Terminerinnerungen und
- in Ausnahmefällen die vollständige Aufzeichnung der eigentlichen Telefongespräche.

Aufgrund des Schutzbedarfs dieser Informationen ist darauf zu achten, dass die Daten gelöscht beziehungsweise unlesbar gemacht werden, bevor defekte oder veraltete Geräte außer Betrieb genommen oder ausgetauscht werden. Nach dem Löschen der Daten muss überprüft werden, ob das Löschen auch erfolgreich war. Die Vorgehensweise hängt dabei stark von der Art und vom Verwendungszweck des Gerätes ab.

Bei "normalen" Rechnern, die als VoIP-Komponenten eingesetzt waren, sollten die Festplatten mit einem geeigneten Tool so gelöscht werden, dass keine Wiederherstellung der Dateien mehr möglich ist. Die kann beispielsweise dadurch geschehen, dass der Rechner von einem externen Boot-Medium gestartet wird und die Festplatten mit Zufallsdaten überschrieben werden. Dabei ist es empfehlenswert, den Überschreibvorgang mehrfach zu wiederholen.

Bei Appliances hängt die Vorgehensweise davon ab, ob in dem Gerät eine Festplatte eingebaut ist oder ob die Daten in einem nichtflüchtigen Speicher gespeichert werden. Oft bieten die Geräte eine "Factory-Reset" Option, mit der sämtliche Konfigurationseinstellungen auf die Werte des Auslieferungszustands zurückgesetzt werden können. Auch nach dem Ausführen eines "Factory-Reset" sollte überprüft werden, ob die Daten wirklich gelöscht beziehungsweise zurückgesetzt wurden oder ob bestimmte Daten oder Dateien noch vorhanden sind.

Neben den Informationen, die auf dem Gerät selbst gespeichert sind, sollte auch überprüft werden, ob auf den Backup-Medien sensitive Informationen enthalten sind. Falls es nicht aus anderen Gründen (beispielsweise Archivierung, Aufbewahrungspflicht aufgrund gesetzlicher Regelungen) erforderlich ist, die Backup-Medien aufzubewahren, so sollten die Medien nach der Außerbetriebnahme des Gerätes ebenfalls gelöscht werden.

Oft sind die Komponenten von außen mit Namen auf Schnellwahltasten, IP-Adressen, Telefonnummern oder sonstigen technischen Informationen beschriftet. Auch diese Beschriftungen sollten vor der Entsorgung entfernt werden.

Ergänzende Kontrollfragen:

- Werden Konfigurationsdateien und Protokoll-Dateien vor der Entsorgung sicher gelöscht bzw. unlesbar gemacht?
- Wird die Beschriftung vor der Entsorgung von den Geräten entfernt?

M 2.378 System-Entwicklung

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator, Benutzer

System-Entwicklung findet im Sinne dieser Maßnahme statt, wenn Hardware, Software oder ein komplexes System, das aus mehreren Software- und Hardware-Komponenten besteht, erstellt, geändert oder ergänzt werden soll.

In allen diesen Fällen muss dieses Vorhaben vor der Durchführung mit der IT-Leitung und den betroffenen Fachabteilungen abgestimmt werden. Hierfür muss eine erste Übersicht der benötigten Leistungen und Anforderungen formuliert werden. Das IT-Sicherheitsteam ist schon zu diesem frühen Zeitpunkt über das Vorhaben einer System-Entwicklung zu informieren, damit die relevanten IT-Sicherheitsaspekte schon bei der Konzeption mit berücksichtigt werden können. Neben den Leistungen, die das System erbringen soll, müssen auf jeden Fall die möglichen Auswirkungen auf die Geschäftsprozesse und auf die IT-Sicherheit in der Organisation betrachtet werden.

Die Anforderungen an die Sicherheit eines IT-Systems sollten bereits vor Beginn der Entwicklung ermittelt und abgestimmt werden. Eine nachträgliche Implementierung von Sicherheitsmaßnahmen ist bedeutend teurer und bietet im Allgemeinen weniger Schutz als Sicherheit, die von Beginn an in den Systementwicklungsprozess oder in den Auswahlprozess für ein Produkt integriert wurde. Sicherheit sollte daher integrierter Bestandteil des gesamten Lebenszyklus eines IT-Systems bzw. eines Produktes sein.

Die hier aufgeführten Empfehlungen orientieren sich am "Planung und Durchführung von IT-Vorhaben in der Bundesverwaltung" (V-Modell) sowie teilweise an den Vorgaben der "Information Technology Security Evaluation Criteria" (ITSEC) und den "Common Criteria for Information Technology Security Evaluation" (CC).

Erstellung des Änforderungskatalogs

Für die Erstellung der Anforderungen ist die Maßnahme M 2.80 *Erstellung eines Anforderungskatalogs für Standardsoftware* zu beachten. Dort werden die wesentlichen Punkte erläutert, die zur Festlegung der funktionalen und der sicherheitsrelevanten Anforderungen berücksichtigt werden müssen,.

Der Anforderungskatalog muss mit dem IT-Sicherheitsteam abgestimmt werden. Falls sich im Laufe der System-Entwicklung Änderungen der Anforderungen ergeben, muss ebenfalls das IT-Sicherheitsteam diesen zustimmen und der Anforderungskatalog aktualisiert werden. Der Anforderungskatalog bildet die Grundlage für die Abnahme und Freigabe des Produktes.

Vorgehensmodell

Die System-Entwicklung muss nach einem durchgängigen, einheitlichen und verbindlichen Vorgehensmodell durchgeführt werden. Diese müssen die strikte Einhaltung des Vorgehensmodell sicherstellen. Das Vorgehensmodell muss sicherheitsspezifische Rollen, Aktivitäten und Ergebnisse umfassen, durch die die Angemessenheit und Umsetzung sicherheitsbezogener Systemeigenschaften kontrolliert werden können.

Vor der Freigabe müssen mindestens die in den ITSEC/CC definierten Phasen

- Anforderungsdefinition,
- Architektur- oder Fach-Entwurf,
- Fein-Entwurf und
- Realisierung durchlaufen werden.

Sicherheitsrelevante Phasenergebnisse der Anforderungsdefinition

In der Anforderungsdefinitionsphase müssen die Bedrohungen, Schwachstellen und Risiken für die IT-Sicherheit der jeweiligen Anwendung, die Sicherheitsaspekte der Einsatzumgebung, die externen Vorgaben und das Projektumfeld untersucht werden. Im Rahmen einer Schutzbedarfsfeststellung wird daraus der Sicherheitsbedarf abgeleitet, der zur Formulierung von Sicherheitsanforderungen führt. Die Sicherheitsanforderungen müssen auf Konsistenz und Vollständigkeit geprüft werden (siehe auch M 2.80 *Erstellung eines Anforderungskatalogs für Standardsoftware*).

Sicherheitsrelevante Phasenergebnisse des Architektur-Entwurfs

In der Architektur-Entwurfsphase müssen die internen Kontrollen für die Anwendung, die Grundfunktionen der Informationssicherheit und die organisatorischen und technischen Sicherheitsmaßnahmen auf fachlicher Ebene spezifiziert werden.

Es muss geprüft werden, dass die Sicherheitsanforderungen durch die Spezifikationen des Architektur-Entwurfs konsistent und ausreichend detailliert dargestellt werden. Hierbei sollte eine klare logische Trennung zwischen Sicherheitskomponenten und anderen Komponenten vorgenommen werden.

Sicherheitsrelevante Phasenergebnisse des Fein-Entwurfs

In der Phase des Fein-Entwurfs müssen die Sicherheits-Spezifikationen des Fach-Entwurfs so weit verfeinert werden, dass sie als Basis für die Realisierung dienen können, ohne dass ein weiterer Interpretationsbedarf besteht. Alle Module, in denen Kontrollfunktionen durchgeführt werden, sicherheitsempfindliche Verarbeitungs- und Kommunikationsabläufe erfolgen und auf sensitive Daten zugegriffen wird oder von denen sensitive Daten übertragen werden, müssen identifiziert werden.

Es muss geprüft werden, ob der Fach-Entwurf durch den Fein-Entwurf konsistent verfeinert wird. Die für die Gewährleistung der Sicherheitsanforderungen notwendigen internen Kontrollen müssen durch die Definition von Programm-Schnittstellen (API, Application Program Interfaces) spezifiziert werden. Für eine bessere Handhabung sollten die Sicherheits-APIs klar strukturiert und von den übrigen Modulen getrennt sein.

Sicherheitsrelevante Phasenergebnisse der Realisierung

In der Realisierungsphase müssen die spezifizierten Sicherheitsanforderungen durch Nutzung der entsprechenden Sicherheits-APIs adäquat umgesetzt werden. Es muss geprüft und getestet werden, ob die Implementation ihrer Spezifikation, insbesondere der Sicherheitsspezifikation genügt.

Mindestanforderungen an die Entwicklungsumgebung

Eine integrierte Entwicklungsumgebung (Integrated Development Environment, IDE) ist ein Anwendungsprogramm zur Entwicklung von Software. Die integrierte Entwicklungsumgebung erleichtert das Entwickeln von IT-Systemen, da alle wesentlichen Bestandteile wie zum Beispiel der Compiler, Debugger oder der Editor zu einer Einheit zusammengefasst sind.

Es muss eine einheitliche und verbindliche Bibliotheksstruktur für die gesamte Entwicklung zugrunde gelegt werden. Namenskonventionen müssen sowohl für den Programmcode als auch für die Benennung von Modulen definiert und vorgeschrieben werden. Ziel ist dabei, wichtige Informationen wie z. B. Entwicklungsstadium und -ort, Dokumentationstyp etc. durch geeignete Bezeichnung hervorzuheben.

Es sind Methoden, Werkzeuge und Rollen zu definieren und einzusetzen, die es erlauben,

- Systeme (Hard- und Software) sowie deren Bestandteile und Eigenschaften festzulegen und zu identifizieren,
- die systematische und kontrollierte Bearbeitung der notwendigen Änderungen und Verbesserungen zu steuern,
- unbeabsichtigte, unkontrollierte oder ungesteuerte Veränderungen zu verhindern,
- alle Zwischen- und Endergebnisse zu archivieren und zu verwalten,
- Entwicklungen dezentral, d. h. in verschiedenen Entwicklungseinheiten nach einem einheitlichen (Sicherheits-)Standard durchzuführen
- alle Benutzer der Entwicklungswerkzeuge und der Entwicklungsdatenbank eindeutig zu identifizieren,
- den Zugriff von Benutzern der Entwicklungswerkzeuge auf die Entwicklungsdatenbank in Abhängigkeit von der Benutzerrolle (need-to-know) zu kontrollieren,
- die Integrität der Entwicklungsdaten zu gewährleisten,
- Modifikationen der Entwicklungsdaten feststellen und zu Personen zuordnen zu können.

Es muss möglich sein, geprüfte und abgenommene Entwicklungsergebnisse festzuschreiben, so dass sie als Basis für die weitere Entwicklung dienen können. Insbesondere muss es möglich sein, an definierten Punkten des Vorgehensmodells die Entwicklung an unterschiedliche Entwicklungseinheiten zur Weiterführung zu vergeben.

Die eingesetzten Entwicklungswerkzeuge müssen es unterstützen, dass alle aufgrund von Modifikationen oder aufgrund von negativen Testergebnissen nötigen Änderungen nachgehalten, durchgeführt und qualitätsgesichert werden.

Auch die physische Umgebung, in der die System-Entwicklung stattfinden soll, muss bei der frühen Planung anhand der Sicherheitsanforderungen

festgelegt werden. Dazu gehören unter anderem auch die Anforderungen an Zutritts- und Zugangskontrollmechanismen.

Qualitätssicherung (QS)

Die Qualitätssicherung muss bei Beginn der Entwicklung geplant werden. Dabei müssen geeignete Maßnahmen zur Einhaltung der Sicherheitsanforderungen festgelegt und in konstruktiver und analytischer Weise im Entwicklungsprozess verankert sein.

Neben der Kontrolle, ob das System die Funktionalitäten gemäß Spezifikation und Anforderungskatalog erfüllt, muss auch das Verhalten des Systems im Fehler- oder Missbrauchsfall überprüft werden.

Es muss QS-Maßnahmen zu definierten Reviewterminen, mindestens am Ende jeder Entwicklungsphase, geben. Darüber hinaus können im Bedarfsfall zusätzlich interne Reviews einberufen werden.

Während der Anforderungsdefinition und der Entwurfsphasen sind Testspezifikationen und Testfälle zu entwerfen und zu dokumentieren, die zur Prüfung der System-Qualität und der Einhaltung der Sicherheitsanforderungen geeignet sind. Während der Realisierungsphase und bei der Abnahme müssen entsprechende Tests durchgeführt werden.

Die Durchführung der Tests ist zu dokumentieren. Automatische Wiederholbarkeit und automatischer Abgleich der Testergebnisse (Regressionstest) sind anzustreben. Praxisdaten als Testdaten sind grundsätzlich nur in anonymisierter Form zulässig (siehe auch M 2.82 *Entwicklung eines Testplans für Standardsoftware* bzw. M 2.83 *Testen von Standardsoftware*).

Überführung in Produktion und Software-Wartung

Es muss einheitliche Richtlinien für die Überführung in die Produktion und für die System-Wartung geben.

Überführung in die Produktion

Die strikte Trennung von Entwicklung und Produktion, speziell der Verarbeitung von Testdaten und Echtdaten, muss gewährleistet werden. Es muss ein klar definiertes Freigabeverfahren für entwickelte Systeme und Anwendungen geben. Erst nach der Freigabe darf der Transfer aus der Test- in die Produktionsumgebung erfolgen. Sämtliche Programmteile, die lediglich Testzwecken dienen, sind vor der Freigabe zu entfernen. Mindestvoraussetzung für eine Freigabe ist das vollständige und erfolgreiche Durchlaufen einer Abnahme mit umfangreichen Tests in der Zielumgebung am Ende des Entwicklungsprozesses. Im Rahmen der Abnahme muss insbesondere festgestellt werden, ob sich die IT-Systeme und IT-Anwendungen in der Zielumgebung gemäß den Sicherheitsanforderungen verhalten.

Es muss sichergestellt sein, dass nur ordnungsgemäß freigegebene Programme bzw. Module zum Einsatz kommen (siehe auch M 2.85 *Freigabe von Standardsoftware*).

- Es muss Verfahren zur sicheren Verteilung von Entwicklungsergebnissen geben (siehe auch M 2.86 *Sicherstellen der Integrität von Standardsoftware*).
- Es muss einheitliche und verbindliche Verfahren zur Installation und Konfiguration der ausgelieferten Anwendungen geben (siehe auch M 2.84 *Entscheidung und Entwicklung der Installationsanweisung für Standardsoftware* bzw. M 2.87 *Installation und Konfiguration von Standardsoftware*).
- Zu keinem Zeitpunkt dürfen Entwickler in der Lage sein, unautorisiert und unkontrolliert IT-Systeme oder Anwendungen während der Entwicklung zum Produktionseinsatz zu bringen oder bereits in der Produktion befindliche IT-Systeme oder Anwendungen nach der Abnahme bzw. Freigabe zu modifizieren (siehe auch M 2.88 *Lizenzverwaltung und Versionskontrolle von Standardsoftware*).
- Es muss ein Verfahren geben, die Übernahme in Abhängigkeit von zeitlichen und lokalen Bedingungen vorzusehen.

Wartung und Problemmanagement

Jegliche unautorisierte Veränderung eingesetzter IT-Systeme muss verhindert werden. Autorisierte Modifikationen müssen durch ein geeignetes Änderungs- und Konfigurationsmanagement nachvollziehbar sein. Im Rahmen des Änderungs- und Konfigurationsmanagements müssen auch Aufbewahrungsfristen für alle System-Komponenten definiert werden.

Auch nicht mehr im Einsatz befindliche Systemkomponenten, wie Programm- oder Modulversionen, Konfigurationsdaten und deren Dokumentation müssen für die Dauer der Aufbewahrungsfrist nachvollziehbar bleiben. Es muss ein klar definiertes Verfahren und eindeutig festgelegte Kompetenzen für die Rückmeldung von Systemproblemen an die zuständige Instanz geben.

Jede autorisierte Modifikation im System aufgrund festgestellter Mängel oder zur Erweiterung der Funktionalität muss gemäß dem gewählten Vorgehensmodell in der einheitlichen Entwicklungsumgebung mit einer kontrollierten Wieder-Überführung in die Produktion erfolgen. Es muss zusätzlich ein klar definiertes Verfahren für den Umgang mit Notfällen geben.

Software-Entwicklung durch Endbenutzer

Standardsoftware ermöglicht oft den Endbenutzern die Entwicklung und Nutzung von eigenen Programmen, um Routinetätigkeiten zu erleichtern (z. B. über Makroprogrammierung). Der unkontrollierte Einsatz solcher selbstentwickelter Programme kann allerdings ein Sicherheitsrisiko darstellen. Daher sollte in jeder Organisation die Grundsatz-Entscheidung getroffen werden, ob solche Eigenentwicklungen erwünscht sind oder nicht und wer diese erstellen darf (siehe M 2.379 *Software-Entwicklung durch Endbenutzer*). Eigenentwicklungen müssen ebenfalls getestet und freigegeben werden, bevor sie in der Produktivumgebung eingesetzt werden dürfen. Ebenso muss geklärt werden, wer diese Programme wartet und Probleme damit behebt. Die Regelungen für den Einsatz von selbstentwickelten Programmen sollte in einer Sicherheitsrichtlinie festgehalten werden.

Ergänzende Kontrollfragen:

- Gibt es in der Organisation eine Sicherheitsrichtlinie für die System-Entwicklung?

M 2.379 Software-Entwicklung durch Endbenutzer

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator, Benutzer

Viele der bei Büroarbeitsplätzen eingesetzten Standardprogramme ermöglichen es den Benutzern, selbst Programme zu entwickeln, z. B. um sich Routinetätigkeiten zu erleichtern. Ein typisches Beispiel dazu ist die Makroprogrammierung unter Microsoft Word oder Access.

Die Kreativität und Einsatzbereitschaft, die Mitarbeiter hierbei an den Tag legen, ist grundsätzlich zu begrüßen, allerdings sollte trotzdem in jeder Institution überlegt werden, wie mit der Makro- bzw. Software-Entwicklung durch Endbenutzer umgegangen werden soll.

Es ist zu bedenken,

- dass die Makro- bzw. Programmersteller im allgemeinen keine geschulten Programmierer sind,
- dass die Sicherheitsrichtlinien des Hauses beachtet werden sollten,
- wie andere Benutzer davon profitieren können (und wer dann die Benutzerbetreuung übernimmt) und
- wie die meist spontan erstellten Programme gepflegt und dokumentiert werden.

Zunächst sollte in jeder Institution die Grundsatz-Entscheidung getroffen werden, ob solche Eigenentwicklungen erwünscht sind oder nicht. Dies ist in jedem Fall in den Sicherheitsrichtlinien zu dokumentieren.

Wenn Eigenentwicklungen unerwünscht sind, sollten sinnvollerweise bei der Installation von Standardprogrammen die Möglichkeiten dazu bereits deaktiviert werden (soweit dies möglich ist).

Sind Eigenentwicklungen dagegen erwünscht, sollten hierfür entsprechende Benutzerrichtlinien entwickelt werden, um Mindestanforderungen an Sicherheit, Dokumentation und Qualität sicherzustellen.

In einer solchen Richtlinie sollte insbesondere festgehalten werden, dass

- die bestehenden Vorschriften zum Datenschutz und zur Datensicherheit eingehalten werden,
- die Eigenentwicklungen sorgfältig dokumentiert werden,
- für Eigenentwicklungen nur die dafür freigegebenen Software-Produkte (z. B. MS Word, MS Excel oder MS Access) verwendet werden. Die Installation weiterer Anwendungen oder Entwicklungsumgebung ohne Genehmigung der IT-Abteilung ist nicht zulässig.

Auch in Eigenentwicklungen wird einiges an Arbeitszeit investiert. Deswegen sollte sichergestellt sein, dass Eigenentwicklungen auch anderen Benutzern zu Gute kommen und dann auch dauerhaft gepflegt werden. Weiterhin sollte ein Ansprechpartner für Probleme mit diesen Eigenentwicklungen vorhanden sein. Eigenentwicklungen sollten auch allen Benutzern in der aktuellen Version zur Verfügung stehen. Daher ist es sinnvoll, alle Eigenentwicklungen,

die für weitere Mitarbeiter interessant sein könnten, an die IT-Abteilung weiterzuleiten. Diese kann dann prüfen, ob eine weitere Verbreitung sinnvoll ist, und kann im weiteren eventuell notwendige Anpassungen vornehmen und Benutzersupport anbieten.

Ergänzende Kontrollfragen:

- Gibt es ein Verfahren für den Umgang mit Software, die durch Endbenutzer entwickelt wurde?
- Ist sichergestellt, dass Eigenentwicklungen gut dokumentiert sind?
- Ist sichergestellt, dass Eigenentwicklungen allen Benutzern in der aktuellen Version zur Verfügung stehen?

M 2.380 Ausnahmegenehmigungen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Vorgesetzte

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Vorgesetzte

In Einzelfällen kann es sinnvoll und notwendig sein, von einer getroffenen Sicherheitsrichtlinie abzuweichen. Ausnahmen sollten möglichst vermieden werden, es ist aber auf jeden Fall besser, eine Ausnahme zuzulassen, als unnachgiebig auf Vorgaben zu bestehen, die im konkreten Einzelfall unsinnig sind. Sollten sich Ausnahmen häufen, ist dies ein Zeichen dafür, dass die vorhandenen Regelungen nicht geeignet sind. Daher müssen dann die Sicherheitsvorgaben überdacht und eventuell angepasst werden.

Ausnahmen müssen aber auf jeden Fall durch eine autorisierte Stelle genehmigt werden. Ausnahmegenehmigungen dürfen nur nach gründlicher Prüfung und in seltenen Fällen erteilt werden. Es muss für alle Ausnahmefälle überprüft werden, ob diese die Sicherheit nicht untergraben. Dafür ist eine Risikobewertung vorzunehmen. Anschließend muss eine schriftliche Begründung verfasst werden, die von den Verantwortlichen zu unterzeichnen ist. Bei der Genehmigung von Ausnahmen sind sowohl Fachverantwortliche als die "Eigentümer" von Informationen und Anwendungen, als auch das IT-Sicherheitsmanagement zu beteiligen.

Ausnahmen dürfen nur genehmigt werden, wenn dass ermittelte Risiko als tragbar eingestuft wurde. Ausnahmegenehmigungen sollten zeitlich klar befristet werden. Es muss regelmäßig überprüft werden (spätestens alle 12 Monate), ob die Ausnahmegenehmigungen noch erforderlich sind und ob Ausnahmegenehmigungen, die während einer bestimmten Phase notwendig waren, anschließend wieder aufgehoben werden.

Für die Erteilung von Ausnahmegenehmigungen sollte ein dokumentiertes Verfahren existieren. Es sollte mindestens folgendes dokumentiert werden:

- Begründung, warum eine Abweichung von den Sicherheitsvorgaben erforderlich ist und welche Vorgaben betroffen sind,
- Beschreibung der Ausgestaltung der Ausnahmegenehmigungen sowie Beschreibung der Auswirkungen und des betroffenen Bereichs, inklusive der Risikobewertung,
- Zeitpunkt der Einrichtung,
- Antragsteller und Genehmigender,
- Befristungen.

Über Abweichungen von den geltenden Sicherheitsvorgaben sind alle betroffenen Mitarbeiter zu informieren.

Ergänzende Kontrollfragen:

- Gibt es ein Genehmigungs- und Dokumentationsverfahren für Ausnahmegenehmigungen?

- Werden die Begründungen für Ausnahmegenehmigungen regelmäßig überprüft?
- Ist sichergestellt, dass alle Ausnahmegenehmigungen aufgehoben werden, sobald sie nicht mehr erforderlich sind?
- Werden die möglichen Konsequenzen von Abweichungen analysiert?

M 2.381 Festlegung einer Strategie für die WLAN-Nutzung

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Bevor in einer Organisation WLANs eingesetzt werden, muss festgelegt sein, welche generelle Strategie die Organisation im Hinblick auf die WLAN-Nutzung einnimmt. Insbesondere ist hierfür zu klären, in welchen Organisationseinheiten, für welche Anwendungen und zu welchem Zweck WLANs eingesetzt und welche Informationen hierüber kommuniziert werden dürfen. Dabei sollte auch festgelegt werden, in welchen räumlichen Bereichen WLANs aufgebaut werden sollen (sinnvoll kann dies also beispielsweise in Umgebungen sein, in denen sich die Benutzer häufig innerhalb bestimmter Bereiche bewegen) und in welchen Bereichen auf keinen Fall WLANs vorhanden sein dürfen (bis hin zur aktiven Abschirmung).

WLAN-Komponenten können beispielsweise eingesetzt werden, um

- eine Institution, eine einzelne Abteilung oder einen Produktionsbereich flächendeckend mit einem Funknetz zu versorgen,
- den Einsatz von mobilen Komponenten in einzelnen Räumen zu ermöglichen, also z. B. in Besprechungsräumen,
- ein WLAN für die Nutzung durch fremde Teilnehmer kommerziell anzubieten (Hotspots).

Funknetze können mit oder ohne Kopplung an andere Netze aufgebaut werden, was ebenfalls die Gefährdungslage deutlich beeinflusst und damit auch die zu ergreifenden Sicherheitsmaßnahmen. Je nach geplantem Einsatzzweck und Einsatzumgebung können die erforderlichen Sicherheitsmaßnahmen erheblich differieren. Dies muss in jedem Fall bei der Formulierung der Sicherheitsrichtlinien und Regelungen für die WLAN-Nutzung berücksichtigt werden. Die Entscheidung sollte zusammen mit den Entscheidungsgründen dokumentiert werden.

Beim Aufbau eines drahtlosen Netzes ist ein erheblicher Planungsaufwand notwendig, um die für einen professionellen Einsatz erforderliche Stabilität, Übertragungsqualität und Sicherheit zu erreichen (siehe auch M 2.383 *Auswahl eines geeigneten WLAN-Standards* und M 5.140 *Aufbau eines Distribution Systems*).

Aufwand für sicheren Betrieb hoch

Die IT-Verantwortlichen sowie das IT-Sicherheitsmanagement einer Institution sollten sich darüber im klaren sein, dass bei drahtlosen Kommunikationssystemen, insbesondere bei WLANs, viele technische Aspekte schnell weiterentwickelt und modifiziert werden. Dies bedeutet für die IT-Verantwortlichen und das IT-Sicherheitsmanagement zum einen, dass für einen sicheren Betrieb von WLANs generell ein höherer Aufwand notwendig ist und zum anderen, dass die IT-Sicherheitsmaßnahmen in kürzeren Abständen als bei anderen Systemen auf ihre Wirksamkeit getestet und an Veränderungen angepasst werden müssen.

Um drahtlose Netze und die damit verbundenen IT-Systeme sicher betreiben zu können, sind die folgenden Punkte wesentlich:

- Die Arbeitsweise und Technik der eingesetzten drahtlosen Kommunikationssysteme müssen von den für den Betrieb Verantwortlichen vollständig verstanden werden.
- Die Sicherheit der eingesetzten Technik sollte regelmäßig evaluiert werden. Ebenso sollten regelmäßig die Sicherheitseinstellungen der benutzten IT-Systeme (z. B. Access Points, Laptops, PDAs) untersucht werden.
- Die WLAN-Nutzung muss in der Sicherheitsrichtlinie der Institution verankert sein, jede Änderung der WLAN-Nutzung muss mit dem IT-Sicherheitsmanagement abgestimmt werden.
- Um die übertragenen Daten auch zuverlässig zu sichern, müssen Vorgaben ausgearbeitet werden, die sich unter anderem mit der Auswahl adäquater Verschlüsselungs- und Authentikationsverfahren, deren Konfiguration und Schlüsselmanagement beschäftigen.
- Es ist zu definieren, welche WLAN-Standards, z. B. IEEE 802.11g, von den WLAN-Komponenten mindestens unterstützt werden sollten, um ein sicheres Zusammenspiel der einzelnen Komponenten zu gewährleisten und die erforderlichen Sicherheitsmechanismen flächendeckend nutzen zu können.

Nutzung von WLAN-Komponenten

Viele von Endbenutzern verwendete IT-Systeme wie Laptops oder PDAs enthalten WLAN-Funktionalitäten, die bei der Auslieferung meistens nicht deaktiviert sind. Es sollte sichergestellt sein, dass hierüber keine "wilde" WLAN-Nutzung erfolgt, sondern es muss klar geregelt sein, ob diese WLAN-Funktionalitäten genutzt werden dürfen, und wenn ja, unter welchen Rahmenbedingungen.

Ergänzende Kontrollfragen:

- Ist die WLAN-Nutzung erlaubt?
- Existiert eine dokumentierte Strategie für die WLAN-Nutzung?
- Wurde festgelegt, welche WLAN-Standards von den eingesetzten WLAN-Komponenten mindestens unterstützt werden sollten?

M 2.382 Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement, Administrator

Für den Einsatz von WLAN-Komponenten in Behörden und Unternehmen müssen geeignete Sicherheitsrichtlinien aufgestellt werden. Diese WLAN-spezifischen Sicherheitsrichtlinien müssen konform zum generellen Sicherheitskonzept und den allgemeinen Sicherheitsrichtlinien der Institution sein. Sie müssen regelmäßig auf Aktualität überprüft und gegebenenfalls angepasst werden. Die WLAN-spezifischen Vorgaben können in den vorhandenen Richtlinien ergänzt oder in einer eigenen Richtlinie zusammengefasst werden.

Eine WLAN-Sicherheitsrichtlinie sollte unter anderem folgende Punkte umfassen:

- Es sollte beschrieben sein, wer in der Institution WLAN-Komponenten installieren, konfigurieren und benutzen darf. Dazu sind auch eine Vielzahl von Randbedingungen festzulegen wie z. B.
  - welche Informationen über WLAN-Komponenten weitergegeben werden dürfen,
  - wo die WLAN-Komponenten benutzt und wo Access Points aufgestellt werden dürfen,
  - an welche anderen internen oder externen Netze das WLAN gekoppelt werden darf.
- Für alle WLAN-Komponenten sollten Sicherheitsmaßnahmen und eine Standard-Konfiguration festgelegt werden.
- Bei einem Verdacht auf Sicherheitsprobleme muss ein Sicherheitsverantwortlicher hierüber informiert werden, damit dieser weitere Schritte unternehmen kann (siehe auch B 1.8 *Behandlung von Sicherheitsvorfällen*).

Incident Handling

- Administratoren, aber auch Benutzer von WLAN-Komponenten sollten über die Gefährdungen durch WLAN-Komponenten und die zu beachtenden Sicherheitsmaßnahmen informiert bzw. geschult werden.

Training zur WLAN-Sicherheit

- Die korrekte Umsetzung der in der WLAN-Sicherheitsrichtlinie beschriebenen Sicherheitsmaßnahmen sollte regelmäßig kontrolliert werden.

Benutzerrichtlinie für WLAN

Um Benutzer nicht mit zu vielen Details zu belasten, kann es sinnvoll sein, eine eigene WLAN-Benutzerrichtlinie zu erstellen. In einer solchen Benutzerrichtlinie sollten dann kurz die Besonderheiten bei der WLAN-Nutzung beschrieben werden, wie z. B.

- an welche anderen internen und externen Netze der WLAN-Client gekoppelt werden darf,
- unter welchen Rahmenbedingungen sie sich an einem internen oder externen WLAN anmelden dürfen,

- ob und wie Hotspots genutzt werden dürfen,
- dass der Ad-hoc-Modus abzuschalten ist, damit kein anderer Client direkt auf den WLAN-Client zugreifen kann,
- welche Schritte bei (vermuteter) Kompromittierung des WLAN-Clients zu unternehmen sind, vor allem, wer zu benachrichtigen ist,

Wichtig ist auch, dass klar beschrieben wird, wie mit Client-seitigen Sicherheitslösungen umzugehen ist. Dazu gehört beispielsweise, dass

- keine sicherheitsrelevanten Konfigurationen verändert werden dürfen,
- stets ein Virenscanner aktiviert sein muss,
- eine vorhandene Personal Firewall nicht abgeschaltet werden darf (siehe auch M 5.91 *Einsatz von Personal Firewalls für Internet-PCs*),
- dass alle Freigaben von Verzeichnissen oder Diensten deaktiviert oder zumindest durch gute Passwörter geschützt sind,
- für die Nutzung externer WLANs nur spezielle Benutzerkonten mit restriktiver Rechtevergabe verwendet werden sollten.

Außerdem sollte die Benutzerrichtlinie ein klares Verbot enthalten, ungenehmigt Access Points anzuschließen. Des Weiteren sollte die Richtlinie insbesondere im Hinblick auf die Nutzung von klassifizierten Informationen, beispielsweise Verschlusssachen, Angaben dazu enthalten, welche Daten im WLAN genutzt und übertragen werden dürfen und welche nicht. Benutzer sollten für WLAN-Gefährdungen sowie für Inhalte und Auswirkungen der WLAN-Richtlinie sensibilisiert werden.

Richtlinie für Administratoren eines WLANs

Daneben sollte eine WLAN-spezifische Richtlinie für Administratoren erstellt werden, die auch als Grundlage für die Schulung der Administratoren dienen kann. Darin sollte festgelegt sein, wer für die Administration der unterschiedlichen WLAN-Komponenten zuständig ist, welche Schnittstellen es zwischen den am Betrieb beteiligten Administratoren gibt, und wann welche Informationen zwischen den Zuständigen fließen müssen. So ist es durchaus üblich, dass für den Betrieb der aktiven Komponenten (Distribution System und Access Points) eine andere Organisationseinheit zuständig ist als für die Betreuung der WLAN-Clients oder für das Identitäts- und Berechtigungsmanagement.

Die WLAN-Richtlinie für Administratoren sollte des Weiteren die wesentlichen Kernaspekte zum Betrieb einer WLAN-Infrastruktur umfassen, wie z. B.

- Festlegung einer sicheren WLAN-Konfiguration und Definition von sicheren Standard-Konfigurationen
- Nutzung eines WLAN-Management-Systems
- Auswahl und Einrichtung von Kryptoverfahren inklusive Schlüsselmanagement
- Regelmäßige Auswertung von Protokolldateien, zumindest von Access Points

- Durchführung von WLAN-Messungen: Die Konfiguration und die Netzabdeckung von Access Points und Clients sollte regelmäßig mittels WLAN-Analysator und Netz-Sniffer kontrolliert werden. Hierbei sollte insbesondere auch nach nicht genehmigten WLAN-Clients und Access Points innerhalb der Organisationsgrenzen gesucht werden.
- Inbetriebnahme von Ersatzsystemen
- Maßnahmen bei Kompromittierung des WLANs

Auch wenn innerhalb einer Institution keine WLANs offiziell installiert sind, sollte trotzdem regelmäßig vom IT-Sicherheitsmanagement veranlasst werden, dass nach ungenehmigt installierten WLAN-Komponenten gescannt wird.

Alle WLAN-Anwender, egal ob Benutzer oder Administratoren, sollten mit ihrer Unterschrift bestätigen, dass sie den Inhalt der WLAN-Sicherheitsrichtlinie gelesen haben und die darin definierten Anweisungen auch einhalten. Ohne diese schriftliche Bestätigung sollte niemand das WLANs nutzen dürfen. Die unterschriebenen Erklärungen sind an einem geeigneten Ort, beispielsweise in der Personalakte, aufzubewahren.

Ergänzende Kontrollfragen:

- Existiert eine aktuelle Sicherheitsrichtlinie für die WLAN-Nutzung?
- Wie wird die Einhaltung der Sicherheitsrichtlinie für die WLAN-Nutzung überprüft?
- Besitzt jeder WLAN-Benutzer ein Exemplar der WLAN-Richtlinie oder ein Merkblatt mit einem Überblick der wichtigsten Sicherheitsmechanismen?
- Ist die Sicherheitsrichtlinie für die WLAN-Nutzung Inhalt der Schulungen zu IT-Sicherheitsmaßnahmen?

M 2.383 Auswahl eines geeigneten WLAN-Standards

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement, Administrator

Im Rahmen der WLAN-Planung ist zunächst eine Ist-Aufnahme durchzuführen, welche der von der Institution betriebenen Systeme in das ISM-Band bei 2,4 GHz sowie in das 5 GHz-Band abstrahlen. Nachdem diese Ist-Aufnahme abgeschlossen wurde, kann daraus ermittelt werden, welcher WLAN-Standard genutzt werden kann. Dabei verwenden die WLAN-Standards IEEE 802.11, IEEE 802.11b und IEEE 802.11g das 2,4 GHz-Band, die Standards IEEE 802.11a und IEEE 802.11h das 5 GHz-Band. Durch die Auswahl des richtigen Frequenzbandes können Störungen des WLANs durch andere von der Institution betriebene Systeme vermieden werden. Nur in den Standards IEEE 802.11 und IEEE 802.11i sind Sicherheitsmechanismen beschrieben.

Neben dieser technischen Betrachtung müssen außerdem die vorhandenen Sicherheitsmechanismen der einzelnen WLAN-Standards gegeneinander abgewogen werden. Generell sollten zur Authentisierung und Verschlüsselung nur als allgemein sicher anerkannte Verfahren eingesetzt werden. Hierbei ist die Verwendung anerkannter kryptografischer Verfahren mit ausreichender Schlüssellänge sowie kollisionsfreier Hash-Verfahren sicherzustellen (siehe auch M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*). Bei Verwendung von WPA oder WPA2 wird die Nutzung von Authentisierungsverfahren mit gegenseitiger Authentisierung empfohlen. Hierbei muss sich der WLAN-Client gegenüber dem Access Point authentisieren und umgekehrt. Hierfür kann entweder ein geheimer Text, der sogenannte Pre-Shared Key, oder das EAP-Framework mit einem RADIUS-Server zur Authentisierung verwendet werden. Bei hohem Schutzbedarf empfiehlt sich die Nutzung von Geräte- und Benutzer-Authentisierung, sodass nur der Institution bekannte (und entsprechend der Sicherheitsrichtlinien konfigurierte) Clients im WLAN zugelassen werden.

WEP unsicher, WPA/WPA2 besser

So verwendet der Standard IEEE 802.11 das als unsicher eingestufte Wired Equivalent Privacy (WEP) mit statischen Schlüsseln. WLANs, in denen WEP zum Einsatz kommt, sollten somit nicht ohne zusätzliche Sicherheitsmaßnahmen in Bereichen eingesetzt werden, in denen vertrauliche Informationen übertragen werden sollen. Hier ist mindestens das von der Wi-Fi Alliance veröffentlichte Wi-Fi Protected Access (WPA) zu wählen. Besser ist die Ergänzung IEEE 802.11i bzw. WPA2 zur Sicherung der WLAN-Kommunikation. Hier wird unter anderem die Verwendung von Pre-Shared Keys mit dem Temporal Key Integrity Protocol (TKIP) zur sicheren Kommunikation im WLAN definiert. IEEE 802.11i selbst schreibt das Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) als zukunftsgerichtetes Verfahren der Authentisierung vor, das durch das Counter Mode Verfahren auch zusätzliche Vertraulichkeit gewährleistet. Ebenso verwendet CCMP den Advanced Encryption Standard (AES) zur Verschlüsselung der Informationen, im Gegensatz zu RC4 in WEP und WPA.

Eine sorgfältige Betrachtung der einzelnen WLAN-Standards, vor allem im Hinblick auf deren Sicherheitsfunktionen, ist unumgänglich und immer durchzuführen. Erst nach einer ausführlichen Bewertung der einzelnen Standards kann eine Festlegung auf einen bestimmten WLAN-Standard erfolgen. Die Entscheidungsgründe müssen dokumentiert werden, damit sie später noch nachvollziehbar sind.

Ergänzende Kontrollfragen:

- Welche Protokolle und Standards wurden für den WLAN-Betrieb ausgewählt?
- Sind die Entscheidungsgründe dokumentiert?

M 2.384 Auswahl geeigneter Kryptoverfahren für WLAN

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement, Administrator

Um einen sicheren Betrieb eines WLANs zu gewährleisten ist, es notwendig, die Kommunikation über die Luftschnittstelle komplett abzusichern. Ohne ausreichende Verschlüsselung besteht die Gefahr, dass unberechtigte Personen über das WLAN übertragene Daten mitlesen können. Ebenso bietet ein nicht ausreichend geschütztes WLAN einen Angriffspunkt auf ein eventuell damit verbundenes LAN. Darüber hinaus ist die Integrität der Daten sicherzustellen, damit Manipulationen an diesen Daten erkannt werden. Ebenso ist eine (gegenseitige) Authentisierung der WLAN-Komponenten untereinander wichtig.

In den WLAN-Standards IEEE 802.11 und 802.11i sind diverse Kryptoverfahren beschrieben, die zur Absicherung eines WLANs verwendet werden können. Diese sind je nach Einsatzgebiet, Schutzbedarf und Größe der Institution auszuwählen und anzuwenden.

Wired Equivalent Privacy (WEP)

WEP ist der älteste und am weitesten verbreitete Verschlüsselungsstandard für WLANs und ist im Standard IEEE 802.11 beschrieben. WEP bietet nur das absolute Minimum an Schutz, um zufälliges Mitlesen oder zufälliges Einbuchen zu verhindern.

WEP veraltet und unsicher

WEP gilt mittlerweile als veraltet und unsicher, da eine Vielzahl von Sicherheitslücken nachgewiesen wurden. WEP ist daher für die Absicherung von WLANs als ungenügend einzustufen und sollte nicht mehr eingesetzt werden.

Falls keinerlei anderen Kryptoverfahren außer WEP zur Verfügung stehen und die WLAN-Komponenten weiter betrieben werden sollen, sollte WEP aktiviert werden. Dann muss die maximale Schlüssellänge gewählt werden und die Schlüssel regelmäßig manuell gewechselt werden (mindestens einmal täglich). Eine solche Entscheidung ist zu dokumentieren und allen Benutzern des WLAN mitzuteilen. Ein solches ungenügend abgesichertes WLAN darf höchstens in einem unkritischen Bereich eingesetzt werden, beispielsweise zum reinen Zugriff auf das Internet. Es ist aber sicher zu stellen, dass über ein WLAN, dass nur durch WEP abgesichert wurde, keine sensiblen Daten übertragen werden oder über die beteiligten WLAN-Komponenten erreichbar sind.

WPA, WPA2 und IEEE 802.11i

IEEE 802.11i gilt als neuer Sicherheitsstandard für WLANs, das in Teilen auch dem Wi-Fi Protected Access 2 (WPA2) der Wi-Fi Alliance entspricht.. Im Gegensatz zu WPA, das dem Draft 3.0 von IEEE 802.11i entspricht und ebenfalls von der Wi-Fi Alliance veröffentlicht wurde, wird in WPA2 und IEEE 802.11i der Advanced Encryption Standard (AES) als Verschlüsselungsalgorithmus verwendet. In WPA, genauso wie in WEP, kommt weiterhin RC4 zum Einsatz. Sowohl WPA als auch WPA2 bzw. IEEE 802.11i bieten mit dem optional anzuwendenden Temporary Key Integrity Protocol (TKIP) durch eine dynamische Schlüsselgenerierung zusätzlichen Schutz. Bei WPA2 und IEEE 802.11i ist darüber hinaus die Verwendung von CCMP als

Implementierungsmethode für AES zur Integritätssicherung zwingend vorgeschrieben.

Nach Möglichkeit sollte ein WLAN flächendeckend einheitlich mit WPA2 unter Verwendung von CCMP (zumindest WPA mit TKIP) abgesichert werden, da hier stärkere Algorithmen zur Verschlüsselung und Integritätssicherung verwendet werden. Schwächere Verfahren sind nach dem Stand der Technik inakzeptabel.

Für die Authentisierung von Benutzern können Pre-Shared Keys (PSK) verwendet werden. Diese werden beim ersten Verbindungsaufbau zur Authentisierung gegenüber einer anderen WLAN-Komponente verwendet. Bei den Pre-Shared Keys sollte darauf geachtet werden, dass diese wesentlich länger sein sollten, als die üblichen sechs bis acht Zeichen, da davon die Sicherheit der Verschlüsselung abhängt. Dieses Verfahren ist allerdings nur für kleinere WLAN-Installationen praktikabel, für große WLANs sollte eine EAP-Methode nach IEEE 802.1X verwendet werden.

Zum besseren Überblick über die verschiedenen Sicherheitsmechanismen dient folgende Tabelle:

	WEP	**WPA**	**802.11i (WPA2)**
Verschlüsselungs-Algorithmus	RC4	RC4	AES
Schlüssellänge	40 bzw. 104 Bit	128 Bit (64 Bit bei der Authentisierung)	128 Bit
Schlüssel	statisch	dynamisch (PSK)	dynamisch (PMK)
Initialisierungsvektor	24 Bit	48 Bit	48 Bit
Datenintegrität	CRC-32	MICHAEL	CCMP

TKIP und CCMP

Das Temporary Key Integrity Protocol (TKIP) basiert als abwärtskompatible Lösung auf WEP, es beseitigt jedoch dessen gröbsten Schwächen. Für TKIP ist in IEEE 802.11i das Problem der mangelhaften Integritätsprüfung in WEP durch den Einsatz des zusätzlichen Verfahrens MICHAEL (zum Message Integrity Check) gelöst worden. TKIP und MICHAEL sind als temporäre Lösung zu verstehen.

CCMP steht für CTR mode (Counter Mode) with CBC-MAC Protocol (Cipher Block Chaining Message Authentication Code). Hierbei wird nicht direkt der Klartext mit AES verschlüsselt, sondern ein aus dem symmetrischen Schlüssel gebildeter Zähler. Das eigentliche Verschlüsselungsergebnis entsteht dann aus der XOR-Verknüpfung eines Blocks des Klartexts mit dem AES-verschlüsselten Zähler. Außerdem wird die Methode Cipher Block Chaining (CBC) zur Integritätssicherung der Daten verwendet. Zur Schlüsselverwaltung und -verteilung wird wieder IEEE 802.1X vorausgesetzt. Die in IEEE 802.11i verwendete Schlüssellänge beträgt 128 Bit.

Extensible Authentication Protocol (EAP)

Als zusätzlicher Schutz der Authentisierung kann das Extensible Authentication Protocol (EAP) gemäß Standard IEEE 802.1X verwendet werden. EAP wird im RFC 3748 genau beschrieben. Der Benutzer meldet sich hier bei einer Authentisierungsinstanz, z. B. an einem RADIUS-Server, an und dieser prüft die Zugangsberechtigung, bevor der Sitzungsschlüssel ausgehandelt wird. EAP unterstützt eine Reihe von Authentisierungsmethoden, so dass auch Zertifikate und Zwei-Faktor-Authentisierungen genutzt werden können.

EAP-Methoden, die in einem WLAN verwendet werden können sind z. B.:

- EAP-TLS

  Bei EAP-TLS, definiert in RFC 2716, wird eine beidseitige Authentisierung anhand von X.509-Zertifikaten durchgeführt. Dazu muss der zu authentisierende Partner beweisen, dass er den privaten Schlüssel kennt, der zu dem öffentlichen Schlüssel gehört, welcher seinem Kommunikationspartner bekannt ist. Folglich müssen Verfahren etabliert werden, die entsprechende Zertifikate verteilen und verwalten können. Eine solche Public Key Infrastructure (PKI) einzurichten und zu betreiben setzt eine sorgfältige Planung voraus (siehe z. B. M 2.232 *Planung der Windows 2000/2003 CA-Struktur*). Der Schlüsselaustausch selbst findet über einen durch TLS gesicherten Tunnel statt.

- EAP-TTLS

  Bei EAP-TTLS wird im Gegensatz zu EAP-TLS auf darauf verzichtet, dass der WLAN-Client ein eigenes Zertifikat besitzen muss. Nur der Server benötigt bei EAP-TTLS ein gültiges Zertifikat. Über den durch TLS gesicherten Tunnel können dann andere, eventuell weniger sichere Verfahren zur Client- bzw. Benutzerauthentisierung benutzt werden. EAP-TTLS ist ebenso wie EAP-TLS ein schlüsselerzeugendes Verfahren, d. h. bei der Kommunikation wird jedes Mal ein neuer Session Key erzeugt, der dann für die Absicherung des Tunnels mittels TLS verwendet wird.

- EAP-PEAP

  Auch EAP-PEAP ist ein schlüsselerzeugendes Verfahren und erfordert, ähnlich wie EAP-TTLS, nur bei dem Authentisierungsserver ein gültiges X.509-Zertifikat. Im Gegensatz zu EAP-TTLS sind zur Client-Authentisierung im gesicherten Tunnel nur andere EAP-Methoden möglich, wie z. B. EAP-MSCHAPv2 oder EAP-TLS. Dabei ist die Kombination mit EAP-MSCHAPv2 für Netze interessant, die hauptsächlich Windows 2000 oder Windows XP als Client-Betriebssystem einsetzen, die diese Methode hier bereits fest enthalten ist.

Weitere EAP-Methoden sind im Standard IEEE 802.1X oder in der Technischen Richtlinie *Sicheres WLAN* des BSI beschrieben.

WPA2 mit EAP

Generell ist es in größeren Installationen sinnvoll, zur Benutzerauthentisierung EAP gemäß IEEE 802.1X zu verwenden. Aktuelle WLAN-Komponenten unterstützen IEEE 802.11i und damit WPA2 bereits. Bei der Beschaffung neuer WLAN-Komponenten ist auf jeden Fall vorher zu prüfen, ob diese auch entsprechende EAP-Methoden unterstützen.

Schlüsselmanagement

Die kryptographischen Schlüssel zum Schutz der Kommunikation oder zur Authentisierung müssen regelmäßig gewechselt werden (siehe M 2.388 *Geeignetes WLAN-Schlüsselmanagement*).

Bei allen WLAN-Komponenten muss darauf geachtet werden, dass diese beim Verbindungsaufbau mit anderen WLAN-Komponenten keine Kryptoverfahren mit geringerer Schutzwirkung als die ausgewählten akzeptieren. Verbindungen mit solchen Komponenten müssen abgelehnt werden.

Ergänzende Kontrollfragen:

- Wurde eine geeignete Verschlüsselungsmethode ausgewählt? Wurde diese Entscheidung dokumentiert?
- Unterstützen alle WLAN-Komponenten den ausgewählten WLAN-Sicherheitsstandard, z. B. IEEE 802.11i, um Problemen bei der Kompatibilität entgegenzuwirken?

M 2.385 Geeignete Auswahl von WLAN-Komponenten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement, Administrator

Zur Auswahl von WLAN-Geräten ist zunächst zu hinterfragen, ob diese in die WLAN-Sicherheitsstrategie hineinpassen. WLAN-Komponenten gibt es in verschiedensten Varianten und Geräteklassen. Diese unterscheiden sich nicht nur in ihrem Leistungsumfang, sondern auch in den Sicherheitsmechanismen und im Bedienkomfort. Zudem stellen sie unterschiedliche Voraussetzungen an Hard- und Software-Komponenten im Einsatzumfeld.

Bei der Vielzahl verschiedener WLAN-Komponenten sind Kompatibilitätsprobleme naheliegend. Wichtige Kriterien für die Auswahl von WLAN-Komponenten sind daher Sicherheit und Kompatibilität.

Anforderungsliste

Wenn beschlossen wurde, innerhalb einer Institution ein WLAN aufzubauen, sollte eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Aufgrund der Bewertung sollten dann die zu beschaffenden Produkten ausgewählt werden. Die Praxis zeigt, dass es aufgrund verschiedener Einsatzanforderungen durchaus sinnvoll sein kann, mehrere Gerätetypen für die Beschaffung auszuwählen. Die Gerätevielfalt sollte aber zur Vereinfachung des Supports eingeschränkt werden. Ein wichtiges Kriterium bei der Beschaffung von WLAN-Komponenten ist die Kompatibilität zu bereits vorhandenen Geräten.

Bei der Beschaffung sollte auch Datendurchsatz und Reichweite hinterfragt werden. Mit externen Antennen kann bei WLAN-Komponenten zusätzlich die Reichweite verbessert werden. Allerdings ist hier sicherzustellen, dass durch die größere Reichweite ein WLAN nicht in Bereiche abstrahlt, in denen es nicht genutzt werden soll oder darf.

Kriterien für Access Points

Bei der Beschaffung von Access Points sollte unter anderem überprüft werden,

- wieviele Kanäle einstellbar sind,
- ob die SSID einstellbar ist,
- ob der SSID-Beacon deaktivierbar ist,
- welche kryptographischen Verfahren implementiert sind (WEP, WPA, WPA2 und weitere),
- ob bei der Authentisierung sowohl der Open System als auch der Shared Key Modus vorgegeben werden kann (letzteres ist leider nicht selbstverständlich),
- inwiefern EAP-Methoden nach IEEE 802.1X unterstützt werden,
- ob eine Administration über sichere Kommunikationswege, z. B. SSH oder SSL, möglich ist und unsichere Protokolle, wie z. B. HTTP oder Telnet, abgeschaltet werden können,
- ob eine IP- bzw. MAC-Adressfilterung möglich ist,

- ob ACLs für die Zugriffe über das WLAN, ein angeschlossenes LAN oder zur Konfiguration der Access Points eingerichtet werden können,
- ob ein Paketfilter integriert ist,
- ob weitere Mechanismen zur Zugriffssteuerung vorhanden sind (Filterung nach verschiedenen Kriterien wie Ports, Applikationen, URLs, etc.),
- ob Tunnel-Protokolle wie PPTP oder IPsec unterstützt werden.

Es sollte unbedingt getestet werden, ob die implementierten kryptographischen Verfahren nicht nur gleich benannt sind, wie bei anderen eingesetzten WLAN-Komponenten, sondern auch korrekt zusammenarbeiten.

Die korrekte Konfiguration der Access Points ist ein wesentlicher Sicherheitsaspekt. Bei einigen Access Points ist eine Konfiguration drahtlos direkt über das WLAN möglich, was von den Herstellern als komfortabel angepriesen wird. Dies birgt aber auch Sicherheitsprobleme, daher sollte darauf verzichtet werden, wenn eine solche Funktionalität aber vorhanden ist, sollte sie zumindest abschaltbar sein (und im Betrieb grundsätzlich abgeschaltet sein). Viele Access Points bieten zur bequemen Konfiguration auch die Möglichkeit, diese über eine serielle oder USB-Schnittstelle an eine Managementkonsole anzuschliessen. Über HTTP oder Telnet können diese dann über das Intranet oder Internet administriert werden. Hierfür ist eine vernünftige Absicherung des Fernzugriffes notwendig, beispielsweise die Absicherung der Kommunikation über SSL oder SSH. Fernzugriffe über das Internet sollten generell kritisch hinterfragt werden.

Der Administrationszugriff auf WLAN-Komponenten sollte nur autorisierten Personen möglich sein. Daher sollte hinterfragt werden, wie dieser abgesichert ist. Wenn dies über Passwörter erfolgt, müssen diese möglichst komplex gewählt werden (siehe M 2.11 *Regelung des Passwortgebrauchs*). Besser ist es, für Administrationszugriffe starke Authentisierungsmethoden einzusetzen (siehe auch M 4.133 *Geeignete Auswahl von Authentikationsmechanismen*).

Die Umsetzung der erforderlichen Sicherheitsregeln an Access Points ist häufig sehr aufwändig. Dazu gehören neben dem Schlüsselmanagement vor allem die notwendigen Einstellungen von verschiedenen Parametern und Optionen. Für einige Access Points gibt es daher mittlerweile Lösungen, um diese innerhalb einer Institution über einen zentralen Server zu steuern. Leider sind dies bisher noch proprietäre Lösungen und werden nur von den WLAN-Komponenten des jeweiligen Herstellers unterstützt.

Da es vor allem bei Netzkoppelelementen aufwendig sein kann, bis der Netzverwalter die korrekte Konfiguration herausgefunden hat, sollte es möglich sein, diese zu speichern.

Die Online-Hilfe und Dokumentation von WLAN-Komponenten sollten sprachlich so formuliert sein, dass zukünftige Benutzer bzw. Administratoren die technischen Beschreibungen nachvollziehen können.

Zusammenwirken mit der zugehörigen Infrastruktur

Im Rahmen der Beschaffung sollten auch das korrekte Zusammenwirken aller WLAN-Komponenten mit der zugehörigen Infrastruktur geprüft werden. Hierzu zählen beispielsweise:

- Die im WLAN genutzte Authentisierungsmethode muss sowohl von den Clients und den Access Points, als auch vom Authentisierungsserver unterstützt werden.
- Falls im WLAN die Authentisierung nach IEEE 802.1X erfolgt, müssen die Access Points die Authentisierungsmethode EAP unterstützen und die mitgeteilten Informationen innerhalb von IEEE 802.1X korrekt verarbeiten.
- Es ist zu prüfen, ob der Authentisierungsserver auf eine eigene Datenbank zur Benutzer-Authentisierung verzichten kann und stattdessen die Authentisierungsanfragen an eine zentrale Benutzerdatenbank mittels sicherer Abfragemethoden durchreichen kann.

Bei der Beschaffung einer größeren WLAN-Installation sind vor der endgültigen Beschaffung entsprechende Teststellungen durchzuführen. Mit Hilfe eines Prüfkatalogs kann die Erfüllung der technischen Anforderungen evaluiert werden. Diese Prüfungen erleichtern eine spätere Durchführung der WLAN-Installation und deren Abnahme.

Ergänzende Kontrollfragen:

- Wurden bei der Auswahl von WLAN-Komponenten Sicherheitsaspekte angemessen berücksichtigt?
- Wurde die Kompatibilität mit bereits vorhandenen WLAN-Komponenten geprüft?

M 2.386 Sorgfältige Planung notwendiger WLAN-Migrationsschritte

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Auf Grund der Schnelllebigkeit der WLAN-Technologie wird sich in der Praxis eine Migration einer bestehenden Installation hin zu neuen Protokollen, Techniken oder Produkten nur selten vermeiden lassen. Dabei ist generell zwischen zwei Migrationsarten zu unterscheiden:

- Migration der Übertragungstechnik (z. B. von IEEE 802.11g nach IEEE 802.11h)
- Migration der WLAN-Sicherheitsmechanismen (z. B. von WEP zu WPA-PSK oder IEEE 802.11i mit IEEE 802.1X)

Im ersten Fall muss der gesamte Planungsprozess für ein WLAN durchlaufen werden, angefangen bei Risikobewertung, bis hin zur Auswahl geeigneter Sicherheitsmaßnahmen.

Im zweiten Fall müssen vorübergehend gegebenenfalls unterschiedliche Sicherheitssysteme parallel betrieben werden und eine erweiterte Konfiguration der Access Points, des Distribution Systems und des Übergabepunktes zum WLAN durchgeführt werden. Die noch nicht migrierten WLAN-Komponenten oder WLAN-Bereiche sind durch entsprechende technische und organisatorische Festlegungen nötigenfalls auf eine eingeschränkte Nutzung zu reduzieren. So kann beispielsweise der Zugriff von noch nicht migrierten Komponenten auf sensible Daten verboten oder der nicht migrierte WLAN-Bereich durch eine zusätzliche DMZ vom restlichen WLAN und LAN abgesichert werden.

Während eines möglicherweise notwendigen Mischbetriebs zweier Sicherheitsmechanismen, z. B. von WPA-PSK bzw. WPA2-PSK und WEP, sind folgende Punkte zu beachten:

- Der Mischbetrieb sollte so kurz wie möglich dauern.
- Falls WEP und Pre-Shared Keys gleichzeitig verwendet werden, so ist verstärkt darauf zu achten, dass die Schlüsselinformationen häufiger (mindestens täglich) gewechselt werden und nur komplexe Passwörter benutzt werden (siehe M 2.388 *Geeignetes WLAN-Schlüsselmanagement*).
- Access Points müssen es erlauben, beide Mechanismen während der Migrationsphase simultan zu betreiben. Access Points, die maximal WEP unterstützen, sind so schnell wie möglich zu ersetzen und aus dem WLAN zu entfernen.
- WLAN-Clients, die lediglich WEP unterstützen (z. B. ein Drucker oder ein PDA) sollten nur eingeschaltet werden, wenn sie benötigt werden. Diese sollten schnellstmöglich durch Clients ersetzt werden, die WPA2 unterstützen.
- Die Konfiguration der WLAN-Komponenten wie einen WLAN-Drucker sollte, sofern möglich, nicht über die Luftschnittstelle erfolgen, sondern über den Konsolen-Port der Komponente.

In jedem Fall sind die einzelnen Migrationsschritte sorgfältig zu planen. Dabei sollte die Migration auch zur Konsolidierung einer gewachsenen WLAN-Infrastruktur genutzt werden und eine Nachschulung der WLAN-Administratoren und WLAN-Benutzer erfolgen. Sofern sich durch die Einführung neuer WLAN-Authentisierungsmechanismen der Anmeldevorgang für die WLAN-Benutzer ändert, sind die Benutzer ebenfalls nachzuschulen. Des Weiteren sollte die WLAN-Benutzerrichtlinie an die neuen Abläufe angepasst werden.

Ergänzende Kontrollfragen:

- Existiert eine Planung für die Migration zweier WLAN-Technologien? Ist die Dauer festgelegt?
- Wurde sichergestellt, dass schwächer geschützte Komponenten keinen Zugriff auf sensible Daten mehr haben?

M 2.387 Installation, Konfiguration und Betreuung eines WLANs durch Dritte

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement, Administrator

Wenn ein WLAN durch einen externen Auftragnehmer installiert, konfiguriert oder betreut werden soll, so sind bei einem WLAN, neben den Empfehlungen in Baustein B 1.11 *Outsourcing*, die im Folgenden beschriebenen Punkte zu beachten:

- Es ist stets zu prüfen, ob eine WLAN-Installation nicht selbst durchgeführt werden kann oder ob dies auch durch die eigenen Mitarbeiter geleistet werden kann. Eine Machbarkeits- und eine Kostenprüfung sollte hierfür durchgeführt werden.
- Die Sicherheitsstrategie und auch die Sicherheitsrichtlinie sollte stets selbst erstellt werden und nicht durch Dritte. Dadurch wird verhindert, dass sich in der Institution niemand mehr ausführlich mit den Sicherheitsaspekten von WLANs auseinandersetzt und somit eventuell notwendige Sicherheitsmaßnahmen vergessen werden. Beratungen und Hilfestellungen durch Dritte in Anspruch zu nehmen ist aber dann sinnvoll, wenn keine internen Ressourcen dafür vorhanden sind.
- Bei der Vergabe einer WLAN-Installation ist ein detailliertes Pflichtenheft zu erstellen. Darin sind alle Mindestanforderungen an die WLAN-Komponenten und alle mit dem WLAN verbundenen Netzteile usw. genau zu definieren. Das Pflichtenheft sollte vertragliche Grundlage bei der Vergabe an einen externen Auftragnehmer sein und später als Prüfgrundlage bei der Abnahme dienen.
- Dem Auftragnehmer ist die Sicherheitsstrategie und die Sicherheitsrichtlinie für den Einsatz eines WLANs vorzulegen. Er muss vertraglich dazu verpflichtet werden, diese einzuhalten und umzusetzen. Dies ist bei der Umsetzung der vertraglich vereinbarten Leistungen regelmäßig zu überprüfen, um frühzeitig eventuelle Probleme zu erkennen. Die Sicherheitsstrategie und die Sicherheitsrichtlinie sollten fester Bestandteil des Pflichtenheftes sein.
- Der Auftragnehmer sollte weitreichende und am besten langjährige Erfahrungen im Aufbau und in der Absicherung eines WLANs haben. Entsprechende Referenzen sind vorzulegen und zumindest stichprobenweise zu prüfen.
- Der Auftragnehmer muss vertraglich dazu verpflichtet werden, die Konfiguration des WLANs und der WLAN-Komponenten, sowie Passwörter, Verbindungsschlüssel und Zugangskennungen und -mechanismen nicht an unbefugte Personen weiterzugeben. Ebenso sollte der Auftragnehmer dazu verpflichtet werden, die durch die Arbeit am übrigen Netz eventuell bekannt gewordenen Informationen und Daten nicht zwischenzuspeichern oder an unbefugte Personen weiterzugeben.

- Vor der Installation eines WLANs durch den Auftragnehmer sind entsprechende Teststellungen durchzuführen. Dabei sollten alle geplanten Sicherheitseinstellungen ausführlich getestet werden. In dieser Phase ist ein eventuell an das WLAN angeschlossene LAN besonders gefährdet und es sollte eine entsprechende Absicherung erfolgen.
- Während der Installation eines WLANs durch den Auftragnehmer sollte darauf geachtet werden, dass keine Hintertüren in das WLAN durch den Auftragnehmer eingebaut werden. Alle Einstellungen und Konfigurationen sind durch den Auftragnehmer genau zu dokumentieren und mit Abschluss der Installation an den Auftraggeber vollständig zu übergeben.
- Nach Abschluss der Installation sollte anhand des Leistungsverzeichnisses eine Abnahme durchgeführt werden. Darüber hinaus können die im Pflichtenheft nach der Vergabe erstellten Ausführungsunterlagen als Prüfungsgrundlage dienen, da hierin beispielsweise Verfahren für Abnahmemessungen spezifiziert sein können.
- Die Abnahme der WLAN-Installation sollte mit Hilfe eines unabhängigen Experten erfolgen, um auch die technischen Details genau überprüfen zu lassen.
- Sofern auch ein Wireless IDS beschafft wurde, müssen entsprechende Testszenarien, die im Vorfeld der Ausschreibung festgelegt wurden, durchgeführt werden. Hier bietet es sich an, das WLAN zunächst in einem Probebetrieb zu fahren. Dabei sollte auch verifiziert werden, ob der gesamte Überwachungsbereich auch über die WLAN-Sensoren erfasst wird. Des Weiteren sollten verschiedene Störfälle simuliert werden.
- Als wesentlicher Schwerpunkt sollte bei der Abnahme zudem die Dokumentation auf Vollständigkeit und eventuelle Inkonsistenzen geprüft werden.
- Sollte das WLAN auch nach der Installation durch einen externen Auftragnehmer betreut werden, so muss der Auftragnehmer auch hier vertraglich verpflichtet werden, alle hierbei bekannt gewordenen Informationen, wie Passwörter, sensible Daten, Konfigurationseinstellungen usw., nicht an unbefugte Personen weiterzugeben. Ebenso sollte ein Notfallvorsorgeplan mit dem Auftragnehmer erstellt werden. Hierbei sollte für jedes möglicherweise im WLAN auftretende Problem der Schweregrad, die Reaktionszeit, die jeweiligen Arbeitsschritte und wer im Notfall informiert werden muss genau definiert werden.

Ergänzende Kontrollfragen:

- Ist dem Auftragnehmer die Sicherheitsstrategie und die Sicherheitsrichtlinie für den WLAN-Einsatz vorgelegt worden?
- Wurde mit dem Auftragnehmer ein Notfallvorsorgeplan für Probleme im WLAN erstellt?

M 2.388 Geeignetes WLAN-Schlüsselmanagement

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Verwendung kryptographischer Sicherheitsmechanismen setzt die vertrauliche, integere und authentische Erzeugung, Verteilung und Installation von geeigneten Schlüsseln voraus (siehe auch M 2.46 *Geeignetes Schlüsselmanagement*). Bei der Verwendung von WEP bzw. WPA-PSK oder WPA2-PSK hängt die Sicherheit des WLANs wesentlich davon ab, dass die verwendeten WLAN-Schlüssel geeignet ausgewählt und nicht kompromittiert wurden. Daher muss ein geeignetes Verfahren zum Schlüsselmanagement ausgewählt werden, passend zu den vorhandenen Kryptomechanismen. Hierbei muss zunächst unterschieden werden zwischen statischem (manuellen) und dynamischem Schlüsselmanagement.

WEP

Bei WEP wird nur ein einziger, statischer Schlüssel verwendet, d. h. in jeder WLAN-Komponente in einem Netz muss derselbe WEP-Schlüssel eingetragen sein. Weiterhin sieht WEP kein dynamisches Schlüsselmanagement vor, so dass die Schlüssel manuell administriert werden müssen. Da WEP-Schlüssel in kürzester Zeit kompromittiert werden können, sollte WEP nicht mehr eingesetzt werden. Falls es aus irgendwelchen Gründen doch eingesetzt wird, müssen die Schlüssel regelmäßig manuell gewechselt werden (mindestens einmal täglich).

WPA / WPA2 mit TKIP oder CCMP

Bei WPA wird TKIP eingesetzt, das die Nutzung dynamischer kryptographischer Schlüssel statt ausschließlich statischer bei WEP erlaubt. Bei IEEE 802.11i (WPA2) kommt CCMP als kryptographisches Verfahren zur Integritätssicherung und zur Verschlüsselung der Nutzdaten hinzu.

TKIP und CCMP sind symmetrische Verfahren, alle Kommunikationspartner müssen daher einen gemeinsamen Schlüssel konfiguriert haben. Dieser Schlüssel wird als Pairwise Master Key (PMK) bezeichnet. Der Pairwise Master Key (PMK) kann über zwei verschiedene Wege auf die beteiligten WLAN-Komponenten gelangen:

- Statische Schlüssel: Der PMK kann (analog zu WEP) manuell als ein statischer Schlüssel, als Pre-Shared Key (PSK) bezeichnet, auf Access Points und Clients konfiguriert werden. Es besteht meist die Möglichkeit den gemeinsamen geheimen Schlüssel auch über Passwörter festzulegen. Diese Passwörter werden über Hash-Funktionen in den PMK umgerechnet. Hat ein solcher PSK eine zu geringe Komplexität (im Sinne der Länge des Schlüssels und der Zufälligkeit der Zeichen), ist er anfällig gegenüber Wörterbuch- bzw. Dictionary-Attacken. Daher sollten diese Passwörter eine hohe Komplexität und eine Länge von mindestens 20 Stellen besitzen. Ab einer gewissen Größe eines WLANs ist das Ausrollen eines neuen Schlüssels mit erheblichen Problemen verbunden.

Die Nutzung der PSK ist in der Kombination mit WPA bzw. WPA2 möglich. Sollte WPA-PSK bzw. WPA2-PSK verwendet werden, ist zu empfehlen, die Schlüssel zum Schutz der Kommunikation oder zur Authentisierung mindestens alle drei bis sechs Monate zu wechseln.

- Dynamische Schlüssel: Eine höhere Sicherheit bietet ein Mechanismus zur dynamischen Schlüsselverwaltung und -verteilung, der dafür sorgt, dass regelmäßig und insbesondere nach einer erfolgreichen Authentifizierung des WLAN-Clients am Access Point ein neuer Schlüssel (PMK) bereitgestellt wird. Für diese Schlüsselverwaltung und -verteilung greift IEEE 802.11i auf einen anderen Standard zurück und zwar auf IEEE 802.1X. Dieser Standard ist zur portbasierten Netzzugangskontrolle in kabelbasierten Netzen entworfen worden. Grundsätzliche Idee in IEEE 802.1X ist, dass die Freischaltung eines Netzports erst dann erfolgt, wenn der Nutzer sich erfolgreich dem Netz gegenüber authentisiert hat. Die Authentisierung erfolgt also auf Schicht 2. Damit so etwas überhaupt funktioniert, spezifiziert IEEE 802.1X eine Schnittstelle zwischen Client, Netzelement und einem Authentisierungssystem. Diese Schnittstelle basiert auf dem Extensible Authentication Protocol (EAP) und einer Adaptierung dieses Protokolls für die Übertragung auf Layer 2 in LAN (als EAP over LAN, EAPOL bezeichnet). Hand in Hand geht damit die Festlegung einer Funktion zur Schlüsselverwaltung und -verteilung.

Generell sollten in regelmäßigen Abständen, mindestens jedoch vierteljährlich, die Schlüsselinformationen bei allen WLAN-Komponenten ausgetauscht werden. Bei größeren Installationen sollte hierfür eine geeignete Funktion in der zentralen WLAN-Management-Lösung enthalten sein, um den Arbeitsaufwand gering zu halten.

Der Wechsel der Schlüsselinformationen an allen WLAN-Komponenten sollte bereits während der Planungsphase genau getestet werden, um dadurch eventuell auftretende Schwierigkeiten zu erkennen.

Ergänzende Kontrollfragen:

- Wurde der Wechsel der Schlüsselinformationen an allen WLAN-Komponenten getestet?
- Gibt es einen Zeitplan für den Wechsel der Schlüsselinformationen?

M 2.389 Sichere Nutzung von Hotspots

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Bei Hotspots handelt es sich um einen räumlich begrenzten Funkbereich, der auf einen Raum, eine Halle oder eine Produktionsstätte begrenzt sein kann. Meistens werden Hotspots explizit für die Nutzung durch fremde Teilnehmer aufgebaut. Ihr Hauptzweck ist üblicherweise der drahtlose Zugang zum Internet. Häufig findet man solche Hotspots in Hotels, Flughäfen, Messehallen, Bahnhöfen und Kongresszentren.

Hotspots sollten immer als unsicheres Netz betrachtet werden, zum einem, da das dort vorhandene Sicherheitsniveau von außen nur schwer einzuschätzen ist und zum anderen, da die meisten Hotspots ihre Dienste in Form von Shared-Networks anbieten. Dadurch kann im Allgemeinen der Zugriff von jedem Endgerät auf jedes andere teilnehmenden Endgerät möglich sein. Ist das Risiko, das bei der Nutzung eines Hotpots entsteht, generell nicht abschätzbar, so ist es auch möglich, die Nutzung von Hotspots durch die WLAN-Sicherheitsrichtlinie vollständig zu verbieten. Dann ist aber auch technisch sicherzustellen, dass ein WLAN-Client nicht auf einen solchen Hotspot zugreifen kann.

Die Betreiber von Hotspots können viel für die Sicherheit der von ihnen angebotenen Funkstrecke und anderen Dienstleistungen tun (siehe M 4.293 *Sicherer Betrieb von Hotspots*), ohne Mitarbeit der Benutzer ist eine vernünftige Absicherung allerdings nicht zu erreichen. Hierzu gehören unter anderem folgende Maßnahmen:

- Die Benutzer sollten nachfragen, welche Sicherheitsvorkehrungen am Hotspot getroffen worden sind, um dessen Sicherheitsniveau und die Vertrauenswürdigkeit des Betreibers einschätzen zu können.
- Vor der Benutzung sollten sie sich nach der Preisgestaltung und der Art der Abrechnung erkundigen. Aus Sicht der Verbraucher ist interessant, wie viel personenbezogene Daten bekannt gegeben werden müssen und wie mit diesen umgegangen wird. Die Benutzer sollten außerdem darauf achten, dass ihre Authentisierungsdaten am Hotspot nicht gespeichert werden oder missbraucht werden können. Die Authentisierung sollte grundsätzlich verschlüsselt erfolgen.
- Jeder Benutzer eines Hotspots sollte sich über seine Sicherheitsanforderungen im Klaren sein und danach entscheiden, ob bzw. unter welchen Bedingungen für ihn eine Nutzung des Hotspots akzeptabel ist.
- Spätestens dann, wenn finanzrelevante, personenbezogene oder andere sensible Daten wie Kreditkartennummern, PINs, Passwörter oder auch E-Mails übertragen werden sollen, muss sichergestellt werden, dass alle notwendigen Sicherheitsmaßnahmen auf dem Client, vor allem Verschlüsselung, aktiviert sind. Als Beispiel wäre hier das sichere Bearbeiten von Emails über eine HTTPS-Webschnittstelle bzw. über die hierfür vorgesehenen sicheren Internetprotokolle (Secure POP, IMAPS, SMTP mit SSL/TLS) zu nennen.

Verschlüsselung nutzen

- Wenn der Betreiber die Verschlüsselung auf der Funkstrecke gewährleistet, könnte prinzipiell auf Verschlüsselung auf der Applikationsebene verzichtet werden. Als zusätzliche Sicherheitsmaßnahme sollte diese aber weiter durchgeführt werden, auch da diese unter eigener Kontrolle steht. Insbesondere Passwörter sollten nie unverschlüsselt über fremde Netze übertragen werden.
- Zum Zugriff auf ein organisationsinternes Netz sollte generell vom WLAN-Client eine verschlüsselte Verbindung über den vertrauenswürdigen Access Point der Institution aufgebaut werden.
- Wenn man sich im Bereich eines Hotspots befindet, diesen aber nicht benutzen möchte, so sollte die WLAN-Schnittstelle am WLAN-Client abgeschaltet sein, um ein zufälliges Einbuchen zu vermeiden.
- Falls der Betreiber für die Authentisierung am Hotspot Zertifikate anbietet, sollten die Benutzer deren Korrektheit überprüfen. Auch wenn dies lästig ist, sollten Angaben wie Fingerprint, Gültigkeitsdauer, Inhaber sowie die Zertifizierungsinstanz des Zertifikates auf Plausibilität überprüft werden.

Ist das Zertifikat korrekt?

- Generell müssen bei allen mobilen Clients, die sich in verschiedene WLANs einbuchen können, weitere lokale Schutzmaßnahmen implementiert werden, wie z. B. Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall, restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene, lokale Verschlüsselung, etc. Weitere Maßnahmen für einen WLAN-Client finden sich in der Maßnahme M 4.297 *Sicherer Betrieb der WLAN-Komponenten*.

Absicherung der Clients

- Für die Nutzung von Hotspots empfiehlt es sich außerdem, spezielle Benutzerkonten mit sicherer Grundkonfiguration und restriktiven Rechten anzulegen. Keinesfalls sollte sich ein Benutzer mit Administratorrechten von seinem Client aus an externen Netzen anmelden.

Ergänzende Kontrollfragen:

- Werden die Benutzer auf die Regelungen und Sicherheitsmaßnahmen hingewiesen, die bei der Nutzung von Hotspots einzuhalten sind?

M 2.390 Außerbetriebnahme von WLAN-Komponenten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Wenn WLAN-Komponenten außer Betrieb genommen werden, müssen alle sensiblen Informationen gelöscht werden. Hierbei müssen insbesondere die Authentikationsinformationen für den Zugang zum WLAN und anderer erreichbarer Ressourcen, die in der Sicherheitsinfrastruktur und anderen Systemen gespeichert sind, entfernt bzw. als ungültig deklariert werden. Dies bedeutet, dass beispielsweise kryptographische Schlüssel sicher gelöscht und Zertifikate für digitale Signaturen gesperrt werden müssen.

Außerbetriebnahme von WLAN-Clients

Als WLAN-Clients findet eine Vielzahl verschiedener Geräte Verwendung. Hierzu zählen unter anderem:

- Laptops
- PDAs, Smartphones und ähnliche Geräte mit WLAN-Unterstützung
- WLAN-fähige Telefone, Drucker und Kameras

Die WLAN-Funktionalität ist typischerweise eine neben diversen anderen Funktionen bei diesen Endgeräten. Bei der Außerbetriebnahme dieser Endgeräte ist daher zu berücksichtigen, ob solche Geräte sicherheitskritische WLAN-Informationen beinhalten, die zu löschen, zu übertragen bzw. zu archivieren sind, z. B.:

- Informationen über den Benutzer des Endgerätes
- Zertifikate bzw. zugehörige private Schlüssel (für Benutzer oder Geräte)
- Kennwörter für WLAN-Zugänge
- Schlüsselmaterial von Authentikationsverfahren wie z. B. WPA-PSK-Schlüssel
- PIM-Daten, also Kontaktinformationen, Termine usw.

Hierfür sind je nach Gerät und Speicherung geeignete Verfahren zur Vernichtung, Löschung oder Wiederverwendung zu nutzen. Bei Zertifikaten ist beispielsweise ein Eintrag in die entsprechende CRL vorzunehmen, um das Zertifikat zu widerrufen.

Falls ein WLAN-Client gestohlen wird, sind mindestens alle oben aufgeführten Informationen zu berücksichtigen, und es ist dafür zu sorgen, dass die Informationen nicht länger zum Zugriff auf WLANs der betroffenen Institution genutzt werden können.

Außerbetriebnahme von Access Points

Bei der Außerbetriebnahme von Access Points ist grundsätzlich das Gleiche zu beachten wie bei WLAN-Clients. Mindestens folgende sicherheitsrelevante Informationen sind, sofern zutreffend, zu löschen, zu übertragen bzw. zu archivieren:

- Pre-Shared Keys (PSK) von WPA bzw. WPA2

- RADIUS-Schlüssel (RADIUS Shared Secrets)
- IPSec-Schlüssel (PSKs bzw. private Schlüssel zu Zertifikaten)
- Benutzerdaten (insbesondere bei integrierten WLAN-Benutzerverwaltungen)
- Konfigurationsinformationen wie z. B. IP-Adressen und Namen von RADIUS-Servern, Name des Access Points selbst, IP-Adresse, SSID

Hierfür sind je nach Gerät und Speicherung geeignete Verfahren zur Vernichtung, Löschung oder Wiederverwendung zu nutzen. Die entsprechenden Verfahren müssen rechtzeitig ausgewählt und getestet werden.

Oft enthalten Access Points weitere Daten (beispielsweise Konfigurationsdaten), die in einem nichtflüchtigen Speicher abgelegt sind, oder sind von außen beschriftet (beispielsweise mit dem Rechnernamen, SSID, IP-Adresse und weiteren technischen Informationen). Diese Informationen sollten nach Möglichkeit vor der Weitergabe des Gerätes entfernt werden, da ein Angreifer auch aus solchen Informationen eventuell Hinweise für mögliche Angriffe ziehen kann.

Es wird empfohlen, anhand der oben gegebenen Empfehlungen eine Checkliste zu erstellen, die bei der Außerbetriebnahme eines Systems abgearbeitet werden kann, damit kein Schritt vergessen wird.

Ergänzende Kontrollfragen:

- Sind geeignete Verfahren zur Vernichtung, Löschung oder Wiederverwendung von sicherheitsrelevanten Informationen auf WLAN-Komponenten festgelegt worden?

M 2.391 Frühzeitige Information des Brandschutzbeauftragten

Verantwortlich für Initiierung: Leiter Haustechnik, Brandschutzbeauftragter

Verantwortlich für Umsetzung: Brandschutzbeauftragter, Haustechnik

Bei allen Arbeiten an Rohr- und Kabeltrassen, die in irgendeiner Form Wanddurchbrüche sowie notwendige Flure, Flucht- und Rettungswege berühren, ist der Brandschutzbeauftragte zu informieren. Diese Information muss schon so deutlich im Vorfeld der eigentlichen Arbeiten erfolgen, dass der Brandschutzbeauftragte ausreichend Gelegenheit hat, alle Aspekte des baulichen vorbeugenden Brandschutzes in die Planung und Durchführung der beabsichtigten Arbeiten einzubringen.

Dem Brandschutzbeauftragten muss, auch während laufender Arbeiten, durch rechtzeitige Information die Gelegenheit gegeben werden, die ordnungsgemäße Ausführung von Brandschutzmaßnahmen kontrollieren zu können, bevor diese durch den Baufortschritt nicht mehr zugänglich sind, z. B. weil eine abgehängte Decke bereits geschlossen worden ist.

Die Einbindung des Brandschutzbeauftragten ist durch entsprechende Organisationsanweisungen sicherzustellen und in den Planungs- und Abnahmeunterlagen der Baumaßnahme zu dokumentieren (siehe auch M 1.6 *Einhaltung von Brandschutzvorschriften*).

Ergänzende Kontrollfragen:

- Ist der Brandschutzbeauftragte über seine Rechte und Pflichten im Zusammenhang mit Arbeiten an Leitungstrassen informiert?
- Gibt es eine schriftlich festgelegte Handlungsanweisung zur Einbindung des Brandschutzbeauftragten in Arbeiten an Leitungstrassen?

M 2.392 Sicherer Einsatz virtueller IT-Systeme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Einführung

Bei einigen Rechner-Plattformen gibt es die Möglichkeit, virtuelle IT-Systeme einzurichten. Das bedeutet, dass auf einem physischen IT-System mehrere Betriebssystem-Instanzen, beispielsweise mehrere Instanzen des gleichen Betriebssystems oder mehrere unterschiedliche Betriebssysteme, praktisch gleichzeitig genutzt werden können. Die hierfür erforderliche Virtualisierungsschicht sorgt in der Regel dafür, dass

- sich jedes virtuelle IT-System für die darin ablaufende Software nahezu wie ein eigenständiger physischer Computer darstellt,
- die einzelnen virtuellen IT-Systeme voneinander isoliert werden und nur über festgelegte Wege miteinander kommunizieren können,
- die einzelnen virtuellen IT-Systeme in geordneter Weise auf die Ressourcen der Hardware zugreifen können.

Abhängig davon, wie die Virtualisierung der Ressourcen realisiert ist, werden diese Funktionen der Virtualisierungsschicht möglicherweise nur eingeschränkt erfüllt. So gibt es beispielsweise Lösungen, bei denen die Betriebssystem-Software leicht angepasst werden muss, bevor sie in einem virtuellen IT-System laufen kann. Ein anderes Beispiel für eingeschränkte Virtualisierung sind Lösungen, bei denen alle virtuellen IT-Systemen auf einem physischen Computer das gleiche Betriebssystem (allerdings verschiedene Instanzen davon) verwenden müssen.

Die Virtualisierungsschicht muss nicht notwendigerweise eine reine Software-Komponente sein. Bei einigen Plattformen unterstützt auch die Hard- oder Firmware die Virtualisierung der Ressourcen. Die Virtualisierungsschicht stellt den virtuellen IT-Systemen in der Regel konfigurierbare Zugriffsmöglichkeiten auf lokale Laufwerke und Netzverbindungen zur Verfügung. Dies erlaubt es den virtuellen IT-Systemen, miteinander und mit fremden IT-Systemen zu kommunizieren.

Virtuelle IT-Systeme (in einigen Fällen auch Virtuelle Maschinen genannt) werden häufig eingesetzt, um den IT-Einsatz zu flexibilisieren oder um die Kapazitäten vorhandener Hardware effizienter zu nutzen. Beispiele für Software-Produkte zur Virtualisierung von IT-Systemen mit x86-Architektur sind Microsoft Virtual PC/Server, Virtuozzo, VMware Workstation/Server und Xen. Im Bereich der zSeries-Großrechner kann eine Virtualisierung beispielsweise über die Nutzung von *Logical Partitions* (LPARs) oder über das Produkt z/VM erfolgen.

Thematische Abgrenzung

Im Bereich der Software-Entwicklung werden die Begriffe *Virtuelle Maschine* und *Virtuelle-Maschinen-Monitor* (VMM) manchmal auch für bestimmte Laufzeitumgebungen, beispielsweise beim Einsatz von Java oder Dot-NET, verwendet. Solche Laufzeitumgebungen werden in dieser Maßnahme nicht betrachtet. Gegenstand der Empfehlungen in dieser Maßnahme sind virtuelle

IT-Systeme, in denen Betriebssysteme ablaufen, die häufig auch direkt auf physischen IT-Systemen zum Einsatz kommen.

Beispiel-Szenario

Als Beispiel wird ein physischer Server S1 betrachtet, auf dem mit Hilfe einer Virtualisierungsschicht die drei virtuellen Server VM1, VM2 und VM3 betrieben werden. Als Basis-Betriebssystem kommt auf dem physischen Server S1 eine Unix-Version zum Einsatz. Die Virtualisierungsschicht ist in diesem Beispiel eine Software-Komponente, die unter Unix läuft. Die beiden virtuellen Server VM1 und VM2 werden mit Windows 2000 betrieben, auf VM3 ist hingegen Unix installiert. Applikationen können sowohl auf den drei virtuellen Servern als auch (unter Umgehung der Virtualisierungsschicht) direkt auf dem Basis-Betriebssystem des physischen Servers S1 ablaufen.

Die folgende Abbildung zeigt ein Schema dieser Beispiel-Konfiguration:

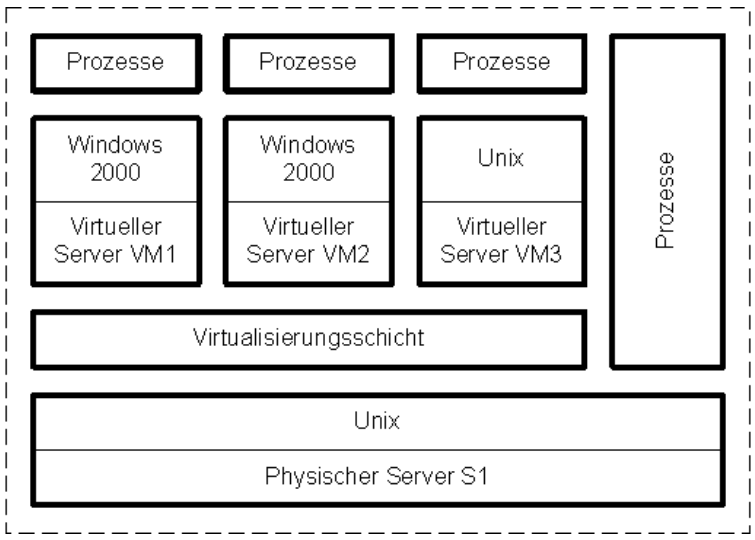


Abbildung: Schema der Beispiel-Konfiguration mit drei virtuellen Servern

Hinweis: Nicht bei allen Lösungen zur Virtualisierung kommt ein vollwertiges Basis-Betriebssystem unterhalb der Virtualisierungsschicht zum Einsatz.

Grundsatzüberlegungen und Konzeption

Zwar verhalten sich virtuelle IT-Systeme für die darin ablaufende Software meist wie nahezu eigenständige physische Computer, dennoch kann die Virtualisierung von Hardware-Ressourcen deutliche Auswirkungen auf die IT-Sicherheit haben.

Einerseits kann die Virtualisierung genutzt werden, um gezielt bestimmten Gefährdungen entgegenzuwirken. Ein Beispiel hierfür ist die verbesserte Trennung unterschiedlicher Programme auf einem Computer voneinander. Dadurch kann unter Umständen die Wahrscheinlichkeit dafür verringert werden, dass bei Problemen in einem Programm auch die anderen Programme beeinträchtigt werden.

Falls Applikationen von eigenständigen physischen IT-Systemen auf virtuelle IT-Systeme verlagert werden, können hierdurch jedoch auch zusätzliche Gefährdungen entstehen. Beispielsweise kann es dabei unter Umständen zu Engpässen bei der Verarbeitungsgeschwindigkeit oder bei der Speicherkapazität kommen.

Zu beachten ist außerdem, dass die Virtualisierungsschicht häufig auch vielfältige Möglichkeiten zur Vernetzung der virtuellen IT-Systeme bietet. Unter Umständen können die einzelnen virtuellen IT-Systeme auf einem physischen Computer dadurch gänzlich unterschiedliche Kommunikationsbeziehungen haben.

Der Einsatz virtueller IT-Systeme muss deshalb gründlich geplant werden. Dabei sollten insbesondere folgende Fragen beantwortet werden:

- Welche Ziele sollen mit der Virtualisierung von IT-Ressourcen erreicht werden?
- Welche Auswirkungen hat dies auf die IT-Risiken?
- Welche Anforderungen bestehen an die Isolation der virtuellen IT-Systeme?
- Können die Anforderungen an Verfügbarkeit und Durchsatz erfüllt werden?
- Ist der Einsatz virtueller IT-Systeme mit den festgelegten (Sicherheits)richtlinien vereinbar?
- Welche zusätzlichen IT-Sicherheitsmaßnahmen werden gegebenenfalls dafür erforderlich?
- Welche Hard- und Software-Komponenten eignen sich für die Virtualisierung?
- Welche Anwendungen sollen sich zukünftig auf virtuelle IT-Systeme stützen?
- Welche Auswirkungen hat dies auf die administrativen und betrieblichen Prozesse?
- Welche Auswirkungen der Virtualisierung von IT-Ressourcen ergeben sich für die Anwender und Benutzer?

Je nach Einsatzszenario sind in der Regel weitere Fragestellungen bei der Planung zu beachten. Die Planung des Einsatzes virtueller IT-Systeme sollte als Entscheidungsvorlage aufbereitet und den zuständigen Führungskräften vorgelegt werden. Die Entscheidung ist zu dokumentieren.

IT-Sicherheitskonzept und IT-Grundschutz-Modellierung

Um eine angemessene Gesamtsicherheit für den IT-Betrieb zu erreichen, müssen alle virtuellen IT-Systeme systematisch im IT-Sicherheitskonzept berücksichtigt werden. In Bezug auf die IT-Grundschutz-Vorgehensweise bedeutet dies insbesondere, dass alle virtuellen IT-Systeme in die IT-Strukturanalyse und in die Modellierung einbezogen werden müssen.

Als Modellierung wird in der IT-Grundschutz-Vorgehensweise die Zuordnung von Bausteinen zu den vorhandenen Zielobjekten (IT-Systeme, Anwendungen, Räume, etc.) bezeichnet. Grundsätzlich erfolgt die Modellierung virtueller IT-Systeme nach den gleichen Regeln wie bei eigenständigen physischen IT-Systemen. Das heißt, es sind die Hinweise in Kapitel 2.2 der IT-Grundschutz-Kataloge zu beachten. Die Zuordnung der IT-Grundschutz-Bausteine richtet sich in erster Linie nach der Funktion des IT-Systems (Server, Client, etc.), nach dem verwendeten Betriebssystem (Unix, Windows, etc.) und nach den darauf betriebenen Applikationen (Datenbank, Web-Server, etc.).

Um die Pflege des IT-Sicherheitskonzepts zu erleichtern und die Komplexität zu reduzieren, sollte besonders sorgfältig geprüft werden, inwieweit die virtuellen IT-Systeme zu Gruppen zusammengefasst werden können. Prinzipiell können auch solche virtuellen IT-Systeme, die sich auf unterschiedlichen physischen Computern befinden, in einer Gruppe zusammengefasst werden. Dies muss jedoch im Einzelfall geprüft werden. Hinweise zur Gruppenbildung finden sich in der IT-Grundschutz-Vorgehensweise.

Falls unterhalb der Virtualisierungsschicht ein vollwertiges und eigenständiges Basis-Betriebssystem zum Einsatz kommt, muss dieses Betriebssystem unabhängig von den virtuellen IT-Systemen in die Modellierung einbezogen werden. Auch hier ist zu prüfen, ob eine Gruppierung vorgenommen werden kann.

Falls die Voraussetzungen für eine Gruppierung von VM1 und VM2 erfüllt sind, könnte die Modellierung für das oben dargestellte Beispiel-Szenario wie folgt aussehen (Auszug):

Baustein	Zielobjekt
B 3.101 Allgemeiner Server	S1
B 3.101 Allgemeiner Server	VM3
B 3.101 Allgemeiner Server	Gruppe aus VM1 und VM2
B 3.102 Server unter Unix	S1
B 3.102 Server unter Unix	VM3
B 3.106 Server unter Windows 2000	Gruppe aus VM1 und VM2

Tabelle: Zuordnung Bausteine zu Zielobjekten

Isolation

Abhängig von Einsatzzweck müssen die einzelnen virtuellen IT-Systeme auf einem physischen Computer mehr oder weniger stark isoliert werden. Das bedeutet, dass auf ein virtuelles IT-Systemen nicht unerlaubt vom Basis-Betriebssystem (sofern vorhanden) und von den anderen virtuellen IT-Systemen aus zugegriffen werden kann.

Eine wirksame Isolation ist bei virtuellen Servern meist wichtiger als beim Einsatz virtueller IT-Systeme auf Arbeitsplatzrechnern. Einen entscheidenden Stellenwert hat die Isolation, wenn virtuelle IT-Systeme dazu genutzt werden, eine Mandantenfähigkeit der Anwendung herzustellen.

Beim Einsatz virtueller IT-Systeme sind deshalb die folgenden Empfehlungen zu beachten:

- Es ist zu prüfen, ob mit der eingesetzten oder geplanten Lösung die Anforderungen an die Isolation der virtueller IT-Systeme erfüllt werden können.
- Sofern unterhalb der Virtualisierungsschicht ein Basis-Betriebssystem eingesetzt wird, muss geprüft werden, ob auch auf diesem Basis-Betriebssystem Anwendungsprogramme laufen dürfen, oder ob dies zu unerwünschten Zugriffsmöglichkeiten auf die virtuellen IT-Systeme führen kann.
- Es muss sichergestellt werden, dass nur die hierfür zuständigen Administratoren die Virtualisierungsschicht konfigurieren sowie virtuelle IT-Systeme einrichten oder löschen können.
- Die Zugriffsrechte auf die virtuellen IT-Systeme müssen gemäß den Anforderungen eingerichtet werden. Als Grundregel gilt auch hier, dass nur die tatsächlich erforderlichen Zugriffsmöglichkeiten erlaubt werden sollten.

Verfügbarkeit und Durchsatz

Der Einsatz mehrerer virtueller IT-Systeme auf einem physischen Computer kann erhebliche Auswirkungen auf die Verfügbarkeit, den Durchsatz und die Antwortzeiten der betriebenen Anwendungen haben. Diese Aspekte sind in der Regel bei Servern deutlich wichtiger als bei Arbeitsplatzcomputern.

Beim Einsatz virtueller IT-Systeme sind im Hinblick auf Verfügbarkeit und Durchsatz die folgenden Empfehlungen zu beachten:

- Der Einsatz virtueller IT-Systeme muss in der Schutzbedarfsfeststellung für den vorliegenden IT-Verbund berücksichtigt werden. Der Schutzbedarf virtueller IT-Systeme kann Auswirkungen auf den Schutzbedarf des physischen Computers haben, auf dem diese virtuellen IT-Systeme betrieben werden.
- Es ist zu prüfen, ob mit der eingesetzten oder geplanten Lösung zur Virtualisierung von Ressourcen die Anforderungen an die Verfügbarkeit und den Durchsatz der Applikationen erfüllt werden können.
- Vor der Überführung in den Wirkbetrieb muss getestet werden, ob beim Einsatz virtueller IT-Systeme akzeptable Antwortzeiten und Verarbeitungsgeschwindigkeiten erreicht werden.
- Die Leistungseigenschaften virtueller Server sollten überwacht werden, damit bei Engpässen zeitnah Anpassungen der Konfiguration vorgenommen werden können. Die Überwachung kann auf der Ebene der virtueller Server oder auf der Ebene des jeweiligen physischen Computers erfolgen. Bei der Festlegung des Überwachungskonzepts ist der Datenschutzbeauftragte zu beteiligen.

Ergänzende Kontrollfragen:

- Ist der Einsatz virtueller IT-Systeme gründlich geplant worden?
- Ist der Einsatz virtueller IT-Systeme in den vorhandenen IT-Sicherheitsrichtlinien definiert?
- Werden alle virtuellen IT-Systeme im IT-Sicherheitskonzept berücksichtigt?

M 2.393 Regelung des Informationsaustausches

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Fachverantwortliche, Mitarbeiter

Informationen können in unterschiedlichen Formen vorliegen. Meistens werden im Bereich des IT-Grundschutzes in Papierform vorliegende Informationen bzw. elektronisch erfasste Informationen betrachtet. Generell müssen alle Informationen angemessen geschützt werden, angefangen von Gedanken und Ideen über geschriebene und gedruckte Darstellungen bis zu elektronischen Nachrichten, Sprach-, Bild oder Videoaufzeichnungen.

Sollen zwischen zwei oder mehreren Kommunikationspartnern Informationen ausgetauscht werden, so sind zu deren Schutz eine Reihe von unterschiedlichen Aspekten zu beachten. Bei jeder Art von Informationsaustausch ist zunächst zu klären,

- wie schutzbedürftig diese sind (siehe M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen*),
- mit wem diese ausgetauscht werden dürfen (siehe M 2.42 *Festlegung der möglichen Kommunikationspartner*) und
- wie diese dabei zu schützen sind.

Hierfür sollten klare und verständliche Regelungen vorliegen, die alle Formen des Informationsaustausches abdecken, also zum Beispiel den mündlichen Austausch ebenso wie Datenaustausch per Datenträger, Mail, Fax, (Mobil-) Telefon oder Internet. Generell sollte sichergestellt sein, dass Informationen nicht in falsche Hände, Augen und Ohren gelangen können und sie nicht unbemerkt verändert werden können.

Allen Mitarbeitern sollte bewusst sein, dass sie dafür verantwortlich sind, interne Informationen angemessen zu schützen. Beispielsweise sollten Ideenskizzen auf Papier nicht in Besprechungsräumen liegengelassen werden, Projektplanungen nicht in der Bahn oder im Restaurant diskutiert werden, Anrufern nicht ungeprüft Interna mitgeteilt werden. Schutzbedürftige Informationen sollten nicht unbeaufsichtigt an Druckern oder Faxgeräten ausgedruckt oder gar liegengelassen werden. Wandtafeln und Whiteboards in Besprechungs-, Schulungs- und Veranstaltungsräumen sollten am Ende der jeweiligen Sitzung gereinigt werden, benutzte Flipchart-Blätter sind gegebenenfalls zu entfernen.

Bei Kommunikationspartnern sollte regelmäßig überprüft werden, ob diese berechtigt sind, die jeweiligen Informationen zu erhalten. So könnte sich unter anderem die Firmenzugehörigkeit, die Post- oder E-Mail-Adresse oder die Faxnummer geändert haben und übermittelte Informationen so die Falschen erreichen. Bei einem Erstkontakt sollte zusätzlich die Identität des Gegenüber überprüft werden, da Visitenkarten auf beliebige Namen ausgestellt werden können. Daher ist es zu empfehlen, bei neuen Geschäftspartnern Rückfrage in deren Behörde oder Unternehmen zu halten oder Referenzen einzuholen.

Wie elektronische Informationen beim Datenaustausch zu schützen sind, ist unter anderem ausführlich in den Bausteinen B 5.2 *Datenträgeraustausch* und B 5.3 *E-Mail* beschrieben.

Ergänzende Kontrollfragen:

- Sind Regelungen bekanntgegeben worden, was beim Datenaustausch zu beachten ist?
- Sind alle Mitarbeiter für mögliche Gefährdungen beim Datenaustausch ausreichend sensibilisiert?

M 3 Maßnahmenkatalog Personal

M 3.26	Einweisung des Personals in den sicheren Umgang mit IT
M 3.27	Schulung zur Active Directory-Verwaltung
M 3.28	Schulung zu Windows 2000 Sicherheitsmechanismen für Benutzer
M 3.29	Schulung zur Administration von Novell eDirectory
M 3.30	Schulung zum Einsatz von Novell eDirectory Clientsoftware
M 3.31	Schulung zur Systemarchitektur und Sicherheit von Exchange 2000 für Administratoren
M 3.32	Schulung zu Sicherheitsmechanismen von Outlook 2000 für Benutzer
M 3.33	Sicherheitsüberprüfung von Mitarbeitern
M 3.34	Einweisung in die Administration des Archivsystems
M 3.35	Einweisung der Benutzer in die Bedienung des Archivsystems
M 3.36	Schulung der Administratoren zur sicheren Installation und Konfiguration des IIS
M 3.37	Schulung der Administratoren eines Apache-Webservers
M 3.38	Administratorenschulung für Router und Switches
M 3.39	Einführung in die zSeries-Plattform
M 3.40	Einführung in das z/OS-Betriebssystem
M 3.41	Einführung in Linux und z/VM für zSeries-Systeme
M 3.42	Schulung des z/OS-Bedienungspersonals
M 3.43	Schulung der Administratoren des Sicherheitsgateways
M 3.44	Sensibilisierung des Managements für IT-Sicherheit
M 3.45	Planung von Schulungsinhalten zur IT-Sicherheit
M 3.46	Ansprechpartner zu Sicherheitsfragen
M 3.47	Durchführung von Planspielen zur IT-Sicherheit
M 3.48	Auswahl von Trainern oder Schulungsanbietern
M 3.49	Schulung zur Vorgehensweise nach IT-Grundschutz
M 3.50	Auswahl von Personal
M 3.51	Geeignetes Konzept für Personaleinsatz und -qualifizierung
M 3.52	Schulung zu SAP Systemen
M 3.53	Einführung in SAP Systeme

M 3.54 Schulung der Administratoren des Speichersystems

M 3.55 Vertraulichkeitsvereinbarungen

M 3.56 Schulung der Administratoren für die Nutzung von VoIP

M 3.57 Szenarien für den Einsatz von VoIP

M 3.58 Einführung in WLAN-Grundbegriffe

M 3.59 Schulung zum sicheren WLAN-Einsatz

M 3.1 Geregelte Einarbeitung/Einweisung neuer Mitarbeiter

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter Personal

Verantwortlich für Umsetzung: Personalabteilung, Vorgesetzte

Neuen Mitarbeitern müssen interne Regelungen, Gepflogenheiten und Verfahrensweisen im IT-Einsatz bekannt gegeben werden. Ohne eine entsprechende Einweisung kennen sie ihre Ansprechpartner zu IT-Sicherheitsfragen nicht, sie wissen nicht, welche IT-Sicherheitsmaßnahmen durchzuführen sind und welche IT-Sicherheitsstrategie die Behörde bzw. das Unternehmen verfolgt. Daraus können Störungen und Schäden für den IT-Einsatz erwachsen. Daher kommt der geregelten Einarbeitung neuer Mitarbeiter eine entsprechend hohe Bedeutung zu.

Die Einarbeitung bzw. Einweisung sollte zumindest folgende Punkte umfassen:

- Alle neuen Mitarbeiter sollten in die Benutzung der für den Arbeitsplatz wesentlichen IT-Systeme und IT-Anwendungen eingewiesen bzw. geschult werden. Außerdem sollten alle neuen Mitarbeiter zu allen relevanten IT-Sicherheitsmaßnahmen sensibilisiert und geschult werden (siehe auch Baustein B 1.13 *IT-Sicherheitssensibilisierung und -schulung*).
- Es sollten alle Ansprechpartner vorgestellt werden, insbesondere die zu IT- und IT-Sicherheitsfragen.
- Die IT-Sicherheitsziele der Behörde bzw. des Unternehmens sollten den neuen Mitarbeitern vorgestellt werden. Alle hausinternen Regelungen und Vorschriften zur IT-Sicherheit müssen erläutert werden. Für alle Arten von potentiellen Sicherheitsvorfällen sollten die Verhaltensregeln und Meldewege dargelegt werden.

Hilfreich zur Durchführung der Einarbeitung ist ein Laufzettel oder eine Checkliste, aus der die einzelnen Aktivitäten und der erreichte Stand der Einarbeitung ersichtlich sind.

Ergänzende Kontrollfragen:

- Wie ist die Einarbeitung von neuem Personal im IT-Bereich geregelt?
- Wie viel Einarbeitungszeit wird jedem neuen Mitarbeiter zur Verfügung gestellt?
- Wird neuen Kollegen ein erfahrener Kollege zur Seite gestellt?

M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen

Verantwortlich für Initiierung: Leiter Personal, Datenschutzbeauftragter, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Personalabteilung, Vorgesetzte

Bei der Einstellung von Mitarbeitern sollen diese verpflichtet werden, einschlägige Gesetze (z. B. § 5 BDSG "Datengeheimnis"), Vorschriften und interne Regelungen einzuhalten. Damit sollen neue Mitarbeiter mit den bestehenden Vorschriften und Regelungen zur IT-Sicherheit bekannt gemacht und gleichzeitig zu deren Einhaltung motiviert werden. Dabei ist es sinnvoll, nicht nur die Verpflichtung durchzuführen, sondern auch die erforderlichen Exemplare der Vorschriften und Regelungen auszuhändigen und den Empfang quittieren zu lassen bzw. für die Mitarbeiter an zentraler Stelle zur ständigen Einsichtnahme vorzuhalten.

Alle Mitarbeiter sollten insbesondere darauf hingewiesen werden, dass alle Arbeitsergebnisse und alle während der Arbeit erhaltenen Informationen ausschließlich zum internen und dienstlichen Gebrauch bestimmt sind.

Ergänzende Kontrollfragen:

- Auf welche Weise wird die Verpflichtung durchgeführt?
- Wird die Verpflichtung schriftlich fixiert?
- Erhält der neue Mitarbeiter die entsprechenden Unterlagen zur Einsicht oder zum Verbleib?
- Ist den Mitarbeitern bekannt, welcher rechtliche Rahmen ihre Tätigkeit bestimmt?

M 3.3 Vertretungsregelungen

Verantwortlich für Initiierung: Leiter Organisation, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Vorgesetzte

Vertretungsregelungen haben den Sinn, für vorhersehbare (Urlaub, Dienstreise) und auch unvorhersehbare Fälle (Krankheit, Unfall, Kündigung) des Personenausfalls die Fortführung der Aufgabenwahrnehmung zu ermöglichen. Daher muss vor Eintritt eines solchen Falles geregelt sein, wer wen in welchen Angelegenheiten mit welchen Kompetenzen vertritt. Dies ist besonders im Bereich der Informationsverarbeitung von Bedeutung, da dafür meist Spezialwissen erforderlich ist und eine zeitgerechte Einarbeitung unkundiger Mitarbeiter für den Vertretungsfall nicht möglich ist.

Für die Vertretungsregelungen sind folgende Randbedingungen einzuhalten:

- Die Übernahme von Aufgaben im Vertretungsfall setzt voraus, dass der Verfahrens- oder Projektstand hinreichend dokumentiert ist.
- Das Benennen eines Vertreters reicht in der Regel nicht aus, es muss überprüft werden, wie der Vertreter zu schulen ist, damit er die Aufgaben inhaltlich übernehmen kann. Stellt sich heraus, dass es Personen gibt, die aufgrund ihres Spezialwissens nicht kurzfristig ersetzbar sind, so bedeutet deren Ausfall eine gravierende Gefährdung des Normalbetriebes. Hier ist es von besonders großer Bedeutung, einen Vertreter zu schulen.
- Es muss festgelegt sein, welcher Aufgabenumfang im Vertretungsfall von wem wahrgenommen werden soll.
- Der Vertreter darf die erforderlichen Zugangs- und Zutrittsberechtigungen nur im Vertretungsfall erhalten.
- Ist es in Ausnahmefällen nicht möglich, für Personen einen kompetenten Vertreter zu benennen oder zu schulen, sollte frühzeitig überlegt werden, welche externen Kräfte für den Vertretungsfall eingesetzt werden können.

Ergänzende Kontrollfragen:

- Wie ist der Vertretungsfall in den einzelnen Organisationseinheiten geregelt?
- Stehen ausreichend kompetente Vertreter zu Verfügung?
- Gab es in der letzten Zeit die Notwendigkeit von unvorhergesehenen Vertretungen?
- Gibt es in einer Organisationseinheit einen "Single Point of Knowledge", eine einzelne Person, die alleine über Spezialwissen verfügt, das für den IT-Einsatz notwendig ist?

M 3.4 Schulung vor Programmnutzung

Verantwortlich für Initiierung: Leiter Personal, Vorgesetzte

Verantwortlich für Umsetzung: Vorgesetzte, Verantwortliche der einzelnen IT-Anwendungen

Durch unsachgemäßen Umgang mit IT-Anwendungen hervorgerufene Schäden können vermieden werden, wenn die Benutzer eingehend in die IT-Anwendungen eingewiesen werden. Daher ist es unabdingbar, dass die Benutzer vor der Übernahme IT-gestützter Aufgaben ausreichend geschult werden. Dies betrifft sowohl die Nutzung von Standardprogrammpaketen als auch von speziell entwickelten IT-Anwendungen.

Darüber hinaus müssen auch bei umfangreichen Änderungen in einer IT-Anwendung Schulungsmaßnahmen durchgeführt werden.

Stehen leicht verständliche Handbücher zu IT-Anwendungen bereit, so kann anstelle der Schulung auch die Aufforderung stehen, sich selbstständig einzuarbeiten. Eine wesentliche Voraussetzung dazu ist allerdings die Bereitstellung ausreichender Einarbeitungszeit.

Ergänzende Kontrollfragen:

- Werden Mitarbeiter, die eine IT-gestützte Aufgabe neu übernehmen sollen, ausreichend geschult? Wird ein Schulungsplan für die Einführung einer neuen IT-Anwendung erstellt?
- Welche IT-Anwendungen sind seit der letzten Überprüfung neu hinzugekommen? Wie wurden die Mitarbeiter eingearbeitet? Welche Schulungsveranstaltungen haben Mitarbeiter seitdem besucht?

M 3.5 Schulung zu IT-Sicherheitsmaßnahmen

Verantwortlich für Initiierung: Vorgesetzte, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Vorgesetzte, IT-Sicherheitsmanagement

Wie sich an vielen konkreten Beispielen wie den Schadensstatistiken von Elektronik-Versicherern belegen lässt, resultieren IT-Schäden oft schlicht aus der Unkenntnis elementarer Sicherheitsmaßnahmen. Um dies zu verhindern, ist jeder einzelne Mitarbeiter zum sorgfältigen Umgang mit der IT zu schulen und zu motivieren. Nur durch die Vermittlung der notwendigen Kenntnisse kann ein Verständnis für die erforderlichen IT-Sicherheitsmaßnahmen geweckt werden.

Im Folgenden werden die Kernthemen, die bei einer Schulung zu IT-Sicherheitsmaßnahmen vermittelt werden sollten, vorgestellt. Eine ausführliche und zielgruppengerichtete Beschreibung von Schulungsinhalten findet sich in M 3.45 *Planung von Schulungsinhalten zur IT-Sicherheit*.

- **Die mitarbeiterbezogenen IT-Sicherheitsmaßnahmen**

  Zu diesem Thema sollen die IT-Sicherheitsmaßnahmen vermittelt werden, die in einem IT-Sicherheitskonzept erarbeitet wurden und von den einzelnen Mitarbeitern umzusetzen sind. Dieser Teil der Schulungsmaßnahmen hat eine große Bedeutung, da viele IT-Sicherheitsmaßnahmen erst nach einer entsprechenden Schulung und Motivation effektiv umgesetzt werden können.

- **Die produktbezogenen IT-Sicherheitsmaßnahmen**

  Zu diesem Thema sollen die IT-Sicherheitsmaßnahmen vermittelt werden, die inhärent mit einem Softwareprodukt verbunden sind und häufig bereits im Lieferumfang enthalten sind. Dies können neben Passwörtern zur Anmeldung, der Pausenschaltung durch Bildschirmschoner auch Möglichkeiten zur Verschlüsselung von Dokumenten oder Datenfeldern sein. So können beispielsweise Hinweise und Empfehlungen über die Strukturierung und Organisation von Dateien den Aufwand zu Datensicherung deutlich reduzieren.

- **Das Verhalten bei Auftreten eines Computer-Virus**

  Hier soll den Mitarbeitern vermittelt werden, wie mit Computer-Viren umzugehen ist. Mögliche Inhalte dieser Schulung sind (siehe M 6.23 *Verhaltensregeln bei Auftreten eines Computer-Virus*):

  - Erkennen des Computer-Virusbefalls
  - Wirkungsweise und Arten von Computer-Viren
  - Sofortmaßnahmen im Verdachtsfall
  - Maßnahmen zur Eliminierung des Computer-Virus
  - Vorbeugende Maßnahmen

- **Der richtige Einsatz von Passwörtern**

  Hierbei sollen die Bedeutung des Passwortes für die IT-Sicherheit sowie die Randbedingungen erläutert werden, die einen wirksamen Einsatz eines Passwortes erst ermöglichen (siehe auch M 2.11 *Regelung des Passwortgebrauchs*).

- **Die Bedeutung der Datensicherung und deren Durchführung**

  Die regelmäßige Datensicherung ist eine der wichtigsten IT-Sicherheitsmaßnahmen in jedem IT-Verbund. Vermittelt werden soll das Datensicherungskonzept (siehe Baustein B 1.4 *Datensicherungskonzept*) der Behörde bzw. des Unternehmens und die von jedem einzelnen durchzuführenden Datensicherungsaufgaben. Besonders wichtig ist dies für solche Bereiche, in denen Benutzer selbst die Datensicherungen durchführen müssen.

- **Der Umgang mit personenbezogenen Daten**

  An den Umgang mit personenbezogenen Daten sind besondere Anforderungen zu stellen. Mitarbeiter, die mit personenbezogenen Daten arbeiten, sind für die gesetzlich erforderlichen Sicherheitsmaßnahmen zu schulen. Dies betrifft beispielsweise den Umgang mit Auskunftsersuchen, Änderungs- und Verbesserungswünschen der Betroffenen, gesetzlich vorgeschriebene Fristen zur Datenlöschung, Schutz der Vertraulichkeit und die Übermittlung der Daten.

- **Die Einweisung in Notfallmaßnahmen**

  Sämtliche Mitarbeiter (auch nicht unmittelbar mit IT befasste Personen, wie Pförtner oder Wachpersonal) sind in bestehende Notfallmaßnahmen einzuweisen. Dazu gehört die Erläuterung der Fluchtwege, die Verhaltensweisen bei Feuer, der Umgang mit Feuerlöschern, das Notfall-Meldesystem (wer als erstes wie zu benachrichtigen ist) und der Umgang mit dem Notfall-Handbuch.

- **Vorbeugung gegen Social Engineering**

  Die Mitarbeiter sollen auf die Gefahren des Social Engineering hingewiesen werden. Die typischen Muster solcher Versuche, über gezieltes Aushorchen an vertrauliche Informationen zu gelangen, ebenso wie die Methoden, sich dagegen zu schützen, sollten erläutert werden. Da Social Engineering oft mit der Vorspiegelung einer falschen Identität einhergeht, sollten Mitarbeiter regelmäßig darauf hingewiesen werden, die Identität von Gesprächspartnern zu überprüfen und insbesondere am Telefon keine vertraulichen Informationen weiterzugeben.

- **Sensibilisierung für IT-Sicherheit**

  Jeder Mitarbeiter ist auf die Bedeutung von IT-Sicherheit hinzuweisen. Ein geeigneter Einstieg in die Sensibilisierung ist es beispielsweise, die Abhängigkeit der Behörde bzw. des Unternehmens und damit der Arbeitsplätze von dem reibungslosen Funktionieren der IT-Systeme aufzuzeigen. Darüber hinaus ist der Wert von Informationen herauszuarbeiten, insbesondere unter den Gesichtspunkten Vertraulichkeit,

Integrität und Verfügbarkeit. Diese Sensibilisierungsmaßnahmen sind in regelmäßigen Zeitabständen zu wiederholen.

Bei der Durchführung von Schulungen sollte immer beachtet werden, dass es nicht reicht, einen Mitarbeiter einmal während seines gesamten Arbeitsverhältnisses zu schulen. Für nahezu alle Formen von Schulungen - insbesondere Front-Desk-Schulungen - gilt, dass sehr viele neue Informationen auf die Teilnehmer einstürzen. Diese gelangen nur zu einem kleinen Teil ins Langzeitgedächtnis, 80% sind meist schon bei Schulungsende wieder vergessen.

Daher sollten Mitarbeiter immer wieder zu Themen der IT-Sicherheit geschult bzw. sensibilisiert werden. Dies kann beispielsweise

- in kürzeren Veranstaltungen zu aktuellen IT-Sicherheitsthemen,
- im Rahmen regelmäßiger Veranstaltungen wie Abteilungsbesprechungen, oder
- durch interaktive Schulungsprogramme, die allen Mitarbeitern zur Verfügung stehen,

erfolgen.

Ergänzende Kontrollfragen:

- Zu welchen Themen zu IT-Sicherheitsmaßnahmen wurde schon geschult?
- Werden neue Mitarbeiter in die IT-Sicherheitsmaßnahmen eingewiesen?
- Welche Schulungsmaßnahmen werden in welchen Intervallen angeboten?
- Decken die Inhalte der Schulungsmaßnahmen die erforderlichen Gebiete ab?

M 3.6 Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern

Verantwortlich für Initiierung: Leiter Personal, Vorgesetzte, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Personalabteilung, Vorgesetzte

Verlässt ein Mitarbeiter die Institution oder wechselt die Funktion, so ist zu beachten:

- Vor dem Weggang ist eine rechtzeitige Einweisung des Nachfolgers durchzuführen. Dafür ist es wünschenswert, dass sich die Arbeitszeiträume wenigstens kurz überschneiden.
- Von dem Ausscheidenden sind sämtliche Unterlagen (wie auch entliehene institutionseigene Bücher), ausgehändigte Schlüssel, ausgeliehene IT-Geräte (z. B. tragbare Rechner, Speichermedien, Dokumentationen) zurückzufordern. Insbesondere sind die Behörden- bzw. Firmenausweise sowie sonstige Karten zur Zutrittsberechtigung einzuziehen. Ferner sind bei biometrischen (z. B. Irisscanner, Fingerabdrücke und Handrückenerkennung) entsprechende Zutrittsberechtigungen zu löschen bzw. auf die getroffene Vertreterregelung anzupassen.
- Es sind sämtliche für den Ausscheidenden eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen. Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt (z. B. mittels eines gemeinsamen Passwortes), so ist nach Ausscheiden einer der Personen die Zugangsberechtigung zu ändern.
- Vor der Verabschiedung sollte noch einmal explizit darauf hingewiesen werden, dass alle Verschwiegenheitserklärungen weiterhin in Kraft bleiben und keine während der Arbeit erhaltenen Informationen weitergegeben werden dürfen.
- Ist die ausscheidende Person ein Funktionsträger in einem Notfallplan, so ist der Notfallplan zu aktualisieren.
- Sämtliche mit Sicherheitsaufgaben betrauten Personen, insbesondere der Pförtnerdienst, sind über den Weggang und Funktionsänderungen von Mitarbeitern zu unterrichten.
- Ausgeschiedenen Mitarbeitern ist der unkontrollierte Zutritt zum Behörden- oder Firmengelände, insbesondere zu Räumen mit IT-Systemen zu verwehren. Auch bei Funktionsänderungen muss unter Umständen die Zutrittsberechtigung zu bestimmten Räumlichkeiten wie Serverräumen entzogen werden.
- Optional kann sogar für den Zeitraum zwischen Aussprechen einer Kündigung und dem Weggang der Entzug sämtlicher Zugangs- und Zugriffsrechte auf IT-Systeme sowie darüber hinaus auch das Verbot, schützenswerte Räume zu betreten, ausgesprochen werden.

Als ein praktikables Hilfsmittel haben sich Laufzettel erwiesen, auf denen die einzelnen Aktivitäten des Ausscheidenden vorgezeichnet sind, die er vor Verlassen der Behörde bzw. des Unternehmens zu erledigen hat.

Ergänzende Kontrollfragen:

- Wird das Ausscheiden eines Mitarbeiters geordnet durchgeführt?
- Werden die zuständigen Stellen über das Ausscheiden eines Mitarbeiters unterrichtet?
- Wie wird sichergestellt, dass sämtliche Zugangsberechtigungen und Zugriffsrechte einer ausscheidenden Person entzogen und gelöscht werden?

M 3.7 Anlaufstelle bei persönlichen Problemen

Verantwortlich für Initiierung: Leiter Personal, Personalrat/Betriebsrat

Verantwortlich für Umsetzung: Personalabteilung, Personalrat/Betriebsrat

Vertrauenspersonen benennen

Für eine unzureichende Aufgabenerfüllung können oftmals persönliche Probleme eines Arbeitnehmers ursächlich sein. Als Probleme lassen sich beispielsweise hohe Schulden, Suchtkrankheiten aber auch Schwierigkeiten am Arbeitsplatz (Über-/Unterforderung, Mobbing) aufzählen. Um dem Betroffenen bei der Bewältigung dieser Probleme zu helfen, kann es in vielen Fällen hilfreich sein, wenn eine Vertrauensperson zur Verfügung steht. Dieser Ansprechpartner sollte dabei sowohl die Interessen des Betroffenen im Auge haben und konkrete Hilfestellung anbieten als auch die Interessen des Unternehmens bzw. Behörde wahren und gemeinsam mit dem Betroffenen nach Lösungsmöglichkeiten suchen.

An diese Vertrauensperson müssen sich aber auch Vorgesetzte und Kollegen wenden können, wenn wiederholt Auffälligkeiten Dritter wahrgenommen wurden, die auf eine verminderte Zuverlässigkeit schließen lassen. Die Vertrauensperson muss dann die Möglichkeit haben, sich an den Betroffenen zu wenden und Hilfe anzubieten.

Eine solche Stelle können Personalrat, Betriebsrat, Betriebsärzte einnehmen. Die Einrichtung einer solchen Anlaufstelle ist allen Mitarbeitern bekannt zu geben. Externe Stellen sind zum Beispiel die Beratungsstellen der gesetzlichen Krankenkassen.

Ergänzende Kontrollfragen:

- An wen können sich Mitarbeiter bei persönlichen Problemen wenden?

M 3.8 Vermeidung von Störungen des Betriebsklimas

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter Personal, Personalrat/Betriebsrat

Verantwortlich für Umsetzung: Vorgesetzte, Personalabteilung, Personalrat/Betriebsrat

Durch ein positives Betriebsklima werden die Mitarbeiter einerseits zur Einhaltung von IT-Sicherheitsmaßnahmen motiviert, andererseits wird die Gefahr von fahrlässigen oder vorsätzlichen Handlungen reduziert, die den IT-Betrieb stören können. Störungen des Betriebsklimas können dabei eine Vielzahl von inner- und außerbetrieblichen Ursachen haben, treten jedoch häufig bei gravierenden innerbetrieblichen Veränderungen auf. Beispiele für solche Veränderungen sind Umstrukturierungen, Sanierungen, Verkauf oder Fusionen von Organisationseinheiten und Outsourcing-Vorhaben. Diese können das Betriebsklima negativ beeinflussen, da sie meistens Ängste unterschiedlicher Art (z. B. Kompetenzverlust, Versagensängste, Arbeitsplatzverlust) hervorrufen. Diese können besser bewältigt werden, wenn das Betriebsklima schon vor den Veränderungen möglichst gut ist.

Auch unter IT-Sicherheitsaspekten sollte daher versucht werden, ein positives Betriebsklima zu erreichen. Die Vielzahl der Möglichkeiten kann hier nicht angeführt werden, es sei lediglich eine Auswahl möglicher Maßnahmen genannt, deren Angemessenheit im Einzelnen zu prüfen wäre:

- Einrichtung eines Sozialraums,
- Vermeidung von Überstunden,
- Vermeidung von großen Resturlaubsansprüchen,
- Einhaltung von Pausenzeiten,
- geregelte Aufgabenverteilung,
- gleichmäßige Arbeitsauslastung,
- leistungsgerechte Bezahlung,
- bestehende Vertreterregelung.

Kommunikation

Kommunikationsprobleme in einer Organisation führen fast zwangsläufig auch zu Sicherheitsproblemen. Dies kann im Extremfall zu bewussten Sicherheitsverletzungen führen. Wenn die Benutzer Sicherheitsmaßnahmen nur als "lästig" empfinden, weil sie nicht über deren Zweck informiert worden sind, kann das bereits dazu führen, dass diese umgangen werden.

Auch das Überbringen schlechter Nachrichten muss möglich sein, ohne dass der Bote deswegen Sanktionen befürchten muss. Es sollte ein Betriebsklima vorhanden sein, in dem es für jeden Betroffenen möglich ist, Sicherheitsvorfälle innerhalb des eigenen Unternehmens bzw. der eigenen Behörde zu melden, so dass diese auch offen angegangen werden können.

Motivation der Mitarbeiter

Mitarbeiter können nicht nur über finanzielle Anreize motiviert werden, wichtig ist vor allem die Anerkennung ihrer Arbeit. Mitarbeiter sollten, wo immer möglich, in Entscheidungen mit einbezogen werden. Zumindest sollten sie über die Gründe für die getroffenen Entscheidungen informiert werden, damit sie auch an deren Umsetzung aktiv mitwirken.

Häufig äußert sich z. B. Protest gegen die Auswahl bestimmter Hard- oder Software darin, dass die Benutzer zu zeigen versuchen, dass die aufgezwungene Hard- oder Software nicht so sicher ist, wie die von ihnen präferierte.

Outsourcing

Das Betriebsklima und das Verhalten von Mitarbeitern kann besonders bei großen Veränderungen, wie etwa bei Outsourcing-Vorhaben, von besonderer Bedeutung sein: unzufriedene oder verärgerte Mitarbeiter können ein solches Vorhaben zum Scheitern verurteilen (z. B. Kündigung von Know-how-Trägern in kritischen Phasen der Veränderung oder bewusstes Ignorieren von Sicherheitsanweisungen), was für das Unternehmen in Folge existenzbedrohend sein kann. Bei größeren Umstrukturierungen oder Outsourcing-Vorhaben ist die Beachtung folgender Aspekte empfehlenswert:

Mitarbeiter einbeziehen

- Die Mitarbeiter sollten frühzeitig in Entscheidungsprozesse wie die Auswahl eines Outsourcing-Dienstleisters eingebunden werden. Im weiteren Projektverlauf sollten sie an der Gestaltung von eventuellen Übernahmeverträgen beteiligt werden.
- Die Mitarbeiter sollten umfassend und frühzeitig über Veränderungen informiert werden und einen Ansprechpartner für Probleme und Fragen haben. Information durch die Zeitung statt durch die Firmen- oder Behördenleitung schafft Misstrauen, zerstört Vertrauen und bereitet Spekulationen und Gerüchten den Boden.
- Bei organisatorischen Veränderungen sollten den betroffenen Mitarbeitern Zukunftsperspektiven aufgezeigt werden. Oftmals sind Outsourcing-Dienstleister darauf angewiesen, dass ein möglichst hoher Anteil der Mitarbeiter des auszulagernden Bereichs zu ihnen wechselt. Nur so kann eine befriedigende Dienstleistungsqualität garantiert werden. Mitarbeiter, die Zukunftsangst haben oder sich unfair behandelt fühlen, lassen in ihrer Arbeitsqualität nach oder verlassen sogar vorzeitig das Unternehmen.
- Anspruchsvolle oder belastende Tätigkeiten, die im Rahmen von Umstrukturierungen nicht zu vermeiden sind, sollten ausreichend gewürdigt und anerkannt werden. Die erforderliche Mehrarbeit sollte honoriert werden.

Ergänzende Kontrollfragen:

- Wie wird das Betriebsklima von den Mitarbeitern beurteilt?
- Wie beurteilen die Vorgesetzten das Betriebsklima?
- Welche Punkte, die das Betriebsklima negativ beeinflussen, werden am häufigsten genannt?
- Gibt es bei größeren Umstrukturierungen einen Verantwortlichen, der für die betroffenen Mitarbeiter als Ansprechpartner zur Verfügung steht?
- Werden die Mitarbeiter in den Veränderungsprozess mit einbezogen und können eigene Vorschläge eingebracht werden?

M 3.9 Ergonomischer Arbeitsplatz

Verantwortlich für Initiierung: Leiter Haustechnik, Personalrat/Betriebsrat

Verantwortlich für Umsetzung: Vorgesetzte, Personalrat/Betriebsrat, Benutzer

Für den sinnvollen und effektiven Einsatz der IT ist es neben der klaren Beschreibung von Aufgaben, Pflichten, Rechten und Verantwortlichkeiten erforderlich, dafür zu sorgen, dass die Nutzung der IT in optimaler Weise erfolgen kann.

Der Arbeitsplatz ist ergonomisch zu gestalten. Stuhl, Tisch, Bildschirm und Tastatur müssen individuell einstellbar sein, um eine möglichst fehlerfreie Bedienung der IT zu ermöglichen und zu fördern. Das beinhaltet u. a., dass Rückenlehne, Sitzhöhe und Sitzfläche des Stuhls verstellbar sein müssen, aber auch, dass die Arbeitsmittel so angeordnet werden können, dass für die jeweilige Arbeitsaufgabe eine möglichst geringe Belastung entsteht.

Ein entsprechend ausgestatteter Arbeitsplatz erleichtert es auch, IT-Sicherheitsmaßnahmen einzuhalten. Gibt es verschließbare Schreibtische oder Schränke, so können Datenträger, Dokumentationen, Unterlagen und Zubehör darin verschlossen werden.

Auch die am Arbeitsplatz eingesetzten IT-Systeme müssen ergonomisch aufgestellt werden. So sollte beispielsweise direkte Lichteinstrahlung auf den Bildschirm aus ergonomischen Gründen vermieden werden. Außerdem sollte an IT-Systeme auch ein ungestörtes Arbeiten möglich sein, also beispielsweise so, dass den Benutzern nicht ständig andere Personen über die Schulter blicken. Dies ist auch sinnvoll, um unbefugtes Einsehen von Informationen zu vermeiden.

Weitere Hinweise sind den Empfehlungen der Berufsgenossenschaften oder Arbeitsschutzexperten zu entnehmen.

Ergänzende Kontrollfragen:

- Sind die Arbeitsplätze ergonomisch gestaltet?
- Beklagen sich Benutzer von IT-Systemen über unzureichende ergonomische Bedingungen?

M 3.10 Auswahl eines vertrauenswürdigen Administrators und Vertreters

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter Personal, Leiter IT, TK-Anlagen-Verantwortlicher, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: -

Den IT-System- oder TK-Anlagen-Administratoren und deren Vertretern muss vom Betreiber großes Vertrauen entgegengebracht werden können. Sie haben - in Abhängigkeit vom eingesetzten System - weitgehende und oftmals alle Befugnisse. Administratoren und ihre Vertreter sind in der Lage, auf alle gespeicherten Daten zuzugreifen, gegebenenfalls zu verändern und Berechtigungen so zu vergeben, dass erheblicher Missbrauch möglich wäre.

Administratoren für IT-Systeme und deren Vertreter müssen sorgfältig ausgewählt werden. Sie müssen regelmäßig darüber belehrt werden, dass die Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen.

Da der Administrator hinsichtlich der Funktionsfähigkeit der eingesetzten Hard- und Software eine Schlüsselrolle inne hat, muss auch bei seinem Ausfall die Weiterführung seiner Tätigkeiten gewährleistet sein. Hierzu müssen die benannten Vertreter über den aktuellen Stand der Systemkonfiguration verfügen sowie Zugriff auf die für die Administration benötigten Passwörter, Schlüssel und Sicherheitstoken haben.

Hat ein Unternehmen oder eine Behörde mehrere Administratoren mit vergleichbaren IT-Systemkenntnissen, so können sich diese auch wechselseitig vertreten, wenn diese dafür noch freie Kapazitäten haben. In allen Bereichen, in denen nur ein Administrator hauptverantwortlich IT-Systeme betreut, sollten zwei Stellvertreter eingearbeitet werden, da bei längerer Abwesenheit des Administrators erfahrungsgemäß auch der Stellvertreter zeitweise nicht für Administrationsaufgaben zur Verfügung steht.

Um die Funktionsfähigkeit des IT-Betriebs zu gewährleisten, muss insbesondere bei bevorstehenden Personalveränderungen oder Veränderungen der Organisationsstruktur geprüft werden, ob die erforderlichen Administrationstätigkeiten auch durch die benannten Administratoren und deren Vertreter bewältigt werden können.

Insbesondere bei bevorstehenden Umzügen kann es durch Administrationsaufgaben an einem weiteren Standort zu einem erheblichen höheren Arbeitsaufkommen des Administrators kommen. Auch in solchen Fällen muss sichergestellt sein, dass der Produktionsbetrieb am bisherigen Standort bis zum Zeitpunkt des Umzugs nicht beeinträchtigt wird.

Ergänzende Kontrollfragen:

- Wie wurde die Zuverlässigkeit des Administrators bzw. seines Stellvertreters festgestellt?

M 3.11 Schulung des Wartungs- und Administrationspersonals

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter Personal, Leiter IT, TK-Anlagen-Verantwortlicher, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Vorgesetzte

Wartungs- und Administrationspersonal benötigt detaillierte Kenntnisse über die eingesetzten IT-Komponenten. Daher sollte es mindestens soweit geschult werden, dass

- alltägliche Administrationsarbeiten selbst durchgeführt,
- einfache Fehler selbst erkannt und behoben,
- Datensicherungen regelmäßig selbsttätig durchgeführt,
- die Eingriffe von externem Wartungspersonal nachvollzogen und
- Manipulationsversuche oder unbefugte Zugriffe auf die Systeme erkannt und rasch behoben

werden können.

Entsprechende Schulungen werden in der Regel von den Herstellern der IT-Systeme bzw. TK-Anlagen angeboten. Administratoren von TK-Anlagen sollten außerdem in der Lage sein,

- das Betriebsverhalten der TK-Anlage mit Hilfe der Kontrollanzeigen an den Geräten zu beurteilen,
- die TK-Anlage selbständig außer- und in Betrieb nehmen zu können.

Ergänzende Kontrollfragen:

- Wurden die Administratoren spezifisch geschult?

M 3.12 Information aller Mitarbeiter über mögliche TK-Warnanzeigen, -symbole und -töne

Verantwortlich für Initiierung: TK-Anlagen-Verantwortlicher, IT-Sicherheitsmanagement, Personalrat/Betriebsrat

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Die Bedeutung der Warnanzeigen, -töne und -symbole der TK-Anlage sollte allen Mitarbeitern bekannt sein. Hierzu zählen insbesondere:

- Aufmerksamkeitston für direktes Ansprechen,
- Aufschalte-Warnton,
- Freisprechanzeige,
- Anzeige für aktiviertes direktes Ansprechen,
- Anzeige für automatischen Rückruf und
- Anzeige/Einblendung bei Dreierkonferenz.

Da die Nutzung bestimmter, eigentlich nicht freigegebener Leistungsmerkmale (Beispiel: Zeugenschaltung) zu Beeinträchtigungen der IT-Sicherheit führen kann, sollten besonders deren Warnanzeigen und -töne bekannt sein.

Ergänzende Kontrollfragen:

- Erkennen die Mitarbeiter, wenn sich jemand auf ein Gespräch aufschaltet?
- Wissen die Mitarbeiter, was an einem Telefon bei direkter Ansprache sicht- und hörbar ist?
- Ist am Telefon erkennbar, dass das Freisprechen aktiviert ist?

M 3.13 Sensibilisierung der Mitarbeiter für mögliche TK-Gefährdungen

Verantwortlich für Initiierung: TK-Anlagen-Verantwortlicher, IT-Sicherheitsmanagement, Personalrat/Betriebsrat

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Die Mitarbeiter müssen über die mit dem Benutzen einer digitalen TK-Anlage verbundenen Gefährdungen informiert werden. Dies könnte z. B. durch eine kurze Unterweisung oder mit Hilfe von Merkblättern geschehen. Es ist darauf hinzuweisen, dass ein abnormes Verhalten der TK-Anlage gemeldet werden soll. Bei Manipulationen an der TK-Anlage sollte eine unabhängige Kontrollinstanz wie IT-Sicherheitsmanagement oder Datenschutzbeauftragte informiert werden.

Ergänzende Kontrollfragen:

- Wird die Sensibilisierung in regelmäßigen Abständen wiederholt?
- Werden neue Mitarbeiter auf mögliche Gefährdungen im TK-Betrieb hingewiesen?

M 3.14 Einweisung des Personals in den geregelten Ablauf eines Datenträgeraustausches

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Mangelnde Information und Einweisung der Mitarbeiter führt in vielen Fällen dazu, dass Restriktionen der Informationsweitergabe nicht oder nur unzulänglich eingehalten werden. Die Festlegungen, welchen Kommunikationspartnern wann welche Daten übermittelt werden dürfen (M 2.42 *Festlegung der möglichen Kommunikationspartner*), ist den an einem Datenträgeraustausch Beteiligten daher zwingend bekannt zu geben. Außerdem sind die prinzipiellen Schritte für den Ablauf eines Datenträgeraustausches zu fixieren (eventuell als Dienstanweisung) und die Mitarbeiter zur Einhaltung zu verpflichten.

Zusätzlich ist eine Sensibilisierung der am Datenträgeraustausch beteiligten Mitarbeiter hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen vor, während und nach dem Transport der Datenträger notwendig.

Werden bestimmte IT-gestützte Verfahren zum Schutz der Daten während des Austausches eingesetzt (wie etwa Verschlüsselung oder Checksummen-Verfahren), so sind diese Mitarbeiter in die Handhabung dieser Verfahren ausreichend einzuarbeiten.

Ergänzende Kontrollfragen:

- Sind allen für die Kommunikation zugelassenen Mitarbeitern die diesbezüglichen Regelungen bekannt?
- Sind die Mitarbeiter mit den eventuell einzusetzenden Verschlüsselungs- oder Checksummen-Verfahren vertraut?
- Sind die für den Datenträgeraustausch Verantwortlichen hinsichtlich möglicher Gefährdungen ausreichend sensibilisiert?

M 3.15 Informationen für alle Mitarbeiter über die Faxnutzung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Alle Mitarbeiter sind auf die Besonderheiten der Informationsübermittlung per Fax hinzuweisen sowie darüber zu informieren, dass die Rechtsverbindlichkeit einer Faxsendung stark eingeschränkt ist. Bei Verwendung herkömmlicher Faxgeräte sollte eine verständliche Bedienungsanleitung am Faxgerät zur Verfügung stehen. Beim Einsatz eines Faxservers sollten die Benutzer mindestens eine Kurzreferenz zur eingesetzten Faxclient-Software erhalten.

Insbesondere ist, ggf. in Form einer Dienstanweisung, festzulegen,

- wer der Fax-Verantwortliche ist und damit für die manuelle Verteilung eingehender Faxsendungen und als Ansprechpartner in Fax-Problemfällen zuständig ist,
- wer das Faxgerät bzw. den Faxserver benutzen darf,
- dass das Versenden von vertraulichen Informationen per Fax vermieden werden sollte,
- dass ein einheitliches Faxvorblatt benutzt werden soll,
- dass sich vor Austausch schutzbedürftiger Informationen über FaxVersand Empfänger und Absender hierüber telefonisch verständigen,
- dass ggf. Einzelsendenachweise bzw. Übertragungsprotokolle für die korrekte Übertragung zu kontrollieren und diese den Unterlagen beizufügen und ggf. zu archivieren sind,
- dass beim Einsatz eines Faxservers mit automatischer Eingangs-Fax-Verteilung für die Akten ein Ausdruck von Eingangs-Faxsendungen zu fertigen ist bzw. diese elektronisch zu archivieren sind,
- dass bei Ausgangsfaxen, die über einen Faxserver versendet werden, für die Akten ein Ausdruck zu erstellen ist bzw. diese elektronisch zu archivieren sind,
- dass die Adressbücher und Verteillisten regelmäßig kontrolliert werden, damit die Faxe nicht versehentlich an falsche Empfänger gesendet werden.

Ergänzende Kontrollfragen:

- Sind alle Mitarbeiter über die korrekte Faxnutzung informiert und werden neue Mitarbeiter entsprechend eingewiesen?
- Wissen alle Mitarbeiter, an wen sie sich bei Faxproblemen wenden können?

M 3.16 Einweisung in die Bedienung des Anrufbeantworters

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Jeder, der einen Anrufbeantworter in seinem Bereich einsetzt, sollte sich mit der Bedienung vertraut machen und so Möglichkeiten und Grenzen des Gerätes kennen lernen. Somit werden Fehlbedienungen weitgehend ausgeschlossen. Darüber hinaus sollten die notwendigen, im Baustein B 3.403 *Anrufbeantworter* genannten IT-Sicherheitsmaßnahmen transparent gemacht werden.

Ergänzende Kontrollfragen:

- Hat jeder Benutzer eines Anrufbeantworters eine Einweisung erhalten?
- Werden Bedienungsanleitungen und Sicherheitshinweise vorgehalten?

M 3.17 Einweisung des Personals in die Modem-Benutzung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Die Mitarbeiter sind über mögliche Gefährdungen, einzuhaltende Sicherheitsmaßnahmen und Regelungen beim Betrieb eines Modems zu unterrichten. Hierbei sind insbesondere die Auswirkungen verschiedener Konfigurationen auf die Betriebssicherheit des Modems zu vermitteln.

Jeder Modem-Benutzer sollte sich mit der Bedienung vertraut machen und so Möglichkeiten und Grenzen des Gerätes kennen lernen.

Ergänzende Kontrollfragen:

- Werden Bedienungsanleitungen und Sicherheitshinweise vorgehalten?

M 3.18 Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement, Benutzer

Wird ein IT-System oder eine IT-Anwendung von mehreren Benutzern verwendet und besitzen die einzelnen Benutzer unterschiedliche Zugriffsrechte auf dort gespeicherte Daten oder Programme, so kann der erforderliche Schutz mittels einer Zugriffskontrolle nur dann erreicht werden, wenn jeder Benutzer sich nach Aufgabenerfüllung am IT-System oder der IT-Anwendung abmeldet. Ist es einem Dritten möglich, an einem IT-System oder in einer IT-Anwendung unter der Identität eines anderen weiterzuarbeiten, so ist jegliche sinnvolle Zugriffskontrolle unmöglich. Daher sind alle Benutzer zu verpflichten, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden. Aus technischen Gründen (z. B. damit alle offenen Dateien geschlossen werden) sollten auch dann Regelungen für die Abmeldung von IT-Systemen und IT-Anwendungen getroffen werden, wenn keine Zugriffskontrolle realisiert ist.

Bildschirmsperre

Ist absehbar, dass nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann an Stelle des Abmeldens auch die manuelle Aktivierung der Bildschirmsperre erfolgen (siehe auch M 4.2 *Bildschirmsperre*). Bei längerer Abwesenheit sollte die Bildschirmsperre automatisch aktiviert werden.

automatisches Abmelden

Einige IT-Systeme und IT-Anwendungen bieten die Möglichkeit, einen Zeitraum vorzugeben, nach dessen Ablauf ein Benutzer bei Inaktivität automatisch vom System abgemeldet wird. Es sollte überlegt werden, ob dieses Verfahren benutzt wird, da es auch zu Datenverlusten führen kann. Eine automatische Abmeldung kann z. B. bei PC-Pools mit starkem Publikumsverkehr zum Einsatz kommen, da hier ein angemeldeter Benutzer den Arbeitsplatz mit Hilfe der Bildschirmsperre unberechtigterweise blockieren kann.

Je nach Arbeitsplatzumgebung ist abzuwägen, welche Vorkehrungen für kurzfristige Abwesenheiten von Benutzern zu treffen sind. So sollte eine automatische Aktivierung der Bildschirmsperre bei Mehr-Benutzer-Systemen schneller erfolgen als bei solchen für einen Benutzer, also z. B. bereits nach 5 Minuten.

Ergänzende Kontrollfragen:

- Werden neue Mitarbeiter oder Vertreter gleichfalls verpflichtet?
- Wird an die Verpflichtung zum Abmelden regelmäßig erinnert?

M 3.19 Einweisung in den richtigen Einsatz der Sicherheitsfunktionen von Peer-to-Peer-Diensten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Gerade beim Einsatz von Peer-to-Peer-Diensten unter WfW und Windows 95, bei denen die Benutzer selbst Sicherheitsaufgaben wahrnehmen müssen, kommt der Einweisung in den richtigen Einsatz der Sicherheitsfunktionen besondere Bedeutung zu. Daher ist jeder Benutzer vorab zumindest zu folgenden Punkten zu schulen:

Datenaustausch über freigegebene Verzeichnisse

- Der Benutzer ist in die korrekte Benutzung der Freigabe von Ressourcen sowie in das korrekte Aufheben der Verzeichnisfreigabe einzuweisen. Insbesondere ist die Möglichkeit zu erläutern, freigegebene Verzeichnisse oder Drucker durch Anhängen des Zeichens "$" an den Freigabenamen zu verbergen. Dadurch ist für andere Benutzer nicht ersichtlich, dass diese Ressource freigegeben ist. Es ist darauf hinzuweisen, dass der Anreiz für Attacken vermindert werden kann, wenn man Freigabenamen benutzt, die keine Rückschlüsse auf den Inhalt zulassen und dass Ressourcen nur solange freigegeben werden sollten, wie dies erforderlich ist.
- Die Bedeutung der Optionen bei Freigabe oder Verbinden von Verzeichnissen bzw. Druckern ist darzustellen und auf die Beachtung der jeweiligen Voreinstellungen ist hinzuweisen:

Beim Start wieder freigeben	Automatische Freigabe beim Starten von WfW ohne Einwirkung des Benutzers
Beim Starten wieder verbinden	Automatisches Verbinden beim Neustart
Kennwort in der Kennwortliste speichern	Speicherung des Passwortes (sicherheitskritisch), so dass es beim nächsten Verbinden nicht mehr eingegeben werden muss

Tabelle: Freigaben

Freigaben müssen wieder entfernt werden

Die Benutzer von Windows 95 und Windows NT/2000 sind darauf hinzuweisen, dass jede erfolgte Freigabe wieder explizit zurückgenommen werden muss, da sie sonst auch nach einem Neustart bestehen bleibt.

- Die Bezeichnungen der möglichen Zugriffsrechte unter WfW und Windows 95 sind nicht sprechend und müssen daher erläutert werden:

Schreibgeschützter Zugriff	Leserecht für Dateien und Ausführungsrecht für Programme
Lese-/Schreibzugriff	Lese-/Schreibrecht für Dateien, Ausführungsrecht für Programme, Recht zum Anlegen und Löschen von Dateien
Zugriff abhängig vom Kennwort	Lese- und Schreibrecht können getrennt vergeben werden

Tabelle: Zugriffsberechtigungen

Unter Windows 95 können Benutzer zwischen den Zugriffsrechten *Schreibgeschützt*, *Alle Zugriffsrechte* und *Benutzerdefiniert* wählen, wenn der Zugriffsschutz auf Benutzer-Ebene realisiert ist. Dann müssen die Benutzer darauf hingewiesen werden, dass Verzeichnisse nie mit *Alle Zugriffsrechte* freigegeben werden sollten, sondern bestenfalls benutzerdefiniert mit Lese- und Schreibrecht für andere Benutzer.

Sicherheitssensibilisierung

- Der Benutzer ist in die von ihm durchzuführenden sicherheitsrelevanten Kontrollen einzuweisen. Dazu muss er insbesondere unterrichtet werden, wie der *Netzwerkmonitor* und die zugehörige Protokollfunktion einzusetzen sind.
- Der Umgang mit Passwörtern und deren Wechsel ist gemäß der Sicherheitsstrategie darzulegen.

Umgang mit Passwörtern

- Der Benutzer muss darüber informiert werden, dass unter WfW und Windows 95
  - in der Datei [*anmeldename*].*pwl* Passwörter für den Zugriff auf Ressourcen anderer Rechner gespeichert werden,
  - unter WfW in der Datei *connect.dat* die Ressourcen anderer WfW-Rechner eingetragen sind, die beim Starten von WfW automatisch wieder verbunden werden,
  - in der Datei *shares.pwl* die eigenen Ressourcen eingetragen sind, die beim Starten automatisch wieder freigegeben werden.

  Diese Dateien können vom Benutzer gelöscht werden, ohne die Systemintegrität zu verletzen. Dies ist insbesondere bei der Datei [*anmeldename*].*pwl* sinnvoll, wenn versehentlich Passwörter gespeichert wurden.
- Sind Namenskonventionen für die im Netz verfügbaren Rechner und Benutzer erstellt worden, sind diese und eventuell bereits vergebene Namen den Benutzern bekannt zu geben.

Namenskonventionen bekannt geben

Ergänzende Kontrollfragen:

- Haben alle Teilnehmer eine ausreichende Schulung zum sicheren Einsatz von Peer-to-Peer-Diensten erhalten?
- Werden einzelne Aspekte der Schulungsinhalte zur Sensibilisierung sporadisch wiederholt?

M 3.20 Einweisung in die Bedienung von Schutzschränken

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Nach der Beschaffung eines Schutzschrankes sind die Benutzer in die korrekte Bedienung einzuweisen. Dies sollte auch bei der Neuübertragung einer Aufgabe erfolgen, die die Nutzung des Schutzschrankes umfasst. Dabei sind zumindest folgende Punkte zu vermitteln:

- Der korrekte Umgang mit dem Schloss des Schutzschrankes ist vorzuführen. Auf typische Fehler ist hinzuweisen, zum Beispiel das Nichtverwerfen von Codeschlössern. Die Regelungen zur Schlüsselverwaltung, Schlüsselhinterlegung und Vertretungsregelung sind aufzuzeigen. Insbesondere ist einzufordern, dass der Schutzschrank bei Nichtbenutzung, auch kurzfristiger Art, verschlossen wird.
- Die Tastatur eines Servers ist unbedingt im Serverschrank aufzubewahren, damit nicht unberechtigte Konsol-Eingaben erfolgen können.
- Im Falle eines Serverschrankes ist darauf hinzuweisen, dass unnötige brennbare Materialien (Ausdrucke, überzählige Handbücher, Druckerpapier) nicht im Serverschrank aufbewahrt werden sollen.
- Datensicherungsträger des Servers sollten in einem anderen Brandabschnitt gelagert werden. Eine Aufbewahrung im Serverschrank ist daher ungeeignet und nur dann zulässig, wenn ein Doppel der Datensicherungsbestände in einem anderen Brandabschnitt ausgelagert ist.
- Wird ein klimatisierter Serverschrank eingesetzt, sollten die Öffnungszeiten des Serverschrankes minimiert werden. Gegebenenfalls ist sporadisch zu kontrollieren, ob im Serverschrank Wasser kondensiert ist.

Ergänzende Kontrollfragen:

- Werden Personen, die einen Schutzschrank betreuen, in dessen Bedienung eingewiesen?

M 3.21 Sicherheitstechnische Einweisung und Fortbildung des Telearbeiters

Verantwortlich für Initiierung: Vorgesetzte, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Vorgesetzte, IT-Sicherheitsmanagement

Der Telearbeiter arbeitet teilweise oder ganz zu Hause. Das bedeutet, dass für die Telearbeit zum Teil andere IT-Sicherheitsmaßnahmen ergriffen werden müssen als für die Arbeit innerhalb der Institution. Deshalb ist es notwendig, dass ein Sicherheitskonzept für die Telearbeitsplätze erstellt wird. Nach Bekanntgabe des Konzeptes muss der Telearbeiter in die zu realisierenden Sicherheitsmaßnahmen eingewiesen und eventuell in ihrem Umgang geschult werden. Darüber hinaus ist der Telearbeiter soweit im Umgang mit dem Telearbeitsrechner zu schulen, dass er einfache Fehlerkorrekturen (z. B. Druckerpatrone wechseln) wahrnehmen kann bzw. einfache Probleme selbständig lösen kann.

Ergänzende Kontrollfragen:

- Liegen für die Telearbeit spezielle IT-Sicherheitskonzepte vor?
- Ist der Telearbeiter für die Realisierung der IT-Sicherheitsmaßnahmen geschult worden?

M 3.22 Vertretungsregelung für Telearbeit

M 3.22 Vertretungsregelung für Telearbeit

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Vorgesetzte

Verantwortlich für Umsetzung: Telearbeiter

Über die Maßnahme M 3.3 *Vertretungsregelungen* hinaus sind im Falle der Vertretung eines Telearbeiters weitere Schritte notwendig. Da der Telearbeiter hauptsächlich außerhalb der Institution tätig ist, muss ein Informationsfluss zu seinem Vertreter vorgesehen werden. Auch eine Dokumentation der Arbeitsergebnisse seitens des Telearbeiters ist unabdingbar. Ggf. sind sporadische oder regelmäßige Treffen zwischen dem Telearbeiter und seinem Vertreter sinnvoll.

Ergänzend dazu muss geregelt werden, wie der Vertreter im unerwarteten Vertretungsfall Zugriff auf die Daten im Telearbeitsrechner oder am Telearbeitsplatz vorhandene Unterlagen nehmen kann.

Ergänzende Kontrollfragen:

- Sind Vertreter für Telearbeiter benannt worden?
- Ist ein Vertretungsfall probeweise durchgespielt worden?

M 3.23 Einführung in kryptographische Grundbegriffe

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Leiter IT

Der Einsatz von Kryptoprodukten kann für die Benutzer zusätzlichen Aufwand bedeuten oder - je nach Komplexität der eingesetzten Produkte - sogar vertiefte Kenntnisse erfordern. Daher sollten alle Mitarbeiter, die kryptographische Verfahren und Produkte einsetzen sollen, für den Nutzen und die Notwendigkeit der kryptographischen Verfahren sensibilisiert werden und eine Einführung in kryptographische Grundbegriffe erhalten. Dies gilt natürlich insbesondere für diejenigen, die ein Kryptokonzept erstellen, Kryptoprodukte auswählen, installieren oder betreuen sollen.

Der folgende Text soll ein elementares Verständnis der grundlegenden kryptographischen Mechanismen vermitteln. Nachfolgend wird an Beispielen erläutert, in welcher Situation welche kryptographische Technik eingesetzt werden kann.

Elemente der Kryptographie

Mathematische Methoden und Techniken, die zum Schutz von Information gegen unbefugte Kenntnisnahme und/oder absichtliche Manipulation dienen können, nennt man kryptographisch. Der Schutz der Information durch kryptographische Methoden ist - im Unterschied zu infrastrukturellen und technischen Sicherungsmaßnahmen - *mathematisch-logischer* Natur.

Bei kryptographischen Verfahren wird ein mathematischer Rechenvorgang - ein *Algorithmus* - in konkrete Technik umgesetzt. Ihre Wirksamkeit beruht darauf, dass ein potentieller Angreifer ein gewisses mathematisches Problem nicht zu lösen vermag - und zwar nicht wegen mangelnder Fähigkeiten, sondern wegen fehlenden Wissens um ganz bestimmte "Schlüssel"-Informationen.

Kryptographische Methoden beziehen sich stets auf folgende Situation: Ein Sender A (dieser wird, wie in der Kryptographie üblich, "Alice" genannt) schickt über einen *unsicheren Kanal* eine Nachricht an einen Empfänger B (er wird "Bob" genannt).

Sender und Empfänger dürfen dabei auch identisch sein, unter einem Kanal ist ein beliebiges Transportmedium zu verstehen. Bei der Verschlüsselung lokaler Daten sind Sender und Empfänger natürlich identisch, unter "Kanal" ist hier das Speichermedium zu verstehen.

Kryptographische Grundziele

Auf Grund theoretischer und praktischer Erwägungen unterscheidet man vier kryptographische Grundziele:

1. Vertraulichkeit/Geheimhaltung: Keine unbefugte dritte Partei E (sie sei "Eve" genannt) soll an den Inhalt der Nachricht bzw. Datei gelangen.
2. Integrität: Unbefugte Manipulationen an der Nachricht bzw. Datei (z. B. Einfügen, Weglassen, Ersetzung von Teilen) sollen entdeckt werden können.

3. Authentizität:
   - Identitätsnachweis (Authentisierung von Kommunikationspartnern): Eine Kommunikationspartei (z. B. Person, Organisation, IT-System) soll einer anderen ihre Identität zweifelsfrei beweisen können.
   - Herkunftsnachweis (Nachrichtenauthentisierung): A soll B beweisen können, dass eine Nachricht von ihr stammt und nicht verändert wurde.
4. Nichtabstreitbarkeit (Verbindlichkeit, non repudiation): Hier liegt der Schwerpunkt verglichen mit der Nachrichtenauthentisierung auf der Nachweisbarkeit gegenüber Dritten.
   - Nichtabstreitbarkeit der Herkunft: Es soll A unmöglich sein, das Absenden einer bestimmten Nachricht an B nachträglich zu bestreiten.
   - Nichtabstreitbarkeit des Erhalts: Es soll B unmöglich sein, den Erhalt einer von A gesendeten Nachricht nachträglich zu bestreiten.

Es ist klar, dass zwischen diesen Zielen Beziehungen bestehen, aber eine wesentliche Einsicht der modernen Kryptographie ist folgende: Die Gewährleistung von Vertraulichkeit bzw. von Authentizität sind unabhängige Grundziele eines kryptographischen Systems: Authentisierung beschränkt den Kreis der möglichen Sender einer Nachricht, Geheimhaltung den der möglichen Empfänger.

Die grundlegende kryptographische Methode zur Wahrung von Vertraulichkeit ist **Verschlüsselung**, die grundlegenden Methoden zur Gewährleistung von Integrität, Authentizität und Nichtabstreitbarkeit sind **Hashfunktionen, Message Authentication Codes (MACs), digitale Signaturen** und **kryptographische Protokolle**. Die einzelnen kryptographischen Konzepte werden im folgenden kurz vorgestellt.

I. Verschlüsselung

Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation - die Zurückgewinnung des Klartextes aus dem Geheimtext - wird Entschlüsselung genannt. In allen modernen Verschlüsselungsalgorithmen sind Klartexte, Geheimtexte und Schlüssel jeweils als Folgen von Bits gegeben.

Um praktisch einsetzbar zu sein, müssen Verschlüsselungsalgorithmen folgende Mindestanforderungen erfüllen:

- Sie sollten entzifferungsresistent sein, d. h. ohne Kenntnis des Schlüssels darf das Chiffrat nicht entschlüsselt werden können, insbesondere muss hierfür die Menge der möglichen Schlüssel "ausreichend groß" sein, da sonst ein einfaches Ausprobieren aller Schlüssel möglich wäre,
- sie müssen einfach einzusetzen sein, und
- Ver-/Entschlüsselung müssen "schnell genug" sein.

Die Forderung nach Entzifferungsresistenz ist immer relativ zu den aktuellen technischen und mathematischen Möglichkeiten zu betrachten. Wichtig bei der Bewertung von Verschlüsselungsalgorithmen ist, dass es zum Nutzungszeitpunkt praktisch nicht möglich sein darf, das Chiffrat ohne Kenntnis des Schlüssels zu entschlüsseln, d. h. nicht mit der dann verfügbaren Technik innerhalb eines akzeptablen Zeitrahmens.

Wenn A und B eine vertrauliche Verbindung einrichten wollen, gehen sie wie folgt vor:
1. sie vereinbaren ein Chiffrierverfahren,
2. sie vereinbaren einen Schlüssel bzw. ein Schlüsselpaar,
3. A verschlüsselt eine Nachricht und sendet diese an B,
4. B entschlüsselt das von A gesendete Chiffrat.

Es gibt zwei große Klassen von Chiffrierverfahren:

Symmetrische Verschlüsselungsverfahren benutzen denselben Schlüssel sowohl für die Ver- als auch für die Entschlüsselung. Symmetrische Verfahren werden deshalb gelegentlich auch als "ein-Schlüssel"-Verfahren bezeichnet, da die Kenntnis eines Schlüssels ausreicht, um chiffrieren und dechiffrieren zu können.

Bekannte symmetrische Verschlüsselungsverfahren sind z. B. DES, Tripel-DES, IDEA oder RC5.

Bei symmetrischen Verfahren unterscheidet man weiter zwischen Stromchiffren und Blockchiffren.

Bei Stromchiffren wird unter Verwendung des Schlüssels eine möglichst zufällig aussehende Bitfolge (ein Bitstrom) generiert, die auf die Klarbitfolge (modulo 2) aufaddiert wird. Die Klarbitfolge wird also Bit für Bit (durch Addition von Schlüsselstrombits) verschlüsselt. Für die Sicherheit von Stromchiffren ist wesentlich, dass niemals zwei (verschiedene) Nachrichten mit demselben Schlüsselstrom verschlüsselt werden - dafür muss mit speziellen Maßnahmen (Synchronisierinformation in Form eines Spruchschlüssels) gesorgt werden. Beispiele für Stromchiffren sind RC4 und SEAL.

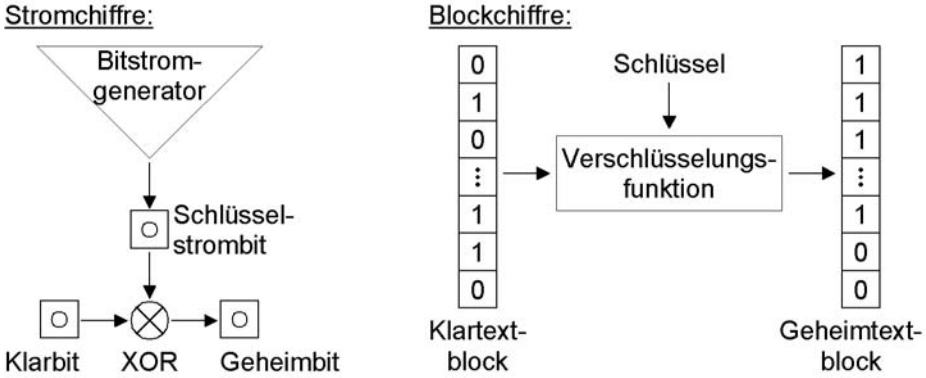


Abbildung: Chiffrierung

Bei Blockchiffren dagegen wird in einem Verschlüsselungstakt jeweils ein ganzer Block von Bits verschlüsselt, heutzutage sind dies in der Regel 64 Bits. Die meisten symmetrischen Verschlüsselungsverfahren sind Blockchiffren, dazu gehören auch DES, IDEA oder RC5. Für Blockchiffren sind eine Reihe von Betriebsarten (Modi) definiert (und standardisiert). Es sind dies

- der ECB (Electronic Code Book)-Modus, bei dem jeder Block für sich - unabhängig von den anderen Blöcken - verschlüsselt wird,
- der CBC (Cipher Block Chaining)-Modus und der CFB (Cipher Feed Back)-Modus, bei diesen Modi wird, nach Wahl eines zusätzlichen Initialisierungsvektors, eine Abhängigkeit der Chiffretextblöcke von allen vorhergehenden Chiffretextblöcken hergestellt, sowie
- der OFB (Output Feedback Modus), dieser Modus kann so aufgefasst werden, dass die verwendete Blockchiffre zur Generierung eines "Blockstroms" verwendet wird, der auf die Klarblöcke bitweise (modulo 2) aufaddiert wird.

Beim Einsatz symmetrischer Verfahren ist generell zu beachten, dass ein Schlüsselaustausch zwischen den Kommunikationspartnern vorausgegangen sein muss. Dieser muss über einen sicheren Kanal (z. B. Kurier, persönliche Übergabe) erfolgen und beide Parteien müssen anschließend den Schlüssel geheim halten. Es gibt verschiedene Verfahren für einen sicheren Schlüsselaustausch. In geschlossenen Systemen ist der Schlüsselaustausch im allgemeinen unproblematisch zu realisieren, da hier meist "sichere Kanäle" vorhanden sind. In offenen Systemen mit einer Vielzahl von Kommunikationspartnern gestaltet sich dies schwieriger. Generell besteht jedoch das Problem, dass bei einer Vielzahl möglicher Kommunikationspartner entsprechend viele Schlüssel vor der eigentlichen Kommunikation ausgetauscht werden müssen und dass dabei die potentiellen Kommunikationspartner vorab bekannt sein müssen.

Asymmetrische (Public Key) -Chiffrierverfahren dagegen benutzen zwei verschiedene (aber mathematisch verwandte) Schlüssel: einen "öffentlichen" Schlüssel (Public Key) für die Verschlüsselung, und einen "privaten" Schlüssel (Private Key) für die Entschlüsselung. Das Schlüsselpaar muss dabei folgende Eigenschaft aufweisen: für alle, die lediglich den "Public Key" kennen, muss es praktisch unmöglich sein, den zugehörigen "Private Key" zu bestimmen oder eine mit dem "Public Key" verschlüsselte Nachricht zu entschlüsseln.

Asymmetrische Verschlüsselung hat also eine "Einbahn"-Eigenschaft: eine Nachricht kann nicht wiederhergestellt werden, wenn der "Private Key" vergessen oder gelöscht wurde.

Die Bezeichnung "Public Key"-Verschlüsselung rührt daher, dass der "Public Key" öffentlich bekannt gemacht werden kann, ohne die Sicherheit des Verfahrens zu kompromittieren. Der "Private Key" hingegen muss **geheim** gehalten werden.

Will nun Alice eine Nachricht verschlüsselt an Bob senden, so holt sich Alice den öffentlichen Schlüssel Bobs aus einer frei zugänglichen Datei und verschlüsselt damit die Nachricht. Nach Erhalt der Nachricht benutzt Bob seinen

geheimen Schlüssel, um die von Alice erhaltene Nachricht zu entschlüsseln. Wenn Alice und Bob ein asymmetrisches Verfahren zum Zweck der Vertraulichkeit verwenden, benötigen sie also keinen sicheren Kanal für den Schlüsselaustausch, aber Alice muss sicher sein, dass sie tatsächlich Bobs öffentlichen Schlüssel benutzt und keinen Schlüssel, der ihr als Bobs Schlüssel untergeschoben wurde. Würde Alice eine Nachricht mit einem untergeschobenen Schlüssel verschlüsseln, so könnte der Täter, dem ja der passende geheime Schlüssel bekannt ist, die Nachricht entschlüsseln. Der Sender benötigt in der Regel die Bestätigung einer vertrauenswürdigen dritten Partei, dass der öffentliche Schlüssel des Empfängers wirklich zu diesem gehört. Diese Bestätigung, das "Zertifikat", wird im allgemeinen auch durch ein kryptographisches Verfahren erzeugt und dem öffentlichen Schlüssel beigefügt.

Zwei bekannte asymmetrische Verschlüsselungsverfahren sind das RSA-Verfahren (benannt nach den Erfindern Rivest, Shamir, Adleman) und die Klasse der Elgamal-Verfahren. Zu letzteren gehören auch die auf Elliptischen Kurven basierenden Verschlüsselungsverfahren.

Symmetrische und asymmetrische Chiffrierverfahren haben z. T. sich ergänzende Vor- und Nachteile:

Vorteile (guter) symmetrischer Verfahren:

- Sie sind schnell, d. h. sie haben einen hohen Datendurchsatz.
- Die Sicherheit ist im wesentlichen durch die Schlüssellänge festgelegt, d. h. bei guten symmetrischen Verfahren sollte es keine Attacken geben, die wesentlich besser sind als das Durchprobieren aller Schlüssel (Brute-Force-Attacken).
- Sie bieten hohe Sicherheit bei relativ kurzem Schlüssel.
- Die Schlüsselerzeugung ist einfach, da gewöhnlich als Schlüssel jede Bitfolge einer festen Länge erlaubt ist und als Schlüssel eine Zufallszahl gewählt werden kann.

Nachteile symmetrischer Verfahren:

- Jeder Teilnehmer muss sämtliche Schlüssel seiner Kommunikationspartner geheim halten.
- Zur Schlüsselverteilung sind sie weniger gut geeignet als asymmetrische Verfahren, insbesondere bei einer großen Anzahl von Kommunikationspartnern.
- Für Verbindlichkeitszwecke sind sie weniger praktikabel als asymmetrische Verfahren, da bei der Verwendung symmetrischer Schlüssel nicht ohne weiteres erkannt werden kann, welcher der beiden Kommunikationspartner die Nachricht verschlüsselt hat. Dies lässt sich nur durch eine zwischengeschaltete dritte Partei sicherstellen, die über entsprechende kryptographische Protokolle in den Nachrichtenfluss eingebunden wird.

Vorteile (guter) asymmetrischer Verfahren:

- Jeder Teilnehmer einer vertraulichen Kommunikation muss nur seinen eigenen privaten Schlüssel geheim halten.

- Sie lassen sich einfach für digitale Signaturen benutzen.
- Sie bieten elegante Lösungen für die Schlüsselverteilung in Netzen, da die öffentlichen Schlüssel bzw. Schlüsselzertifikate frei zugänglich auf zentralen Servern gespeichert werden können, ohne die Sicherheit des Verfahrens zu beeinträchtigen.
- Sie sind gut geeignet für Nicht-Abstreitbarkeitszwecke.

Nachteile asymmetrischer Verfahren:

- Sie sind langsam, d. h. sie haben im allgemeinen einen geringen Datendurchsatz.
- Sicherheit: für alle bekannten Public-Key-Verfahren gilt:
  - Es gibt wesentlich bessere Attacken als das Durchprobieren aller Schlüssel, deshalb werden (im Vergleich zu symmetrischen Verfahren) relativ lange Schlüssel benötigt, um ein gleich hohes Maß an Sicherheit zu erreichen.
  - Die Sicherheit beruht "nur" auf der vermuteten, aber von der Fachwelt anerkannten, algorithmischen Schwierigkeit eines mathematischen Problems (zum Beispiel die Zerlegung einer großen Zahl in die Primfaktoren).
- Die Schlüsselerzeugung ist i. allg. komplex und aufwendig, da die Erzeugung "schwacher" Schlüsselpaare vermieden werden muss.

Hybride Verfahren versuchen, die Vorteile beider Arten von Verschlüsselung zu kombinieren: sie benutzen asymmetrische Verschlüsselung, um einen Sitzungsschlüssel ("Sessionkey") für ein symmetrisches Verfahren zu übermitteln, und verschlüsseln die Massendaten mit dem symmetrischen Verfahren. Der Sessionkey wird gewöhnlich nur für eine Sitzung (Übertragung) verwendet und dann vernichtet. Das asymmetrische Schlüsselpaar wird je nach Umständen für einen langen Zeitraum verwendet.

II. Integritätsschutz

Das Ziel des Integritätsschutzes ist es, dass ein Empfänger einer Nachricht feststellen kann, ob er diese Nachricht unverfälscht erhalten hat. Das Grundprinzip des Integritätsschutzes besteht darin, die Nachricht unverschlüsselt und unverändert zu übersenden, gleichzeitig aber bestimmte Kontrollinformationen mitzuschicken, die die Kontrolle auf Unverfälschtheit der eigentlichen Nachricht ermöglichen. Voraussetzung dazu ist allerdings, dass der Empfänger die Kontrolldaten unmanipuliert erhält. Für diese Kontrolldaten stellen sich damit folgende Bedingungen:

- Der Umfang der Kontrollinformationen muss möglichst gering sein, um die zusätzlich zu übertragenden Informationen zu minimieren.
- Praktisch jede Manipulation, auch nur eines einzelnen Bits der Nachricht muss anhand der Kontrollinformationen feststellbar sein.
- Die Kontrollinformationen müssen unmanipulierbar übertragen bzw. Manipulationen müssen entdeckt werden können.

Zur Berechnung der Kontrollinformationen werden typischerweise zwei Verfahren verwendet: Hashfunktionen und Message Authentication Codes.

Eine (Einweg-)**Hashfunktion** ist eine Datentransformation mit folgenden Eigenschaften:

- Kompressionseigenschaft: Beliebig lange Bitfolgen werden auf Bitfolgen fester, i. allg. kürzerer Länge abgebildet (typischerweise 128 - 160 Bit).
- "Einweg"-Eigenschaft: Es muss "praktisch unmöglich" sein, zu einem vorgegebenen Hashwert eine Nachricht zu finden, deren Hashwert der vorgegebene Hashwert ist.
- Kollisionswiderstand: Es muss "praktisch unmöglich" sein, zwei Nachrichten zu finden, die zum gleichen Hashwert führen.

Mit Hilfe einer beiden Kommunikationspartnern bekannten Hashfunktion können A und B die Integrität einer Nachricht überprüfen: Alice hasht ihre Nachricht, und übermittelt diese und den Hashwert so an Bob, dass die Unverfälschtheit des Hashwertes gewährleistet ist. Bob hasht die empfangene Nachricht ebenfalls und vergleicht sein Ergebnis mit dem von Alice gelieferten Hashwert. Stimmen beide Werte überein, so kann er davon ausgehen, dass kein Bit der Nachricht verändert wurde.

Ein **Message Authentication Code (MAC)** ist eine kryptographische Checksumme zur Nachrichtensicherung, also eine Datentransformation, bei der zusätzlich ein geheimer Schlüssel in die Berechnung eingeht, mit folgenden Eigenschaften:

- Kompressionseigenschaft: Beliebig lange Bitfolgen werden auf Bitfolgen fester, i. allg. kürzerer Länge abgebildet.
- Fälschungssicherheit: Für jeden, der nicht im Besitz des Schlüssels ist, muss es "praktisch unmöglich" sein, den MAC-Wert einer neuen Nachricht zu berechnen, selbst wenn er in den Besitz einiger alter Nachrichten mit den zugehörigen MAC-Werten gelangt ist.

Besitzen Alice und Bob einen MAC und einen gemeinsamen, geheimen MAC-Schlüssel, so authentisiert Alice ihre Nachricht einfach dadurch, dass sie den MAC-Wert der Nachricht berechnet und zusammen mit der Nachricht an Bob schickt. Bob berechnet seinerseits den MAC-Wert der empfangenen Nachricht mit dem auch ihm bekannten MAC-Schlüssel. Stimmt dieser mit Alices Wert überein, so kann er davon ausgehen, dass die Nachricht authentisch ist (d. h. dass sie nicht verändert wurde und wirklich von Alice stammt). Alice hat also ihre Nachricht durch Verwendung des nur ihr und Bob bekannten Schlüssels gegenüber Bob authentisiert.

MACs werden häufig auf Basis symmetrischer Chiffrierverfahren konstruiert. Die bekannteste Variante ist hierbei die Verschlüsselung einer Nachricht mit DES oder einem anderem Block-Chiffrierverfahren im CBC- oder CFB-Mode. Dabei wird als MAC der letzte verschlüsselte Block an die Nachricht angehängt. Daneben gibt es aber auch MACs, die nicht auf Chiffrierverfahren beruhen. Der MAC-Wert einer Nachricht kann als fälschungssichere, schlüsselabhängige, kryptographische Checksumme dieser Nachricht angesehen werden. Die Anwendung von MACs zum Zweck der Authentisierung

erfordert, dass beide Parteien den geheimen Authentisierungsschlüssel zuverlässig schützen. Als Nebeneffekt des Integritätsschutzes kann mit oben skizzierten Verfahren gleichzeitig vom Empfänger der Nachricht nachgeprüft werden, dass die als unmanipuliert verifizierte Nachricht nur vom tatsächlich bekannten Sender verschickt werden konnte. Dieser Schluss lässt sich ziehen, da nur dieser Sender die notwendigen Schlüssel zur Verschlüsselung bzw. Ermittlung der Kontrollinformationen besitzt.

III. Authentizitätsnachweise

Bei der Authentisierung von Benutzern gegenüber Kommunikationspartnern/IT-Systemen bzw. Clients gegenüber Servern sollen

- illegitime Zugriffe erkannt und abgewehrt werden,
- legitime Zugriffe erlaubt werden und
- sensible Daten auch bei Übertragungen über Netze geschützt bleiben.

Dazu sind Verfahren erforderlich, die allen Beteiligten die Feststellung der Identität ihrer Kommunikationspartner unmißverständlich erlauben. Dies schließt einen Zeitaspekt ein: Alice will Bob in "real time" davon überzeugen, dass tatsächlich sie mit ihm kommuniziert. Die Haupttechniken für solche Authentisierungen sind kryptographische Challenge-Response-Protokolle.

Hierbei sendet Bob Daten an Alice und fordert sie auf (Challenge), ihm den Besitz eines Geheimnisses (also einer Schlüsselinformation) nachzuweisen, und Alice demonstriert ihm diesen Besitz ohne das Geheimnis selbst preiszugeben, indem sie eine vom Geheimnis und seiner Challenge abhängige Antwort sendet (Response). Bob wiederum überprüft anhand der Antwort, dass zur Berechnung der Antwort wirklich das korrekte Geheimnis verwendet wurde.

Für eine "starke" Authentisierung dürfen sich die Challenges nicht wiederholen. Bei Challenge-Response-Verfahren können sowohl symmetrische als auch asymmetrische Techniken verwendet werden.

Beispiel: Alice und Bob verständigen sich vorab auf ein symmetrisches Verschlüsselungsverfahren und einen gemeinsamen kryptographischen Schlüssel. Zur Authentisierung sendet Bob eine Zufallszahl als Challenge an Alice. Alice wiederum verschlüsselt diese Zufallszahl mit dem gemeinsamen geheimen Schlüssel und sendet das Ergebnis zurück an Bob. Im nächsten Schritt entschlüsselt Bob die Nachricht und vergleicht, ob das Ergebnis seine anfangs gewählte Zufallszahl ist. Bei Gleichheit ist es tatsächlich Alice, da nur sie den geheimen Schlüssel kennt.

IV. Digitale Signatur

Das kryptographische Konstrukt einer digitalen Signatur dient dem Ziel, für digitale Dateien und Nachrichten ein Pendant zur handschriftlichen Unterschrift einsetzen zu können. Dazu werden einige der schon erläuterten kryptographischen Verfahren wie Hashfunktionen und asymmetrische Verfahren zusammengeführt. Die wesentliche Voraussetzung für digitale Signaturen ist, dass jeder Teilnehmer ein nur ihm bekanntes Geheimnis besitzt, mit dem er zu beliebigen Dateien eine digitale Signatur bilden kann. Anhand von

öffentlichen Informationen muss es dann möglich sein, diese digitale Signatur zu überprüfen.

In diesem Sinne ist eine digitale Signatur ein spezieller Integritätsschutz mit zusätzlichen Besonderheiten. Eine **digitale Signatur** ist eine Kontrollinformation, die an eine Nachricht oder Datei angehängt wird, mit der folgende Eigenschaften verbunden sind:

- Anhand einer digitalen Signatur kann eindeutig festgestellt werden, wer diese erzeugt hat, und
- es ist authentisch überprüfbar, ob die Datei, an die die digitale Signatur angehängt wurde, identisch ist mit der Datei, die tatsächlich signiert wurde.

Kann also anhand der öffentlich zugänglichen Informationen die digitale Signatur verifiziert werden, so ist einerseits die Integrität der signierten Datei gegeben und andererseits die Nichtabstreitbarkeit, da nur die Person, der die digitale Signatur eindeutig zugeordnet werden kann, diese Signatur anhand ihrer geheimen Informationen gebildet haben kann. Zu beachten ist, dass unterschiedliche Dateien auch unterschiedliche digitale Signaturen zur Folge haben und das geringste Änderungen an den Dateien zu nicht verifizierbaren Signaturen führen.

Beispiel: Ein weit verbreitetes Verfahren für digitale Signaturen ist die umgekehrte Anwendung des RSA-Verfahrens. Dabei besitzt jeder Teilnehmer einen nur ihm bekannten geheimen Signierschlüssel. Öffentlich zugänglich sind Verifizierschlüssel-Zertifikate, in denen der passende öffentliche Schlüssel und die Angaben zum Besitzer des passenden geheimen Signierschlüssels unfälschbar miteinander verknüpft sind. Diese Zertifikate werden von vertrauenswürdigen Stellen herausgegeben, die zuvor die Personalien der Teilnehmer geprüft haben.

Um für eine beliebige Datei eine digitale Signatur zu berechnen und zu prüfen, wird nun wie folgt vorgegangen:

1. Schritt: Alice berechnet den Hashwert der ausgewählten Datei.
2. Schritt: Alice verschlüsselt diesen Hashwert mit dem nur ihr bekannten geheimen Signierschlüssel. Das Ergebnis ist die digitale Signatur von Alice zu dieser Datei.
3. Schritt: Alice überträgt die digitale Signatur gemeinsam mit dem Verifizierschlüssel-Zertifikat und der Datei an Bob.
4. Schritt: Bob verifiziert das Zertifikat (z. B. mit dem öffentlichen Schlüssel einer Zertifizierungsstelle).
5. Schritt: Bob berechnet den Hashwert der erhaltenen Datei.
6. Schritt: Anhand des im Verifizierschlüssel-Zertifikat enthaltenen öffentlichen Verifizierschlüssels entschlüsselt Bob die digitale Signatur.
7. Schritt: Bob vergleicht den in Schritt 4 berechneten Hashwert und die entschlüsselte Signatur. Sind sie identisch, so ist die digitale

Signatur verifiziert. Besteht keine Gleichheit, kann Bob keine weiteren Schlüsse ziehen.

8. Schritt: Nach der Verifikation der digitalen Signatur kann Bob als Ergebnisse festhalten:
   - Falls sichergestellt ist, dass tatsächlich nur Alice den geheimen Schlüssel besitzt, kann Bob sicher sein, dass die digitale Signatur von Alice, die im Verifizierschlüssel-Zertifikat aufgeführt ist, erzeugt wurde.
   - Die erhaltene Datei ist identisch mit der Datei, für die Alice die digitale Signatur berechnet hat.

Betont sei, dass digitale Signaturen ausschließlich die Ziele Integrität und Nichtabstreitbarkeit sicherstellen, jedoch in keiner Weise die Vertraulichkeit. Eine digital signierte Nachricht wird im Klartext übertragen, ist sie vertraulich, muss sie **zusätzlich** verschlüsselt werden.

Enthält eine digital signierte Datei eine Willenserklärung des Signierers, kann dann anhand der Signatur diese Willenserklärung unabstreitbar dem Signierer, ggf. auch vor Gericht, zugerechnet werden.

Die verwendeten Verifizierschlüssel-Zertifikate wiederum sind selbst von der vertrauenswürdigen Stelle digital signierte Dateien, die analog überprüft werden können und die Auskunft geben über den Verifizierschlüssel und die Person, die den dazu passenden geheimen Signierschlüssel besitzt.

Man beachte die Unterschiede zwischen MACs und digitalen Signaturen:

- Die digitale Signatur kann durch jeden, der das Verifizierschlüssel-Zertifikat besitzt, verifiziert werden, MACs dagegen nur durch die Parteien, die den geheimen Authentisierungsschlüssel kennen.
- Alices digitale Signatur einer Nachricht kann nur von Alice erstellt werden, der MAC-Wert einer Nachricht dagegen von beiden Parteien, Alice und Bob (und allen anderen, die den geheimen Authentisierungsschlüssel kennen). Es ist deshalb unmöglich, MACs für den Zweck der Verbindlichkeit einzusetzen.

Mit Artikel 3 des Informations- und Kommunikationsdienste-Gesetzes (Bundesgesetzblatt 1879, Teil 1, 1997) ist für die Bundesrepublik Deutschland ein Gesetz zur digitalen Signatur in Kraft getreten. Dieses regelt, welche Sicherheitsanforderungen die technischen Komponenten, die für digitale Signaturen eingesetzt werden, erfüllen müssen und welche Aufgaben Zertifizierungsstellen, die Verifizierschlüssel-Zertifikate ausstellen, haben. Darüber hinaus wird geregelt, wie die erforderliche Sicherheit der Komponenten und Zertifizierungsstellen geprüft wird. Im Ergebnis wird digitalen Signaturen nach dem Signaturgesetz auch vor Gericht eine hohe Sicherheit zugebilligt.

Schlüsselmanagement

Bei jedem Einsatz von Verschlüsselung entsteht die Aufgabe, die Schlüssel angemessen zu verwalten. Es stellt sich die Frage, wie man

- Erzeugung/Initialisierung,
- Vereinbarung/Etablierung,
- Verteilung/Transport,
- Wechsel/Update,
- Speicherung,
- Beglaubigung/Zertifizierung,
- Rückruf,
- Wiedergewinnung im Fall von Vernichtung/Verlust,
- Vernichtung/Löschen,
- Archivierung und
- Escrow (treuhänderische Hinterlegung)

während des gesamten Lebenszyklus der Schlüssel durchführt. Das Schlüsselmanagement kann und wird sich gewöhnlich auch kryptographischer Techniken bedienen. Es muss für die Gesamtheit der Kryptomodule eines kryptographisch basierten Sicherungssystems durchgeführt werden. Geheime Schlüssel müssen vor unbefugter Aufdeckung, Modifizierung und Ersetzung geschützt werden. Öffentliche Schlüssel müssen vor unbefugter Modifizierung und Ersetzung geschützt werden. Angemessenes Schlüsselmanagement ist die Voraussetzung dafür, dass Information durch kryptographische Methoden überhaupt geschützt werden kann. Schlüsselmanagement benötigt eigens dieser Aufgabe gewidmete Ressourcen!

Zertifizierungsstellen

Trust Center bzw. Zertifizierungsstellen werden immer dann benötigt, wenn man für eine nicht mehr überschaubare Anzahl von Teilnehmern asymmetrische Kryptoverfahren für die digitale Signatur oder für Verschlüsselung einsetzen will. Solche Verfahren benötigen bei der Signaturbildung bzw. der Verschlüsselung einen anderen Schlüssel als bei der Signaturprüfung bzw. der Entschlüsselung. Dazu wird benutzerbezogen ein Schlüsselpaar korrespondierender Schlüssel erzeugt. Ein Schlüssel, der so genannte öffentliche Schlüssel, wird öffentlich bekanntgegeben. Der andere Schlüssel, der so genannte private Schlüssel, ist absolut geheim zu halten. Mit dem privaten Schlüssel - und nur mit diesem - kann eine digitale Signatur erzeugt bzw. ein Text entschlüsselt und mit dem zugehörigen öffentlichen Schlüssel - und nur mit diesem - verifiziert bzw. verschlüsselt werden. Will man nun die Echtheit der öffentlichen Schlüssel und die sichere Zuordnung der Schlüssel zu Personen sicherstellen, bedarf es der bereits erwähnten Trust Center / Zertifizierungsstellen, die die Zuordnung einer Person zu einem öffentlichen Schlüssel durch ein Zertifikat bestätigen.

Innerhalb solcher Zertifizierungsstellen werden typischerweise folgende Aufgaben wahrgenommen:

- Schlüsselgenerierung: Es sind für die Zertifizierungsstelle und ggf. für Teilnehmer Schlüsselpaare zu generieren.
- Schlüsselzertifizierung: Die Teilnehmerdaten, der korrespondierende öffentliche Schlüssel und weitere Daten werden zu einem Zertifikat zusammengefasst und von der Zertifizierungsstelle digital signiert.

- Personalisierung: Das Zertifikat und ggf. öffentlicher und privater Schlüssel werden auf eine Signaturkomponente (i. a. eine Chipkarte) übertragen.
- Identifizierung und Registrierung: Die Teilnehmer werden gegen Vorlage eines Ausweispapieres identifiziert und registriert.
- Verzeichnisdienst: Zertifikate werden in einem öffentlichen Verzeichnis abrufbar gehalten. Darüber hinaus muss der Verzeichnisdienst Auskunft darüber geben, ob ein Zertifikat gesperrt ist oder nicht.
- Zeitstempeldienst: Für bestimmte Daten kann es notwendig sein, diese mit einem vertrauenswürdigen Zeitpunkt zu verknüpfen. Dazu wird der Zeitpunkt an die Daten angehängt und das Ergebnis vom Zeitstempeldienst digital signiert.

Trust Center können außerdem zusätzlich Schlüsselaufbewahrung als Dienstleistung anbieten, wenn die kryptographischen Schlüssel für Verschlüsselung eingesetzt werden sollen. Um bei Schlüsselverlust noch auf die verschlüsselten Daten zugreifen zu können, kann dann der Schlüsselbesitzer (und nur dieser) eine Schlüsseldublette erhalten, die im Trust Center geschützt aufbewahrt wird.

Schlüsselverteilungszentralen

Die Sicherheit symmetrischer Verschlüsselungsverfahren hängt davon ab, ob der gemeinsam benutzte geheime Schlüssel nur den zum Zugriff auf die geschützten Informationen berechtigten Benutzern bekannt ist. Im Falle des Schutzes gespeicherter Daten, auf die nur deren Eigentümer Zugriff haben soll, ist dies relativ einfach zu gewährleisten, da dieser Eigentümer lediglich den Schlüssel so schützen muss, dass Unbefugte nicht darauf zugreifen können.

Anders sieht es jedoch aus, wenn Nachrichten, die von einem Sender über ein unsicheres Übertragungsmedium an einen Empfänger zu übermitteln sind, mit einem symmetrischen Verschlüsselungsverfahren geschützt werden sollen. In diesem Fall muss der geheime Schlüssel sowohl beim Sender als auch beim Empfänger vorliegen, d. h. es muss eine Möglichkeit geschützten Informationsaustauschs zwischen den beiden Partnern verfügbar sein. In der Praxis wird dies oft durch die verschlüsselte Verteilung von Kommunikationsschlüsseln durch so genannte Schlüsselverteilungszentralen (Key Distribution Centers, KDCs) realisiert, wobei ganze Hierarchien voneinander sicherheitstechnisch abhängiger Schlüssel aufgebaut werden. Die hier zum Einsatz kommenden Verfahren sind teilweise sehr komplex und hängen hinsichtlich ihrer Sicherheit von einer Vielzahl von Komponenten ab, insbesondere von der physischen, organisatorischen, personellen und technischen Sicherheit der KDCs und der zur Kommunikation mit den KDCs vereinbarten Schlüssel.

Eine Kompromittierung eines geheimen Schlüssels, d. h. sein Bekanntwerden gegenüber einem unberechtigten Dritten, führt zum Verlust der Vertraulichkeit aller Daten, deren Verschlüsselung mit diesem Schlüssel erfolgte bzw. davon abhängt. Dies ist insbesondere dann kritisch, wenn einer der zentralen Schlüssel einer Schlüsselverteilungshierarchie kompromittiert wurde.

Einsatz kryptographischer Verfahren

Bei sachgemäßem Einsatz sind kryptographische Verfahren hervorragend geeignet, folgende Bedrohungen abzuwehren:

- Kenntnisnahme von Informationen durch Unbefugte,
- bewusste Manipulation von Daten durch Unbefugte und
- Manipulationen an der Urheberschaft von Informationen.

Der alleinige Einsatz von Kryptographie reicht allerdings **nicht** aus, um alle Bedrohungen abzuwehren.

- Der Einsatz kryptographischer Methoden trägt nichts dazu bei, um die Verfügbarkeit von Daten zu gewährleisten (bei unsachgemäßem Gebrauch von Verschlüsselung droht sogar Datenverlust!).
- Kryptographische Methoden können gegen Denial-of-Service-Attacken (siehe auch G 5.28 *Verhinderung von Diensten*) nichts ausrichten. Sie können aber zur frühzeitigen Erkennung solcher Attacken beitragen.
- Sie helfen auch nicht gegen zufällige Verfälschungen von Informationen (etwa durch "Rauschen"). Sie können Verfälschungen aber nachträglich erkennbar machen.

M 3.24 Schulung zur Lotus Notes Systemarchitektur für Administratoren

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Um ein Lotus Notes-System korrekt und sicher administrieren zu können, ist die Schulung der verantwortlichen Administratoren unumgänglich. Schon kleine Konfigurationsfehler können dazu führen, dass Sicherheitslücken entstehen. Beispiele hierfür sind das unkontrollierte Anlegen von Cross-Zertifikaten und falsche Zugriffslisten (ACLs) für Datenbanken. Aus diesem Grund müssen Administratoren über die Systemarchitektur von Lotus Notes und insbesondere über die Sicherheitsmechanismen informiert werden.

Bild 1 zeigt (vereinfacht) die allgemeine Architektur, der ein Client-Server-Modell zugrunde liegt. Auf dem sogenannten Notes-Server werden Datenbanken gehalten, die durch die Lotus Domino-Server-Software zum Zugriff über Netz angeboten werden. Der Zugriff auf die Datenbanken durch den Benutzer kann durch zwei Client-Programme erfolgen:

Zugriff via Lotus Notes Client-Software

1. Durch den originären Notes-Client, der von Lotus Notes als Client-Software bereitgestellt wird. Der Zugriff erfolgt hier über das proprietäre Notes-Protokoll. Der Notes-Client leitet Bearbeitungsanfragen an den Domino-Server weiter, der die Verarbeitung im Auftrag des Clients auf den Datenbanken durchführt.

Zugriff via Browser

2. Durch einen Browser (Web-Client). Seit der Notes Version 4.6 ist es auch möglich, mit einem normalen Browser auf die Datenbanken eines Domino-Servers zuzugreifen. Dazu wurde ein spezielles Web-Server-Modul bereitgestellt, das als HTTP-Server fungiert. Die Inhalte der Datenbanken werden beim Zugriff dynamisch durch die sogenannte HTML-Engine in das HTML-Format umgewandelt, damit eine Anzeige im Browser möglich ist. Als Transportprotokoll kommt das Hyper Text Transfer Protocol (HTTP) zum Einsatz.

   Eine lokale Speicherung von Datenbanken (Repliken) ist, im Unterschied zum Notes-Client, mit dem Web-Client nicht möglich.

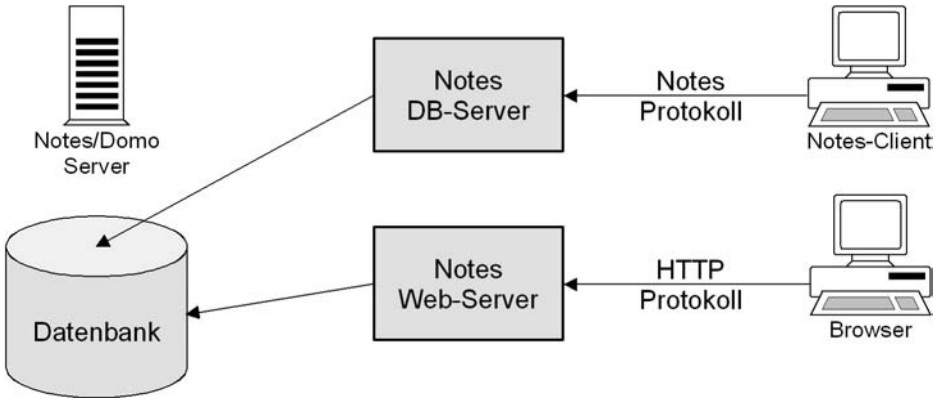


Abbildung: Überblick über die Lotus Notes Architektur

zweistufige Zugriffskontrolle

Die Zugriffskontrollen eines Notes-Servers sind zweistufig ausgelegt (siehe Bild 2) und basieren auf der Benutzerauthentisierung durch die Notes-ID oder durch die Web-Authentisierungsmechanismen "Benutzername und Passwort" oder "SSL-Zertifikat". Ist ein Benutzer authentisiert, so wird beim Zugriff auf eine Datenbank eines Servers zunächst geprüft, ob der Benutzer generell auf den Server zugreifen darf. Ist dies erlaubt, so wird in einer zweiten Stufe geprüft, ob der Benutzer die angeforderte Operation auf der jeweiligen Datenbank durchführen darf.

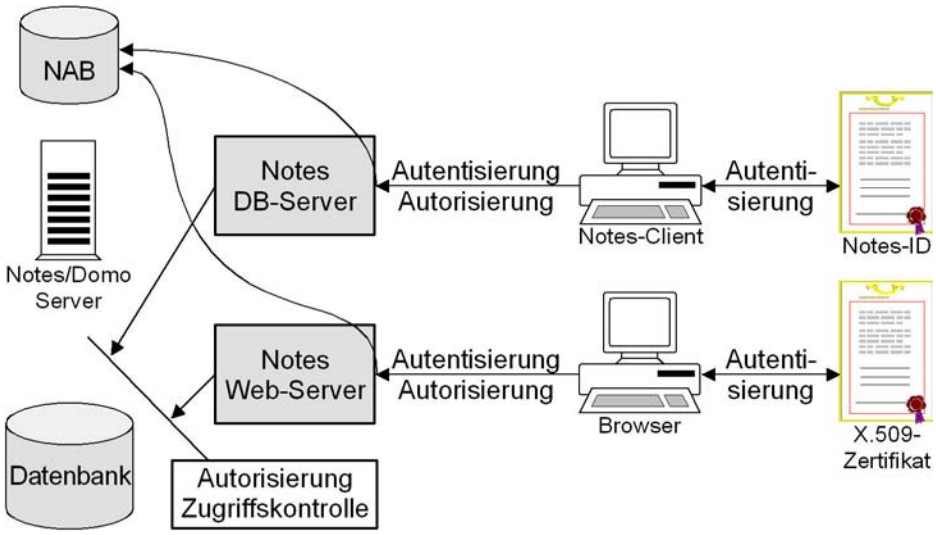


Abbildung: Authentisierung und Zugriffskontrollen bei Lotus Notes

Der Zugriff auf einen Server kann auf verschiedene Arten eingeschränkt werden (siehe M 4.119 *Einrichten von Zugangsbeschränkungen auf Lotus Notes Server*). Ähnliches gilt für die möglichen Zugriffsbeschränkungen auf Datenbanken (siehe M 4.120 *Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken*). Problematisch kann dabei sein, wenn die Zugriffsbe-

schränkungen auf Datenbanken so konfiguriert werden, dass sie eine bestimmte Zugriffsbeschränkung auf die Server voraussetzen. Werden die Zugriffbeschränkungen auf die Server verändert, können leicht Fehlkonfigurationen entstehen (siehe Beispiel unten).

Die Schulung der Administratoren sollte folgende Aspekte berücksichtigen und mindestens folgende Themen umfassen:

- Welche Möglichkeiten bietet die Zugriffskontrolle auf Server?
- Welche Möglichkeiten bietet die Zugriffskontrollen auf Datenbanken?
- Anhand welcher Kriterien und in welcher Reihenfolge entscheidet Lotus Notes, ob einem Benutzer den Zugriff auf Inhalte in einer Datenbank gestattet wird?
- Wie funktioniert die Benutzerauthentisierung?
- Wie funktioniert die Authentisierung mittels asymmetrischer kryptographischer Verfahren?
- Welche Mechanismen für Verschlüsselung und digitale Signatur gibt es und wie ist der Zusammenhang mit symmetrischen und asymmetrischen kryptographischen Verfahren?
- Wie werden Zertifikate für kryptographische Schlüssel erzeugt, verteilt, verwaltet und genutzt?
- Mit welchen Verfahren kann die Client-Server-Kommunikation (Notes-Client, Web-Client) geschützt werden?
- Wie kann eine hohe Verfügbarkeit von Notes Systemen erreicht werden?
- Wie ist eine effiziente Datensicherung für Notes-Clients und -Server zu gestalten?

Die angegebene Themenliste stellt nur eine Auswahl der wichtigsten Themen dar, die an den Anwendungsfall angepasst und erweitert werden müssen.

Beispiel:

Im folgenden wird kurz dargestellt, welche Mechanismen bei der Zugriffskontrolle beim Datenbankzugriff via HTTP ohne SSL ablaufen. Dieser Prozess sollte den Administratoren erläutert werden, um ein Grundverständnis für die Funktionsweise der Zugriffskontrolle zu vermitteln.

- Ein Benutzer versucht eine zugriffsbeschränkte Operation auf einer Datenbank.
- Der Server überprüft, ob der anonyme Zugriff auf den Server für das HTTP-Protokoll erlaubt ist.
- Ist der anonyme Zugriff erlaubt, so finden folgende Überprüfungen statt:
  - Der Server sucht nach einem Eintrag "Anonymous" in der Datenbank-ACL. Existiert dieser, so erhält der Benutzer anonymen Zugriff mit den entsprechenden Rechten.

  - Ist kein Eintrag für "Anonymous" vorhanden, überprüft der Server den "-Default-"-Eintrag.
  - Erlaubt der "-Default-"-Eintrag mindestens "Leser (Reader)"-Rechte, so erhält der Benutzer anonymen Zugriff mit den "Default" -Rechten.
- Ist der anonyme Zugriff auf den Server nicht erlaubt und ist die Authentisierung über Benutzername und Passwort aktiviert, so fordert der Server über den Browser diese Authentisierungsdaten an.
- Der Server überprüft, ob für den angegebenen Benutzer ein Personendokument im NAB (Namens- und Adressbuch) existiert und kontrolliert anhand der dort angegebenen Informationen die Eingaben des Benutzers (Benutzername und Internet-Passwort).
- Stimmen die Authentisierungsinformationen überein, so wird der erste Eintrag im Benutzernamen-Feld des Personendokumentes benutzt, um den Benutzer zu identifizieren und diesem entsprechende Zugriffsrechte über die Datenbank-ACL zuzuordnen.

Auch wenn eine Rollentrennung zwischen der Administration des Lotus Notes Systems und des zugrundeliegenden Betriebssystems in Kraft ist, sollte den Lotus Notes Administratoren Grundlagenwissen zum Betriebssystem vermittelt werden. Anderenfalls wird eine Zusammenarbeit bei der Problemlösung erschwert.

Ergänzende Kontrollfragen:

- Sind die Administratoren auf den Umgang mit den Notes-System vorbereitet und insbesondere in sicherheitsrelevanten Aspekten geschult?

M 3.25 Schulung zu Lotus Notes Sicherheitsmechanismen für Benutzer

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

komplexes System

Lotus Notes ist ein komplexes System, bei dem es wie bei allen komplexen Systemen bei fehlerhafter Nutzung oder Fehlkonfiguration unbeabsichtigt zu Sicherheitslücken kommen kann. Dies gilt in besonderem Maße, wenn Benutzer ohne entsprechende Schulung mit einem Notes-System umgehen. Zwar wird die Systemkonfiguration in der Regel so eingestellt, dass diese nur in Grenzen durch die Benutzer verändert werden kann, jedoch kann auch Unkenntnis über die einem Benutzer zur Verfügung stehenden Sicherheitsmechanismen und -einstellungen dazu führen, dass das System unsicher genutzt wird.

Umgang mit Notes Datenbanken

Daher sollten alle Benutzer im Umgang mit Lotus Notes geschult werden. Neben der reinen Nutzung der Client-Software ist es jedoch auch notwendig, die Funktionsweise der Datenbanken, mit denen ein Benutzer voraussichtlich arbeiten wird, zu erläutern und die Benutzer im Umgang mit der Datenbank zu schulen. Dies ist erforderlich, da Notes Datenbanken viele Funktionen anbieten können, so dass sie mehr als einen reinen Datenspeicher darstellen (daher auch die Bezeichnung "Notes-Applikationen" für Datenbanken).

Sicherheitsmechanismen

Den Benutzern müssen insbesondere die ihnen zur Verfügung stehenden Sicherheitsmechanismen deutlich gemacht werden, so dass sie in der Lage sind, diese korrekt und sinnvoll einzusetzen. Eine Schulung sollte u. a. folgende Themen behandeln:

- Überblick über Zugriffskontrollmechanismen auf einem Server
- Überblick über Zugriffskontrollmechanismen auf Datenbanken
- Detaillierte Darstellung der Nutzung von Zugriffslisten auf Datenbanken (Access Control List, ACL)
- Sicherer Umgang mit der Notes-ID und Nutzung der Inhalte einer Notes-ID
- Authentisierung an der Web-Schnittstelle und deren Schwächen und Stärken
- Einstellen von Zugriffsbeschränkungen beim Web-Zugriff auf Datenbanken
- Überblick über die Funktionsweise von symmetrischen und asymmetrischen kryptographischen Verfahren
- Umgang mit kryptographischen Zertifikaten (Anerkennen von Zertifikaten, Bedeutung von Cross-Zertifikaten)
- Sicherer Umgang mit Internet-Zertifikaten
- Erzwingen der Kommunikationsabsicherung durch Portverschlüsselung und SSL-Nutzung

- Beschränkungen für die Ausführung aktiver Inhalte im Notes-Client (Execution Control List, ECL)
- Nutzen der Verschlüsselungsverfahren für Datenbanken (Datenbank- und Feldverschlüsselung)
- Nutzen der E-Mail-Verschlüsselung und Zweck von E-Mail-Signaturen (Notes-Client und Browser)
- Sicherheitsunterschiede beim Zugriff mit dem Notes-Client und mit dem Browser

Kenntnis über Sicherheitsrichtlinien

Diese Themenliste muss anhand des vorliegenden Anwendungsfalls ggf. angepasst und erweitert werden. Neben der reinen Schulung zu den Notes-Sicherheitsmechanismen müssen die Benutzer jedoch auch Kenntnis über die Sicherheitsrichtlinien ihrer Organisation besitzen, damit diese bei der Nutzung der Sicherheitsmechanismen auch entsprechend umgesetzt werden können (siehe M 2.207 *Festlegen einer Sicherheitsrichtlinie für Lotus Notes*).

Ergänzende Kontrollfragen:

- Sind die Benutzer mit den Notes-Sicherheitsmechanismen vertraut und werden diese auch angewandt?
- Sind alle Benutzer mit den Inhalten der organisationseigenen Sicherheitsrichtlinie für Lotus Notes vertraut?

M 3.26 Einweisung des Personals in den sicheren Umgang mit IT

Verantwortlich für Initiierung: Leiter Personal, Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Personalabteilung, Vorgesetzte

Viele IT-Sicherheitsprobleme entstehen durch fehlerhafte Nutzung bzw. Konfiguration der IT. Um solchen Problemen vorzubeugen, sollten alle Mitarbeiter in den sicheren Umgang mit der IT eingewiesen werden. Hierzu sollten alle Mitarbeiter entsprechend geschult werden (siehe auch M 3.4 *Schulung vor Programmnutzung*, M 3.5 *Schulung zu IT-Sicherheitsmaßnahmen* und M 2.198 *Sensibilisierung der Mitarbeiter für IT-Sicherheit*).

Benutzerrichtlinien

Den IT-Benutzern sollten spezifische Richtlinien an die Hand gegeben werden, was sie im Umgang mit der IT beachten müssen. In einer solchen Richtlinie sollte verbindlich vorgeschrieben werden, welche Randbedingungen beim Einsatz der betrachteten IT-Systeme einzuhalten und welche IT-Sicherheitsmaßnahmen zu ergreifen sind. Dabei sind die Benutzer klar und unmissverständlich darauf hinzuweisen, was sie auf keinen Fall machen dürfen. Diese Richtlinien sollten verbindlich, verständlich und verfügbar sein. Um die Verbindlichkeit zu dokumentieren, sollten sie von der Behörden- bzw. Unternehmensleitung oder zumindest vom IT-Verantwortlichen unterzeichnet sein. Sie sollten kurz und verständlich gehalten sein, so dass sie beispielsweise als Merkzettel aufgehängt werden können. Zusätzlich sollten sie im Intranet abrufbar sein.

Positiv formulieren!

Benutzerrichtlinien sollten grundsätzlich nur Regelungen enthalten, die auch umgesetzt werden können. Benutzerrichtlinien sollten so positiv wie möglich formuliert werden. Beispielsweise könnte eine Benutzerrichtlinie statt:

> "Benutzer dürfen keine Software selbständig aufspielen."

folgenden Eintrag enthalten:

> "Alle IT-Systeme werden in einer Standardkonfiguration ausgeliefert, die auf Ihre spezifischen Arbeitsbedingungen angepasst wurde und Ihnen maximale Sicherheit bietet. Bei Problemfällen können wir Ihnen durch eine Neuinstallation der Standardkonfiguration eine schnelle Problemlösung garantieren. Bitte verändern Sie daher die Einstellungen möglichst nicht. Wenn Sie zusätzliche Hard- oder Software benötigen, wenden Sie sich bitte an den Benutzerservice."

Beispiele für Benutzerrichtlinien finden sich unter den Hilfsmitteln zum IT-Grundschutz.

Eine Benutzerrichtlinie für die allgemeine IT-Nutzung sollte mindestens die folgenden Punkte umfassen:

- Hinweis, dass keine IT-Systeme oder IT-Komponenten ohne ausdrückliche Erlaubnis benutzt werden dürfen
- Hinweis, dass nur diejenigen Mitarbeiter Informationen auf IT-Systemen ändern dürfen, die dazu autorisiert sind.

- Umgang mit Passwörtern (siehe M 2.11 *Regelung des Passwortgebrauchs*)
- Nutzungsverbot nicht freigegebener Software (siehe M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*)
- Hinweis, dass dienstliche IT-Systeme nur für dienstliche Zwecke eingesetzt werden dürfen
- Hinweise zur sicheren Verwahrung und Aufstellung von IT-Systemen und Datenträgern
- Schutz vor Computer-Viren
- Durchführung von Datensicherungen
- Nutzung von Internet-Diensten

Neben solchen Richtlinien müssen klare Aussagen darüber vorliegen, welche Benutzer auf welche Informationen zugreifen dürfen, an wen diese weitergegeben werden dürfen und welche Maßnahmen bei einem Verstoß gegen diese Richtlinien unternommen werden.

Auch bei kurzer Abwesenheit Arbeitsmittel schützen

Bei Verlassen des Arbeitsplatzes sollte sich jeder Benutzer davon überzeugen, dass jedes Arbeitsmittel (Dokumente, Datenträger, etc.) sicher verwahrt ist (siehe auch M 2.37 *"Der aufgeräumte Arbeitsplatz"*). Alle IT-Systeme sollten durch Passwörter gegen unbefugten Zugriff geschützt sein. Bei unbeaufsichtigten IT-Systeme sollten alle offenen Sitzungen beendet worden sein oder zumindest ein Bildschirmschoner aktiviert sein.

Die Grundkonfiguration aller IT-Systeme sollte möglichst eingeschränkt sein. In der Standardkonfiguration von Arbeitsplatzrechnern sollten nur die Dienste vorhanden sein, die von allen Benutzern einer Gruppe benötigt werden (siehe auch M 4.109 *Software-Reinstallation bei Arbeitsplatzrechnern*). Weitere Programme oder Funktionalitäten sollten nur dann aufgespielt bzw. freigeschaltet werden, wenn die Benutzer in deren Handhabung eingewiesen und für eventuelle Sicherheitsprobleme sensibilisiert wurden.

Jede Benutzerordnung sollte in Zusammenarbeit mit Vertretern aller beteiligten Gruppen erstellt werden, insbesondere sollten Betriebs- bzw. Personalrat und Datenschutz- sowie IT-Sicherheitsbeauftragte rechtzeitig beteiligt werden. Bei jeder Änderung einer Benutzerordnung ist darauf zu achten, dass diese wieder im Vorfeld beteiligt werden. Die geänderte Benutzerordnung muss allen Benutzern bekannt gegeben werden.

Sicherheitsaufgaben gehören in Aufgabenbeschreibung

Die Aufgabenbeschreibung sollte alle für die IT-Sicherheit relevanten Aufgaben und Verpflichtungen enthalten. Dazu gehört u. a. die Verpflichtung auf die hausinternen IT-Sicherheitsleitlinien (siehe auch M 2.198 *Sensibilisierung der Mitarbeiter für IT-Sicherheit*).

Werden IT-Systeme oder Dienste in einer Weise genutzt, die den Interessen der Behörde bzw. des Unternehmens widersprechen, sollte jeder, der davon Kenntnis erhält, dies seinen Vorgesetzten mitteilen. Gegebenfalls sind disziplinarische Maßnahmen einzuleiten.

M 3.27 Schulung zur Active Directory-Verwaltung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Das Active Directory ist die zentrale Datenbank von Windows 2000, in der Benutzerdaten, Gruppenzugehörigkeiten und andere Verwaltungsdaten abgelegt werden. Als Clients können im Active Directory nicht nur Windows 2000, sondern auch Windows XP Systeme verwaltet werden.

Für die Administration eines Windows 2000/XP Netzes werden detaillierte Kenntnisse des Active Directory und seiner grundlegenden Konzepte benötigt. Ansonsten kann es leicht zu Fehlkonfigurationen kommen, die erhebliche sicherheitstechnische Auswirkungen haben können. Eine Schulung der Administratoren auf diesem Gebiet und insbesondere zu Active Directory Sicherheitsthemen ist daher unerlässlich.

Im Folgenden wird in kurzen Stichpunkten zusammengefasst, welche Fachkenntnisse mindestens zur sicheren Administration des Active Directory notwendig sind. Um diese Stichpunkte auch begrifflich besser einordnen zu können, wird zunächst ein kurzer Abriss des Active Directory, seiner Strukturen und Komponenten dargestellt.

Active Directory - Abriss

Integrität verschiedener Domänen

Das Active Directory Konzept von Windows 2000 greift weiter als das Domänen-Konzept von Windows NT, da das Active Directory eine Integration verschiedener Domänen in ein Gesamtverzeichnis erlaubt. Das folgende Bild zeigt die mögliche Gesamtstruktur eines Windows 2000/XP Netzes:

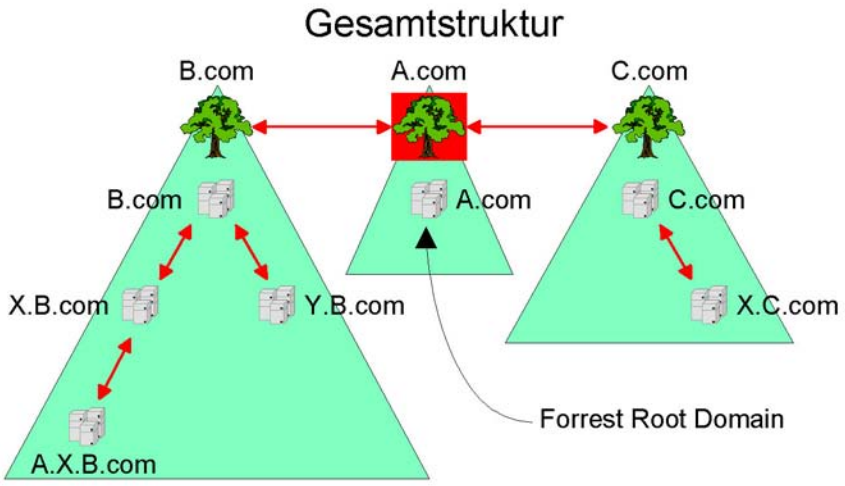


Abbildung: Gesamtstruktur eines Windows 2000/XP Netzes

Zwischen all diesen Domänen bestehen direkte (einzelne Pfeile) bzw. indirekte (über mehrere Pfeile hinweg) Kerberos-Vertrauensbeziehungen, so dass die Authentisierung eines Benutzers oder Computers über jeden Domain Controller des Forests vorgenommen werden kann. Windows 2000/XP nutzt zur

Namensauflösung von Rechnern das DNS (Domain Name Service) Verfahren des Internets, so dass jede Domäne über einen eindeutigen Namen im DNS-Format verfügen muss. Die Domänen sind dabei entsprechend ihrer Namen in einer Baumstruktur angeordnet. Eventuell sind in einem Windows 2000 Netz (Forest) mehrere solcher Bäume zusammengefasst. Die Gliederung eines Windows 2000 Netzes in Bäume hat Auswirkungen auf die technische Realisierung der Netzfunktionalität, jedoch keine unmittelbaren Auswirkungen für die Rechtevergabe und Delegation von administrativen Tätigkeiten. Hinweise zur Strukturierung eines Windows 2000 Netzes finden sich in M 2.229 *Planung des Active Directory*.

Forest Root Domäne

Die Administration von Windows 2000 erfolgt im Wesentlichen innerhalb der einzelnen Domänen. Übergreifende Bedeutung für das Active Directory hat dabei nur die so genannte *Forest Root* Domäne. Das ist die erste Domäne, die in einem Windows 2000 Netz installiert wird. Der Administrator dieser Forest Root Domäne ist in der Windows 2000 Voreinstellung das einzige Mitglied der beiden Gruppen *Schema-Admins* und *Organisations-Admins*.

Schema-Admins

Mitglieder der Gruppe *Schema-Admins* können die Struktur der Active Directory Datenbank, das so genannte *Schema* ändern. Durch das Schema wird bestimmt, aus welchen Objekten das Active Directory aufgebaut werden kann (Definition von Objekttypen), wie die Objekte selbst aufgebaut sind (Definition von Objektattributen) und wie die Objekte im Active Directory angeordnet werden können (Definition der Struktur). Schemaänderungen sind immer ein weitreichender Eingriff in ein Windows 2000 Netz, da sie immer alle Domänen des Forests betreffen. Außerdem können bestimmte Änderungen im Active Directory nicht mehr rückgängig gemacht werden.

Organisations-Admins

Die Mitglieder der Gruppe *Organisations-Admins*, zu der in der Voreinstellung der Administrator der Forest Root Domäne gehört, haben besondere Befugnisse in allen Domänen des Netzes. Sie können z. B. neue Domänen in den Forest aufnehmen und haben Administratorrechte auf allen Domänen Controllern des Netzes.

Domänen-Admins

Innerhalb einer einzelnen Domäne erfolgt die Administration durch Mitglieder der jeweiligen (domänen-spezifischen) Gruppe *Domänen-Admins*. Diese Gruppe verfügt innerhalb einer Domäne über unbeschränkte administrative Berechtigungen. Es ist jedoch möglich, einzelne administrative Aufgaben auch für andere Benutzerkonten zu ermöglichen und so administrative Aufgaben zu delegieren (siehe auch M 2.230 *Planung der Active Directory-Administration*).

Eine Delegation administrativer Aufgaben innerhalb einer Domäne kann auch so erfolgen, dass lediglich die Administration eines Teils der Benutzerkonten und Computer einer Domäne delegiert wird. Dies ist innerhalb der Grenzen der so genannten OUs (Organizational Units) möglich, die zur Gruppierung von Benutzer- bzw. Computerkonten innerhalb der Domäne dienen.

Gruppenrichtlinien

Eine Vielzahl von Windows 2000/XP Konfigurationsparametern ist in den *Gruppenrichtlinien* zusammengefasst. Neben den lokalen Gruppenrichtlinien auf jedem einzelnen Windows 2000/XP Rechner gibt es auch Gruppenrichtlinien, die im Active Directory gespeichert sind. Dies gestattet es, Rechner oder Benutzerkonten zentral zu konfigurieren. Wirkungsbereich einer solchen, im

AD gespeicherten Gruppenrichtlinie, können u. a. ganze Domänen oder OUs sein. Hier dienen OUs zur Gruppierung gleichartig konfigurierter Rechner oder Benutzerkonten. Da sich OUs schachteln lassen und mit einer einzelnen OU mehrere Gruppenrichtlinien verbunden sein können, wirken auf einen einzelnen Rechner u. U. viele verschiedene Gruppenrichtlinien ein (siehe auch M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000* und M 2.326 *Planung der Windows XP Gruppenrichtlinien*).

verteilte Datenbank

Technisch gesehen ist das Active Directory als eine verteilte Datenbank realisiert, die auf den Domänen-Controllern des Windows 2000 Netzes angesiedelt ist. Mit einigen Ausnahmen enthält jeder Domänen-Controller dabei nur die Daten seiner eigenen Domäne. Diese Ausnahmen sind:

- Jeder Domänen-Controller enthält die Schema- und Konfigurationsdaten des gesamten Forests.
- Mindestens ein Domänen-Controller jeder Domäne enthält zusätzlich noch den *Global Catalog*.

Global Catalog

Der Global Catalog enthält die komplette Baumstruktur des Active Directory des gesamten Forests, für jedes der Objekte in diesem Baum enthält der Global Catalog allerdings nur bestimmte Attribute.

Im Unterschied zu Windows NT lassen sich die meisten Änderungen an jedem Domänen-Controller einer Domäne durchführen. Um die Eindeutigkeit bestimmter kritischer Datensätze zu bewahren, gibt es allerdings

- zwei ausgezeichnete Aufgaben für Domänen-Controller innerhalb des Forests (*Schema Master* und *Domain Naming Master*) und
- drei ausgezeichnete Aufgaben für Domänen-Controller innerhalb einer jeden Domäne (*PDC Emulator*, *RID Master*, *Infrastructure Master*).

Flexible Single Master Operations

Diese Rollen werden in der Windows 2000 Terminologie auch als FSMO-Rollen (FSMO = Flexible Single Master Operations) bezeichnet. Bestimmte Änderungen können daher nur an dem Rechner vorgenommen werden, dem die jeweilige Rolle zugeordnet ist.

Der Abgleich der Daten zwischen den einzelnen Domänen-Controllern kann über zwei verschiedene Replikationsmechanismen erfolgen. Welcher Mechanismus verwendet wird, lässt sich ebenso konfigurieren wie die Zeitabstände, in denen die Replikation erfolgt.

Durch das Konzept der verteilten Datenbank kann eine gewisse Ausfallsicherheit des Active Directory erreicht werden, problematisch sind dabei jedoch die Inhaber der FSMO-Rollen.

Schulungsinhalte

Grundwissen

Die Administration eines Windows 2000/XP Netzes wird im Allgemeinen, je nach Größe und Komplexität des Netzes, nicht von einem einzelnen Administrator, sondern von einer ganzen Reihe von Administratoren mit speziellen Aufgaben und Tätigkeitsbereichen durchgeführt. Insoweit besteht auch nicht für alle Administratoren eines Windows 2000/XP Netzes der gleiche Schulungsbedarf. Zur Gewährleistung eines sicheren Betriebes muss jedoch jeder Administrator über ein hinreichendes Grundwissen verfügen, um seine eigenen Tätigkeiten in einen Gesamtkontext einordnen zu können.

Schulungsinhalte sollten in jedem Fall die folgenden Stichpunkte umfassen und diese erläutern. Wie tief ein Administrator sich mit den einzelnen Punkten beschäftigen muss, hängt von seinem späteren Tätigkeitsfeld ab.

Grundlagen

- Überblick über die Sicherheitsmechanismen von Windows 2000
- Neuerungen in Sicherheitsmechanismen von Windows XP (mit Berücksichtigung der von aktuellen Service Packs hervorgerufenen Änderungen)
- Sicherheitsverwaltung (MMC, Security Editor, GPMC)
- Active Directory und DNS
- Vertrauensbeziehungen zwischen Domänen
- Notwendiger physikalischer Schutz aller Domänen-Controller als Träger der Kerberos Daten

Active Directory

- Allgemeines: Planung, Einrichtung, Administration
- Schema-Verwaltung
- Replikation
- Backup
- Rechtevergabe
- Authentisierung
- Gruppenrichtlinien

PKI (Public Key Infrastruktur)

- Funktionsweise einer PKI
- Zertifikate und Zertifikatstypen
- Planung einer PKI

- Einrichten einer PKI
- Verwalten einer PKI
- Benutzerinteraktion mit der PKI

EFS (Encrypting File System)

- Funktionsweise des EFS
- Konfiguration des EFS (Recovery-Agent, Zertifikate)
- Schlüsselbackup
- Schutz verschlüsselt gespeicherter Dateien bei der Netzkommunikation

IPSec

- Funktionsweise des IPSec
- Konfiguration des IPSec
- Umgang mit *ipsecmon.exe* oder einem IPSec-Monitor eines Drittherstellers

WFP (Windows File Protection)

- Funktionsweise der WFP
- Konfigurationsmöglichkeiten der WFP

DFS (Distributed File Service)

- Funktionsweise des DFS
- Administration des DFS
- Planung der DFS-Struktur
- Schutz der über DFS zugreifbaren Daten

Die einzelnen Active Directory Themen sollten dabei wie folgt detaillierter dargestellt werden:

Schema-Verwaltung

Im Normalfall ist eine installationsspezifische Veränderung des AD-Schemas durch einen Administrator nicht notwendig. Die Schulung kann sich insofern auf die Problematik und Auswirkungen von Schema-Veränderungen beschränken.

Sollen individuelle Anpassungen des Schemas vorgenommen werden, sind weitergehende Schulungen zu Interna des Active Directory notwendig.

Replikation des Active Directory

- Verwendete Mechanismen zur Replikation des Active Directory (RPC und SMTP)
- Voreingestellte Parameter zur Replikation von Active Directory Inhalten
- Problematik der dezentralen Administration des AD im Zusammenhang mit Replikationskonflikten

Backup

- Problematik des Erstellens eines "Backups des Active Directory"
- Wiedereinspielen von Backups eines Domänen-Controllers
- Zu ergreifenden Maßnahmen bei Ausfall von Domänen-Controllern, die FSMO-Rollen innehaben

Rechtevergabe im Active Directory

- Vergabe von Zugriffsrechten auf AD-Objekte auf Attributsebene
- Vererbung von Zugriffsrechten und Blockade der Vererbung
- Mögliche Zugriffsrechte
- Delegation von administrativen Aufgaben auf der Ebene einzelner OUs

Authentisierung

- Kerberos
- PKI
- Smart Cards

Gruppenrichtlinien

- Lokale Gruppenrichtlinien und im Active Directory gespeicherte Gruppenrichtlinien
- Konfigurationsmöglichkeiten mit Hilfe von Gruppenrichtlinien
- Wann werden Gruppenrichtlinien angewandt? Wie lässt sich dies konfigurieren?
- Gruppenrichtlinienobjekte (GPOs) sind Objekte im Active Directory
- Gruppenrichtlinienobjekte können an Standorte / Domänen / OUs gebunden werden
- Reihenfolge, in der Gruppenrichtlinien abgearbeitet werden
- Möglichkeiten, die Anwendung von Gruppenrichtlinien zu kontrollieren
  - Vergabe von Zugriffsrechten auf Gruppenrichtlinien
  - *No Override* Eigenschaft der Bindung eines Gruppenrichtlinienobjektes an ein AD-Objekt
  - *Block Policy Inheritance* Eigenschaft von AD-Objekten
- Möglichkeiten zur selektiven Anwendung der Gruppenrichtlinien unter Windows XP:
  - *Sicherheitsfilter*
  - *WMI Filters*

Ergänzende Kontrollfragen:

- Wurden alle Administratoren für die Arbeit mit Windows 2000/XP geschult?
- Ist der Umgang mit allen relevanten Sicherheitsmechanismen dargestellt worden?

M 3.28 Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Vorgesetzte, Leiter IT

Die Sicherheit der auf Windows 2000/XP Rechnern gespeicherten Daten hängt zu einem großen Teil auch vom korrekten Umgang der Benutzer mit den Windows 2000/XP Sicherheitsmechanismen ab. Um diese effektiv nutzen zu können, sollten Benutzer von Windows 2000/XP Rechnern entsprechend geschult werden.

Benutzersicht auf Sicherheitsmechanismen

Beim Umgang mit Windows 2000/XP Rechnern kann ein großer Teil der sicherheitsrelevanten Einstellungen dem Benutzer durch entsprechende Vorarbeiten und Voreinstellungen des Administrators abgenommen werden. Um einheitliche und überprüfbare Rechnerkonfigurationen zu erhalten, ist ein solches Vorgehen unabdingbar.

Zugriffsrechte auf eigene Dateien und Verzeichnisse

Einige sicherheitsrelevante Einstellungen können allerdings vom Benutzer selbst vorgenommen werden. Dazu gehören die Zugriffsrechte auf die eigenen Dateien und Verzeichnisse eines Benutzers. Die Zugriffsrechte darauf können einzelnen Benutzern oder Benutzergruppen eingeräumt bzw. verweigert werden. Widersprechen sich die für einen Benutzer konfigurierten Zugriffsrechte (z. B. weil der Benutzer Mitglied der beiden Gruppen A und B ist, wobei der Zugriff für Gruppe A zugelassen ist, während er für Gruppe B verweigert wird), so wird der Zugriff verweigert. Generell gilt zunächst auch hier, dass die Zugriffsrechte auf die eigenen Dateien eines Benutzers vom Administrator voreingestellt und automatisch auf neue Dateien und Ordner übertragen werden. Da Benutzer jedoch in der Regel die Möglichkeit besitzen, die Zugriffsrechte zu verändern, ist es notwendig, dass jeder Benutzer entsprechend geschult wird (siehe dazu auch M 4.149 *Datei- und Freigabeberechtigungen unter Windows 2000/XP*).

Encrypting File System

Ein weiterer Punkt, auf den eine Benutzerschulung eingehen muss, ist die Verwendung des verschlüsselnden Dateisystems EFS (Encrypting File System). Neben der Vermeidung von Fallstricken bei der Benutzung des EFS sollte hier vor allem vermittelt werden, in welchem Ausmaß EFS die Vertraulichkeit von Dateien schützen kann, und wo dieser Schutz aufhört (siehe auch M 4.147 *Sichere Nutzung von EFS unter Windows 2000/XP*).

Schulungsinhalte

Die folgenden Stichpunkte fassen notwendige Schulungsinhalte für den sicheren Umgang von Benutzern mit Windows 2000/XP zusammen:

Verwendung von Zugriffsrechten im NTFS Dateisystem

- Schutz von Dateien durch Zugriffsrechte
- Vererbung von Zugriffsrechten
- Kopieren und Verschieben von Dateien
- Übergabe einer Datei an einen neuen Besitzer

- Sensibilisierung für Beschränkungen des Schutzes von Dateien durch Zugriffsrechte
  - Benutzer mit administrativen Rechten können Zugriffsrechte umgehen.
  - Bei direktem Zugriff auf die Hardware (z. B. nach Diebstahl) lassen sich Zugriffsrechte umgehen.
  - Dateien sind beim Transport über das Netz nicht geschützt.

Benutzung von EFS (siehe auch M 4.147 *Sichere Nutzung von EFS unter Windows 2000/XP*)

- Nutzen von EFS (EFS bietet einen zusätzlichen Schutz der Vertraulichkeit von Dateien)
- Bedienung von EFS
- Problematik des "nachträglichen Verschlüsselns"
- Geeignete Passwort-Auswahl (Passwortqualität ist wesentlich für die Effektivität von EFS)
- Verwendung eines zusätzlichen Startpasswortes mittels SYSKEY (wesentlich bei Verwendung lokaler Benutzerkonten)
- Sensibilisierung für Beschränkungen des Schutzes durch EFS
  - Benutzer mit administrativen Rechten können die Verschlüsselung umgehen.
  - Verschlüsselt gespeicherte Dateien sind beim Transport über das Netz nicht geschützt, es sei denn, EFS wird mit WebDAV verwendet.

Sonstige Sicherheitshinweise

- Sicheres Löschen von Dateien (siehe auch M 4.56 *Sicheres Löschen unter Windows-Betriebssystemen*, die analog auch auf Windows 2000/XP zutrifft)
- Sicherheitshinweise zum automatischen Erkennen von CD-ROMs bzw. zur Autostart-Funktion (siehe auch M 4.57 *Deaktivieren der automatischen CD-ROM-Erkennung*)
- Sicherheitshinweise zum sicheren Umgang mit USB-Speichermedien (siehe auch M 4.200 *Umgang mit USB-Speichermedien*)
- Sicherheitshinweise zur sicheren Benutzung von Windows XP-spezifischen Sicherheitstechnologien wie Sicherheitszentrum, Windows Firewall und WPA (WiFi Protected Access)

Ergänzende Kontrollfragen:

- Wurde eine Benutzerschulung zur Windows 2000/XP Sicherheit durchgeführt?
- Sind die Benutzer in die Vergabe von Zugriffsrechten auf eigene Dateien eingewiesen worden?
- Wurden die Benutzer auf die Sicherheitsmechanismen der verwendeten Werkzeuge hingewiesen und in deren Nutzung geschult?

M 3.29 Schulung zur Administration von Novell eDirectory

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Für die Administration eines eDirectory-Verzeichnisdienstes werden detaillierte Kenntnisse über dieses Produkt und seine grundlegenden Konzepte benötigt. Sind diese Kenntnisse nicht vorhanden, kann es leicht zu Fehlkonfigurationen kommen, die erhebliche sicherheitstechnische Auswirkungen haben können. Eine Schulung von Administratoren auf diesem Gebiet ist daher unerlässlich.

Im Folgenden wird kurz zusammengefasst, welche Themen bei der Schulung der Administratoren behandelt werden sollten.

hierarchische Struktur

Der eDirectory-Verzeichnisdienst ist baumartig hierarchisch strukturiert. Die einzelnen Knotenpunkte des Verzeichnisbaums bestehen aus den *Container*-Objekten, die wiederum andere Objekte enthalten können, und den so genannten *Leaf*-Objekten, welche die Endpunkte (Blätter) des Verzeichnisbaums darstellen. Jedes Objekt gehört einer eindeutigen Objektklasse an. Die Objektklasse definiert die Werte bzw. Attribute oder auch Eigenschaften, welche einem Objekt dieser Objektklasse zugewiesen werden können. Zudem werden hierarchische Relationen darin definiert, d. h. was potentielle Vater- und Kindobjekte sein können. Es gibt dafür bereits eine Anzahl seitens eDirectory vordefinierter Objektklassen. Die Definitionen der Objektklassen werden im so genannten Schema festgehalten. Werden Veränderungen an der Definition einzelner Objektklassen vorgenommen, z. B. eine Erweiterung des zugehörigen Attributsatzes, so geschieht dies über eine Änderung bzw. Erweiterung des Schemas. Eine Schemaänderung ist gewissermaßen die sensibelste Operation überhaupt, die an einem eDirectory-Verzeichnisbaum vorgenommen werden kann. Diese hat Auswirkungen auf den gesamten Baum, so dass die bisherige Konzeption des Baums neu überdacht werden muss. Die Administration des eDirectory-Schemas verlangt daher eine hohe Kompetenz im Verzeichnisdienst und ein sehr hohes Sicherheitsbewusstsein.

Zugriffsrechte und Vererbung

Jedem einzelnen Objekt und jeder Objektklasse können Zugriffsrechte auf die einzelnen Attribute des Objektes erteilt werden. Die explizite Zuweisung erfolgt dabei über die *Trustee*-Beziehungen, d. h. Eintragung von Trustees in die *Access Control List* (ACL). Die Rechte reichen dabei von *Supervisor*, d. h. einem vollständigen Administrationsrecht, bis hin zum *Browsen*, was das Durchlaufen des entsprechenden Verzeichnisbaum-Abschnittes gestattet. Die Zugriffsrechte auf die Objekte vererben sich dabei standardmäßig in der Baumhierarchie von oben nach unten. Es ist jedoch möglich, Einfluss auf den Vererbungsprozess zu nehmen, in dem so genannte *Inherited Rights Filter* (IRF) eingeführt werden. Mit diesen Filtern können automatische Vererbungen explizit ausgeblendet werden. Weiterhin besteht die Möglichkeit, so genannte Sicherheitsäquivalenzen zwischen einzelnen Objekten bzw. Objektklassen X und Y zu definieren. Dabei werden sämtliche Trustees von Objekt X automatisch auch zu Trustees von Objekt Y, d. h. das Objekt Y besitzt zumindest die gleichen Zugriffsmöglichkeiten wie Objekt X.

effektive Rechte

Schließlich kommen beim eDirectory-Zugriff dann die *effektiven Rechte* zum tragen, welche die Folge der oben genannten Rechtevergabe darstellen und bei jedem einzelnen Zugriff dynamisch berechnet werden.

Authentisierung

Im Intranet greifen die Benutzer über geeignete Clientsoftware auf das eDirectory zu. Der Zugriff der Clients auf das eDirectory erfolgt dabei über ein proprietäres Protokoll, bei dem der private Schlüssel des sich anmeldenden Benutzers vom eDirectory verschlüsselt an den Client geschickt wird. Bei dieser Verschlüsselung ist das Benutzerpasswort involviert. Gibt der Benutzer nun sein Passwort ein, so kann der Client den privaten Schlüssel entschlüsseln, und zwischen dem Client und dem eDirectory-Server findet ein Challenge-/Response-Verfahren zur Authentisierung statt. Bei erfolgreicher Authentisierung besitzt der Benutzer nun die für ihn definierten Zugriffsrechte auf das eDirectory.

LDAP-Zugriff

Netzapplikationen und Internet-Benutzer greifen in der Regel über das LDAP-Protokoll auf den eDirectory-Verzeichnisdienst zu. Hierbei gibt es standardmäßig drei verschiedene Anbindungsarten: den *anonymous bind*, den *proxy user anonymous bind* sowie den *NDS-user bind*. Die Voreinstellung ist, dass der anonyme Login dabei die Rechte des [Public] Objektes hat, welches standardmäßig das uneingeschränkte *Browse*-Recht auf den gesamten Verzeichnisbaum besitzt. Der anonyme Login setzt keine Authentisierung voraus. Für die Passwort-Authentisierung kann konfiguriert werden, ob dabei das Passwort im Klartext übertragen werden darf oder nicht. Für eine gesicherte Anbindung über LDAP steht das SSL-Protokoll zur Verfügung, und zwar wahlweise mit ein- oder zweiseitiger Authentisierung.

Zertifikatsserver

Der eDirectory-Zertifikatsserver spielt eine wichtige Rolle für die Rechtevergabe und damit für die Systemsicherheit. Ebenso hängen die Authentisierungen im Netz sowie der Aufbau eines verschlüsselten Kanals (via SSL) vom Zertifikatsmanagement ab. Die sorgfältige Administration des eDirectory-Zertifikatsservers ist daher besonders wichtig.

Partitionierung

Der eDirectory-Verzeichnisdienst erlaubt zur Verbesserung der Skalierbarkeit und Performance eine Partitionierung der Verzeichnisdatenbank auf mehrere Server. Für die Partitionierung eines Verzeichnisbaums sind dabei eine Reihe von Regeln zu beachten, siehe dazu M 2.237 *Planung der Partitionierung und Replikation im Novell eDirectory*

Replikation

Wie die Vorgängerprodukte unterstützt der eDirectory-Verzeichnisdienst *Repliken* zur Erhöhung der Fehlertoleranz und des Systemdurchsatzes. Dabei gibt es mehrere Typen von Repliken, nämlich *Master Replica*, *Read/Write Replica*, *Read-Only Replica*, *Filtered Read/Write Replica*, *Filtered Read-Only Replica* sowie *Subordinate Reference Replica*. Detaillierte Hinweise hierzu finden sich in M 2.237 *Planung der Partitionierung und Replikation im Novell eDirectory*

rollenbasierte Administration und Delegation

eDirectory unterstützt die rollenbasierte Administration sowie die Delegation von Administrationsaufgaben. Entsprechend den bei der Planung getroffenen Entscheidungen (siehe M 2.236 *Planung des Einsatzes von Novell eDirectory* sowie M 2.238 *Festlegung einer Sicherheitsrichtlinie für Novell eDirectory*) müssen die verschiedenen Administratoren für ihre jeweilige Aufgabe geschult werden. Dies gilt besonders für die Gruppe der Schema-

administratoren, die in der Lage sind, das gesamte Datenbankdesign des Verzeichnisbaums zu verändern (siehe oben).

Clientsoftware

Auch die Administration der eDirectory-Clientsoftware und des LDAP-Zugriffs setzt detaillierte Kenntnisse über die Konfigurationsmöglichkeiten des Systems voraus. Dabei spielt auch das zugrunde liegende Betriebssystem eine Rolle für die Definition einer Sicherheitsumgebung, insbesondere der Dateisystemsicherheit.

Weiterhin müssen auch die für das Logging und Monitoring zuständigen Administratoren genauestens in ihre Tätigkeit eingewiesen werden.

Schulungsinhalte

Grundwissen

Die Administration eines eDirectory-Verzeichnisbaums wird im Allgemeinen, je nach Größe des Netzes, nicht von einem einzelnen Administrator, sondern von einer ganzen Reihe von Administratoren mit speziellen Aufgaben und Tätigkeitsbereichen durchgeführt. Insoweit besteht auch nicht für alle Administratoren eines eDirectory-Verzeichnisses der gleiche Schulungsbedarf. Zur Gewährleistung eines sicheren Betriebes muss jedoch jeder Administrator über ein hinreichendes Grundwissen verfügen, damit er seine eigenen Tätigkeiten in einen Gesamtkontext einordnen kann.

Schulungsinhalte sollten in jedem Fall die folgenden Stichpunkte umfassen und diese erläutern. Wie tief sich ein Administrator mit den einzelnen Aspekten beschäftigen muss, hängt von seinem späteren Tätigkeitsfeld ab.

Grundlagen
- Überblick über die Sicherheitsmechanismen von eDirectory
- Sicherheitsverwaltung (ConsoleOne, iMonitor)
- Baumstruktur und Namensauflösung
- Vererbung innerhalb des Verzeichnisbaums
- notwendiger physikalischer Schutz aller eDirectory-Server inklusive Replica

Verzeichnisdienst
- Allgemeines: Planung, Einrichtung, Administration
- Schema-Verwaltung
- Partitionierung
- Replikation
- Backup
- Rechtevergabe
- Rechtevererbung und Kalkulation der effektiven Rechte
- Authentisierung

Public Key Infrastruktur (PKI)
- Funktionsweise einer PKI
- Zertifikate und Zertifikatstypen
- Planung einer PKI
- Benutzerinteraktion mit der PKI
- eDirectory-Key Management Objects
- Administration des eDirectory-Zertifikatsservers

Secure Sockets Layer (SSL)
- Funktionsweise des SSL-Protokolls
- Konfiguration von SSL

Lightweight Directory Access Protocol (LDAP)
- LDAP-Zugriff auf das eDirectory
- mögliche Anbindungen der Benutzer

Novell Client
- Funktionsweise des Novell Clients
- Authentisierung des Novell Clients

Die einzelnen Themen sollten dabei wie folgt detaillierter dargestellt werden:

Schema-Verwaltung

Oftmals ist eine installationsspezifische Veränderung des eDirectory-Schemas durch einen Administrator nicht notwendig. Die Schulung kann sich insofern auf die Problematik und die Auswirkungen von Schema-Veränderungen beschränken. Sollen individuelle Anpassungen des Schemas vorgenommen werden, sind weitergehende Schulungen zu Interna von eDirectory notwendig.

Replikation
- Verwendete Mechanismen zur Replikation
- Voreingestellte Parameter zur Replikation von eDirectory-Inhalten
- Problematik der dezentralen Administration des eDirectory im Zusammenhang mit Replikationskonflikten

Backup
- Problematik des Erstellens eines "Backups des eDirectory"
- Wiedereinspielen von Backups eines eDirectory-Servers
- zu ergreifende Maßnahmen beim Ausfall von eDirectory-Servern, die die Baumstruktur definieren (d. h. die erste eDirectory-Installation innerhalb eines Verzeichnisbaums)

Rechtevergabe im eDirectory
- Vergabe von Zugriffsrechten auf eDirectory-Objekte auf Attributsebene
- Vererbung von Zugriffsrechten und Blockade der Vererbung
- Definition von Sicherheitsäquivalenzen
- effektive Zugriffsrechte
- rollenbasierte Administration
- Delegation von administrativen Aufgaben

Auch wenn eine Rollentrennung zwischen der Administration des eDirectory-Verzeichnisses und des zugrunde liegenden Betriebssystems in Kraft ist, sollte den eDirectory-Administratoren Grundlagenwissen zum Betriebssystem vermittelt werden. Anderenfalls wird eine Zusammenarbeit bei der Problemlösung erschwert.

Ergänzende Kontrollfragen:

- Wurden alle Administratoren für die Arbeit mit eDirectory geschult?
- Ist der Umgang mit allen relevanten Sicherheitsmechanismen dargestellt worden?

M 3.30 Schulung zum Einsatz von Novell eDirectory Clientsoftware

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Vorgesetzte

Für den Einsatz im Intranet wird der eDirectory-Verzeichnisdienst auf einem oder in der Regel mehreren Servern installiert. Die im eDirectory eingerichteten Benutzer und Benutzergruppen können dann über geeignete eDirectory-Clientsoftware auf den Verzeichnisdienst zugreifen, entsprechend der ihnen im eDirectory erteilten Rechte.

Authentisierung des Benutzers

Je nach Art der eingesetzten Clientsoftware erfolgt der Zugriff auf eDirectory für den Benutzer transparent, so dass eine Schulung zu eDirectory-spezifischen Aspekten der Software für den Benutzer nicht notwendig ist. Sofern der eingesetzte Client jedoch eine Authentisierung des Benutzers gegenüber dem eDirectory erfordert, wie z. B. der Novell Client für Windows, müssen dem Benutzer in einer Schulung zumindest die folgenden Inhalte vermittelt werden:

- Funktionsweise und Anwendung des verwendeten Login-Mechanismus,
- Umgang mit Passwörtern sowie
- Umgang mit SSL-Authentisierung über Benutzer-Zertifikat oder Passwort.

Durchlaufen des Verzeichnisbaums

Wird ein LDAP-Client verwendet, der dem Benutzer ein Durchlaufen des hierarchisch angeordneten Verzeichnisbaums oder die Formulierung eigener Suchanfragen auf der Ebene von LDAP-Attributen erlaubt, so ist zusätzlich eine Schulung der Benutzer zu den Themen

- Informationsmodell von eDirectory und
- effiziente Formulierung von Suchanfragen

erforderlich.

unterschiedliche Client-Applikationen

Neben den generellen Verzeichnisdienst-Clients (dem *Novell Client für Windows* sowie Libraries für Unix-Betriebssysteme) gibt es noch eine Klasse weiterer Client-Applikationen für eDirectory, die ganz speziell zur Benutzerverwaltung in (auch heterogenen) IT-Landschaften dienen: das *Novell Account Management Modul*. Diese Applikationen sind in den Anmeldevorgang der entsprechenden Betriebssysteme eingebunden und übernehmen so auch die Authentisierung von Benutzern. Daneben stehen die NDS-AS (NDS Authentication Service) für eine ganze Reihe von Plattformen (Linux, FreeBSD, HP-UX, MVS, OS/390, Solaris) zur Verfügung. NDS-AS setzt den Einsatz von Netware voraus (ab Netware 5.0, SP 4A).

Single Sign On

Die Authentisierung ist ein wesentlicher Aspekt beim sicheren Betrieb von eDirectory. Aus Sicht des Verzeichnisdienstes sollte dabei sichergestellt sein, dass sich sowohl der Client gegenüber dem System authentisiert, als auch der Benutzer gegenüber dem Client. War die Authentisierung erfolgreich, so bietet eDirectory einen automatisierten Zugriff auf sämtliche für ihn zugängliche Objekte und Services (so genannte *Background Authentication*). Auf diese Weise wird ein *Single Sign On* realisiert.

Challenge-Response-Verfahren

Die Authentisierung umfasst dabei folgende Schritte: Der Benutzer gibt beim Novell Client seinen Benutzernamen ein, welcher direkt an das eDirectory weitergeleitet wird. eDirectory sucht den zugehörigen privaten Schlüssel aus seinem Verzeichnis und verschlüsselt diesen. Bei dieser Verschlüsselung ist das Benutzerpasswort sowie ein Geheimnis des Clients involviert. Dieser verschlüsselte *private key* wird an den anfragenden Client übertragen. Der Benutzer wird nun nach seinem Passwort gefragt, welches er dem Client mitteilt. Der Client entschlüsselt daraufhin mit Hilfe dieses Passwortes und dem Client-Credential den privaten Schlüssel und hält ihn im Arbeitsspeicher. Auf Basis dieses *private keys* sowie dem Zertifikatsgegenstück findet nun die eigentliche Authentisierung mit dem eDirectory gemäß einem *Challenge-/Response*-Verfahren statt. Ist dieses erfolgreich, so ist der Benutzer eingeloggt und der private Schlüssel des Benutzers wird aus dem Arbeitsspeicher des Clients gelöscht.

Nach außen erscheint das System somit wie ein Passwort-gestütztes Authentisierungsschema, nach innen werden asymmetrische kryptographische Mechanismen eingesetzt.

Die Sicherheit der auf eDirectory-Servern gespeicherten Daten hängt zu einem großen Teil auch vom korrekten Umgang der Benutzer mit den Sicherheitsmechanismen ab. Um diese effektiv nutzen zu können, sollten Benutzer von eDirectory-Clientsoftware entsprechend geschult werden.

Benutzersicht auf Sicherheitsmechanismen

Zugriffsrechte auf eigene Dateien und Verzeichnisse

Beim Umgang mit eDirectory-Clientsoftware kann ein großer Teil der sicherheitsrelevanten Einstellungen dem Benutzer durch entsprechende Vorarbeiten und Voreinstellungen des Administrators abgenommen werden. Um einheitliche und überprüfbare Client-Konfigurationen zu erreichen, ist ein solches Vorgehen unabdingbar. Einige sicherheitsrelevante Einstellungen müssen allerdings vom Benutzer selbst vorgenommen werden. Dazu gehören in der Regel auf der Ebene des Betriebssystems die Zugriffsrechte auf die eigenen Dateien und Verzeichnisse eines Benutzers. Eine Verwaltung der Zugriffsrechte auf Dateien mit den Mitteln von eDirectory ist direkt nur für Datei-Server auf Basis des Betriebssystems *Netware* möglich. Indirekt sind Dateizugriffsrechte auf anderen Plattformen über die *Organizational Roles* administrierbar.

Schulungsinhalte

Die folgenden Stichpunkte fassen die relevanten Schulungsinhalte zusammen. Anhand des Nutzungsszenarios sollte hieraus eine geeignete Auswahl getroffen werden:

- Funktionsweise und Anwendung des verwendeten Login-Mechanismus,
- Umgang mit Passwörtern,
- Umgang mit SSL-Authentisierung über Benutzer-Zertifikat oder Passwort,
- Informationsmodell von eDirectory,
- effiziente Formulierung von Suchanfragen,
- Grundkenntnisse über die unterliegenden Betriebssysteme und deren Sicherheitskonfiguration sowie
- sicheres Löschen von Dateien (siehe z. B. auch M 4.56 *Sicheres Löschen unter Windows-Betriebssystemen*).

Ergänzende Kontrollfragen:

- Wurde eine Benutzerschulung zur eDirectory-Sicherheit durchgeführt?
- Wenn Benutzer Zugriffsrechte auf eigene Verzeichnisobjekte vergeben können, wurden sie in den notwendigen Konzepten und Mechanismen geschult?
- Wurden die Benutzer auf die Sicherheitsmechanismen der verwendeten Werkzeuge hingewiesen und in deren Nutzung geschult?

M 3.31 Schulung zur Systemarchitektur und Sicherheit von Exchange 2000 für Administratoren

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Leiter IT

Um ein Exchange 2000 System korrekt und sicher administrieren zu können, ist die Schulung der verantwortlichen Administratoren unumgänglich. Schon kleine Konfigurationsfehler können dazu führen, dass die Systemsicherheit beeinträchtigt wird. Aus diesem Grund müssen Administratoren über die Systemarchitektur und besonders über die Sicherheitsmechanismen von Exchange 2000 informiert werden.

Kenntnisse über Active Directory

Exchange 2000 integriert sich in hohem Maße in das Active Directory von Windows 2000. Das Active Directory ist die zentrale Datenbank von Windows 2000, in der Benutzerdaten, Gruppenzugehörigkeiten und andere Verwaltungsdaten abgelegt werden. Für die Administration von Exchange 2000 werden daher Kenntnisse über das Active Directory und seine grundlegenden Konzepte benötigt. Sonst kann es leicht zu Fehlkonfigurationen kommen, die erhebliche sicherheitsrelevante Auswirkungen haben können. Eine Schulung der Administratoren auf diesem Gebiet ist daher unerlässlich (siehe auch M 3.27 *Schulung zur Active Directory-Verwaltung*).

Routing Group

Bei der Installation von Exchange 2000 auf einem Windows 2000 Server wird eine Schema-Erweiterung vorgenommen, um spezifische Exchange-Objekte sowie zusätzliche Attribute zu bereits bestehenden Objekten zu erzeugen. Im weiteren Verlauf der Installation sind die sogenannten *Routing Groups* und die *Administrative Gruppe* festzulegen. Dabei ist die Routing Group ein Verbund von Exchange 2000 Servern, die über eine hohe Bandbreite miteinander kommunizieren. Die administrative Gruppe legt die administrativen Grenzen des E-Mail-Systems bzw. von Teilsystemen fest. Diese Grenzen können durchaus domänenübergreifend sein, müssen jedoch innerhalb eines *Forests* liegen.

Global Catalog Server

Das Exchange 2000 System verlangt die ständige Verfügbarkeit eines *Global Catalog Servers*, der von speziellen Windows 2000 Domänen Controllern angeboten wird. Außerdem müssen die Windows 2000 Netzdienste (speziell DNS) eingerichtet und funktionsfähig sein. Danach muss die externe Anbindung und die Verbindung zu eventuell vorhandenen fremden E-Mail-Systemen, z. B. X.400 oder ccMail, vorgenommen werden. Dabei sind die jeweiligen Protokolle zu aktivieren und es müssen entsprechende Regeln auf den betroffenen Firewalls definiert werden.

Schließlich müssen dann noch E-Mail-Konten und News-Gruppen konfiguriert werden. Dies geschieht mittels Windows 2000 Gruppenrichtlinien. Weitere allgemeine Hinweise zu Gruppenrichtlinien finden sich in M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000*.

Die beschriebenen Aspekte beziehen sich jedoch nur auf die Server-Komponente des Exchange/Outlook 2000-Systems. Für das Gesamtsystem ist zusätzlich auch die Administration der Client-Komponente wichtig.

Entsprechend dem oben skizzierten Vorgehen ergeben sich in der Folge eine Reihe administrativer Aufgaben, die von einem oder mehreren spezialisierten

Teams bewerkstelligt werden müssen. Eine intensive Schulung der Administratoren und ihrer Stellvertreter ist deshalb für das reibungslose Funktionieren des Systems besonders wichtig.

Die Schulung der Administratoren sollte zumindest folgende Themen umfassen:

Grundlagen

- Überblick über die Sicherheitsmechanismen von Windows 2000
- Sicherheitsverwaltung (MMC-Snap-In)
- Active Directory und DNS
- Vertrauensbeziehungen zwischen Domänen
- Möglichkeiten der Zugriffskontrolle auf Server

Active Directory

- Replikation
  - Verwendete Mechanismen zur Replikation des Active Directory (RPC und SMTP)
  - Voreingestellte Parameter zur Replikation von Inhalten des Active Directory
  - Problematik der dezentralen Administration des AD im Zusammenhang mit Replikationskonflikten
- Backup
  - Problematik beim Erstellen eines "Backups des Active Directory"
  - Wiedereinspielen von Backups eines Domänen-Controllers
- Rechtevergabe
  - Zugriffsrechte auf AD-Objekte können auf Attributsebene vergeben werden
  - Vererbung von Zugriffsrechten und Blockade der Vererbung
  - Mögliche Zugriffsrechte
  - Delegation von administrativen Aufgaben auf der Ebene einzelner OUs
- Gruppenrichtlinien
  - Lokale Gruppenrichtlinien und im Active Directory gespeicherte Gruppenrichtlinien
  - Konfigurationsmöglichkeiten durch Gruppenrichtlinien
  - Wann werden Gruppenrichtlinien angewandt? Wie lässt sich dies konfigurieren?
  - Gruppenrichtlinienobjekte (GPOs) als Objekte im Active Directory

- Gruppenrichtlinienobjekte können an Standorte / Domänen / OUs gebunden werden
- Reihenfolge, in der Gruppenrichtlinien abgearbeitet werden
- Möglichkeiten, die Anwendung von Gruppenrichtlinien zu kontrollieren (Zugriffsrechte, *No Override*, *Block Policy Inheritance*)

Exchange 2000

- Architektur eines Exchange 2000 Systems
- Grundlegende Konzepte und Routineaufgaben
- Routing Groups
- Administrative Gruppen
- Connectors zu fremden E-Mail-Systemen
- Outlook Web Access (OWA)
- E-Mail-Filter
- E-Mail-Folder und Public Folder sowie die Rechtevergabe auf diese Objekte
- Schutz der Client-Server-Kommunikation (Outlook 2000 Client, Browser, eingesetzte Verfahren)

Outlook 2000

- Benutzerprofile
- aktive Inhalte und potentiell gefährliche Dateiformate
- Auto-Reply-Funktion

Ergänzende Kontrollfragen:

- Wurden alle Administratoren für die Arbeit mit Windows 2000 und Active Directory geschult?
- Ist der Umgang mit allen relevanten Sicherheitsmechanismen von Exchange 2000 dargestellt worden?
- Wurden im Rahmen der Schulung die möglichen E-Mail-Clients, insbesondere Outlook 2000, behandelt?

M 3.32 Schulung zu Sicherheitsmechanismen von Outlook 2000 für Benutzer

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Exchange/Outlook 2000 ist ein komplexes System, so dass es bei Fehlnutzung oder Fehlkonfiguration unbeabsichtigt zu Sicherheitslücken kommen kann. Dies gilt besonders dann, wenn die Benutzer nicht hinreichend im Umgang mit Exchange/Outlook 2000 geschult sind. Zwar wird die Systemkonfiguration in der Regel so eingestellt, dass diese nur in Grenzen durch die Benutzer verändert werden kann. Unkenntnis über die einem Benutzer zur Verfügung stehenden Sicherheitsmechanismen und -einstellungen können jedoch dazu führen, dass das System unsicher genutzt wird.

Grundlagen über Exchange 2000

Daher sollten alle Benutzer im Umgang mit Outlook 2000 geschult werden. Neben der reinen Nutzung der Client-Software ist es jedoch auch notwendig, den E-Mail-Benutzern die grundlegende Funktionsweise des Exchange 2000 Systems zu erläutern.

Den Benutzern muss insbesondere vermittelt werden, welche Sicherheitsmechanismen ihnen zur Verfügung stehen, so dass sie in der Lage sind, diese korrekt und sinnvoll einzusetzen. Eine Schulung sollte u. a. folgende Themen behandeln:

- Überblick: Zugriffskontrolle auf einen Exchange-Server
- Überblick: Zugriffskontrolle auf E-Mail-Konten
- Anerkennen von Zertifikaten (Was bedeuten Cross-Zertifikate?)
- Authentisierung an der Web-Schnittstelle sowie deren Schwächen und Stärken
- Sicherer Umgang mit Internet-Zertifikaten
- Erzwingen der Kommunikationsabsicherung: Port-Verschlüsselung und SSL-Nutzung
- Beschränkungen für die Ausführung aktiver Inhalte in Outlook 2000
- E-Mail-Verschlüsselung und E-Mail-Signaturen
- Aktivierung der erweiterten Sicherheit von Outlook 2000
- Speicherung von Benutzerprofilen
- Umgang mit Offline-Ordnern
- Sicherheitseinstellungen für persönliche Ordner (Verschlüsselung)
- Gefährdungen bei der Nutzung der *Out of Office*-Funktionalität
- Umgang mit Verteilerlisten
- Umgang mit Stellvertreterberechtigungen (*send as*)
- Verhaltensregeln für die Nutzung des Outlook Web Access (sofern diese Funktionalität überhaupt zur Verfügung gestellt wird)
- Umgang mit Outlook-Formularen

Diese Liste stellt nur einen Ausschnitt aus den notwendigen Sicherheitsthemen dar und muss organisationsspezifisch angepasst und erweitert werden. Neben der reinen Schulung zu den Sicherheitsmechanismen von Outlook 2000 müssen die Benutzer jedoch auch die geltenden Sicherheitsvorschriften kennen, damit diese bei der Nutzung der Sicherheitsmechanismen auch entsprechend umgesetzt werden können.

M 3.33 Sicherheitsüberprüfung von Mitarbeitern

Verantwortlich für Initiierung: Leiter Personal, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Personalabteilung, Vorgesetzte

Die Möglichkeiten, die Vertrauenswürdigkeit von neuem oder fremdem Personal überprüfen zu lassen, sind in Deutschland, aber auch in vielen anderen Ländern, rechtlich sehr eingeschränkt. Dazu kommt, dass die Ergebnisse meist wenig aussagekräftig sind, wie z. B. bei polizeilichen Führungszeugnissen. Grundsätzlich sollte aber vor der Übernahme von neuen oder externen Mitarbeitern in Projekte überprüft werden, ob

- diese hinreichende Referenzen haben, z. B. aus anderen, ähnlichen Projekten, und
- der vorgelegte Lebenslauf des Bewerbers aussagekräftig und vollständig ist.

Darüber hinaus kann es sinnvoll sein, sich akademische und berufliche Qualifikationen bestätigen zu lassen, beispielsweise durch Nachfragen an der Universität oder früheren Arbeitgebern oder Kunden. Auch die Identität des Bewerbers sollte verifiziert werden, z. B. durch Vorlage von Ausweispapieren.

Wenn externes Personal intern eingesetzt wird oder im Rahmen von Projekten, Kooperationen oder Outsourcing-Vorhaben auf interne Anwendungen und Daten zugreifen kann, sollten vergleichbare Überprüfungen wie für eigene Mitarbeiter durchgeführt werden. Bei der Vertragsgestaltung mit externen Dienstleistern sollte vertraglich festgehalten werden, welche Seite solche Überprüfungen durchzuführen hat und in welcher Tiefe diese erfolgen.

Ergänzende Kontrollfragen:

- Wie wird die Vertrauenswürdigkeit von eigenen und fremden Mitarbeitern überprüft?
- Werden die Referenzen von neuen Mitarbeitern hinterfragt?

M 3.34 Einweisung in die Administration des Archivsystems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Archivverwalter, Administrator

Um ein Archivsystem korrekt und sicher administrieren zu können, müssen sich die Verantwortlichen und hier vor allem die Administratoren und Archivverwalter mit den eingesetzten Systemen auskennen. Hierfür ist eine Schulung der verantwortlichen Archivverwalter und Administratoren notwendig. Dadurch sollen Konfigurationsfehler und Fehlverhalten vermieden werden. Die Schulung sollte mindestens folgende Themen umfassen:

- Systemarchitektur und Sicherheitsmechanismen des verwendeten Archivsystems und des darunterliegenden Betriebssystems,
- Installation und Bedienung des Archivsystems, Handhabung der verwendeten Archivmedien und Kennzeichnung der Archivmedien (siehe auch M 2.3 *Datenträgerverwaltung*),
- Einsatzbedingungen (Klimatisierung, etc.) des Archivsystems und der Archivmedien,
- Dokumentation der Administrationstätigkeiten,
- Protokollierung der Systemereignisse am Archivsystem,
- Vorgehensweise bei der Auffrischung der Datenbestände (siehe M 2.263 *Regelmäßige Aufbereitung von archivierten Datenbeständen* und M 2.264 *Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung*),
- Grundbegriffe von Verschlüsselung und digitaler Signatur, wenn kryptographische Verfahren verwendet werden,
- Vorgehensweise bei der Vernichtung ausgesonderter Archivmedien,
- Systemüberwachung und Wartung (Operating) des Archivsystems,
- Eskalationsprozeduren, z. B. bei
  - Nichteinhaltung von Reaktionszeiten,
  - Unterschreiten der Rest-Speicherkapazität der Archivmedien,
  - Manipulation oder Sabotage des Archivsystems oder Ereignissen höherer Gewalt sowie
  - unberechtigten Zugriffen auf archivierte Daten.

Die Schulung der Administratoren und Archivverwalter ist zu dokumentieren. Bei Systemänderungen sollten die Administratoren und Archivverwalter entsprechend weitergebildet werden.

Ergänzende Kontrollfragen:

- Sind die Administratoren des Archivsystems den Vorgaben entsprechend geschult worden?
- Werden die Administratoren regelmäßig weitergebildet, z. B. bei Änderungen am System?

M 3.35 Einweisung der Benutzer in die Bedienung des Archivsystems

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Archivverwalter

Die Archivierung ist eine besonders verantwortungsvolle Aufgabe und stellt hohe Anforderungen an die Bedienung. Die dafür vorgesehenen Mitarbeiter sind auf diese Verantwortung besonders hinzuweisen und vorzubereiten. Hierzu müssen die Benutzer entsprechend geschult werden.

Eine derartige Schulung sollte unter anderem folgende Themen umfassen:

- Vorgehensweise bei der Umwandlung analoger Daten:

  Die korrekte Vorgehensweise bei der Erfassung der Dokumente, der Umwandlung in die elektronische Form sowie der elektronischen Archivierung sind zu erläutern und anhand von praktischen Beispielen zu üben.

- Rechtliche Rahmenbedingungen der Archivierung:

  Bei der Archivierung sind rechtliche Anforderungen einzuhalten (siehe M 2.245 *Ermittlung der rechtlichen Einflussfaktoren für die elektronische Archivierung*). Diese Anforderungen und die Folgen bei Nichteinhaltung müssen den Benutzern deutlich gemacht werden.

- Schutz der Vertraulichkeit und Integrität der Dokumente:

  Die korrekte Vorgehensweise bei der Behandlung vertraulicher Dokumente sowie bei der Integritätssicherung und -prüfung archivierter Dokumente ist zu demonstrieren. Auf mögliche Folgen bei fehlerhafter Bedienung ist hinzuweisen.

- Besonderheiten bei der Verwendung von WORM-Medien:

  Auf die Besonderheiten bei der Speicherung auf einmal beschreibbare Medien ist besonders hinzuweisen, das heißt es ist zu beachten, dass einmal gespeicherte Daten nicht mehr gelöscht werden können (allenfalls eine neue Version könnte erneut archiviert werden). Dies kann nicht nur zu Kapazitätsengpässen, sondern auch zu Datenschutz- oder Vertraulichkeitsproblemen führen, da Daten nur als "zu löschen" markiert, aber nicht tatsächlich gelöscht werden.

- Organisationsspezifische Sicherheitsrichtlinien und ihre Anwendung bei der elektronischen Archivierung:

  Bei der Konzeption des Archivsystems sind üblicherweise diverse Sicherheitsmaßnahmen vorgesehen worden, die von den einzelnen Benutzern des Archivsystems umgesetzt werden müssen. Dies kann z. B. die Art der Kennzeichnung der Archivmedien oder auch den Umgang mit als vertraulich oder anderweitig klassifizierten Informationen betreffen. Alle Benutzer müssen auf diese organisationsspezifischen Sicherheitsrichtlinien hingewiesen werden.

Die Schulung der Mitarbeiter ist zu dokumentieren.

Ergänzende Kontrollfragen:

- Sind für die Benutzer des Archivsystems Schulungen zur Bedienung vorgesehen?
- Wird die Teilnahme der Benutzer an den Schulungen dokumentiert?

M 3.36 Schulung der Administratoren zur sicheren Installation und Konfiguration des IIS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement,

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement,

Die Gefahr eines Angriffs auf einen aus dem Internet erreichbaren IIS ist sehr groß. Aus diesem Grunde sollten nicht nur funktionale Aspekte bei der Installation und Konfiguration eine Rolle spielen. Insbesondere die Sicherheit ist von großer Bedeutung, da nicht nur der Server selbst bedroht ist, sondern dieser u. U. auch als Ausgangspunkt für Angriffe auf das gesamte Netz missbraucht werden kann.

Sicherheitslücken im IIS basieren zum einen auf Schwachstellen der Software, z. B. Programmierfehler. Obwohl Microsoft bei Bedarf neue Hotfixes und in gewissen Abständen Service Packs veröffentlicht, werden sowohl in Windows wie auch in allen Versionen des IIS immer wieder Schwachstellen entdeckt, für die erst nach einiger Zeit Hotfixes verfügbar sind und die erst nach längerer Zeit in Service Packs berücksichtigt werden. Zum anderen entstehen Sicherheitslücken durch fehlerhafte Konfiguration des Systems, beispielweise durch standardmäßig installierte Beispielanwendungen und Scripts.

Um eine sichere Installation und Konfiguration des IIS zu gewährleisten, müssen die verantwortlichen Administratoren über entsprechende Kenntnisse und Qualifikationen verfügen. Das bedeutet, dass den Administratoren die relevanten Gefahren und Sicherheitslücken bekannt sind und dass sie wissen, welche wirksamen Maßnahmen zur Absicherung des IIS-Systems durchzuführen sind.

Aus diesem Grund sind regelmäßige Schulungsmaßnahmen für die Administratoren durchzuführen.

Bei der Planung von Schulungsmaßnahmen ist zu beachten, dass der IIS nicht alleine betrachtet werden kann. Voraussetzung für eine sichere Installation des IIS ist ein sicher konfiguriertes Betriebssystem. Außerdem steht ein Web-Server in der Regel nicht alleine, sondern ist in eine Systemumgebung (weitere Server und Clients) eingebunden. Aufgrund dieser Komplexität ist ein umfangreiches Schulungsprogramm zu empfehlen, in dem folgende Themenschwerpunkte zu berücksichtigen sind:

- Gefahren und Risiken bei vernetzten Systemen
- Gefahren und Risiken eingesetzter Dienste, beispielsweise http, ftp, telnet
- Sicherheitslücken im Betriebssystem und der IIS-Software
- Grundlegende Architektur der IIS-Software
- Funktionalitäten der einzelnen Komponenten
- Zusammenspiel mit dem Betriebssystem
- Zugriffsrechte auf Dateien
- Bedienung der Admin-Werkzeuge

- Sichere Einbindung in die Systemumgebung, z. B. durch Einrichten einer Demilitarisierten Zone (DMZ)
- Sichere Installation und Konfiguration des Betriebssystems, z. B. Konfiguration der Netzeinstellungen
- Sichere Installation und Konfiguration des IIS, z. B. Absicherung von virtuellen Verzeichnissen

Damit sichergestellt ist, dass die Administratoren auch über aktuelle Sicherheitsrisiken im Zusammenhang mit dem IIS und über aktuelle Entwicklungen in der Informationstechnik informiert sind, sollten die Schulungen in regelmäßigen Abständen, z. B. halbjährlich, durchgeführt werden.

Ergänzende Kontrollfragen:

- Welche Schulungsmaßnahmen werden in welchen Intervallen angeboten?
- Decken die Inhalte der Schulungsmaßnahmen die erforderlichen Gebiete ab?

M 3.37 Schulung der Administratoren eines Apache-Webservers

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Um den Apache-Webserver korrekt und sicher administrieren zu können, ist eine Schulung der verantwortlichen Administratoren unumgänglich. Schon kleine Konfigurationsfehler können dazu führen, dass Sicherheitslücken entstehen. Besonders die korrekte Konfiguration von Zugangsbeschränkungen zu bestimmten Bereichen des Webangebots erfordert gute Kenntnisse der vorhandenen Möglichkeiten und ihrer Beschränkungen.

Aufgrund der starken Interaktion zwischen den Sicherheitsmechanismen der Apache-Software und des zugrundeliegenden Betriebssystems müssen den Administratoren des Apache-Webservers auch die Sicherheitsmechanismen des Betriebssystems bekannt sein. Dies gilt auch dann, wenn die Administratoren des Apache-Webservers nicht gleichzeitig auch für die Administration des Betriebssystems zuständig sind.

Neben den Aspekten der allgemeinen Betriebssystemsicherheit sollten folgende Aspekte Gegenstand der Schulung sein:

- Methoden der Installation des Apache-Webservers (Installation über die Paketverwaltung des Betriebssystems, Binärversionen der Apache Foundation, gegebenenfalls Kompilieren aus dem Quellcode).
- Konfigurationsmöglichkeiten des Apache-Webservers, Syntax der Konfigurationsdateien.
- Möglichkeiten zur Einbindung des Apache-Webservers in den Startprozess des Betriebssystems.
- Mechanismen der Benutzerauthentisierung beim Apache-Webserver, Einsatzgebiete, Vor- und Nachteile der einzelnen Mechanismen.
- Einrichten und Verwalten von Zugangsbeschränkungen beim Apache-Webserver.
- Zusammenspiel der Konfiguration von Zugangsbeschränkungen in der Apache-Konfiguration mit Zugriffsberechtigungen auf Betriebssystem- und Dateiebene, beispielsweise bei Verwendung von URL-Rewriting oder symbolischen Links.
- Möglichkeiten zur Aufteilung von Kompetenzen zwischen den Server-Administratoren und "Redakteuren", Entwicklung von Rechte- und Rollenkonzepten.
- Möglichkeiten zur Abbildung eines "organisatorischen" Rechte- und Rollenkonzepts mit Hilfe der Benutzer- und Rollenverwaltung des Betriebssystems.
- Einsatzmöglichkeiten und Konfiguration von SSL beim Apache-Webserver.
- Maßnahmen zur Sicherstellung der Verfügbarkeit beim Apache-Webserver.

- Möglichkeiten und Risiken beim Einsatz von CGI-Skripten und Server-Erweiterungen. Kriterien zur Auswahl geeigneter Erweiterungen und Programmiermethoden.
- Datensicherung beim Apache-Webserver.

Ergänzende Kontrollfragen:

- Sind die Administratoren auf den Umgang mit dem Apache-Webserver vorbereitet und insbesondere in sicherheitsrelevanten Aspekten geschult?
- Sind die Administratoren im Umgang mit dem genutzten Betriebssystem und seinen sicherheitsrelevanten Aspekten geschult?

M 3.38 Administratorenschulung für Router und Switches

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Für den sicheren Betrieb von Routern und Switches ist es wichtig, dass alle Arbeiten durch Personal durchgeführt werden, das in der Lage ist, alle gebotenen Funktionen und Sicherheitsmerkmale optimal zu nutzen. Daher ist es unerlässlich, dass die Administratoren entsprechend geschult werden.

In den Schulungen sollten ausreichende Kenntnisse zu den für die Einrichtung und den Betrieb von Routern und Switches notwendigen Vorgehensweisen, Werkzeugen und Techniken vermittelt werden. Dies gilt auch für herstellerspezifische Aspekte zum gewählten Produkt. In dieser Maßnahme werden Anforderungen an Schulungen beschrieben, die Administratoren in die Lage versetzen, Router und Switches in einer typischen Umgebung installieren und betreiben zu können.

In den Schulungen sollten die Grundlagen, Konzepte und Kenntnisse der Kommandos zu Einrichtung, Betrieb, Wartung und Fehlersuche vermittelt werden. Eine Schulung sollte eine ausgewogene Mischung aus Theorie und Praxis darstellen.

Auch wenn in einer Gruppe von Administratoren die Aufgaben so verteilt sind, dass jeder Administrator nur einen bestimmten Verantwortungsbereich hat, ist es unverzichtbar, dass alle Administratoren ein allgemeines Grundwissen besitzen. Die individuellen Schwerpunkte können davon ausgehend gezielt ausgebaut und gepflegt werden. Zu vielen Produkten gibt es von den Herstellern oder spezialisierten Anbietern hierfür ein umfangreiches Angebot an aufeinander aufbauenden und individuell vertiefenden Seminaren. Das Angebot an qualifizierten Schulungen stellt ebenfalls ein Kriterium dar, das bei der Entscheidung für einen bestimmten Hersteller berücksichtigt werden sollte.

Budget für Schulungen

Für Schulungsmaßnahmen sollte bereits bei der Beschaffung von IT-Komponenten ein Budget eingeplant werden und ein Schulungsplan für Administratoren erstellt werden. Die Inhalte einer Schulung sollten die folgenden Punkte umfassen:

- Grundlagen
  - ISO/OSI Schichten Modell
  - Netztopographien / -topologien und Übertragungstechniken
  - Verkabelung
  - Aktive Netzkomponenten
  - Grundlagen von IP und der damit zusammenhängenden Protokolle (IP-Adressierung, Subnetting, IP, ICMP, TCP, UDP)
  - Überblick über Hersteller und Produkte
- Switching

  - Funktionsweise eines Switches
  - "Cut Through" und "Store and Forward"
  - Transparent Bridging Funktion (IEEE 802.1d)
  - Spanning Tree Algorithmus (IEEE 802.1d)
  - VLAN (VLAN Typen, Tagging, IEEE 802.1q)
- Routing
  - Funktionsweise eines Routers
  - Statisches und dynamisches Routing
  - Dynamische Routing-Protokolle (RIPv1, RIPv2, OSPFv2, BGPv4, IGRP, EIGRP)
- WAN-Anbindung
  - Grundlagen der WAN-Technologien und Protokolle
  - Vermittlungsarten (Fest-, Wählverbindung)
  - Virtuelle Private Netze (VPN)
  - Weitverkehrsverbindungen (xDSL, ISDN)
  - WAN-Protokolle (PPP, Frame Relay)
- Einrichtung
  - Zusammenbau und Verkabelung
  - Einrichtung und Konfiguration von Routern und Switches (Schwerpunkt: Betriebssystem)
- Betrieb
  - Management der Geräte, Werkzeuge
  - Integration in Netzmanagementsysteme (NMS)
  - Protokollierung (syslog)
  - Sicherung und Verwaltung von Konfigurationsdateien
- Fehlerbehebung
  - Fehlerquellen und Ursachen
  - Mess- und Analysewerkzeuge
  - Teststrategien zur Fehlersuche
  - Anforderungen an sichere Netzinstallationen
- IT-Sicherheit
  - Grundlagen der IT-Sicherheit sowie für Router und Switches relevante IT-Sicherheitsaspekte
  - Authentisierung, Autorisierung
  - Kryptoverfahren und Anwendungen

- Angriffsszenarien (Denial of Service Attacken, ARP-Spoofing, IP-Spoofing)
- Gefahrenquelle "Default-Einstellungen"
- Vorsorgemaßnahmen, Reaktion und Analyse
- Incident Handling

Ergänzende Kontrollfragen:

- Steht ein Budget für Schulungsmaßnahmen zur Verfügung?
- Wurde ein Schulungsplan für Administratoren in Anlehnung an die erwähnten Punkte erstellt?

M 3.39 Einführung in die zSeries-Plattform

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator

Komponenten von zSeries-Hardware und Software

Die zSeries-Architektur ist der Nachfolger der 1964 eingeführten S/360-Architektur und wird bei heutigen Mainframe-Installationen häufig eingesetzt. Die zSeries-Systeme (als Teil von IBMs eServer-Familie) können sowohl für Stapelverarbeitungen und Transaktionen als auch für E-Business-Anwendungen eingesetzt werden.

Zum Betrieb der zSeries-Plattform stehen die Betriebssysteme OS/390 (31 Bit-Architektur) und z/OS (64 Bit-Architektur) zur Verfügung. Da das z/OS-Betriebssystem als Nachfolger von OS/390 gilt, sollte es bei neuen Installationen eingesetzt werden.

Nachfolgende Abschnitte enthalten eine Übersicht über die Komponenten der zSeries-Plattform, sie erheben jedoch keinen Anspruch auf Vollständigkeit. Umfangreiche und detaillierte Informationen sind in der einschlägigen Literatur des Herstellers IBM zu finden (siehe Literaturhinweise am Ende der Maßnahmenbeschreibung).

Das z/OS-Betriebssystem ist in der Maßnahme M 3.40 *Einführung in das z/OS-Betriebssystem* beschrieben, das Betriebssystem Linux für z/OS in der Maßnahme M 3.42 *Schulung des z/OS-Bedienungspersonals*.

Historie

Die Basis für die zSeries-Architektur entstand im Jahr 1964, als IBM die S/360-Architektur entwickelte und einführte. Von Anfang an war es Ziel der Architektur, dass Maschinencode auf allen damaligen und zukünftigen Modellen ohne wesentliche Modifikationen lauffähig sein sollte.

Im Laufe der Zeit erweiterte IBM sukzessiv die S/360-Architektur, wobei sich die Bezeichnung mehrfach änderte, erst zu *S/370*, danach zu *S/390* und jetzt zur aktuellen *zSeries*. Die wesentlichen Grundlagen der Architektur (z. B. Maschinencode, Register und Adressierung oder auch die Festlegung der Relation zwischen Bit und Byte) wurden jedoch immer beibehalten und gelten heute noch.

Mainframe-Architektur

IBMs Dokumentation *z/Architecture Principles of Operations* teilt das zSeries-System in die Bestandteile

- Main Storage,
- einem oder mehreren Central Processing Units (CPUs),
- Operator Facilities,
- einem Channel Subsystem und
- I/O Devices

auf. Die *I/O Devices* hängen an sogenannten *Control Units* (CU), die wiederum am *Channel Subsystem* hängen.

Die S/390-Architektur entspricht - mit Ausnahme der neuen zSeries-Funktionen - im wesentlichen der zSeries-Architektur. Im Folgenden werden einige Aspekte der z/Architektur dargestellt:

EBCDIC Code

zSeries-Systeme verwenden beim Abspeichern den sogenannten *EBCDIC*-Code (*Extended binary coded decimal interchange code*) mit einer Länge von acht Bit, im Gegensatz zu dem bei anderen Rechner-Architekturen verwendeten *ASCII*-Code (sieben Bit). Kommunizieren Rechner miteinander, die unterschiedliche Formate einsetzen, sind Konvertierungen der Codes erforderlich.

Register

Ein zSeries-Rechner arbeitet mit verschiedenen Registern von 64 Bit Länge (z. B. Kontrollregister oder Mehrzweckregister). Der *Instruction Operation Code* (IOC) bestimmt, welches Register verwendet wird.

Beim S/390-Rechner sind die Register 32 Bit lang.

Programmverzweigung (Linkage Convention)

Die zSeries-Architektur verwendet beim Aufruf eines Unterprogramms mehrere Mehrzweckregister. Die Verwendung bestimmter Register ist in der Literatur auch als *Linkage Convention* bekannt.

Alternativ ist die Benutzung eines *Linkage Stacks* möglich, wofür andere Assembler-Instruktionen zur Verfügung stehen.

Speicherschutz

Ein zusätzlicher Speicherschutz stellt bei der zSeries-Architektur sicher, dass Fehler beim Speicherzugriff weitgehend vermieden werden. Die Hardware teilt den Hauptspeicher in 4 kB große Blöcke auf und vergibt pro Block einen Speicherschutzschlüssel, der bei der späteren Verarbeitung überprüft wird.

Diese Art des Speicherschutzes stellt eine der Stärken des Betriebssystems dar, da Überschreiben fremden Speichers im normalen Problem-Modus weitgehend ausgeschlossen ist.

Ein-/Ausgabe

Der zSeries-Ein-/Ausgabe-Verkehr wird durch ein *Channel Subsystem* gesteuert. Bis zu 65536 Ein-/Ausgabe-Einheiten können über Steuereinheiten (*Control Units*) an das *Channel Subsystem* angeschlossen und mittels *Channel Paths* mit diesem verbunden werden.

Die einzelnen Anschlüsse werden vom *Channel Subsystem* als logische Verbindungen (*Subchannels*) geführt. Sie sind über *Channel Paths* mit dem *Channel Subsystem* verbunden.

Operator Facilities

Mit dieser Funktion kann der Systemadministrator, ähnlich der BIOS-Kommunikation beim PC, mit dem zSeries-System in Verbindung treten und Systemanpassungen vornehmen.

Zur Kommunikation dient ein herkömmlicher PC, der an das *Service Element* angeschlossen ist und als *Management Console* bezeichnet wird (siehe auch

Abschnitt *Ein-/Ausgabe - zSeries-Mainframe-Konsolen*). Diese Konsole dient ausschließlich der Nutzung durch den Systemadministrator bzw. das Wartungspersonal des Herstellers.

Betriebssystem-Unterstützung

Die z/Architektur unterstützt alle drei existierenden Hardware-Adressierungsbereiche, 24 Bit-, 31 Bit- und 64 Bit-Adressierung. Betriebssysteme und Middleware-Produkte wurden für die Möglichkeit der erweiterten Adressierung angepasst. Viele Beschränkungen, z. B. die 2 GB-Grenze bei S/390-Systemen oder jetzt weitgehend unnötige Funktionen, wie z. B. die Verlagerung von Seiten des Hauptspeichers in den erweiterten Speicher (*Expanded Storage*), fallen damit weg. Dadurch kann der Durchsatz des Systems in vielen Fällen erhöht werden. *Expanded Storage* wird jedoch weiterhin bei S/390-(31-Bit)-Anwendungen und z/VM unterstützt.

Anmerkung: Das S/390-System ist zwar in Bezug auf die Hardware ein 32 Bit-System, die Software darauf läuft jedoch mit 31 Bit, da das erste Bit zur Umschaltung zwischen 24 und 31 Bit-Modus benötigt wird.

Unterschiede der S/390-Architektur zur zSeries-Architektur

Der Hauptunterschied zwischen S/390- und zSeries-Systemen ist die erweiterte Adressierbarkeit. Während die S/390-Architektur nur die 31 Bit- Adressierung unterstützt, wurden in den Rechnern der zSeries fast alle Register auf 64 Bit erweitert. Ein Umschalten zwischen den beiden Modi ist jederzeit möglich.

Die neuesten zSeries-Systeme sind noch immer kompatibel zu früher entwickelten 31 Bit-Programmen, es laufen sogar noch 24 Bit-Programme.

Hardware

Mainframe-Hardware ist in den verschiedensten Varianten verfügbar. Modelle und Ausstattung lassen sich flexibel zusammenstellen, periphere Einheiten können weitgehend beliebig daran angeschlossen werden. Eine vollständige Darstellung kann an dieser Stelle nicht gegeben werden.

Nachfolgend eine kurze Übersicht über die wichtigsten Merkmale:

Modelle

Zur Zeit sind die Typen S/390 (G5, G6 und Multiprise) aus der S/390-Architektur verfügbar, aus der zSeries-Architektur die Typen z800-Server, z900-Server und z990-Server (Stand Ende 2003).

Prozessoren

Die Systeme sind auf bis zu 32 Prozessoren aufrüstbar, wobei diese bei der zSeries-Architektur dynamisch (d. h. während des Betriebs) hinzugefügt werden können.

Hauptspeicher

Je nach Typ können zwischen 1 GB bis max. 256 GB Hauptspeicher verwendet werden.

Kanäle

Verfügbar sind 256 bis max. 512 Kanäle, wobei unterschiedliche Kanaltypen zusammen betrieben werden können (*Escon*, *Ficon*). Je nach Konstellation gibt es Einschränkungen.

Logical Partitioning

Ein zSeries-System lässt sich in bis zu 15, bei z990-Servern in bis zu 30, sogenannte logische Partitionen (*Logical Partition, LPAR*) aufteilen. Dies wird durch das interne PR/SM-Feature (teils Hardware, teils Microcode im *Licensed Internal Code*) unterstützt. Jede einzelne Partition verhält sich dabei wie ein separates System. Auf den *LPARs* lassen sich unterschiedliche Betriebssysteme installieren, so dass der Einsatz von Linux (für zSeries) parallel mit dem z/OS-Betriebssystem auf dem gleichen Rechner möglich ist.

Komponenten

- Multichip Module (MCM)

  Die wesentlichen Komponenten des Rechners sind in sogenannten *Multichip Modules* zusammengepackt und auf einem Glaskeramikträger aufgebracht. Ein MCM beinhaltet *Processor Unit Chips* (PUs), Chips für den L2-Cache und dessen Ansteuerung sowie die Ein-/Ausgabe-Steuerung. Die Verbindung aller Komponenten auf dem Träger erfolgt über waagerechte und senkrechte Leitungsverbindungen, die über Kontakte mit der Platine verbunden sind.

- Thermo Conduction Module (TCM)

  Die in einem MCM entstehende Wärme leitet ein auf dem MCM sitzender Kühler (TCM) ab.

- SMP

  Das MCM stellt einen in sich symmetrischen Multiprozessor (SMP) dar.

- Logical Channel Subsystem (LCSS)

  Das LCSS ist eine Erweiterung des früher schon verfügbaren *Channel Subsystems* (CSS), das es erlaubt, von allen *Processor Units* aus bis zu 512 Kanäle anzusprechen.

- HiperSockets

  Die schnelle TCP/IP-basierende Verbindung zwischen LPARs und *Virtual Servers* (Linux) stellt eine Art TCP/IP-Netz innerhalb des Servers dar.

- Intelligent Resource Director (IRD)

  Der *Intelligent Resource Director* unterstützt den *Workload Manager* (WLM) und besteht aus den wesentlichen Teilen

  - LPAR CPU Management,
  - Dynamic Channel Path Management (DCM) und
  - Channel Subsystem Priority Queueing (CSSPQ).

Bei Problemen im System kann der *Workload Manager* dynamisch über den IRD veranlassen, dass LPAR-Gewichtungen verändert, Kanal-Pfade umgehängt oder im *Channel Subsystem* I/O-Prioritäten verändert werden.

Prozessoren und Einsatz

Die Prozessoren sitzen auf MCMs und bestehen im wesentlichen aus den folgenden Typen:

- Processor Units (Mikroprozessor-Chips),
  - CPU (CP),
  - Ein-/Ausgabe-Prozessoren,
  - Reserve-PUs,
- Level 2 Cache Chips,
- System-Assist-Prozessoren (*SAPs,* Ausführung des Channel Subsystems),
- Storage Control Chips,
- Memory Bus Adapter Chips und
- Clock Chips.

Die Anzahl der standardmäßig gelieferten CPs und SAPs ist abhängig von dem jeweils bestellten Modell. Die Anzahl der Reserve-PUs ist abhängig davon, wie viele PUs insgesamt vorhanden und noch nicht mit Funktionen belegt sind.

Reserve-PUs lassen sich leicht über den *Licensed Internal Code Configuration Control (LICCC)* via *Host Management Console (HMC)* den folgenden Funktionen zuordnen:

- Central Processor (CP)
- Integrated Facility for Linux (IFL)
- Internal Coupling Facility (ICF)
- System Assist Processor (SAP)

Kryptographische Komponenten

Die zSeries bietet verschiedene kryptographische Hardware-Komponenten an, die die Daten-Ver- und -Entschlüsselung unterstützen.

- Cryptographic Coprocessor Facility (CCF)

  Dieser Coprozessor ist auf dem Prozessormodul der 9672- und zSeries-Hardware angeordnet (außer z990). Es sind ein oder zwei CCFs je Modul erhältlich. Im CCF können die Schlüssel *DES Master Key, Key Management Master Key (PKA KMMK*) und *Signature Master Key (PKA SMK)* gespeichert werden.

- Peripheral Component Interconnect Crypto Coprocessor (PCI-CC)

  zSeries-Systeme unterstützen die PCI-CC-Karte, die zusätzlich eingesetzt werden kann, um die Funktionalitäten und Performance des CCF zu unterstützen.

- Peripheral Component Interconnect Crypto Accelerator (PCI-CA)

  Diese neue Krypto-Karte wurde speziell entwickelt, um die SSL-Ver- und -Entschlüsselung auf zSeries-Systemen zu beschleunigen.

- z990 PCIX-CC Enhanced Cryptographic Functionality

  Der PCIX Cryptographic Coprocesser ersetzt die CCF- und PCI-CC-Krypto-Hardware im z990-Server.

Ein-/Ausgabe

Die Ein- oder Ausgabe von Daten läuft bei der zSeries-Plattform über ein Netz von Verbindungen, die im folgenden kurz beschrieben werden:

Channel Subsystem (CSS)

Das *Channel Subsystem* ist eine Einheit (aus Hard- und Software), die für die Verarbeitung der Daten von und zu den Ein-/Ausgabe-Einheiten zuständig ist und die CPU entlastet. Es besteht aus Kanälen (*Channel Paths*), die wiederum in Unterkanäle (*Subchannels*) unterteilt sind. Die Unterkanäle führen die Kanalprogramme (*Channel programs*) aus. Bei dem zSeries-System z990 wurde das CSS zum *Logical Channel Subsystem* (LCSS) erweitert und unterstützt jetzt mehr als 15 CPUs.

Escon / MIF

Escon-Kanäle sind serielle Kanäle, die als Folgeentwicklung der alten Parallel-Channel-Entwicklung gelten können. Das *Multiple Image Facility* (EMIF bis z/900 oder MIF ab z/990) unterstützt den parallelen Zugriff von Ressourcen über LPAR-Grenzen hinweg (resource sharing). *Escon*-Kanäle werden über sogenannte *Directors* den Einheiten zugeordnet.

Ficon

Ficon-Express-Kanäle (Fibre channels) können parallel zu *Escon*-Kanälen betrieben werden. Bei der z990 können bis zu 120 solcher *Ficon*-Kanäle angeschlossen werden. Die Übertragungsrate reicht bis zu 100 MB pro Sekunde. Auch *Ficon*-Kanäle werden über *Directors* den Einheiten zugeordnet.

Integrated Cluster Bus (ICB)

ICBs werden unter anderem im Rahmen der Sysplex-Kommunikation als *Coupling Link* für Highspeed-Verbindungen zwischen Systemen benutzt.

OSA/Express

OSA/Express bietet einen zSeries-Kanalanschluss für Ethernet-Geräte wie z. B. Switches oder Router.

Channel To Channel (CTC)

Channel-To-Channel-Verbindungen gestatten schnelle Verbindungen zwischen zwei zSeries-Rechnern und werden von diversen Software-Produkten, wie z. B. JES3 und VTAM, unterstützt.

zSeries-Mainframe-Konsolen

Die *Host Management Konsole (HMC)* erlaubt die folgenden Aktionen:

- Setzen von Datum und Zeit,
- Konfigurieren von LPARs und Systemen,
- Reset von Subsystemen,
- Boot Manager (Initial Program Load - IPL - einer LPAR),
- Laden des Microprogramms (Initial Microcode Load - IML - eines zSeries Systems),
- Eingriff bei Fehlerbedingungen,
- Ersatz-MVS-Konsole und
- Fehlerkorrekturen seitens des Herstellers (Microcode-Patches).

Es können zwei Konsolen (Primary und Alternate) angeschlossen werden. Sie sind für das komplette System zuständig (alle LPARs) und nicht nur für ein spezielles Betriebssystem. Der Zugriff auf diese Konsolen muss aus Sicherheitsgründen gut geschützt sein.

Die *z/OS-System-Konsolen* (MVS) sind für die Steuerung und Kontrolle eines z/OS-Betriebssystems zuständig und lassen sich für verschiedene Zwecke konfigurieren, z. B. als Konsole für alle Nachrichten aus dem Bandbereich (Tape-Pool). Es sind mehrere MVS-Konsolen pro z/OS möglich, wovon nur eine die Master-Konsole sein kann. Im Fehlerfall schaltet diese Konsole auf die nächste verfügbare um. Der Zugriff auf die MVS-Konsolen (speziell auf die Master-Konsole) muss aus Sicherheitsgründen gut geschützt sein.

Remote Support Facility (RSF)

zSeries-Systeme sind meist durch eine Remote-Konsole mit dem Hersteller verbunden. Diese Funktion meldet erkannte Hard- und Software-Probleme automatisch weiter, so dass Fehler oft behoben werden können, bevor der Anwender einen Fehler selbst erkennt. Prinzipiell unterstützt diese Verbindung auch die Installation von Patches durch den Hersteller, dies muss jedoch vorher vereinbart und die Remote-Access-Verbindung entsprechend geschützt werden.

Parallel-Sysplex-Konzept

Sind die Anforderungen von einem System (einer LPAR) nicht mehr zu bewältigen, können mehrere LPARs zu einem logischen Verbund, dem *Parallel Sysplex* zusammengefasst werden. Dieser stellt sich nach außen als eine Einheit dar.

Der *Parallel Sysplex* ist eine Zusammenarbeit von bis zu 32 z/OS-Systemen, dies entspricht maximal 512 Prozessoren in einem Rechnerverbund. Innerhalb dieses Verbundes können Lasten auf den Rechnern verteilt werden. Treten an einer Maschine Probleme auf, lässt sich diese aus dem Verbund lösen. Die Last wird von den im *Sysplex* verbleibenden Maschinen übernommen.

- Coupling Facility (CF)

  Die *Coupling Facility* (CF) hat die Aufgabe, die Arbeitslast der Systeme zu steuern und Informationen für alle Systeme zur Verfügung zu stellen. Sie ist für die flexible Lastverteilung und die Skalierung zuständig. Die CF übernimmt Aufgaben des *Locking*, *Caching* und *Queuing*. Sie wird über den CFCC (*Coupling Facility Control Code*) gesteuert.

- Sysplex Timer

  Damit die einzelnen Systeme innerhalb des *Sysplex* zusammenarbeiten können, ist der *Sysplex Timer* nötig. Er übernimmt die Aufgabe, allen im *Sysplex* befindlichen Systemen eine synchrone Tageszeit zu liefern.

- Work Load Manager (WLM)

  Der *Work Load Manager* ist Teil einer jeden Betriebssystem-Instanz und übernimmt in Verbindung mit der *Coupling Facility* einen wichtigen Teil der Steuerung des *Sysplex Clusters*. Ein Teil des WLM ist der *System Resource Manager* (SRM). Dieser übernimmt die Überwachung der angeschlossenen Systeme. Überwacht werden durch den SRM z. B. Prozessorlast, Plattenauslastung, Hauptspeichernutzung und andere Parameter. Die Informationen werden dazu genutzt, die Last auf die im *Sysplex* angeschlossenen Systeme zu verteilen (siehe Abschnitt zum Thema *Intelligent Resource Director*).

- Cloning

  Alle Systeme eines *Sysplex Clusters* werden auf Basis eines Plattensatzes erstellt. Die lokale Anpassung erfolgt im Normalfall über Variablen der Systemkonfiguration.

Peripherie

Platten

Im Gegensatz zu anderen Betriebssystemen ist der Plattenbereich eines z/OS-Betriebssystems in sogenannte *Volumes* aufgeteilt. Ein *Volume* umfasst bei der Emulation einer Platte vom Typ 3390 Mod. 3 einen Speicherbereich von ca. 2,7 GB und ist in Zylinder und Spuren aufgeteilt.

Die *Volumes* sind an Steuereinheiten angeschlossen. Zur Steigerung der Performance und Betriebssicherheit ist ein paralleler Anschluss an verschiedene Steuereinheiten möglich. Diese werden bestimmten Aufgaben zugeordnet (z. B. JES-Spool-Datei oder System-Residenz) und lassen sich über *Subchannel*-Adressen ansprechen.

Band

Das z/OS-Betriebssystem unterstützt verschiedene Bandeinheiten, von einzelnen Stationen bis zu Robotersystemen, in denen die Bänder automatisch verwaltet und zur Verfügung gestellt werden. Darüber hinaus gibt es auch virtuelle Band-Systeme (z. B. *VTS* von IBM oder *VSM* von StorageTek), die Dateien zuerst auf integrierten Festplatten zwischenspeichern. Danach werden diese Dateien sehr effektiv auf Bänder in diesen Einheiten geschrieben (Komprimierung und Ausnutzung der gesamten Bandlänge). VTS oder VSM

werden vom z/OS-Betriebssystem als Bandeinheit 3490 verarbeitet, d. h. aus der Sicht des Betriebssystems handelt es sich um ein normales Band.

Drucker

Drucker werden von z/OS-Betriebssystemen sowohl direkt am Kanal als auch als Netzwerkdrucker im SNA- oder TCP/IP-Netz unterstützt. Bei entsprechend großen Druckvolumina, z. B. in Druckzentren, erledigen z/OS-Systeme auch reine Druckaufgaben.

Terminalfamilie 327x

Klassische 3270-Terminals an den entsprechenden Steuereinheiten sind heute praktisch nicht mehr in Betrieb. 3270-basierte Terminals haben als PC-Terminalemulation jedoch einen hohen Stellenwert und befinden sich noch recht häufig im Einsatz (bekannt als "grüner Schirm"). Sie basieren auf dem TN3270-Protokoll und lassen sich so betreiben, wie die 327x-Terminals aus früheren Jahren (von Modell 2 bis Modell 5 in verschiedenen Bildschirm-Formaten).

SNA-Komponenten (Systems Network Architecture)

SNA ist eine hierarchisch aufgebaute Netztechnologie mit vordefinierten Verbindungen. Die Knoten im Netz sind in der Regel als Hardware-Komponenten ausgeführt und werden als *Physical Units* (PUs) bezeichnet. Die Endpunkte im Netz sind entweder Software-Schnittstellen zu einer Applikation (*Application Control Block*, ACB) oder ein Terminal bzw. Terminal-Emulator oder Drucker. Daneben gibt es seit längerer Zeit die APPN-Technologie (*Advanced Peer to Peer Network*), die sich von der hierarchischen Form deutlich unterscheidet.

SNA kommt heute als alleiniges Netzprotokoll nur noch selten zum Einsatz. SNA-Netzinstallationen sind vielfach abgelöst oder durch ein TCP/IP-Netz ergänzt, so dass die Anzahl der im Betrieb befindlichen SNA-Hardware-Komponenten stark rückläufig ist.

SNA-Topologie

Das hierarchische SNA-Netz war in der Vergangenheit so aufgebaut, dass unter einem VTAM ein Front-End-Prozessor 3745/46 angeschlossen war. Angeschlossen an diesen waren die *Control Units*, an denen letztlich die Endgeräte (Terminals, Drucker oder Applikationen) betrieben wurden. Diese Konstellation ist heute zwar immer noch im Einsatz, Front-End Prozessoren und auch *Control Units* werden von IBM jedoch nicht mehr vertrieben (aber noch unterstützt). Die Anbindung an TCP/IP Netze erfolgt heute meistens über die Software-Funktion *Enterprise Extender*. SNA in der heutigen Ausprägung wird hauptsächlich noch im Rechenzentrum benutzt, um SNA-basierende Applikationen wie z. B. TSO (*Time Sharing Option*) anzubinden, während das Netzwerk von TCP/IP abgedeckt wird.

- Physical Units (PUs)

  Physical Units stellen physische Knoten im SNA-Netz dar. An diesen können weitere Einheiten hängen. Zu den PUs gehören z. B. die oben erwähnten Front-End-Prozessoren 3745/46. Darüber hinaus existieren Komponenten, die die früher vorhandenen *Control Units* (3174) emulieren

und deren Funktion wahrnehmen. VTAM im z/OS-Betriebssystem stellt ebenfalls eine *Physical Unit* dar. Aus historischen Gründen werden selbst neuere Funktionen (wie z. B. APPN) bei VTAM Displays immer noch als *Physical Units* dargestellt, obwohl diese Bezeichnung hierbei eigentlich ohne Bedeutung ist.

- Logical Units (LUs)

  Eine *Logical Unit* stellt sich entweder als Schnittstelle zu einer Applikation, als ein Terminal (oder Terminal-Emulator auf einem PC) oder als ein Drucker dar.

Weitere Informationen zu SNA finden sich in der Maßnahme M 3.40 *Einführung in das z/OS-Betriebssystem* im Abschnitt *Communications Server*.

Support Elements (SEs)

Jede zSeries-Hardware besitzt zwei *Support Elements* (S/390-G5 Modelle haben nur ein SE), die eine Konfiguration und Kontrolle des Systems erlauben. SEs sind über ein schnelles internes Ethernet-Netz untereinander und mit den Prozessoren verbunden (ein *Support Element* ist ein IBM Laptop PC). Sie erlauben die Systemkommunikation im Rahmen der *Operator Facilities*.

Firmware

Licensed Internal Code (LIC)

Zwischen der Hard- und der Software existiert auf einer weiteren Ebene der Microcode (*Licensed Internal Code*). Für den LIC gibt es bei PCs keine direkte Entsprechung, am ehesten ist er mit dem BIOS bei einem PC vergleichbar (siehe Abschnitt zum Thema *IML*).

Processor Resource/System Manager (PR/SM)

Der *Processor Resource/System Manager* ist eine LIC-Funktion und erlaubt die logische Aufteilung der physischen zSeries-Hardware in verschiedene Teile, *Logical Partitions (LPARs)* genannt. Jeder logische Rechner beinhaltet sein eigenes Betriebssystem, wobei verschiedene Betriebssysteme parallel eingesetzt werden können (also zum Beispiel z/OS, OS/390, TPF, Linux oder VSE/ESA auf einer Hardware). Die gemeinsame Nutzung aller Ressourcen wird von PR/SM kontrolliert.

Initial Microcode Load (IML)

Der IML ist ein Vorgang, der den LIC in einen nicht zugreifbaren Speicherbereich lädt. Der IML bezieht sich immer auf die gesamte Maschine, d. h. mit IML werden alle LPARs auf der Maschine neu initialisiert (und damit auch die Betriebssysteme gestoppt). IML ist ein Teil der *Operator Facilities* und kann über die HMC-Konsole aktiviert werden. Der Aufruf des IML muss entsprechend geschützt werden.

Hardware Configuration Definition (HCD)

Zur Anpassung der Software-Konfiguration an die Hardware wird eine Datei (*I/O Definition File*, IODF) erstellt, in der die logischen *Subchannels* auf den physischen *Channel Pathid* abgebildet werden. Dem Bediener stehen dazu

verschiedene Tools zur Verfügung. Auf diese Tools sollte nur autorisiertes Personal Zugriff haben.

Betriebssystem

Für die S/390- und der zSeries-Architektur sind verschiedene Betriebssysteme verfügbar (Stand Januar 2004):

S/390-Architektur (24 und 31 Bit):

- OS/390 Version 2, Release 10
- Linux on S/390
- z/VM Version 3, Release 1
- z/VM Version 4, Release 2 bis 4
- VSE/ESA Version 2, Release 5, 6, 7
- TPF Version 4, Release 1 (nur ESA-Mode)

z/Series-Architektur (64 Bit):

- OS/390 Version 2, Release 10
- z/OS Version 1, Release 2 bis 5
- Linux on zSeries
- z/VM Version 3, Release 1
- z/VM Version 4, Release 2 bis 4

Weitergehende Informationen über die Betriebssysteme OS/390 und z/OS sind in der Maßnahme M 3.40 *Einführung in das z/OS-Betriebssystem* zu finden.

Betrieb

IML

Der Start eines zSeries-Systems beginnt mit dem *Initial Microcode Load* (IML). Er wird entweder über die HMC-Konsole manuell initiiert oder mittels entsprechender Definitionen automatisch angestoßen. Der IML-Vorgang lädt den Microcode und stellt die Systeminfrastruktur bereit (alle LPARs verfügbar, kein Betriebssystem geladen). Während des IML-Vorgangs wählt der Bediener die gewünschte I/O-Konfiguration aus.

IPL

Das z/OS-Betriebssystem wird durch den *Initial Program Load* (IPL) von der *Host Management Console (HMC)* aus aktiviert. Dabei muss mindestens die IPL-Ladeadresse und der IPL-Parameterstring (Ladeadresse der IOCDS-Datei) angegeben werden. Nach der NIP-Phase (*Nucleus Initialization Process*) kommuniziert das z/OS-System mit dem Bediener über die MVS-Master-Konsole. Die weiteren Schritte hängen von den Definitionen des Betriebssystems ab. Entweder wird das System manuell aktiviert (Ausnahmefall) oder automatisch.

Operation

Zu den Betriebsaufgaben gehört das Starten und Stoppen der Tasks und Jobs, Aktivieren von Ressourcen, Beantworten von Systemanfragen (*Replies*) und Bereitstellen von Bandstationen (wenn nötig).

Monitoring

Das System kommuniziert mit dem Operator über Nachrichten und *Replies*, die an der MVS-Konsole ausgegeben bzw. eingegeben werden. Eine laufende Kontrolle der Nachrichten ist daher notwendig. Dies kann entweder manuell (relativ aufwendig) oder besser über Automatismen erfolgen (separate Programme). Gleiches gilt für die Kontrolle der Stapelverarbeitung.

Literaturhinweise

Für das zSeries-System existiert eine Vielzahl an Literatur und Dokumentationen. Die folgende Aufstellung beschränkt sich auf die wichtigsten und für die Sicherheit des zSeries-Systems besonders relevanten Quellen der Firma IBM. Die Aufstellung ist jedoch keineswegs vollständig.

Redbooks

Formnummer	Titel
SG24-5975-nn	IBM @server zSeries 900 Technical Guide
SG24-6863-nn	IBM @server zSeries 990 Technical Introduction
SG24-6851-nn	z/OS Version 1 Release 3 and 4 Implementation
SG24-6540-nn	Putting the latest z/OS Security Features to work
SG24-7023-nn	Linux on IBM eServer zSeries and S/390: Best Practices
SG24-6981-nn	ABCs of z/OS System Programming Volume 1 (Introduction to z/OS and storage concepts, TSO/E, ISPF, JCL, SDSF, MVS delivery and installation)
SG24-6982-nn	ABCs of z/OS System Programming Volume 2 (z/OS implementation and daily maintenance, defining subsystems, JES2 and JES3, LPA, LNKLST, authorized libraries, catalogs)
SG24-5653-nn	ABCs of System Programming Volume 3 (Introduction to DFSMS, storage management)
SG24-5654-nn	ABCs of System Programming Volume 4 *(Communication Server, TCP/IP, and VTAM)*
SG24-5655-nn	ABCs of System Programming Volume 5 (Base and Parallel Sysplex, system logger, global resource serialization, z/OS system operations, automatic restart management, hardware management console, performance)
SG24-6989-nn	ABCs of z/OS System Programming Volume 9 *(z/OS UNIX System Services)*
SG24-6990-nn	ABCs of z/OS System Programming Volume 10 (Introduction to z/Architecture, zSeries processor design, zSeries connectivity, LPAR concepts, and HCD)
TIPS0382	z/OS V1R3 and V1R5 Technical Guide
SG24-7035-nn	Unix System Services z/OS V1R4 Implementation
SG24-6968-nn	Implementing PKI Services on z/OS
SG24-5637-nn	OS/390 Parallel Sysplex Configuration Volume 1
SG24-5638-nn	OS/390 Parallel Sysplex Configuration Volume 2
SG24-5639-nn	OS/390 Parallel Sysplex Configuration Volume 3

IBM Dokumentation

Formnummer	Titel
SA22-7832-nn	z/Architecture Principles of Operation
SA22-7591-nn	z/OS Initialization and Tuning Guide
SA22-7592-nn	z/OS Initialization and Tuning Reference
SA22-7683-nn	Security Server RACF Security Administrator's Guide
SA22-7681-nn	Security Server RACF System Programmer's Guide
SA22-7682-nn	Security Server RACF Macros and Interfaces
SA22-7684-nn	Security Server RACF Auditor's Guide
SA22-7801-nn	z/OS Unix System Services Users Guide
GA22-7800-nn	z/OS Unix System Services Planning
SA22-7670-nn	z/OS SDSF Operation and Customization
SA22-7532-nn	z/OS JES2 Initialization and Tuning Guide
SA22-7533-nn	z/OS JES2 Initialization and Tuning Reference
SA22-7549-nn	z/OS JES3 Initialization and Tuning Guide
SA22-7550-nn	z/OS JES3 Initialization and Tuning Reference
SA22-7783-nn	z/OS TSO/E Customization
SA22-7692-nn	z/OS MVS Planning: Workload Management
SA22-7597-nn	z/OS MVS JCL Reference
SA22-7593-nn	z/OS MVS Installation Exits
SC34-4826-nn	HTTP Server Planning, Installing and Using
SC31-8775-nn	z/OS CS : IP Configuration Guide
SC31-8776-nn	z/OS CS : IP Configuration Reference
SA22-7600-nn	z/OS MVS Planning : Global Resource Serialization
SA22-7623-nn	z/OS MVS Recovery and Reconfiguration Guide
SA22-7625-nn	z/OS MVS Setting up a Sysplex
SA22-7630-nn	z/OS MVS System Management Facilities (SMF)
SA22-7642-nn	z/OS MVS Using the Subsystem Interface
SC26-7402-nn	z/OS DFSMSdfp Storage Administration Reference
SC35-0422-nn	z/OS DFSMShsm Storage Administration Reference
SC26-7405-nn	z/OS DFSMSrmm Implementation and Cust. Guide
SC26-7414-nn	z/OS DFSMSdfp Utilities
SC33-7989-nn	z/OS HCM User's Guide
GC35-0033-nn	Device Support Facilities User's Guide and Reference
SH19-8163-nn	MVS/DITTO V2 User's Guide and Reference
SC33-1701-nn	CICS RACF Security Guide
SG24-5363-nn	IMS V6 Security Guide

M 3.40 Einführung in das z/OS-Betriebssystem

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator

Komponenten von zSeries-Hardware und Software

In seinen Grundstrukturen unterscheidet sich z/OS kaum von anderen Betriebssystemen. Sein Aufbau ist eingeteilt in Hardware-nahe Funktionen, Betriebssystemprozesse und Benutzerprozesse. Zwischen dem eigentlichen Betriebssystem (*Base Control Program*) und den Benutzerprozessen existieren eine Reihe von Subsystemen, von denen die bekanntesten das *Job Entry Subsystem* für die Behandlung der Stapelverarbeitung, die *Time Sharing Option* für die Unterstützung des interaktiven Betriebs und die *Unix System Services* für den Unix-kompatiblen Betrieb sind.

Die folgende Beschreibung gilt für die Betriebssysteme OS/390 und z/OS. Zur Vereinfachung wird nur noch z/OS aufgeführt, eventuell vorhandene Unterschiede zu OS/390 werden angesprochen, wo sie existieren.

Base Control Program (BCP)

Dieser Teil des z/OS-Betriebssystems ist mit dem Unix-Kernel vergleichbar. Hierin sind die wesentlichen Funktionen des Betriebssystems vereint, die dementsprechend im Kernel-Modus laufen.

Subsysteme

Subsysteme erledigen Aufgaben des Betriebssystems, die nicht im Kernel angesiedelt sind, und laufen in einem separaten Adressraum. Wird ein Subsystem vor dem JES-Start vom MVS-Kernel aktiviert, erfolgt seine Interpretation durch das z/OS selbst (dies erledigt dann der *Master Scheduler*), was mit gewissen Einschränkungen verbunden ist. Ansonsten startet das *Job Entry Subsystem* weitere Subsysteme. Eine Definition in der Konfigurations-Datei des z/OS (PARMLIB) legt fest, wie und in welcher Reihenfolge solche Subsysteme gestartet werden.

Subsysteme werden von IBM und von anderen Software-Herstellern geliefert.

Job Entry Subsystem (JES2/3)

Ein Stapelverarbeitungsauftrag wird im z/OS *Batch-Job* genannt. Dieser besteht aus einer Reihe von prozeduralen Anweisungen, die gemäß der *Job Control Language* (JCL) aufgebaut sind. Ein Batch-Job kann aus einem oder einer größeren Anzahl von Ablaufschritten (Steps) bestehen. Auch *TSO-User* oder *Started Tasks* werden dem System über JCL bekannt gemacht.

Das *Job Entry Subsystem* (JES) dient zur Verwaltung der Job-Verarbeitung (hauptsächlich Batch-Jobs, aber auch *Started Tasks* und *TSO-User*) und deren Ein- bzw. Ausgaben. Aus historischen Gründen gibt es bis heute zwei unterschiedliche Systeme, JES2 und JES3.

Das JES2/3 wird als *Primary Subsystem* in der Subsystem-Tabelle von z/OS geführt und sollte in einem z/OS-System als erste Task gestartet werden, da erst im Anschluss daran Batch-Jobs gestartet werden können.

Die Verarbeitung der Jobs wird über sogenannte *Initiators* kontrolliert. Dabei werden unter anderem Klassen, Prioritäten und Anzahl von Jobs definiert, die parallel im System arbeiten. Ein- und Ausgaben werden in einer zentralen

Datei gespeichert, die *Spool* genannt wird. Mehrere *Logical Partitions* (LPARs) lassen sich zu einem JES-Verbund zusammenlegen, bei JES3 *Complex*, bei JES2 *Multiple Access Spool* (MAS) genannt.

Beide JES-Subsysteme beinhalten ähnliche Funktionen. JES3 bietet über den Standard hinaus Funktionen wie *Networking* (zur Automation von Batch-Jobs), *Clustering* (LPAR-ähnlicher Verbund mit Global/Local-Funktion, jedoch nur auf JES-Basis) und *Locate* (Job wird nur gestartet, wenn alle Ressourcen verfügbar sind). Viele Funktionen stehen dem Bediener parallel zu den JES-Subsystemen über andere z/OS-Funktionen zur Verfügung (z. B. über GRS, Sysplex, Job Scheduler Programme).

NJE (*Network Job Entry*) erlaubt das Versenden und Empfangen von Dateien, Batch-Jobs und auch deren Ausgaben zwischen den einzelnen Netzknoten eines Verbundes. So ist es damit z. B. möglich, einen Batch-Job vom System A zum System B zu schicken, dort zu verarbeiten und die Ausgabe dann am System C auszugeben.

Time Sharing Option (TSO)

Im Online-Betrieb ermöglicht TSO einen Multi-Tasking- und Multi-User-Betrieb.

Der *TSO Terminal Control Address Space* (TCAS), ein eigener Adressraum, verwaltet dabei den Ablauf. Er initiiert und terminiert die einzelnen Benutzeradressräume (einen pro Benutzer) und verwaltet den Nachrichtenfluss zwischen Terminal und Adressraum.

TSO unterstützt über eine einfache Scriptsprache sogenannte *Command Lists* (*Clists*), häufiger ist jedoch die modernere Interpreter-Sprache REXX im Einsatz. Zu Vereinfachung der Kommunikation steht dem Bediener ein weiteres Software-Paket zur Verfügung, das *Interactive System Productivity Facility* (ISPF). Es erlaubt einen Dialog im *Full Screen Modus*. Neben den Standardfunktionen von ISPF kann der Bediener eigene Dialoge für neue Applikationen entwickeln.

Communications Server (CS)

Der *Communications Server* für z/OS beinhaltet die Software-Komponenten, die für die Kommunikation von und zu einem Mainframe nötig sind. TCP/IP-Komponenten, wie z. B. FTP-Server und TN-Server, sind in diesem Paket ebenso enthalten wie SNA-Komponenten.

Der *Communications Server* liefert die folgenden Funktionalitäten:

- Bereitstellung der TCP/IP- und SNA-Dienste
- Lastverteilung auf die Netzkomponenten in einem *Sysplex*-Verbund
- Kontrolle und Steuerung der VPN-Kommunikation
- Implementierung der Sicherheitskomponenten für Applikationen
- Telnet-3270- und Secure-Telnet-3270-Unterstützung, Telnet/SSH zu den *Unix System Services* des z/OS
- Unterstützung von IPv6 für das z/OS-Betriebssystem

Systems Network Architecture (SNA)

Ein Knoten im SNA-Netz ist durch eine *Network Addressable Unit* (NAU) definiert. Die Wege zwischen den einzelnen Knoten werden in Form von Routen konfiguriert. Die Weiterentwicklung des statischen SNA-Netzes, *Advanced Peer to Peer Networking* (APPN) genannt, erlaubt den Einsatz dynamischer Netzkonfigurationen ähnlich dem TCP/IP-Netz.

Der *Communications Server* bildet eine Gateway-Funktion zwischen der heute üblichen IP-Netzinfrastruktur und den noch vielfach vorhandenen SNA/APPN-basierenden Komponenten, wie z. B. TSO-, IMS- oder CICS-Anwendungen.

SNA-Kommunikationsbeziehungen werden häufig über das IP-Netz mittels *Enterprise Extender* betrieben. Voraussetzung dafür ist APPN/HPR (*High Performance Routing*).

Klassische SNA-Netze gelten als relativ sicher, da die Netzzugänge komplett definiert sein müssen und das Gesamtnetz somit geschlossen ist. Als weiterführende Sicherheitsmaßnahme kann der *Session Management Exit* (SME) von VTAM eingesetzt werden.

TCP/IP

TCP/IP ist unter den *Unix System Services* (USS) im z/OS implementiert. Der TCP/IP-Service unter z/OS bietet ähnliche Funktionen wie die IP-Dienste anderer Unix-Versionen. Über den Telnet TN3270 IP-Service ist der Zugriff auf SNA-basierende Anwendungen (TSO, CICS, IMS usw.) möglich. Unter TCP/IP stehen für z/OS eine ganze Reihe von Applikationen zur Verfügung, wie z. B. ein HTTP-Webserver, Unterstützung für File-Transfer via FTP, E-Mail via SMTP, Network File System (NFS), Domain Name Service (DNS) und weitere Services. TCP/IP unterstützt Verschlüsselung über IPSec, SSH und TLS (SSL).

Durch den Einsatz von Dynamic VIPA (*Virtual IP Address*) wird es ermöglicht, dass beim Ausfall eines Systems innerhalb eines *Parallel Sysplex Clusters* eine IP-Addresse automatisch von einem Backup-System übernommen werden kann. Unterstützt die Anwendung diese Funktionalität auch, trägt dies wesentlich zur Erhöhung der Verfügbarkeit bei.

Durch Einsatz des *Workload Managers* ist es darüber hinaus möglich, eine Lastverteilung der Netzdienste auf mehrere CPUs innerhalb eines *Sysplex-Verbundes* zu erreichen.

TCP/IP gewinnt immer mehr an Bedeutung, wohingegen die Bedeutung des SNA-Netzes abnimmt (speziell bei der Neuentwicklung von Applikationen).

Kerberos

z/OS unterstützt das Authentisierungssystem *Kerberos*.

AnyNet

Die Bezeichnung *AnyNet* steht für zwei Funktionalitäten, die mit dem *Communications Server* ausgeliefert werden:

- SNA over TCP/IP und
- AnyNet Sockets over SNA.

SNA over TCP/IP erlaubt es Applikationen, die nur das SNA-Protokoll unterstützen, mit einem TCP/IP-Netz verbunden zu werden, ohne dass die Applikationen angepasst werden müssen.

AnyNet Sockets over SNA erlaubt es Applikationen unter z/OS *Unix System Services* (USS), Verbindungen über ein vorhandenes SNA-Netz aufzubauen.

System Authorization Facility (SAF)

Die SAF ist ein Teil des z/OS-Betriebssystems und dient als Sicherheitsschnittstelle zwischen dem System und dem Sicherheitssubsystem (z. B. RACF, TopSecret, ACF2).

Resource Manager, z. B. IMS, DFHSM, JES oder CICS, fragen über die SAF-Schnittstelle bei RACF bzw. dem jeweiligen Sicherheitssubsystem an (RACROUTE Macro), ob ein Anwender berechtigt ist, auf eine Ressource zu zugreifen. SAF gibt die Antwort des Sicherheitssubsystems an den *Resource Manager* zurück, woraufhin dieser den Zugriff gewährt (*Return Code* ist gleich Null) oder ablehnt (*Return Code* ist größer Null).

SecureWay Security Server für z/OS

Der *Secure Way Security Server* für z/OS bildet eine Sicherheitsplattform für das Mainframe-System. Der *Secure Way Security Server* umfasst folgende Komponenten:

RACF (Resource Access Control Facility)

RACF ist eine Zusatz-Software zur Absicherung des z/OS-Betriebssystems. RACF arbeitet mit Kennungen, Gruppen und Ressourcen (Dateien, Klassen), die in der RACF-Datenbank eingetragen sein müssen. Anhand dieser Definitionen regelt RACF nicht nur den Zugang zum System, sondern auch die Zugriffe auf die Ressourcen. Jede Ressource, z. B. Datei, muss über ein entsprechendes RACF-Profil geschützt sein. Durch den Einsatz von Platzhaltern ist es möglich, mit einem generischen Profil eine Gruppe von Ressourcen zu schützen, womit die Verwaltung vereinfacht wird. Zugriffe auf diese so geschützten Ressourcen müssen dann entweder einzelnen Usern oder Usergruppen durch die RACF-Administration vergeben werden.

Im RACF gibt es Attribute, die einem Besitzer höhere Rechte einräumen können:

- *SPECIAL* - berechtigt zur Administration des RACF (Verwalten von Gruppen, Kennungen und Ressourcen).
- *OPERATIONS* - für *Space Manager*, mit diesem Recht können Dateien verwaltet werden.
- *AUDITOR* - für die Überwachung der Tätigkeiten im Sicherheitsbereich in der Funktion eines Audits.

Diese Rechte können zusätzlich auf Gruppenebene vergeben werden *(Group Special, Group Operations, Group Auditor).*

Für die Berechtigung zur Nutzung interaktiver Programme, z. B. TSO oder *Unix System Services*, bietet RACF zusätzliche Segmente an. In diesen Segmenten werden die Rechte zur Nutzung der interaktiven Programme festgelegt. Darüber hinaus können Abrechnungsinformationen (*Accounting*) oder Ressourcenbeschränkungen (dem Anwender zur Verfügung stehender Hauptspeicher, Anzahl zu startender Tasks) in diesen Segmenten festgeschrieben werden.

Jeder Anwender (darunter fallen die Kennungen von *Batch-Jobs*, *TSO-Usern* und *Started Tasks*) wird im laufenden System von RACF über sogenannte ACEEs (*Accessor Environment Element*) verwaltet. Das sind Kontrollblöcke, die bei der Initialisierung des Adressraumes angelegt werden.

Public Key Infrastructure (PKI)

RACF bietet den gesicherten Systemzugang mittels digitaler Zertifikate an. Dies ist besonders für den Einsatz im Internet/Intranet sinnvoll. RACF kann Zertifikate erzeugen, signieren, prüfen und verwalten. Die Zertifikate können in der RACF-Datenbank oder in einer speziellen Hardware gespeichert werden. Der Aufbau einer Public Key Infrastructure mit eigenen RACF-Zertifikaten ist hiermit möglich. Auch der Zugang zu geschützten Webserver-Bereichen kann über Zertifikate erfolgen.

Firewall Technologies

Die *Firewall Technologies* des *Secure Way Security Server* für z/OS ermöglichen die Trennung interner und externer Netzbereiche. Sie unterstützen folgende Funktionalitäten:

- Packet Filter
- sichere Tunnel mit IPSec-Technik zum Aufbau von VPNs (Virtual Private Networks)
- Socks Server
- FTP Proxy Server
- Network Address Translation (NAT) von einer internen zu einer externen Adresse und zurück

Für den Einsatz von IPSec wird zusätzlich der *Communications Server* für z/OS benötigt.

LDAP

Zusammen mit dem *Secure Way Security Server* liefert IBM einen LDAP-Server aus. Dieser unterstützt die gängigen LDAP-Clients und kann somit als Auskunftssystem dienen. Zur Verwaltung großer Datenmengen kann sowohl die RACF-Datenbank als auch eine unabhängige DB2-Datenbank eingesetzt werden.

Distributed Computing Environment (DCE)

DCE ist eine Sammlung von Tools und Diensten, welche die Erstellung, Nutzung und Pflege von verteilten Anwendungen unterstützen. DCE unter z/OS unterstützt das *Distributed File System* (DFS), welches innerhalb der DCE-Umgebung die gemeinsame Nutzung von Daten (*Sharing*) erlaubt, und

Network File System (NFS), welches unter anderem Unix-Workstations gestattet, auf Daten der z/OS-Rechner zuzugreifen.

Integrated Cryptographic Service Facility (ICSF)

Das ICSF ist ein Software-Element, das mit der Krypto-Hardware und dem *Secure Way Security Server* zusammenarbeitet, um die Ver- und Entschlüsselung zu beschleunigen.

Sysplex Failure Managements (SFM)

Die *SFM Policy* erkennt, ob Fehler an einem im *Sysplex*-Verbund arbeitenden System aufgetreten sind und leitet gegebenenfalls entsprechende Maßnahmen ein. Ohne SFM wird, falls eine Maschine im Verbund Probleme hat, eine Nachricht an den Operator gesendet. Der Operator kann daraufhin das fehlerhafte System aus dem Verbund nehmen und Recovery-Maßnahmen einleiten. SFM erlaubt die Installation einer Policy, die bei bestimmten Fehlern automatisch festgelegte Recovery-Aktionen initiiert und so den Betrieb der Maschine aufrechterhalten kann.

Automatic Restart Manager (ARM)

Der ARM erlaubt ein schnelles Wiederherstellen von Subsystemen, die aufgrund kritischer Ressourcen (z. B. *Deadlocks*) angehalten wurden. Hierdurch werden die aktiven Systemeingriffe durch das Operating reduziert.

Global Resource Serialization (GRS)

GRS stellt in einer Multitasking/Multiprocessing-Umgebung sicher, dass der Zugriff auf Ressourcen, die von mehr als einem Rechner benutzt werden, koordiniert abläuft. Im Rahmen einer *Sysplex*-Konfiguration sollte GRS in jedem Fall eingesetzt werden.

GRS kann einerseits im *RING*-Modus konfiguriert werden. Dabei wird ein *RSA Message Control Block* (Ring System Authority) sequentiell von z/OS-System zu z/OS-System transportiert, in dem jedes System seine Anforderungen einträgt. Jedes System kopiert sich die RSA Message in den eigenen Speicher, d. h. die Information ist nicht aktueller, als bei der zuletzt vorbeigekommenen RSA-Information.

Als weitere, modernere Konfiguration steht der *STAR*-Modus zur Verfügung. Dabei sind alle z/OS-Systeme im Sysplex mit einer *Lock Structure* in der *Coupling Facility* verbunden, wobei jedes z/OS-System nur die eigene Sicht im lokalen Speicher halten muss. Die Abfrage nach Ressourcen durch GRS ist im *STAR*-Modus effektiver als im *RING*-Modus.

Unix System Services (USS)

USS ist keine Unix-Portierung, sondern ein POSIX-kompatibles Subsystem von MVS. Früher wurde es als *Open Edition MVS* vertrieben. Die Aufgabe des USS Subsystems liegt im Betrieb POSIX-kompatibler Anwendungen. Hierfür wurde das *Hierarchical File System* (HFS) und eine *Unix Shell* eingeführt.Parallel zu HFS steht seit geraumer Zeit auch das Filesystem zFS zur Verfügung, das für alle neuen Entwicklungen benutzt wird (siehe auch nachfolgenden Abschnitt *Dateisysteme und Zugriffsarten*).

Unter USS laufen viele Programme, die auch unter POSIX-konformen Unix-Betriebssystemen laufen können. So sind die Funktionen von TCP/IP für z/OS größtenteils unter USS realisiert. Ebenso steht ein HTTP-Webserver zur Verfügung, der als *Daemon* unter USS oder als *Started Task* unter MVS laufen kann.

System Managed Storage (SMS)

SMS vereinfacht das Verwalten von Daten auf Festplatten, indem diese Funktion viele Aufgaben, z. B. das Anlegen von Dateien auf bestimmten Festplatten, die Festlegung von Charakteristiken der *Datasets* usw., übernimmt. Hierzu werden sogenannte ACS-Routinen (*Automated Control Storage*) definiert, die nach vorgegebenen Regeln den Plattenspeicher verwalten. *Datasets* werden dabei anhand ihrer Namensgebung in vorher festgelegte Plattenpools gespeichert. Da Mainframe-Systeme nicht selten über eine große Anzahl von Platten verfügen, vereinfacht SMS die Verwaltung der Dateien außerordentlich. Die Verwaltung von SMS kann über das interaktive Dialog-System ISMF erfolgen (*Interactive Storage Management Facility*).

Im Rahmen des SMS-Konzepts gibt es eine Reihe von Software-Produkten, die die effiziente Verwaltung von Daten in einer Umgebung mit dem z/OS-Betriebssystem ermöglichen (z. B. DFHSM- oder DFxxx-Produkte). Darüber hinaus stehen als *Storage Management* Funktionen eine Reihe von Dienstprogrammen zur Verfügung, die die Verwaltung der Datenbestände unterstützen.

Hierarchical Storage Manager (HSM)

HSM ist ein wesentlicher Bestandteil des SMS-Konzeptes von z/OS. Das Programm-Produkt unterstützt die Verwaltung der z/OS-Dateien, die Datensicherung sowie die effektive Nutzung von Speichermedien. Gesteuert über sogenannte *Policies* (Regel-Definitionen) werden von HSM zu vorgegebenen Zeiten Dateien auf andere Medien verschoben (migriert) und dabei komprimiert. Es gibt zwei Migrations-Level:

- Migration-Level 1 auf HSM-eigene Platten
- Migration-Level 2 auf Bänder (in Roboterstationen) oder nach VTS (*Virtual Tape System*)

Migrierte Dateien können erst wieder gelesen werden, wenn sie über den HSM wieder erstellt worden sind. Diese Funktion kann entweder manuell initiiert werden oder erfolgt automatisch, wenn die Datei angesprochen wird (*Recall*-Funktion).

Weiterhin können *logische Dumps* (bestimmte Dateien) oder *Full Volume Dumps* (der Inhalt einer ganzen Festplatte) zu bestimmten Zeiten gestartet werden und somit automatisch Datensicherungen durchgeführt werden.

System Management Facility (SMF)

SMF ist die zentrale Protokollierungsfunktion im z/OS-Betriebssystem. Nahezu alle Komponenten und auch viele ISV-Produkte (*Independent Software Vendor*) schreiben SMF-Sätze, in denen die Aktivitäten protokolliert werden. Auch RACF schreibt solche Sätze. Hier ist besonders der Satztyp 80 wichtig für spätere Auswertungen.

Resource Measurement Facility (RMF)

RMF protokolliert das Systemverhalten in Bezug auf Kapazität und Performance. Die Protokolldaten werden als SMF-Sätze gesichert und stehen für spätere Auswertungen zur Verfügung. RMF ist optional, alternative Programme (Monitore) sind am Markt verfügbar.

Generalized Trace Facility (GTF)

Der Begriff *Trace* stellt die Möglichkeit dar, den Datenfluss zwischen zwei Komponenten im System (z. B. einer Anwendung und einem Endbenutzer) mitzuschreiben und in einer Datei zur späteren Auswertung zur Verfügung zu stellen. GTF ist die zentrale *Trace*-Funktion von z/OS, die *Traces* von vielen z/OS-Komponenten ermöglicht. Darüber hinaus werden auch *Traces* der Netzfunktionen unterstützt. Zum Auswerten der *Traces* stehen verschiedene Programme zur Verfügung, z. B. ACFTAP für Netzanalysen. Für *Online-Traces* bietet sich auch NLDM an (*Network Logical Data Manager*), eine Komponente der *NetView* Software.

Transaktionsmonitore und Datenbanksysteme

IMS TM (Information Management System Transaction Monitor)

IMS TM wird die Transaktionskomponente des IMS-Systems genannt, mit der die IMS-Transaktionen in einem IMS-System verwaltet und gesteuert werden. (In älteren IMS-Versionen ist diese Funktion auch unter dem Kürzel *DC* bekannt.)

IMS DB (Information Management System Database)

IMS DB wird die Datenbankkomponente des IMS-Systems genannt, mit der die IMS-Datenbanken in einem IMS-System verwaltet werden. Bei IMS-Datenbanken handelt es sich um hierarchische Datenbankmodelle.

CICS TS (Customer Information Control System Transaction Server)

CICS TS ist ein weiterer Transaktionsmonitor. Mit CICS TS werden die CICS-Transaktionen in einem System verwaltet und gesteuert. Als Datenbank werden häufig VSAM-Files oder DB2-Datenbanken eingesetzt.

DB2 (Database 2)

DB2 ist ein Programmpaket, mit dessen Hilfe relationale Datenbanken erstellt und verwaltet werden können. Über IMS TM, CICS TS oder über die Sprache SQL (*Structured Query Language*) können Daten in der Datenbank in Tabellen abgelegt oder aus dieser Datenbank extrahiert werden.

IMS, CICS und DB2 sind nicht im Fokus des Bausteins *S/390- und zSeries-Mainframe* und werden nur am Rande betrachtet.

File Transfer Protocol (FTP)

FTP-Programme erlauben den Transport von Daten sowohl zwischen z/OS-Systemen, als auch zu und von anderen Plattformen.

FTP ist nicht im Fokus des Bausteins *S/390- und zSeries-Mainframe* und wird nur am Rande betrachtet.

Middleware

MQSeries (Message Queueing System)

MQSeries stellt eine Verbindung zwischen unterschiedlichen Applikationen auf der Basis von Nachrichten (Messages) her, beispielsweise zwischen CICS, IMS oder Batch-Applikationen. Über entsprechende APIs (*Application Programming Interfaces*) werden die Nachrichten an MQSeries weitergegeben und danach an die vorgegebenen Ziele ausgeliefert. Ist die Lieferung nicht möglich, werden die Nachrichten zwischengespeichert (*Queued*) und erst dann weitergeleitet, wenn der Verbindungsaufbau wieder möglich ist.

MQSeries ist nicht Gegenstand des Bausteins *S/390- und zSeries-Mainframe*.

Dateisysteme und Zugriffsarten

Dateien werden unter z/OS mit bestimmten Charakteristiken angelegt, z. B. Größe, Art der Speicherung (innere Struktur), auf welcher Platte sich die Datei befindet und unter welchem Dateinamen die Datei gespeichert und normalerweise zu finden ist. Insbesondere in Bezug auf die innere Struktur der Dateien bestehen teilweise erhebliche Unterschiede zu anderen, häufig eingesetzten Betriebssystemen. Nachfolgend die wichtigsten Dateitypen:

HFS (Hierarchical File System)

Das HFS-Filesystem ist mit typischen Unix-Dateisystemen vergleichbar. Es wird in einem MVS *Dataset* abgelegt, das MVS-seitig mit den üblichen Werkzeugen verarbeitet werden kann (z. B. Datensicherung über HSM). Gegenüber USS stellt sich das Filesystem hierarchisch dar. Daten in diesem Filesystem werden im EBCDIC-Zeichensatz gespeichert.

z/OS File System (zFS)

Das zFS entspricht konzeptionell dem HFS, jedoch können hier mehrere Filesysteme in einem z/OS *Dataset* gespeichert werden und die Daten lassen sich auch im ASCII-Zeichensatz abspeichern. Laut IBM ist zFS das strategische Filesystem, in dem nur noch neue Funktionen entwickelt werden. zFS kann bis jetzt nicht als Root-Filesystem verwendet werden.

MVS Physical Sequential (PS) Datasets

In dieser Art von *Dataset* können Daten nur sequentiell gelesen oder geschrieben werden. *Physical Sequential Datasets* dienen im Systemumfeld oft der Verarbeitung großer Datenmengen.

MVS Partitioned Organized (PO) Datasets

Partitioned Organized Datasets können mit einer Bibliothek verglichen werden. In einem *PO Dataset* gibt es einen Index (*Directory*) und die einzelnen Bücher (*Member*). Die *Member* enthalten die Informationen. Bei häufigem Abspeichern von *Membern* muss die Datei zeitweise reorganisiert werden. Dies kann durch die Benutzung einer PDSE-Datei (*Partitioned Dataset Enhanced*) umgangen werden.

Virtual Storage Access Method (VSAM)

Im z/OS-Betriebssystem stellt VSAM eine der wichtigsten Zugriffsmethoden auf Dateien dar. Die Datensätze werden über einen Index oder eine relative Byte-Adresse gefunden. Vier VSAM-Dateiarten lassen sich unterscheiden:

- ESDS (Entry Sequenced Data Set)
- KSDS (Key Sequenced Data Set),
- RRDS (Relative Record Data Set) und
- LDS (Linear Data Set).

Weitere Zugriffsmethoden

Neben der allgemein bekannten VSAM-Methode gibt es weitere Methoden wie *Sequential Access Method* (SAM) und *Queued Sequential Access Method* (QSAM) sowie diverse andere Methoden, die hier wegen ihrer geringeren Verbreitung nur am Rande erwähnt werden.

Server- und Client-Konzepte

Durch die Erweiterung des z/OS-Betriebssystems um den *Unix System Server* (USS) können Rechner mit diesem Betriebssystem zusätzliche Server- und Client-Funktionen wahrnehmen. Beispiele für solche Server-Funktionen sind unter anderem der HTTP-Server, der FTP-Server oder der *Domain Name Server*. Die FTP-Funktion lässt sich z. B. auch als Client einsetzen. Darüber hinaus wird das z/OS-System in heutigen 2-Schicht- oder 3-Schicht-Architekturen vielfach als Datenbank-Server eingesetzt, wo es mit anderen Plattformen kommuniziert.

Konfiguration des z/OS (OS/390)

I/O-Config

Die Eingabe-/Ausgabe-Konstellation eines z/OS-Betriebssystems wird im Rahmen des HCD-Dialogs über eine I/O-Konfiguration erstellt und über das *Operator Facility* (via HMC-Konsole) für die jeweilige *LPAR* abgelegt. Zum *IML*-Zeitpunkt ist bereits festgelegt, welche I/O-Profile für die spätere Auswahl zur Verfügung stehen. Ein dynamisches Nachkonfigurieren während des Betriebs ist jederzeit möglich (siehe Maßnahme M 3.39 *Einführung in die zSeries-Plattform*).

IPL Volume

Zum Starten eines z/OS-Betriebssystems benötigt das System ein spezielles *IPL-Volume*, eine Platte mit einer speziellen *Bootstrap-Routine*, die die notwendigen Betriebssystemprogramme lädt und zum Starten bringt. Dieser Vorgang entspricht einem Boot-Vorgang bei Unix und nennt sich bei z/OS *Initial Program Load* (IPL).

Parmlib / Proclibs

Eine (oder mehrere) Parameter-Datei(en) stehen über den *Parmlib*-Mechanismus zur Verfügung, um alle wesentlichen z/OS-Systemparameter zu definieren. Dazu gehört z. B., welche Subsysteme gestartet werden sollen, welche Sicherheitsmechanismen aktiviert werden und welche Bibliotheken autorisiert

sein sollen. Alle wichtigen System-Jobs - auch *Started Tasks* genannt - stehen auf Prozedur-Bibliotheken (*Proclibs*) bereit, um zum Startzeitpunkt aktiviertwerden zu können (siehe Maßnahme M 3.39 *Einführung in die zSeries-Plattform*). Dieser Bereich muss sehr sorgfältig definiert und geschützt werden, da hier wesentliche Sicherheitsmechanismen verankert sind.

Kataloge

Dateien werden über Kataloge geführt und dem System bekannt gegeben. Als oberste Instanz existiert der *Master-Katalog*, an den über *Alias*-Definitionen verschiedene Benutzerkataloge angebunden sind.

Arbeitsdateien

Zur Minimalkonfiguration eines z/OS-Betriebssystems gehören mehrere Arbeitsdateien, die bei Produktionsbeginn angelegt sein müssen:

- Syslog
- JES2/3 Spool und Checkpoint
- SMF-Dateien
- Log-Writer-Dateien
- Couple Datasets (bei Sysplex)
- Page Datasets zum Auslagern von Hauptspeicher

M 3.41 Einführung in Linux und z/VM für zSeries-Systeme

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator

Neben den unter z/OS laufenden *Unix System Services* (USS) steht auch Linux für die zSeries-Hardware zur Verfügung.

Linux für zSeries entspricht dem Linux für andere Plattformen, die Modifikationen im Kernel beziehen sich ausschließlich auf Anpassungen an die zSeries-Hardware (Systemumgebung, CPU-Architektur und Hardware-abhängige Treiber). Da das zSeries-Linux eine Portierung darstellt, arbeitet es mit dem ASCII-Zeichensatz (im Gegensatz zum USS HFS-Dateisystem, das im EBCDIC-Modus läuft). Derzeit sind zwei Linux-Versionen für diese Plattformfamilie erhältlich: eine 31 Bit-Version für S/390-Hardware und eine 64 Bit-Version für die zSeries-Hardware (das S/390-System ist zwar ein 32 Bit-System, die Software darauf läuft jedoch mit 31 Bit, da das erste Bit zur Umschaltung zwischen 24 Bit- und 31 Bit-Modus benötigt wird).

Betriebsarten von Linux unter zSeries

Es sind drei unterschiedliche Betriebsarten von Linux unter zSeries möglich:

- Linux Native auf zSeries Hardware
- Linux in einer zSeries LPAR
- Linux unter dem Träger-System z/VM

Linux Native auf zSeries Hardware

In dieser Betriebsart wird Linux als Single-System auf der zSeries Hardware eingesetzt. Dies bedeutet, dass die gesamte zSeries Hardware vom Linux-System benutzt wird. Single-Systeme stellen in der Praxis derzeit eher eine Ausnahme dar.

Linux in einer zSeries LPAR

Bei dieser Variante erfolgt der Betrieb von Linux in einer *LPAR (Logical Partition)* auf der zSeries-Maschine. Der *LPAR*-Mode der zSeries-Hardware erlaubt den Betrieb von mehreren unabhängigen Betriebssystem-Installationen auf einer zSeries-Maschine. Jede einzelne Partition verhält sich wie eine unabhängige Hardware. Auf diesen *LPARs* können unter anderem *z/OS* oder *Linux* als Betriebssystem installiert werden.

Die Betriebsart *Linux in einer zSeries LPAR* kommt zum Beispiel in Betracht, wenn zusätzlich zu einem schon vorhandenen z/OS-Datenbank-Server Internet-Applikationen, wie z. B. Webserver, betrieben werden sollen.

Die Konsolidierung von Linux und z/OS auf einem physischen zSeries-System an Stelle zweier getrennter Systeme reduziert nicht selten den Aufwand für die Installation und den Betrieb.

Linux unter dem Träger-System z/VM

Linux unter z/VM

Es können mehrere Linux-Installationen auf einem zSeries-Rechner oder innerhalb einer LPAR unter dem Träger-System z/VM betrieben werden. Das

z/VM stellt sogenannte virtuelle Maschinen zur Verfügung, unter denen die einzelnen Linux-Installationen unabhängig von einander betrieben werden können.

Die Betriebsart *Linux unter dem Träger-System z/VM* kommt zum Beispiel in Betracht, wenn die z/Series-Hardware im Rahmen eines Server-Konsolidierungsprojektes eingesetzt wird. Hierbei wird die Installation von Linux durch das System-Cloning erleichtert. Es können viele Linux-Systeme parallel auf einer Maschine betrieben werden. Darüber hinaus erleichtert diese Konstellation eine zentrale Kontrolle und Administration.

Communications Server for Linux on zSeries

Linux für zSeries unterstützt ohne zusätzliche Komponenten TCP/IP. Der *Communications Server for Linux on zSeries* als separates Produkt ermöglicht zusätzlich eine Kommunikation über SNA oder TCP/IP mit anderen Systemen in den folgenden Bereichen:

- Advanced Peer to Peer Networking (APPN)
- High Performance Routing (HPR)
- TN3270E Server
- Telnet Redirector
- SSL data encryption scalability
- Client Authentication
- Application Programming Support
- Advanced Program to Program Communication (APPC)
- Common Programming Interface for Communications (CPI-C)

Das Programm bietet den Administratoren und Bedienern Unterstützung bei der Installation, Konfiguration und Problemanalyse.

HiperSockets

HiperSockets erlauben eine LPAR-übergreifende Kommunikation. Mit dieser Funktion lässt sich innerhalb des Systems ohne eine zusätzliche physische Verbindung ein "systeminternes Netz" über TCP/IP aufbauen.

Ein von Linux abgesetzter TCP/IP-Auftrag wird auf Maschinenebene abgefangen und an die adressierte Partition umgeleitet. Dies ist mit Übertragungsraten von mehreren GByte/s möglich. Gegenüber dem Linux-Betriebssystem verhält sich diese Kommunikationsschnittstelle wie ein herkömmliches TCP/IP-Netz. Auch z/OS-Systeme in einer anderen LPAR lassen sich so mit Linux-Systemen verbinden.

Integrated Facility for Linux (IFL)

Diese Hardware-Funktion gestattet den zusätzlichen Einsatz von Linux auf einem System. Die speziellen IFL-Prozessoren bringen zusätzliche Rechenkapazität.

IFL wird von PR/SM wie eine separate LPAR verwaltet, die jedoch nur Linux-Betriebssysteme (oder z/VM mit Linux-Betriebssystemen) unterstützen kann.

z/VM

Das Betriebssystem z/VM ermöglicht eine - Software-basierte - Aufteilung des Rechners in mehrere parallele *Virtual Machines*. z/VM verwaltet mit dem *Control Program* (CP) die Hardware der Partition und stellt den Gast-Betriebssystemen die *Virtual Machines* zur Verfügung.

Die Hardware-Zugriffe erfolgen über das CP, das dem aufrufenden Betriebssystem das Ergebnis in seiner gewünschten Form präsentiert.

Darüber hinaus stellt z/VM das *Conversational Monitoring System* (CMS) zur Verfügung, in dem z. B. Scripts ablaufen können, um korrektive Maßnahmen durchzuführen oder neue Systeme zu aktivieren.

Linux-Sicherheitsaspekte

Hardware

Die Verbindung zwischen den Linux Betriebssystemen oder zwischen Linux und z/OS-Systemen kann über *HiperSockets* erfolgen. Diese sind integraler Bestandteil der Hardware und ermöglichen eine schnelle und - bei korrekter Konfiguration - sichere TCP/IP-Verbindung.

Durch den z/VM-Einsatz wird die Bereitstellung und Absicherung der Hardware zu einem Teil durch eine Software-Lösung ersetzt. Die Ressourcen sind deshalb nicht als reale Hardware verfügbar, sondern werden virtuell in der Software (z/VM) abgebildet. Dem entsprechend müssen die Ressourcen mit Software-Mitteln abgesichert werden.

RACF/VM

Die *Resource Access Control Facility for z/VM* (RACF/VM) erweitert die Standard-Security des z/VM um eine Zugriffskontrolle für die Ressourcen des z/VM-System. Daneben überprüft es die Zugriffe auf die Systemressourcen und die *Virtual Machine*.

DIRMAINT

Die zentrale Konfigurationsdatei von z/VM ist das *z/VM-System-Directory*. Die Verwaltung dieser Datei wird von *DIRMAINT* unterstützt, wobei die *DIRMAINT*-Funktion die folgenden Aufgabenbereiche abdeckt:

- Distributed Virtual Machine Management
- automatische Minidisk-Administration (Allokieren, Löschen, usw.)
- Unterstützung der Benutzer
- Auditing
- Backup/Recovery des Directory

Auch wenn das Directory mit einem herkömmlichen Editor bearbeitet werden kann, ist *DIRMAINT* für alle Installationen mit größeren User-Anzahlen

empfehlenswert, da die dialoggestützte *DIRMAINT*-Funktion die Verwaltung vereinfacht. Dies hilft bei der Vermeidung von Eingabefehlern.

Access Control

Die Steuerung der Zugriffskontrolle ist bei Linux im Wesentlichen über drei Mechanismen möglich:

- Permission Bits wie bei anderen Unix-Betriebssystemen
- Mandatory Access Control (MAC)
- Access Control Lists (ACLs)

Während die erste Methode in der Regel für normale Sicherheitsanforderungen ausreicht, sollten MAC und ACLs bei höheren Sicherheitsanforderungen in Betracht gezogen werden. Für MAC und ACLs sind zusätzliche Software-Komponenten erforderlich.

Pluggable Authentication Module (PAM)

Zur Zentralisierung der Benutzerverwaltung bietet es sich für Linux auf LPARs an, die Verwaltung der Userids über ein z/OS-RACF abzuwickeln. Dazu muss das Linux-System über ein *Pluggable Authentication Module* (PAM) verfügen und mit dem vorgeschalteten LDAP-Server des z/OS-RACF-Systems über die *HiperSockets* Verbindung aufnehmen.

Ist die Kennung im RACF administriert und sind User-ID und Passwort korrekt, so wird der Zugang zu dem Linux-System freigegeben. Dateizugriffe lassen sich jedoch nach wie vor nur über die Sicherheitsmechanismen von Linux (Permisson Bit) realisieren.

Transaction Processing Facility (TPF)

TPF ist ein weiteres Betriebssystem für die zSeries-Plattform und stellt eine Sonderform dar. Es handelt sich dabei um ein transaktionsorientiertes System, das speziell im Bereich Flugzeugbuchung eingesetzt wird, wo es besonders auf hohe Performance ankommt. Transaktionen laufen hierbei direkt im Kernel-Modus.

TPF wird an dieser Stelle aus Gründen der Vollständigkeit erwähnt und ist nicht Gegenstand des Bausteins *S/390- und zSeries-Mainframe*.

M 3.42 Schulung des z/OS-Bedienungspersonals

Verantwortlich für Initiierung: Leiter IT, Leiter Personal

Verantwortlich für Umsetzung: Administrator, Vorgesetzte

Der Betrieb von z/OS-Systemen ist komplex und so gestaltet, dass viele Bereiche daran beteiligt sind. Es ist deshalb darauf zu achten, dass das Bedienungspersonal die für seine Tätigkeit benötigte Ausbildung erhält. Neben den Empfehlungen aus Maßnahme M 3.11 *Schulung des Wartungs- und Administrationspersonals* sind für die Mitarbeiter im z/OS-Bereich zusätzlich die folgenden Hinweise zu beachten:

- Die Administratoren sollten durch regelmäßige Teilnahme an Schulungsmaßnahmen und Anwendertagungen entsprechend ihren Aufgaben ausgebildet werden. Es sollte überlegt werden, die Ausbildung anhand eines Schulungsplanes festzulegen.
- Zusätzlich sollten RACF-Adminstratoren in allen sicherheitsrelevanten Bereichen des z/OS-Systemes ausgebildet werden.
- Die Auditoren sollten entsprechend ihren Aufgaben geschult werden. Die Aufgaben der Auditoren sind in Maßnahme M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS* beschrieben.
- Es sollte überlegt werden, ob eine regelmäßige sicherheitstechnische Schulung für alle Mitarbeiter, die mit z/OS-Systemen arbeiten, durchgeführt werden sollte. Dabei sollte den Mitarbeitern das vorhandene Regelwerk, die Sicherheitsdefinitionen und die Gründe, die zu den Sicherheitsmaßnahmen geführt haben, erläutert werden (*Sensibilisierung für ein Sicherheitsdenken*).

Ergänzende Kontrollfragen:

- Werden alle Administratoren und Auditoren ihren Aufgaben entsprechend ausgebildet?
- Ist ein Schulungsplan für die Administratoren vorhanden?

M 3.43 Schulung der Administratoren des Sicherheitsgateways

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Ein Sicherheitsgateway stellt ein zentrales Element bei der Absicherung eines Netzes gegen Gefährdungen von außen dar. Deswegen ist es unerlässlich, dass die Administratoren des Sicherheitsgateways ausreichend geschult sind, damit sie in der Lage sind, alle gebotenen Funktionen und Sicherheitsmerkmale optimal zu nutzen.

In den Schulungen sollten ausreichende Kenntnisse zu den für die Einrichtung und den Betrieb der Komponenten des Sicherheitsgateways notwendigen Vorgehensweisen, Werkzeugen und Techniken vermittelt werden. Dies gilt auch für herstellerspezifische Aspekte zu einzelnen Produkten, die als Komponenten des Sicherheitsgateways eingesetzt werden. Für die Anforderungen an die Schulungen für Betriebssysteme von Rechnern, die als Komponenten des Sicherheitsgateways eingesetzt werden sowie für aktive Netzkomponenten (insbesondere Router, die als Paketfilter Teil eines Sicherheitsgateways sind) sollten die Hinweise in den jeweiligen Bausteinen der Betriebssysteme beziehungsweise im Baustein B 3.302 *Router und Switches* berücksichtigt werden.

Allgemein sollten in den entsprechenden Schulungen folgende Elemente enthalten sein:

- Grundlagen und Konzepte der Administration, Kenntnisse der Kommandos zu Einrichtung, Betrieb, Wartung und Fehlersuche für jede Komponente des Sicherheitsgateways. Eine Schulung sollte eine ausgewogene Mischung aus Theorie und Praxis darstellen.
- Grundlagen der IT-Sicherheit, insbesondere Vorsorgemaßnahmen, Reaktion, Analyse und Incident Handling (siehe beispielsweise auch Baustein B 1.8 *Behandlung von Sicherheitsvorfällen*)
- Angriffsszenarien (z. B. Denial of Service Angriffe, ARP-Spoofing, IP-Spoofing, DNS-Spoofing, Viren und andere Schadsoftware)
- Grundlagen der Strukturierung von Netzen
- ISO/OSI Schichten Modell
- Grundlagen von IP und der damit zusammenhängenden Protokolle (IP-Adressierung, Subnetting, IP, ICMP, TCP, UDP) und der verschiedenen Möglichkeiten zur Filterung anhand der Header-Daten
- Grundlagen des Routing, statisches und dynamisches Routing, Grundlagen der eingesetzten Routing-Protokolle und ihrer Sicherheitsaspekte
- Grundlagen der wichtigsten eingesetzten Protokolle der Anwendungsschicht (beispielsweise SMTP, HTTP und HTTPS, Secure Shell, SMB/CIFS) und der verschiedenen Möglichkeiten zur Filterung anhand von Protokollbefehlen oder Befehlsparametern
- Grundlagen zum Thema Virtuelle Private Netze (VPN)

- Grundlagen zum Thema Intrusion Detection/Intrusion Prevention (IDS/IPS)
- Grundlagen zum Umgang mit verschlüsselten Daten (Verschlüsselung z. B. mit HTTPS oder IPSec) und Möglichkeiten zur Behandlung verschlüsselter Daten
- Betrieb
  - Management der Geräte, Werkzeuge
  - Protokollierung
  - Sicherung und Verwaltung von Konfigurationsdaten
- Fehlerbehebung
  - Fehlerquellen und Ursachen
  - Mess- und Analysewerkzeuge, Werkzeuge zur automatischen Überprüfung der einzelnen Komponenten des Sicherheitsgateways auf korrekte Funktion
  - Teststrategien zur Fehlersuche
  - Anforderungen an sichere Netzinstallationen
- Relevante rechtliche Aspekte wie Datenschutz, rechtliche Aspekte der Netzanbindung (in Deutschland beispielsweise Teledienstegesetz) und ähnliche Regelungen

Auch wenn in einer Gruppe von Administratoren die Aufgaben so verteilt sind, dass jeder Administrator nur einen bestimmten Verantwortungsbereich hat, ist es unverzichtbar, dass alle Administratoren ein allgemeines Grundwissen besitzen. Die individuellen Schwerpunkte können davon ausgehend gezielt ausgebaut und gepflegt werden. Zu vielen Produkten gibt es von den Herstellern oder spezialisierten Anbietern hierfür ein umfangreiches Angebot an aufeinander aufbauenden und individuell vertiefenden Seminaren. Das Angebot an qualifizierten Schulungen stellt ebenfalls ein Kriterium dar, das bei der Entscheidung für einen bestimmten Hersteller berücksichtigt werden sollte.

Für Schulungsmaßnahmen sollte bereits bei der Beschaffung von IT-Komponenten ein Budget eingeplant werden und ein Schulungsplan für Administratoren erstellt werden. Die Inhalte einer Schulung sollten die folgenden Punkte umfassen:

Ergänzende Kontrollfragen:

- Steht ein Budget für Schulungsmaßnahmen zur Verfügung?
- Wurde ein Schulungsplan für Administratoren in Anlehnung an die erwähnten Punkte erstellt?

M 3.44 Sensibilisierung des Managements für IT-Sicherheit

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Sicherheit ist Führungsaufgabe!

Eine nachdrückliche und aktive Unterstützung durch die Behörden- bzw. Unternehmensleitung ist essentiell, damit Sicherheitskampagnen für die Mitarbeiter erfolgreich sein können. Daher ist es unabdingbar, dass vor dem Beginn von Sensibilisierungsmaßnahmen zu IT-Sicherheit für Mitarbeiter das Management für Sicherheitsfragen sensibilisiert wird.

Die wichtigsten Informationen, die dem Management dabei geliefert werden müssen sind:

- **Darstellung der Sicherheitsrisiken und damit verbundenen Kosten**

  Die Aufmerksamkeit der Entscheidungsträger kann z. B. durch Berichte über Sicherheitsvorfälle erreicht werden, die die eigene Institution ebenso betreffen könnten (aus Institutionen derselben Branche oder mit ähnlicher IT). Beispiele konkreter Sicherheitsvorfälle aus der Nachbarschaft oder bei vergleichbaren Institutionen können die Rückendeckung des Managements erleichtern. Solche Beispiele finden sich mittlerweile nicht nur in Fachzeitschriften, sondern auch in Tageszeitungen (z. B. nach Hackerangriffen oder Virenvorfällen) und natürlich in großer Menge im Internet. Tatsächliche Schadensfälle aus der Vergangenheit aus der eigenen Institution können ebenfalls zu diesem Ziel eingesetzt werden.

  Die Darstellung von finanziellen Schäden in konkreten Zahlen ist erfahrungsgemäß schwierig. Statistiken und Auswertungen, wie sie beispielsweise von den Polizeien (BKA, FBI) oder Sicherheitsfachzeitschriften von Zeit zu Zeit veröffentlicht werden, bieten in manchen Fällen geeignete Informationen.

- **Auswirkungen auf die Geschäftsprozesse**

  Des Weiteren ist es wichtig, dass die Auswirkungen von IT-Sicherheitsvorfällen auf die geschäftskritischen Prozesse geschildert werden. Mögliche Abhängigkeiten von IT-Anwendungen und IT-Systemen sind der Geschäftsführung nicht immer bekannt.

  Eine Auflistung von möglichen Sicherheitsrisiken reicht jedoch in der Regel nicht aus, um die Unterstützung des Managements zu gewinnen. Eine ausgewogene Argumentation sollte darüber hinaus auch die folgenden Punkte beinhalten.

- **Rechtliche Sicherheitsanforderungen**

  Gesetze und andere juristische Vorgaben können ebenfalls Anforderungen an die IT-Sicherheit in einer Institution nach sich ziehen, hierzu gehören beispielsweise Datenschutzgesetze, Sozialgesetzbuch, Handelsgesetzbuch, Bürgerliches Gesetzbuch, Strafgesetzbuch, etc.

  Viele gesetzliche Formulierungen zu IT-Sicherheitsanforderungen sind allgemein gehalten und können unter Umständen unverbindlich erscheinen.

In der Tat lassen sich hieraus jedoch konkrete Verpflichtungen für die Gewährleistung eines angemessenen IT-Sicherheitsniveaus ableiten. Eine Institution muss untersuchen, welche Regularien und Gesetze im Einzelnen Fall zur Wirkung kommen können.

- **Vorteile einer Zertifizierung**

  Eine Zertifizierung der IT-Sicherheitsprozesse bestätigt offiziell die hohe Wertschätzung der IT-Sicherheit in einer Institution. Das Vertrauen der Geschäftspartner und der Öffentlichkeit in die IT der Institution wird dadurch gestärkt. Eine Zertifizierung kann außerdem bei Ausschreibungen Wettbewerbsvorteile mit sich bringen.

- **Standard-Vorgehensweisen zur IT-Sicherheit für die Branche**

  Eine zusätzliche Motivation für den Einsatz von IT-Sicherheitsstandards ist das Verhalten anderer ähnlicher Organisationen. Informationen zu Branchen-Standards können aus Fachzeitschriften der Branchen, aus Veranstaltungen oder durch Kontakte zu Kammern und Verbände bezogen werden.

Ein geeigneter Einstieg für die Sensibilisierung der Leitungsebene ist ein kurzer Bericht, gefolgt von einer Präsentation, die mit aktuellen Beispielen (extern und intern) das Thema IT-Sicherheit erläutert. Hierbei sollte beispielsweise aufgezeigt werden, dass technische Maßnahmen ohne gleichzeitige personelle und organisatorische Maßnahmen sinnlos sind. Um die Unterstützung des Managements zu bekommen, ist es hilfreich, den Nutzen solcher Maßnahmen aufzuzeigen.

Durch die Präsentation von Sicherheitsrisiken und Lösungsalternativen kann das Management für die Notwendigkeit der Umsetzung von IT-Sicherheitsmaßnahmen überzeugt werden.

IT-Sicherheit wird erfahrungsgemäß in einer Institution nur dann erfolgreich umgesetzt, wenn alle Vorgesetzten hier mit gutem Beispiel vorangehen. Sinnvoll ist es daher, alle Führungskräfte explizit darauf zu verpflichten, ihre Mitarbeiter auf die Einhaltung der IT-Sicherheitsvorgaben hinzuweisen und zu sensibilisieren.

Ergänzende Kontrollfragen:

- Unterstützt die Leitungsebene die Durchführung von Sensibilisierungsmaßnahmen zu IT-Sicherheit in ausreichendem Maße?
- Geht die Initiative für IT-Sicherheit von der Behörden- bzw. Unternehmensleitung aus?

M 3.45 Planung von Schulungsinhalten zur IT-Sicherheit

Verantwortlich für Initiierung: Leiter Personal, IT-Sicherheitsmanagement-Team

Verantwortlich für Umsetzung: Vorgesetzte, Personalabteilung, IT-Sicherheitsmanagement-Team

Alle Mitarbeiter sollten, bezogen auf ihren Arbeitsplatz, fundiertes Fachwissen besitzen und in diesem Rahmen auch über Belange der IT-Sicherheit Bescheid wissen.

Dafür sollte es auf verschiedene Zielgruppen zugeschnittene Schulungen zu IT-Sicherheit geben, z. B. für IT-Benutzer aus den verschiedenen Fachbereichen, Vorgesetzte, IT-Sicherheitsmanagement-Team, IT-Verantwortliche, Administratoren, etc.

Zu Beginn einer Schulungsmaßnahme muss der Qualifikationsstand und der Ausbildungsbedarf der Mitarbeiter analysiert werden. Dabei sind folgende Fakten zu ermitteln:

- Ausbildungsabschlüsse
- Berufserfahrung, Weiterbildungen, Zusatzkenntnisse
- Aufgaben und Rollen der Mitarbeiter in ihrer Organisationseinheit

Die Schulungsinhalte sollten so modularisierbar sein, dass jede Zielgruppe hinreichend und in angemessener Tiefe geschult werden kann. Im Folgenden werden wichtige Inhalte verschiedener Schulungsmodule vorgestellt, die für die jeweiligen Personengruppen rollenbezogen ausgewählt und eventuell zurechtgeschnitten werden müssen. Dieser Überblick soll dazu dienen, bei der Durchführung interner bzw. der Entscheidung für externe Schulungsveranstaltungen die passenden Inhalte auszuwählen. Daneben sollten alle für den jeweiligen IT-Verbund relevanten Bausteine der IT-Grundschutz-Kataloge daraufhin überprüft werden, ob die erforderlichen Maßnahmen nicht nur angeordnet, sondern auch geschult wurden.

Die hier beschriebenen Module sollten den Zielgruppen zugewiesen werden, wie dies in der folgenden Matrix exemplarisch aufgezeigt wird. Dabei wird mit "X" gekennzeichnet, dass das jeweilige Modul für die entsprechende Rolle empfohlen wird. "O" bedeutet optional, das heißt, es sollte von Fall zu Fall entschieden werden, ob die Inhalte des jeweiligen Schulungsmoduls für die entsprechende Rolle benötigt werden.

Schulungsmodule

Modul 1: Grundlagen der IT-Sicherheit

Modul 2: IT-Sicherheit am Arbeitsplatz

Modul 3: Gesetze und Regularien

Modul 4: IT-Sicherheitskonzept der Organisation

Modul 5: Risikomanagement

Modul 6: IT-Sicherheitsmanagement

Modul 7: IT-Systeme

Modul 8: Operativer Bereich

Modul 9: Technische Realisierung von Sicherheitsmaßnahmen

Modul 10: Notfallvorsorge/Notfallplanung

Modul 11: Neue Entwicklungen im IT-Bereich

Modul 12: Betriebswirtschaftliche Seite der IT-Sicherheit

Modul 13: Infrastruktur-Sicherheit

Modul / Funktion	1	2	3	4	5	6	7	8	9	**10**	**11**	**12**	**13**
Vorgesetzte	X	X	X	X							O	X	
IT-Sicherheitsmanagement	X	X	X	X	X	X	X	X	X	X	X	X	X
Datenschutzbeauftragter	X	X	X	X							X	O	
Infrastrukturverantwortliche	X	X	X	X	X	O				X			X
Benutzer	X	X											
Administratoren	X	X		X	X		X	X	X	X	X		O

Tabelle: Vorgeschlagene Schulungsmodule je Funktion

Die beiden Module 1 und 2 dienen als Basisschulung aller Mitarbeiter. Die Module 3 und folgende zeigen auf, welche Vertiefungsgebiete je nach Fachaufgaben außerdem gelernt werden sollten.

IT-Sicherheit beginnt mit Zutrittskontrolle

Je nach Art der Institution kann es sinnvoll sein, weitere Zielgruppen und die zugehörigen Ausbildungsziele zu definieren, z. B. Verwaltungsmitarbeiter oder Sicherheitsdienst mit dem Fokus auf deren Aufgabengebiet, aber auch deren Basiswissen über IT. Wichtig ist, dass bei der Schulung für IT-Sicherheit auch das Personal nicht vergessen wird, das nicht in erster Linie mit IT in Verbindung gebracht wird, wie Pforten- und Reinigungspersonal. Für diese ist allerdings im Allgemeinen kein komplexes Schulungsmodul erforderlich.

Modul 1: Grundlagen der IT-Sicherheit

Angesichts des beachtlichen Nutzens und der erheblichen Arbeitserleichterungen, die ein sinnvoller Einsatz der IT bewirken kann,

dürfen die gravierenden Gefahren nicht aus dem Auge verloren werden, die ein allzu sorgloser oder gar fahrlässiger Umgang mit dieser Technologie nach sich ziehen kann. Eine der wichtigsten Aufgaben des Schulungskonzeptes besteht daher in der Sensibilisierung der Mitarbeiter für das Thema IT-Sicherheit, die unter anderem folgende Themen umfassen sollte:

- Motivation
  - Statistiken zur IT-Sicherheit
  - Fallbeispiele für Gefährdungen und Risiken
  - Studien zur IT-Sicherheit
- Erläuterung der Grundprinzipien der IT-Sicherheit
  - Vertraulichkeit, Integrität und Verfügbarkeit als Grundlagen
  - Unterschied zwischen Security und Safety
- Gründe für Angriffe auf die IT-Sicherheit
  - Wirtschaftsspionage
  - staatliche Ermittlungen
  - Neugier, spielerische Herausforderung
  - kriminelle Ziele
- IT-Sicherheitsstrukturen der Organisation
  - Aufgaben und Ziele der Organisation
  - Einsatz von IT
  - Richtlinien und Vorgaben der Organisation
  - Ziele und Inhalte des IT-Sicherheitskonzeptes der Organisation
  - Aufgaben und Verpflichtungen der einzelnen Mitarbeiter
- Wesentliche Sicherheitsregeln für Mitarbeiter
  - Überblick über interne Sicherheitsregelungen
  - Umgang mit Passwörtern
  - Nutzung von E-Mail und Internet
  - Virenschutz und Datensicherung

Modul 2: IT-Sicherheit am Arbeitsplatz

Mitarbeiter können oft bereits durch die Beachtung einfacher Vorsichtsmaßregeln dazu beitragen, dass Schäden vermieden werden. Das Modul zur Umsetzung von IT-Sicherheit am Arbeitsplatz sollte unter anderem die folgenden Themenschwerpunkte umfassen:

- Sensibilisierung von Benutzern
- Motivation und Aufzeigen typischer Fehler von Anwendern:
  - leichtsinniger Umgang mit Passwörtern
  - Verzicht auf Verschlüsselung
  - mangelnder Schutz von Informationen
  - mangelndes Misstrauen
  - Laptop-Diebstahl
- Organisation und Sicherheit
  - Die IT-Sicherheitsvorgaben der Institution und deren Bedeutung für den Arbeitsalltag
  - Verantwortlichkeiten und Meldewege in der Institution (mit persönlicher Vorstellung der IT-Sicherheitsbeauftragten)

- Zugangs- und Zugriffsschutz
- Technische Sicherheit
- E-Mail- und Internet-Sicherheit
- Schad-Software
- Sicherheitsaspekte relevanter IT-Systeme und Anwendungen
- Rechtliche Aspekte
- Verhalten bei Sicherheitsvorfällen
  - Erkennung und Aufbereitung von Sicherheitsvorfällen
  - Meldewege und Ansprechpartner
  - Eskalationsstrategie

Die hier angegebenen Themen stellen lediglich eine Auswahl dar. Ein Schulungsmodul "IT-Sicherheit am Arbeitsplatz" sollte stets den individuellen Gegebenheiten der entsprechenden Organisation angepasst sein.

Modul 3: Gesetze und Regularien

Dieses Schulungsmodul soll allen, die im IT-Bereich an verantwortlicher Stelle tätig sind, den rechtlichen Rahmen ihres Handelns umreißen. Häufig werden Mitarbeiter nur in einem formalen Akt, meist bei der Einarbeitung, darauf verpflichtet, einschlägige Gesetze, Vorschriften und Regelungen einzuhalten. Es ist aber wichtig, nicht nur alle Mitarbeiter zu verpflichten, sondern ihnen die Vorschriften auch nahe zu bringen sowie Herkunft und Auswirkungen von Regelungen zu erläutern.

Es sollte ein grober Überblick über Gesetze und Verordnungen gegeben werden, die Auswirkungen auf den IT-Betrieb bzw. die IT-Sicherheit haben können. Dies kann je nach Branche und Land, in dem eine Organisation tätig ist, extrem unterschiedlich sein. Außerdem sollten Standards und Richtlinien zum IT-Einsatz und zur IT-Sicherheit, die in der eigenen Organisation einzuhalten sind, vorgestellt werden.

Dazu gehören beispielsweise

- Datenschutz im Unternehmen oder der Behörde
  - Rolle und Aufgabe des Datenschutzbeauftragten
  - Datenschutzgesetze
  - Organisationspflichten
  - rechtliche Situation im Zusammenhang mit Protokoll-Dateien
- Arbeits- und arbeitsschutzrechtliche Bestimmungen
  - Rolle des Arbeitsschutzbeauftragten
  - Regelungen zu Bildschirmarbeitsplätzen
- Gesetze und Normen zur Infrastruktur im Bereich IT
  - Brandschutz
  - Sichere Verkabelung usw.
- Juristische Haftungsrisiken und IT-Nutzung
  - Haftung für Online-Inhalte
  - Haftungsrisiken, wenn Mitarbeiter verbotene Online-Inhalte nutzen
  - Weiterleitung von digitalen Daten

  - rechtliche Situation beim Hosting
  - Haftung des Unternehmens nach außen
  - Allgemeine Geschäftsbedingungen (AGB)
  - Nutzung von Telekommunikationsdiensten (z. B. TKG)
  - Haftung bei der Privatnutzung von IT-Komponenten
  - rechtliche Probleme bei der Mitarbeiterüberwachung
- Verantwortlichkeiten
  - Haftungsverteilung innerhalb eines Unternehmens oder einer Behörde
  - Verantwortlichkeiten bei der Notfallplanung
- Virenschutz
  - Organisationsverschulden bei Virenproblemen
  - Regresspflichten bei durch Viren verursachten Schäden
- Wirtschaftsrechtliche Bestimmungen:
  - Ausfuhrbestimmungen für IT-Produkte
  - Lizenz- und Urheberrecht für Software
  - Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
- Authentikation
  - Haftungszuordnung
  - Beweisrecht im Bereich Authentikation
- Netz- und Server-Sicherheit
  - Zugriffsvoraussetzungen
  - Datenschutz im Netz
- Hacker-Strafrecht
  - Grenzen der Strafbarkeit im Bereich Hacking
  - Notwehr
  - indirekte Hacker-Angriffe
  - Verfolgung von Hacker-Straftaten
- Vertragsrecht im Netz
  - Informationspflichten
  - digitale Signaturen und ihre rechtliche Stellung

Modul 4: IT-Sicherheitskonzept der Organisation

Dieses Schulungsmodul dient der weiteren Vertiefung der im entsprechenden Basismodul "IT-Sicherheit am Arbeitsplatz" einführend behandelten Themen. Darüber hinaus soll es die System- und Aufgabenverantwortlichen in die Lage versetzen, an der permanenten Fortschreibung und - aufgrund neuer technischer, organisatorischer und rechtlicher Entwicklungen - notwendigen Anpassung des IT-Sicherheitskonzeptes mitzuwirken.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Übersicht über das IT-Sicherheitskonzept der Organisation
- spezifische Vorschriften, die sich aus dem IT-Sicherheitskonzept für die Bereiche Management, Organisation, Infrastruktur und IT-Betrieb ergeben
- Anpassung dieser Vorschriften an neue technische, organisatorische und rechtliche Gegebenheiten
- Revision und Fortschreibung des IT-Sicherheitskonzeptes

Modul 5: Risikomanagement

Dieses Schulungsmodul soll den Verantwortlichen die Bedrohungen der IT-Umgebung aufzeigen und es ihnen ermöglichen, die daraus für die Organisation resultierenden Risiken abzuschätzen. Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Definitionen und Beispiele zu den Begriffen: Risiko, Gefährdung, Bedrohung, Schwachstelle, Sicherheitslücke, Sicherheitsziel
- Typische Gefährdungen und Bedrohungen:
  - Höhere Gewalt: Feuer, Wasser, Explosion, Sturm, atmosphärische Entladung, Streik, Demonstration, etc.
  - Organisatorische Mängel: Fehlende oder unzureichende Regelungen, Ungeeignete Rechtevergabe, Unkontrollierter Einsatz von IT-Systemen, etc.
  - Menschliche Fehlhandlungen: mangelnde Sorgfalt, unsachgemäße Behandlung, Unwissenheit, etc.
  - Technisches Versagen: Stromausfall, Ausfall der Klimaanlage, Überspannung, Ausfall von Schaltelementen oder Schaltkreisen, Störungen in der Mechanik oder Elektronik, etc.
  - Vorsätzliche Handlungen: Viren, Würmer, Trojaner, Diebstahl, Sabotage, Spionage, Manipulation, inklusive Gegenüberstellung von Angreifertypen und Motivationen, z. B. bei Innentätern oder bei Angreifern von außen
- Risikoanalyse: Risikoanalysestrategien, Beurteilung einer Bedrohung nach Eintrittswahrscheinlichkeit und Schadenshöhe
- Festlegung von Schutzzielen: Grad der Akzeptanz verschiedener Risiken, Definition inakzeptabler Risiken
- Maßnahmenkatalog zur Beseitigung inakzeptabler Risiken

Modul 6: IT-Sicherheitsmanagement

Dieses Schulungsmodul zeigt wichtige Grundlagen für IT-Sicherheitsverantwortliche auf, um IT-Sicherheit in der Organisation umzusetzen. Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- IT-Sicherheitsmanagement
  - Aufbau und Aufgaben des IT-Sicherheitsmanagements
  - IT-Sicherheitsprozess, -ziele und -strategien
  - Organisation und Verantwortlichkeiten
  - Standards zum IT-Sicherheitsmanagement wie ISO/IEC 13335, ISO/IEC 17799, IT-Grundschutz, ITIL
- IT-Sicherheitskonzept
  - Ziele und Inhalte eines IT-Sicherheitskonzeptes
  - Aufbau eines IT-Sicherheitskonzeptes
  - Verpflichtung von IT-Benutzern, System- und Aufgabenverantwortlichen zur Umsetzung des IT-Sicherheitskonzeptes
- System- und anwendungsspezifische IT-Sicherheitsrichtlinien

- Berechtigungsmanagement
  - Berechtigungskonzepte, Gestaltung der Rechtevergabe
  - Zugriffsrechte auf Systemressourcen, Zuweisung und zeitliche Begrenzung
  - Authentisierung (z. B. Stärken und Auswahl von Mechanismen)
  - Remote Zugriff (z. B. bei Telearbeit)
- Training und Sensibilisierung zur IT-Sicherheit
  - Festlegung von IT-Sicherheitstrainingsprogrammen für die verschiedenen Funktionsträger
  - Entwickeln einer Sicherheitskultur
- Evaluierung und Zertifizierung im Bereich IT-Sicherheit
  - Produkt-/System-Zertifizierung (z. B. nach ITSEC, Common Criteria usw.)
  - Zertifizierung der IT-Umgebung und des IT-Sicherheitsmanagements (z. B. nach IT-Grundschutz)
  - Experten-Zertifikate (z. B. TISP, CISA, CISSP, IT-Sicherheitskoordinator, Security+ usw.)
- Spezielle Probleme in der IT-Sicherheit
  - Kostenproblem
  - Akzeptanzproblem

Modul 7: IT-Systeme

Dieses Schulungsmodul beschreibt die Steuerungsinstrumente, die in den verschiedenen Phasen des Lebenszyklus von IT-Systemen die Einhaltung der Sicherheitsnormen gewährleisten.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- IT-Sicherheitsmaßnahmen in den Lebenszyklus-Phasen
  - Planung
  - Beschaffung/Entwicklung
  - Test und Evaluierung
  - Implementierung bzw. Installation
  - produktiver Betrieb
  - Einstellung des Betriebes
- Sicherheitsplanung für den Systembetrieb
  - Feststellung des Einsatzzweckes und -nutzens eines bestimmten IT-Systems
  - Festlegung der Schutzmaßnahmen für dieses System
  - Bestimmung der für den Systembetrieb Verantwortlichen
  - Installation und Konfiguration der in jeder Phase des Lebenszyklus erforderlichen Sicherheitsmechanismen
- Festlegung eines Konfigurations- und Änderungsmanagements in Abhängigkeit von den Sicherheitszielen
- Festlegung der Voraussetzungen für die Freigabe für den Wirkbetrieb
- Tests und Freigabe der Sicherheitsmechanismen

Modul 8: Operativer Bereich

Dieses Schulungsmodul beschreibt die Prozeduren und Maßnahmen, die im täglichen Einsatz operationelle Systeme und Anwendungen schützen.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Infrastruktur-Maßnahmen
  - Zugangskontrollen, Werkschutz, Alarmanlagen, etc.
  - Haustechnik, Energie- und Wasserversorgung, etc.
  - Brandschutzeinrichtungen
  - Klimaanlagen
- Organisatorische Maßnahmen
  - Dokumentation von Systemen und Konfigurationen, Applikationen, Software, Hardware-Bestand, etc.
  - Regelmäßige Kontrolle von Protokolldateien
  - Regelungen für die Datensicherung
  - Regelungen für den Datenträgeraustausch
  - Lizenzverwaltung und Versionskontrolle von Standardsoftware
- Maßnahmen im Bereich Personal
  - Auswahl, Einarbeitung und Schulung von Mitarbeitern
  - Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern
  - Funktionen und Verantwortlichkeiten
  - Funktionstrennung und funktionsbezogene Rechtevergabe
  - Vertretungsregelungen
  - Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
- Maßnahmen im Bereich Hardware und Software
  - Grundlagen Betriebssystem-Sicherheit
  - Sichere Konfiguration von Hardware und Software
  - Virenschutz, Spam-Abwehr, Patchmanagement
  - Nutzung der in der Hardware bzw. den Anwendungsprogrammen vorhandenen Sicherheitsfunktionen
  - Implementierung zusätzlicher Sicherheitsfunktionen
  - Rechteverwaltung
  - Protokollierung
- Maßnahmen im Bereich Kommunikation
  - Sichere Konfiguration von TK-Anlagen
  - Sichere Konfiguration von Netzdiensten
  - Firewall-Konzepte, IDS-Systeme, Penetrationstests
  - E-Mail- und Internet-Sicherheit
  - Absicherung externer Remote-Zugriffe
  - Virtual Private Networks (VPN)
  - Sichere Nutzung mobiler IT-Systeme und drahtloser Kommunikation
  - Information über Sicherheitslücken (z. B. über CERTs) und Umgang mit Sicherheitsvorfällen

Modul 9: Technische Realisierung von Sicherheitsmaßnahmen

Dieses Schulungsmodul vermittelt Kenntnisse über die Möglichkeiten der technischen Realisierung der in den Modulen 6 bis 8 abstrakt beschriebenen Steuerungs- und Kontrollinstrumente.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Basiswissen Kryptographie
  - Problemabgrenzung Vertraulichkeit, Integrität, Authentizität
  - Grundbegriffe wie Klartext, Chiffrat, Schlüssel
  - Symmetrische und asymmetrische Verschlüsselung
  - Public Key Infrastrukturen
  - Digitale Signaturen
  - Aufzählung "guter" und "schlechter" bekannter Algorithmen
- Identifizierung und Authentikation, z. B.
  - Begriffsdefinition (Wissen, Besitz, Eigenschaft)
  - Authentisierung durch Wissen: Passwörter, Einmal-Passwörter, Challenge-Response-Verfahren, digitale Signaturen
  - Authentisierung durch Besitz: Token, Chipkarten, Magnetstreifenkarten
  - Biometrische Verfahren: Fingerabdruckerkennung, Iriserkennung, Gesichtserkennung, etc.
  - Single Sign-On
  - Berechtigungsmanagement
- Protokollierung und Monitoring, z. B.
  - Technische Möglichkeiten des "Transaction Logging"
  - Intrusion Detection Systeme (IDS): Unterschiede zwischen aktiven und passiven Systemen
  - Zwangsprotokollierung aller Administratoraktivitäten
  - Datenschutzaspekte
- Überblick über Administrationswerkzeuge
  - Werkzeuge, mit denen Sicherheitsvorgaben realisiert und kontrolliert werden können
  - Zusatzprodukte zur Ergänzung bzw. Verbesserung der Sicherheitsfunktionen von Betriebssystemen ("gehärtete Betriebssysteme")
  - Netzmanagement-Software
  - Remote-Management-Software
- Firewalls
  - Internet-Technik (OSI-Modell, TCP/IP)
  - Realisierungsformen (statische Paketfilter, Stateful Inspection, Application Level Gateways)
  - Content Security
  - Hochverfügbare Firewalls

- Schutz der Vertraulichkeit: Kryptographische Verfahren und Produkte, Zugriffsschutz z. B. durch Festplattenverschlüsselung, Kryptographie auf den verschiedenen Schichten des OSI-Modells
  - Protokolle für Schicht 1 und 2 (ISDN-Verschlüsselung, ECP und CHAP, WLAN, Bluetooth)
  - Protokolle für Schicht 3 (IPsec, IKE, SINA)
  - Protokolle für Schicht 4 (SSL, TLS, WTLS)
  - E-Mail-Kryptografie (GnuPG, PGP, S/MIME)
  - Kryptografie im Browser (HTTPS, Code-Signing, Form-Signing)
- Schutz der Verfügbarkeit
  - Organisatorische Maßnahmen zur Erhöhung der Verfügbarkeit (SLAs, Change Management, Vermeidung von SPOF)
  - Datensicherung, Datenwiederherstellung
  - Speichertechnologien
  - Netzkonfigurationen zur Erhöhung der Verfügbarkeit
  - Infrastrukturelle Maßnahmen zur Erhöhung der Verfügbarkeit
  - Verfügbarkeit auf der Client-Seite
  - Verfügbarkeit auf der Anwendungsebene
  - Verfügbarkeit auf der Server-Seite (Server-Standby, Failover)
  - Methoden zur Replikation von Daten
  - Disaster Recovery
- Technische Möglichkeiten zum Schutz von TK-Anlagen
  - Schutz vor Abhören
  - Schutz der Datenleitungen z. B. durch alarmüberwachte und plombierte Leitungsschächte, gesicherte Verteiler (Knoten), Verschlüsselung der Nachrichten, etc.
  - Verbindungsaufbau nur durch Rückruf
  - Verhinderung von Gebührenbetrug, Sicherung der Datenträger mit Gebührendaten
  - Sicherung von Wartungs-, Fernwartungs- und Administratorzugängen
  - Protokollierung jedes Systemzugangs, Löschungsschutz der Protokolldateien
- Erkennen von Schwachstellen des eigenen Systems mittels Penetrationstests
- Hacker-Methoden, Web-Seiten-Hacking, Schutz vor: Sniffer, Scanner, Password Cracker, etc.

Modul 10: Notfallvorsorge/Notfallplanung

Dieses Schulungsmodul soll die Grundlagen zur Erstellung eines Notfall- und Wiederanlaufplanes vermitteln. Thematisch stellt es einen Aufbaukurs zum Modul 5 "Risikomanagement" dar.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Überblick über Notfallvorsorge, Incident Handling, Business Continuity
- Aufbau einer Notfallorganisation

  - Definition des Notfalles
  - Festlegung von Verantwortlichkeiten
  - Bildung von Krisenstäben: Zentraler Krisenstab, Operative Stäbe, Unterstützungsteams
  - Erstellung von Alarm- und Eskalationsplänen
  - Festlegung der Mindestanforderungen für einen Notbetrieb
  - Planung für die Verlagerung kritischer Arbeitsbereiche in Ausweichstandorte
  - Ersatzbeschaffungsplan
  - Abschluss von Service-Verträgen mit Recovery-Dienstleistern
  - Wiederanlaufplanung
  - Erstellung eines Planes für regelmäßige Notfallübungen
- Dokumente zum Notfallplan
  - Notfallhandbuch
  - Flowcharts zu den Alarmierungs- und Meldeplänen
  - Checklisten für verschiedene Notfallszenarien
  - Dokumentationen von Hard- und Software, Systemkonfigurationen, Datenbeständen, Datensicherung, ...
  - Hersteller- und Lieferantenverzeichnis

Modul 11: Neue Entwicklungen im IT-Bereich

Der rasanten Weiterentwicklung im Bereich der IT muss auch durch das Schulungskonzept Rechnung getragen werden. Dieses Schulungsmodul soll daher IT-Systembetreiber über neue Innovationen auf ihrem Gebiet informieren. Um stets auf dem aktuellen Stand zu sein, sollte dieses Seminar periodisch - etwa alle 2 Jahre - wieder besucht werden.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Neue Entwicklungen in den Bereichen
  - Hardware/Software, Systemumgebung, System-Architekturen
  - Hardware-Typen
  - Betriebssysteme
  - Dienstprogramme
  - Anwendungssoftware
  - Systemplanung
  - Workflow
  - Damit verbundene neue Bedrohungen und Schwachstellen
- Rechnernetze
  - Netzkoppelelemente
  - Netzarchitektur
  - Monitoring
  - Zugriffskontrolle
  - Kryptographie
  - Netztrennung
  - Damit verbundene neue Bedrohungen und Schwachstellen
- Speicher und Archivierungsumgebungen
  - Speichertechnologien (DAS, NAS, SAN, IP Storage, etc.)
  - Archivierungstechnologien (Systeme, Medien, Software)
- Elektronische Kommunikation und Internet-Technologien

Modul 12: Betriebswirtschaftliche Seite der IT-Sicherheit

Dieses Schulungsmodul ist speziell für das Management und Entscheidungsträger gedacht, um IT-Sicherheit übergreifend in die Unternehmensplanung zu integrieren.

Folgende Inhalte gehören unter anderem zu diesem Themengebiet:

- Betriebswirtschaftliche Vorteile der IT-Sicherheit
  - Risikominimierung
  - Beschleunigung der Bearbeitung
  - Reduzierung des Aufwands
  - Umsatzerhöhung
  - Erschließen neuer Geschäftsfelder
  - sonstiger Nutzen
- Kalkulation einer IT-Sicherheitsinvestition
  - Erstellung einer Kostenübersicht
  - Abgrenzung gegenüber Betriebs- und Fortschreibungskosten
  - Verdeckte Kosten
- Investitionsrechnung in der IT-Sicherheit
  - Investitionsrechnung
  - Argumentation gegenüber dem Management
- Verzahnung von IT-Sicherheitsmaßnahmen im Unternehmen
  - Berücksichtigung der Geschäftsprozesse und der Geschäftsvorfälle bei den Sicherheitsmaßnahmen
  - Einfluss- und Verantwortungsbereiche, typische Stolpersteine
  - IT-Sicherheit bei der IT-Beschaffung und in IT-Projekten
- Erfolgsfaktoren der IT-Sicherheit
  - Wie gelingt ein Projekt zur IT-Sicherheit?
  - Klärung der Erwartungshaltung
  - Konzeption von IT-Sicherheitslösungen
  - Erstellen eines Lösungskonzepts
  - Verfassen eines Betriebskonzepts
  - Prüfen der Konzepte
  - Gliedern in Teilprojekte
  - Umsetzen der Teilprojekte
  - Modul- und Funktionstests
  - Akzeptanz- und Integrationstests
  - Inbetriebnahme
- Häufige Fehler bei der Umsetzung von IT-Sicherheit
  - Fehler bei der Projektleitung
  - andere typische Fehler

Modul 13: Infrastruktursicherheit

Dieses Modul befasst sich mit dem Schutz der Informationstechnik mit Hilfe von baulichen und technischen Maßnahmen. Wichtige Punkte dabei sind unter Anderem:

- Objektschutz
  - Umgebung
  - Umfriedung
  - Freiland-Schutz
  - Mechanischer Schutz
  - Technische Überwachung
  - Geräteschutz
- Zutrittskontrolle
  - Pförtnerdienst
  - Verschluss von Räumen
  - Technische Zutrittskontrolle
- Stromversorgung
  - Überspannungsschutz
  - Unterbrechungsfreie Stromversorgung
  - Trassen / Verkabelung
- Brandschutz
- Klimatisierung
- Schutz gegen Wasser

Ergänzende Kontrollfragen:

- Werden die Schulungsinhalte zur IT-Sicherheit den Bedürfnissen der Zielgruppe entsprechend angepasst?

M 3.46 Ansprechpartner zu Sicherheitsfragen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

In jeder Organisation sollten Ansprechpartner zu Sicherheitsfragen vorhanden sein, sowohl für scheinbar einfache wie auch für technische Fragen. Dies können die IT-Administratoren, die IT-Anwendungsverantwortlichen oder IT-Sicherheitsbeauftragten sein (siehe z. B. M 2.12 *Betreuung und Beratung von IT-Benutzern*, M 6.60 *Verhaltensregeln und Meldewege bei Sicherheitsvorfällen*).

Leider ist die Hemmschwelle, konkrete Sicherheitsprobleme weiterzumelden, immer noch sehr hoch. Wenn der IT-Sicherheitsbeauftragte den Mitarbeitern auch als Ansprechpartner zu allgemeinen IT-Sicherheitsfragen bekannt ist, senkt dies die Hemmschwelle, ihm konkrete Sicherheitsprobleme zu melden. Da viele Sicherheitsfragen bei der privaten Nutzung von IT-Systemen auftreten, sollten IT-Sicherheitsbeauftragte auch zu vermeintlich nicht dienstlichen Belangen Informationen weitergeben, z. B. zur Problematik von Viren und Trojanern beim Internet-Surfen oder zum Schutz von Daten beim E-Commerce. Dies fördert die Offenheit für Sicherheitsmaßnahmen, steigert die Akzeptanz der IT-Sicherheitsbeauftragten und zudem können viele vermeintlich private Probleme auch im Büro-Umfeld auftreten.

Allen Mitarbeitern sollten die Ansprechpartner zu Sicherheitsfragen ebenso wie die Meldewege für Sicherheitsvorfälle bekannt sein. Hierzu könnte z. B. im internen Telefonverzeichnis oder im Intranet eine Liste mit Namen, Telefonnummern und E-Mail-Adressen der jeweiligen Ansprechpartner enthalten sein.

Ergänzende Kontrollfragen:

- Gibt es Ansprechpartner zu Sicherheitsfragen innerhalb der Behörde oder des Unternehmens?
- Sind die Ansprechpartner zu Sicherheitsfragen allen Mitarbeitern bekannt?

M 3.47 Durchführung von Planspielen zur IT-Sicherheit

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Sicherheitsschulungen werden häufig als trocken empfunden. Dadurch wird häufig nicht der gewünschte Lerneffekt erreicht. Ein Rollenspiel bleibt bei den Teilnehmern länger und prägnanter in Erinnerung als auf Folien präsentiertes Material. Plan- oder Rollenspiele können helfen, die Bedrohungen deutlicher zu machen und typische Schwachstellen, aber auch Lösungsmöglichkeiten in der eigenen Arbeitsumgebung aufzuzeigen.

Planspiele können aus praktischen Beispielen, z. B. anhand aktueller Vorfälle aus den Medien, zusammengestellt werden oder bei Schulungsdienstleistern in Auftrag gegeben werden. Dabei sollten die Inhalte der Planspiele möglichst auf die eigene Institution angepasst werden. Dadurch können sich die Mitarbeiter besser mit den aufgezeigten Lösungen identifizieren. Durch die Simulation z. B. von Sicherheitsvorfällen, die geschäftskritische Prozesse beeinträchtigen können, sind die Mitarbeiter außerdem bei einem Ernstfall bestens vorbereitet.

Genau wie bei Schulungen ist die zielgruppengerechte Planung von Inhalten auch hier sehr wichtig. Die Teilnehmer sollen die Relevanz der Rollenspiele erkennen können und in ihrem Arbeitsumfeld unmittelbar davon profitieren können.

Bei allen Bemühungen, die Benutzer auf die Bedeutung von IT-Sicherheit aufmerksam zu machen, sollte eine positive und konstruktive Grundstimmung bewahrt werden. Angst vor Sicherheitsvorfällen kann einerseits zur Verdrängung von Sicherheitsproblemen und andererseits zu Panikreaktionen verleiten.

Beispiel:

- Die Mitarbeiter einer Fluggesellschaft haben den Ausfall ihres Check-In Programms simuliert und Alternativlösungen getestet. Einige Monate später ereignete sich ein Vorfall, der die Verfügbarkeit der Flugzeuge stark einschränkte und damit auch die Abfertigung beeinträchtigte. Obwohl es sich nicht um den gleichen Notfall handelte, waren die Mitarbeiter auf die Notfallbehandlung gut vorbereitet und konnten viel effizienter reagieren als die Mitarbeiter der Konkurrenz, die keine vergleichbaren Notfälle geübt hatten.

M 3.48 Auswahl von Trainern oder Schulungsanbietern

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement, Leiter Personal

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Personalabteilung

Für die Durchführung von Sensibilisierungsprogrammen und Schulungen zur IT-Sicherheit muss zunächst geklärt werden, ob die Sensibilisierung und Ausbildung zu Sicherheitsfragen durch eigene Mitarbeiter oder Externe durchgeführt werden und in welcher Form die Ausbildung erfolgen soll.

Eigene Mitarbeiter?

Wenn eigene Mitarbeiter Schulungen durchführen sollen, müssen diese das benötigte Fachwissen sowie die Fähigkeit, dieses Wissen zu vermitteln, besitzen. Zur Vermittlung von IT-Sicherheitswissen reichen technische Kenntnisse alleine nicht aus, darüber hinaus müssen die Trainer über didaktische, pädagogische und kommunikative Fähigkeiten verfügen. Wichtig ist unter anderem, dass Trainer auch die Sprache ihres jeweiligen Zielpublikums beherrschen, also die zu schulenden IT-Sicherheitsaspekte in die jeweiligen Arbeits- und Projektzusammenhänge stellen können. Außerdem müssen interne Trainer auch die erforderliche Zeit bekommen, um sich auf die Schulungen vorbereiten und diese durchführen zu können.

Externe Fachkräfte?

In vielen Fällen kann es kosteneffizienter sein, die Schulung durch externe Fachkräfte durchführen zu lassen. Dann ist zu klären, welche finanziellen Ressourcen dafür zu Verfügung stehen. Die externen Trainer sollten sorgfältig ausgewählt werden.

Auch bei externer Durchführung von Schulungen müssen interne Ressourcen dafür eingeplant werden:

- Es muss ein Verantwortlicher benannt werden, der qualifizierte Externe auswählt, die Lehrinhalte und Lehrmethoden vorgibt und die Schnittstelle zwischen den Externen und den eigenen Mitarbeitern bildet.
- Die Mitarbeiter sind für die Dauer der Veranstaltungen abwesend.
- Außerdem sollten die Mitarbeiter die durchgeführten Schulungen bewerten und diese Erfahrungen regelmäßig intern ausgewertet werden.

Erfahrungsgemäß gibt es für viele Bereiche Schulungsanbieter, die geeignete Kurse in der gewünschten Form anbieten. Hier sollte nachgefragt werden, ob die Kursinhalte die gewünschten Kenntnisse vermitteln können.

Es sollte regelmäßig hinterfragt werden, ob Ausbilder, Trainer und Betreuer auf dem aktuellen Wissensstand aufsetzen.

Ergänzende Kontrollfragen:

- Sind eigene Mitarbeiter geeignet, Schulungen zur IT-Sicherheit durchzuführen? Haben diese alle notwendigen Ressourcen?
- Sind die Angebote verschiedener Schulungsanbieter verglichen worden, welche inhaltlich, qualitativ und preislich am besten geeignet sind?
- Kann auf den Ausfall eines Trainers oder eines Termins flexibel reagiert werden?

M 3.49 Schulung zur Vorgehensweise nach IT-Grundschutz

Verantwortlich für Initiierung: IT-Sicherheitsmanagement-Team

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement-Team, Vorgesetzte

IT-Sicherheitsverantwortliche und Mitglieder des IT-Sicherheitsmanagements müssen die IT-Grundschutzmethodik gut kennen, um sie anwenden zu können. Um sich in die Vorgehensweise nach IT-Grundschutz einzuarbeiten, gibt es verschiedene Möglichkeiten:

- Selbststudium
- Web-Kurs des BSI zum Einstieg in die IT-Grundschutz-Vorgehensweise
- Externe Schulungsanbieter von IT-Grundschutz-Schulungen (Auf den BSI-Webseiten findet sich eine Liste von Schulungsanbietern zum Thema IT-Grundschutz. Das BSI hat dabei Schulungsqualität und Schulungsinhalte nicht bewertet.)
- Erarbeitung eigener IT-Grundschutz-Schulungen.

Bei der Planung einer neuen IT-Grundschutz-Schulung oder Beurteilung einer extern angebotenen Schulung sollten die folgenden Themen betrachtet werden:

1. Sensibilisierung für IT-Sicherheit
2. Was ist ein ISMS (Informationssicherheitsmanagementsystem)?
   Wie wird ein funktionierender IT-Sicherheitsprozess etabliert?
3. Überblick über das IT-Grundschutzkonzept (Philosophie, Anwendungsgebiet, Struktur)
4. Erstellung einer IT-Sicherheitsleitlinie
   - Definition von IT-Sicherheitszielen
   - Definition des IT-Verbundes
5. IT-Sicherheitsmanagement
   - Organisationsstrukturen (Darstellung geeigneter Organisationsstrukturen für das IT-Sicherheitsmanagement)
   - Rollen (IT-Sicherheitsbeauftragte, IT-Sicherheitsmanagement-Team, etc.)
   - Verantwortlichkeiten
6. IT-Sicherheitskonzept: Typischer Aufbau und Inhalte
7. Strukturanalyse
   - Erstellung eines Netzplans
   - Gruppenbildung
   - Erhebung der IT-Systeme
   - Erfassung der IT-Anwendungen

8. Schutzbedarfsfeststellung
   - Vorgehensweise
   - Definition der Schutzbedarfskategorien inklusive individueller Anpassung der Bewertungstabellen
   - Schadensszenarien
   - Schutzbedarfsfeststellung für IT-Anwendungen, IT-Systeme Kommunikationsverbindungen und IT-Räume
9. Modellierung nach IT-Grundschutz
   - Überblick über die IT-Grundschutz-Bausteine
   - Schichtenmodell
     - Übergeordnete Aspekte der IT-Sicherheit
     - Sicherheit der Infrastruktur
     - Sicherheit der IT-Systeme
     - Sicherheit im Netz
     - Sicherheit der Anwendungen
   - Prüfung auf Vollständigkeit
   - Lebenszyklusmodell der Maßnahmen
10. Basissicherheits-Check
    - Darstellung der Vorgehensweise
    - Umsetzungsstatus
11. Ergänzende Sicherheitsanalyse: Risikoanalyse basierend auf IT-Grundschutz
12. Realisierung der IT-Sicherheitsmaßnahmen
    - Sichtung aller fehlenden Maßnahmen
    - Konsolidierung der Maßnahmen
    - Kosten und Aufwandsabschätzungen (Budgetierung)
    - Realisierung der Maßnahmen (Umsetzungsreihenfolge, Verantwortliche, Realisierungsplan)
13. Hilfsmittel zur Arbeit mit den IT-Grundschutz-Katalogen

    Das BSI stellt verschiedene Hilfsmittel zur Verfügung, die die praktische Arbeit mit den IT-Grundschutz-Katalogen erleichtern. Die Folgenden sollten den Anwendern vorgestellt werden:
    - Leitfaden als Motivation für IT-Sicherheit
    - Web-Kurs als Einstieg in die IT-Grundschutz-Vorgehensweise
    - Tabellen und Formblätter als Hilfsmittel bei der Umsetzung
    - Musterrichtlinien und Profile als Beispielanwendungen

- IT-Grundschutz-Tool als Unterstützung bei der Erstellung, Verwaltung und Fortschreibung von IT-Sicherheitskonzepten dem IT-Grundschutz entsprechend. Das BSI bietet hierfür das IT-Grundschutz-Tool GSTOOL an.

14. Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz: Überblick Zertifizierungsschema

In einer umfassenden IT-Grundschutz-Schulung sollten die Teilnehmer auch Gelegenheit haben, die dargestellte Vorgehensweise anhand von Beispielen zu üben.

Zur Gestaltung neuer IT-Grundschutz-Schulungen wird unter den Hilfsmitteln auf den BSI-Webseiten zu IT-Grundschutz ein Foliensatz zur Verfügung gestellt. Dieser kann benutzt werden, um eigene Schulungen hierauf aufzubauen. Alle Lehrinhalte werden in Übersichten und Strukturgrammen kurz angeschnitten. Es wird aufgezeigt, welche Inhalte eine Schulung beinhalten sollte, die in die Vorgehensweise IT-Grundschutz und die Anwendung der IT-Grundschutz-Kataloge einführen soll.

M 3.50 Auswahl von Personal

Verantwortlich für Initiierung: Leiter Personal, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Personalabteilung, Vorgesetzte

Bereits bei der Formulierung der Anforderungen sollten die erforderlichen Qualifikationen und Fähigkeiten genau beschrieben sein. Ob diese bei Bewerbern tatsächlich vorhanden sind, sollte zunächst anhand der Unterlagen nachgeprüft, anschließend im Gespräch geklärt werden.

Personen, die sicherheitsrelevante Aufgaben ausüben sollen (beispielsweise Sicherheitsverantwortliche, Datenschutzbeauftragte, Administratoren, Mitarbeiter mit Zugang zu finanzwirksamen oder vertraulichen Informationen), müssen vertrauenswürdig und zuverlässig sein (siehe hierzu auch M 3.33 *Sicherheitsüberprüfung von Mitarbeitern*).

Besonders ist darauf zu achten, dass keine Interessenkonflikte oder Abhängigkeiten entstehen, die die Aufgabenerfüllung gefährden. Interessenkonflikte können insbesondere dann auftreten, wenn ein Mitarbeiter gleichzeitig verschiedene Rollen inne hat, die ihm zu weitreichende Rechte geben oder sich ausschliessen. Außerdem sollten die Aufgaben von Mitarbeitern auch nicht von Interessenkonflikten außerhalb der Behörde oder des Unternehmens beeinträchtigt werden, beispielsweise durch frühere Stellen oder durch anderweitige Verpflichtungen. Um nach einem Stellenwechsel Interessenkonflikte zu vermeiden, können Konkurrenzverbote und Karrenzzeiten vereinbart werden.

Soweit die fachlichen Qualifikationen in Teilbereichen noch nicht ausreichend vorhanden sind, müssen Mitarbeiter die Gelegenheit bekommen, diese zu erweitern. Um die erforderlichen Qualifikationen und Fähigkeiten zu erhalten und zu aktualisieren, sollten alle Mitarbeiter regelmäßig geschult werden und auf die Bedeutung von Informationssicherheit hingewiesen werden (siehe auch Baustein B 1.13 *IT-Sicherheitssensibilisierung und -schulung*).

Auch bei der Auswahl von Mitarbeitern für befristete Stellen oder Dienstleistern sollten diese Punkte berücksichtigt werden.

Ergänzende Kontrollfragen:

- Wie wurde die Zuverlässigkeit neuer Mitarbeiter festgestellt?
- Sind die Angaben in den vorgelegten Unterlagen korrekt und nachprüfbar?
- Sind weitere Schulungen zur Arbeitsplatzqualifikation erforderlich?

M 3.51 Geeignetes Konzept für Personaleinsatz und -qualifizierung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter Personal

Verantwortlich für Umsetzung: Personalabteilung, Vorgesetzte

Für jeden Mitarbeiter sollten die wahrzunehmenden Aufgaben beschrieben sein. "Jeder sollte wissen, was er zu tun hat" . Die Aufgaben sollten so zugeschnitten sein, dass keine Überschneidungen entstehen, damit es keine Probleme mit Zuständigkeiten gibt. Mitarbeiter sollten alle Ansprechpartner kennen, die mit ihrem Aufgabengebiet Schnittstellen haben. Dazu gehören insbesondere alle, die ähnliche Aufgaben erledigen oder dabei unterstützen. Beispielsweise sollten Mitarbeiter wissen, wer für den IT-Support zuständig ist, damit einerseits Probleme unmittelbar nach dem Auftreten abgestellt werden können und andererseits kein Mitarbeiter auf falsche Support-Mitarbeiter hereinfällt (siehe G 5.42 *Social Engineering*).

Vertreterregelungen sind frühzeitig festzulegen. Teambildung

Die Rollen, die ein Mitarbeiter wahrnehmen soll, müssen klar definiert sein. Darauf aufbauend sind alle erforderlichen Berechtigungen zu vergeben (siehe M 3.1 *Geregelte Einarbeitung/Einweisung neuer Mitarbeiter* und M 3.2 *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*).

Alle Mitarbeiter sollten sowohl für ihre Aufgaben als auch für die Nutzung der dafür eingesetzten IT-Systeme geschult sein. Außerdem müssen die Mitarbeiter natürlich in alle zu beachtenenden Sicherheitsvorgaben eingewiesen werden. Dafür empfiehlt es sich, ein Schulungskonzept zu erstellen (siehe Baustein B 1.13 *IT-Sicherheitssensibilisierung und -schulung*).

Ergänzende Kontrollfragen:

- Sind die Aufgabengebiete der Mitarbeiter schriftlich fixiert?
- Ist die Vertreterregelung erfasst?
- Sind den Mitarbeitern die Zuständigkeitsbereiche der Kollegen innerhalb der Institution bekannt?
- Besteht ein Schulungskonzept für die Mitarbeiter?

M 3.52 Schulung zu SAP Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement,

Verantwortlich für Umsetzung: Vorgesetzte, Administrator, Benutzer,

Ein SAP System ist sowohl in der Administration und im Betrieb als auch in der Benutzung komplex. Alle Personen, die mit einem SAP System arbeiten, müssen daher zwingend geschult werden. Dies gilt in besonderem Maße für Administratoren.

Schulungen

Schulungen zu allen SAP Themen und Produkten werden von SAP selbst und von Dritten angeboten. Das Spektrum reicht dabei von Schulungen, die für Personen geeignet sind, die SAP Systeme in ihrer normalen Büroarbeit nutzen - also ausführliche, applikationsspezifische Inhalte abdecken - bis hin zu Schulungen, die für die Ausbildung von Administratoren geeignet sind und ausführliche technische Inhalte abdecken. Für große Unternehmen oder Behörden mit vielen Mitarbeiten ist es sinnvoll, eigene Schulungsvarianten zu entwickeln und intern anzubieten.

Die Schulungsinhalte sind dem Nutzungsspektrum der zu schulenden Personen anzupassen. Ein Teil der Schulung sollte immer auch sicherheitsrelevante Themen ansprechen, so dass eine Sensibilisierung für den sicheren Umgang mit SAP Systemen erfolgt.

Es empfiehlt sich, in regelmäßigen Abständen das Bewusstsein für die Sicherheit aufzufrischen (Security-Awareness-Programm) und auf veränderte oder neue Situationen, Mechanismen oder Verfahren hinzuweisen. Generell ist es wichtig, dass das Sicherheitsbewusstsein im Lauf der Zeit von einer rein informellen Einstellung zu einer proaktiven verändert wird.

Online-Informationen

SAP Informationsquellen

SAP stellt online umfangreiche Informationen zu den angebotenen Produkten und Lösungen zur Verfügung. Alle Informationen sind über das Internet verfügbar (siehe M 2.346 *Nutzung der SAP Dokumentation)*.

Administratoren sollten diese Informationsquellen regelmäßig nutzen, um sich insbesondere über die Java-basierten Technologien zu informieren. Dabei sollten speziell die sicherheitsrelevanten Themen Beachtung finden.

Ergänzende Kontrollfragen:

- Sind Benutzer im Umgang mit dem SAP System geschult worden?
- Sind Administratoren geschult worden?
- Nutzen Administratoren regelmäßig die Online-Informationen, um sich über neue Technologien - auch bezüglich der Sicherheit - zu informieren?

M 3.53 Einführung in SAP Systeme

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator, Benutzer

Kernkomponenten einer SAP Systeminstallation

Eine SAP Systeminstallation besteht vereinfacht dargestellt aus folgenden Kernkomponenten:

- SAP NetWeaver ApplicationServer
  Der SAP NetWeaver ApplicationServer führt die SAP Applikationen oder Module aus.
- Datenbank-Instanz
  Die Datenbank-Instanz hält die Datenbank, in der alle Daten des SAP Systems gespeichert werden.
- SAP Clients
  Die SAP Clients bestehen aus dem SAPGui oder einem normalen Browser.

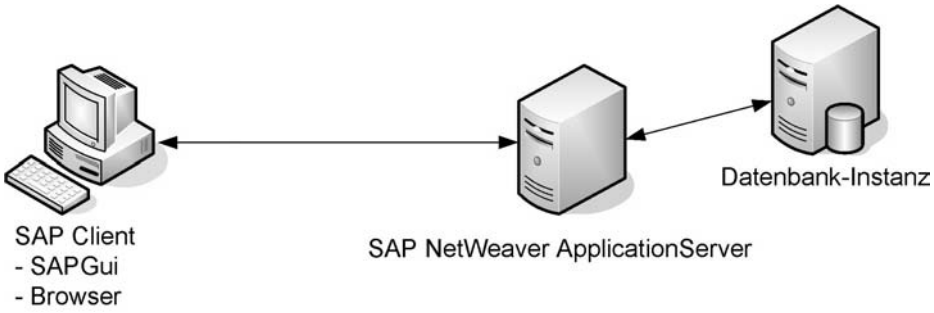


Abbildung: SAP Systemüberblick

Der SAP NetWeaver ApplicationServer besteht generell aus zwei Komponenten: dem ABAP-Stack und dem Java-Stack. Hier werden je nach verwendeter Programmiersprache die eigentlichen Funktionen der Applikationen und Module ausgeführt.

ABAP-Stack

Der ABAP-Stack ist die traditionelle Ausführungsumgebung eines SAP Systems. Dies trifft insbesondere auf die Systemversionen zu, die allgemein mit dem Begriff SAP R/3 bezeichnet werden, da die R/3 Komponenten und Module im ABAP-Stack ausgeführt werden.

Der ABAP-Stack besteht aus der so genannten SAP Basis, einer Sammlung aus (ABAP-) Programmen und Funktionen, die die Grundfunktionalitäten (z. B. Benutzerverwaltung) implementieren. Zusätzlich können dann weitere ABAP-Programme installiert werden. Diese sind in anwendungsspezifischen Modulen (z. B. HCM, FI) zusammengefasst. Die Programme des ABAP-Stack werden über so genannte Transaktionen gestartet. Dabei ist nicht jedem ABAP-Programm eine Transaktion zugeordnet. Vielmehr existieren Transaktionen, die Programme aufrufen, die den Start von anderen Programmen erlauben (z. B. Transaktion SE38, Start von Programmen).

Java-Stack

Der Java-Stack besteht aus einzelnen so genannten System-Diensten, die die System-Funktionen des Java-Stacks implementieren. Zusätzlich können weitere Dienste und Applikationen installiert werden, um den Funktionsumfang zu erweitern. Applikationen können dabei auf die Funktionen der unterschiedlichen Dienste zugreifen. Auf die Dienste, Funktionen und Applikationen des Java-Stack wird in der Regel über Internet-basierte Protokolle (z. B. HTTP) zugegriffen.

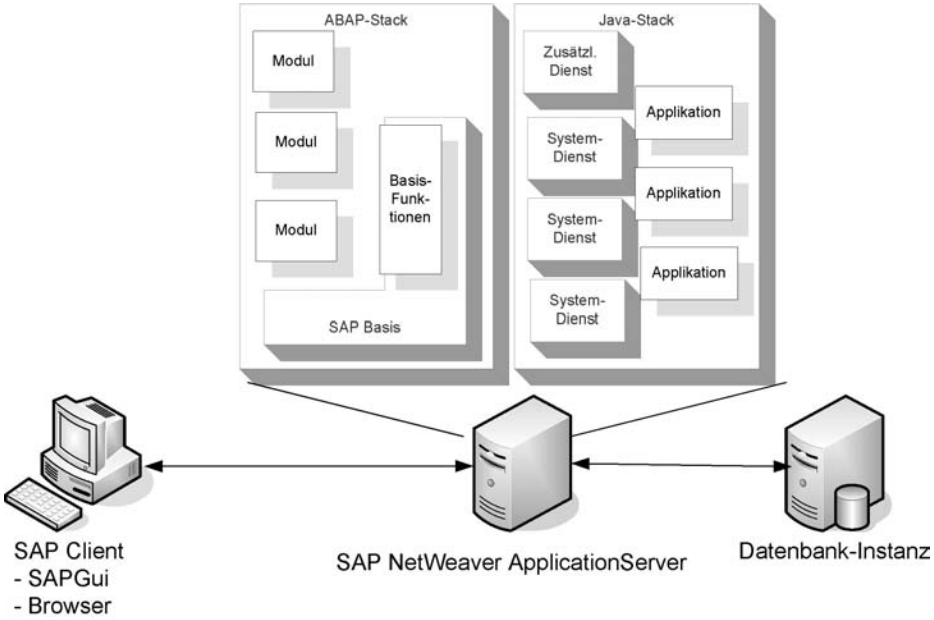


Abbildung: ABAP und Java Stack eines SAP Systems

Instanzen

Damit SAP Systeme auch mit großen Benutzerzahlen umgehen können, besteht die Möglichkeit, ein SAP System aus mehreren einzelnen so genannten Instanzen von NetWeaver ApplicationServern (insgesamt dann Cluster genannt) aufzubauen. Diese tragen die Benutzerlast dann gemeinsam und bilden aus Client-Sicht ein einziges SAP System. Die Arbeitsverteilung zwischen den einzelnen Servern erfolgt durch systeminterne Mechanismen. Eine der Instanzen ist die Hauptinstanz und wird auch Zentral-Instanz genannt. Die Zentral-Instanz kann durch weitere Installationen von SAP NetWeaver ApplicationServern um weitere Instanzen erweitert werden. Die einzelnen Instanzen kommunizieren miteinander, damit der Cluster von den Clients als ein SAP System wahrgenommen wird.

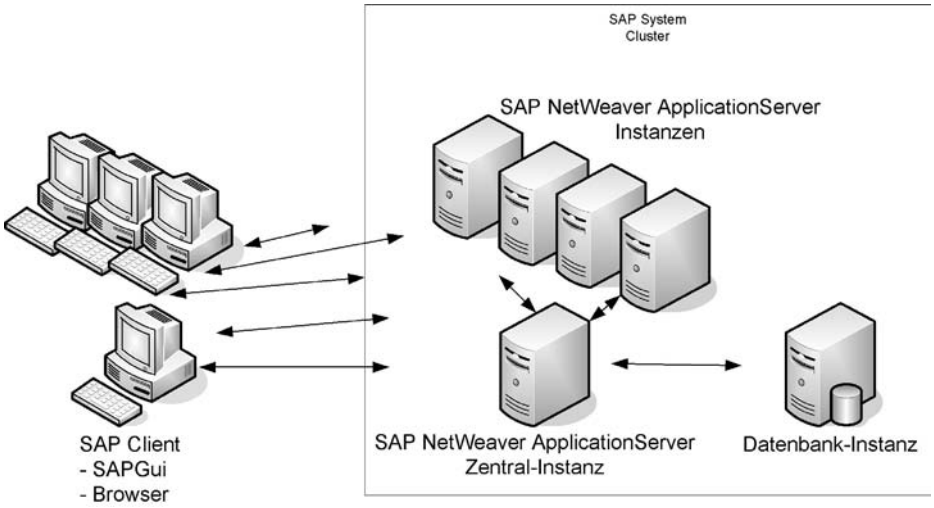


Abbildung: SAP Instanzen

Mandanten und DDIC

Der ABAP-Stack ist verwaltungstechnisch in so genannte Mandanten gegliedert. Zusätzlich existiert das so genannte Data Dictionary (DDIC), in dem alle Objekte des ABAP-Stacks gehalten werden. Die wichtigsten sind die Tabellen, die ABAP-Programme sowie sonstige in ABAP-Programmen verwendete Objekte. Mandanten stellen eine in sich geschlossene Menge von Benutzern, Funktionen und Tabellen dar. Zugriffe zwischen Mandanten sind in der Regel nicht möglich. Eine Ausnahme bilden hier die so genannten mandanten-unabhängigen Objekte (z. B. Tabellen), die von jedem Mandanten aus zugegriffen werden können. Änderungen an solchen Objekten wirken sich dann auf alle anderen Mandanten aus.

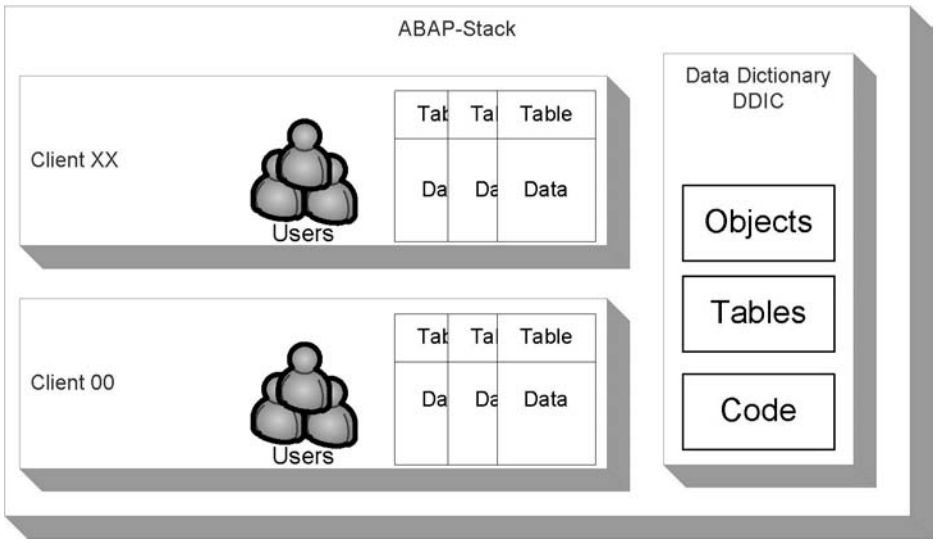


Abbildung: Mandanten eines SAP Systems

Benutzer

In Bezug auf Benutzer unterscheidet der ABAP-Stack zwischen unterschiedlichen Benutzerarten: solche mit eigenem Benutzerstammsatz und

solche ohne eigenen Benutzerstammsatz. Da Benutzer mit eigenem Benutzerstammsatz über die Transaktion SU01 verwaltet werden, werden diese Benutzer oft auch SU01-Benutzer genannt. Im Gegensatz dazu ist so genannten Internet-Benutzern kein eigener Benutzerstammsatz zugeordnet. Internet-Benutzer wurden bisher über die Transaktion SU05 verwaltet. Dieses Vorgehen ist von SAP mittlerweile nicht mehr empfohlen. Vielmehr ist empfohlen, auch Internetbenutzer über die Transaktion SU01 anzulegen und einen Verweis auf einen so genannten Referenzbenutzer einzutragen, der auch von unterschiedlichen Internet-Benutzern referenziert werden kann. Für SU01-Benutzer können in Abhängigkeit von der Verwendung folgende Typen spezifiziert werden, die mit unterschiedlichen Einschränkungen verbunden sind:

- Dialog-Benutzer: Der Benutzer darf sich interaktiv am SAP System anmelden (Dialoganmeldung).
- System-Benutzer: Eine Dialoganmeldung am SAP System ist nicht möglich. Der Benutzer kann für die Hintergrundverarbeitung (Batch-Jobs) verwendet werden.
- Kommunikations-Benutzer: Der Benutzer kann die technischen Kommunikationsarten (z. B. Remote Function Call, RFC) nutzen. Eine Dialoganmeldung am SAP System ist nicht möglich.
- Service-Benutzer: Der Benutzer wird als technischer Benutzer eingesetzt. Eine Dialoganmeldung ist möglich.
- Referenz-Benutzer: Der Benutzer dient als Referenz für Internet-Benutzer. Eine Anmeldung am System ist nicht möglich.

SAP Informationsquellen

SAP Systeme sind komplex und bestehen aus vielen Komponenten. Um Betreiber von SAP Systemen mit Hinweisen und Empfehlungen zu den SAP Produkten zu unterstützen, nutzt SAP die so genannten SAP Hinweise (SAP Notes). Diese werden über eindeutige Nummern identifiziert und können über den SAP Service Marketplace (siehe M 2.346 *Nutzung der SAP Dokumentation*) abgerufen werden.

M 3.54 Schulung der Administratoren des Speichersystems

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Leiter IT

Ein Speichersystem ist die Instanz, die viele oder gar alle immateriellen Werte der Organisation trägt. Zudem wird die Administration von Speichersystemen mit steigender Funktionalität immer komplexer und erfordert stets aktuelle Kenntnisse. Deswegen ist es unerlässlich, dass die Administratoren des Speichersystems ausreichend geschult sind, damit sie in der Lage sind, Probleme aus eigenem Handeln heraus zu vermeiden, technische Probleme rechtzeitig zu erkennen und die Funktionen und Sicherheitsmerkmale optimal zu nutzen.

In den Schulungen sollten ausreichende Kenntnisse zu den für die Einrichtung und den Betrieb der Komponenten des Speichersystems notwendigen Vorgehensweisen, Werkzeugen und Techniken vermittelt werden. Über Kenntnisse der grundlegenden IT-Technik hinaus gilt dies auch für herstellerspezifische Aspekte zu einzelnen Produkten, die als Komponenten des Speichersystems eingesetzt werden. Das bedeutet, dass beim Einsatz von neuen Produkten die Administratoren speziell zu diesen Produkten nachgeschult werden müssen.

Für Schulungsmaßnahmen sollte bereits bei der Beschaffung von IT-Komponenten ein ausreichendes Budget eingeplant werden und ein Schulungsplan für Administratoren erstellt werden. Die Inhalte einer Schulung sollten die folgenden Punkte umfassen:

- Grundlagen zu Speichersystemen und Speichernetzen
  - Überblick über Netze und Protokolle
  - Aufbau von Massenspeichersystemen
  - Funktionsweise eines Storage Area Network (im Fall eines SAN-Einsatzes)
  - SAN-Switching (im Fall eines SAN-Einsatzes)
  - Datensicherung von Massenspeichern
- Einrichtung von Speichersystemen und Speichernetzen
  - Zusammenbau und Verkabelung
  - Einrichtung und Konfiguration von Speichereinheiten, SAN-Switches und Backup-Geräten
- Betrieb von Speichersystemen und Speichernetzen
  - Management der Geräte, Software-Werkzeuge
  - Integration in Netzmanagementsysteme (NMS)
  - Protokollierung
  - Einstellung, Verwaltung und Sicherung der Konfiguration.

- Fehlerbehebung bei Speichersystemen und Speichernetzen
  - Fehlerquellen und Ursachen
  - Mess- und Analysewerkzeuge
  - Teststrategien zur Fehlersuche
- IT-Sicherheit bei Speichersystemen und Speichernetzen
  - Grundlagen der IT-Sicherheit sowie relevante IT-Sicherheitsaspekte
  - Virenschutz
  - Authentisierung, Autorisierung
  - Kryptoverfahren und Anwendungen
  - Gefahrenquelle "Default-Einstellungen"
  - Vorsorgemaßnahmen, Reaktion und Analyse
  - Incident Handling
  - Disaster Recovery Maßnahmen

Auch wenn in einer Gruppe von Administratoren die Aufgaben so verteilt sind, dass jeder Administrator nur einen bestimmten Verantwortungsbereich hat, ist es unverzichtbar, dass alle Administratoren ein allgemeines Grundwissen besitzen. Die individuellen Schwerpunkte können davon ausgehend gezielt ausgebaut und gepflegt werden. Zu vielen Produkten gibt es von den Herstellern oder spezialisierten Anbietern hierfür ein umfangreiches Angebot an aufeinander aufbauenden und individuell vertiefenden Seminaren. Das Angebot an qualifizierten Schulungen stellt ebenfalls ein Kriterium dar, das bei der Entscheidung für einen bestimmten Hersteller berücksichtigt werden sollte.

Ergänzende Kontrollfragen:

- Steht ein ausreichendes Budget für Schulungsmaßnahmen für die Speichersysteme zur Verfügung?
- Wurde ein Schulungsplan für Administratoren in Anlehnung an die erwähnten Punkte erstellt?

M 3.55 Vertraulichkeitsvereinbarungen

Verantwortlich für Initiierung: Leiter Personal, Datenschutzbeauftragter, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Personalabteilung, Vorgesetzte

Externe Mitarbeiter erhalten häufig für die Erfüllung ihrer Aufgaben Zugang zu vertraulichen Informationen oder erzielen Ergebnisse, die vertraulich behandelt werden müssen. In diesen Fällen müssen sie verpflichtet werden, diese entsprechend zu behandeln. Hierüber sollten Vertraulichkeitsvereinbarungen (Non-Disclosure-Agreements) abgeschlossen werden, die vom externen Mitarbeiter unterzeichnet wird.

In einer Vertraulichkeitsvereinbarung sollte beschrieben sein,

- welche Informationen vertraulich behandelt werden müssen,
- für welchen Zeitraum diese Vertraulichkeitsvereinbarung gilt,
- welche Aktionen bei Beendigung dieser Vereinbarung vorgenommen werden müssen, z. B. Vernichtung oder Rückgabe von Datenträgern,
- wie die Eigentumsrechte an Informationen geregelt sind,
- welche Regelungen für den Gebrauch und die Weitergabe von vertraulichen Informationen an weitere Partner gelten, falls dies notwendig ist,
- welche Konsequenzen bei Verletzung der Vereinbarung eintreten.

In der Vertraulichkeitsvereinbarung kann auch auf die relevanten Sicherheitsrichtlinien und weitere Richtlinien der Organisation hingewiesen werden. In dem Fall, dass externe Mitarbeiter Zugang zu organisationsinternen IT-Infrastruktur haben, sollten diese neben der Vertraulichkeitsvereinbarung auch die IT-Sicherheitsrichtlinien für die Nutzung der jeweiligen IT-Systeme unterzeichnen.

Eine Vertraulichkeitsvereinbarung bietet die rechtliche Grundlage für die Verpflichtung externer Mitarbeiter zur vertraulichen Behandlung von Informationen. Aus diesem Grund muss sie alle relevanten Gesetze und Bestimmungen für die Organisation in dem speziellen Einsatzbereich berücksichtigen, klar formuliert sein und aktuell gehalten werden.

Es kann sinnvoll sein, verschiedene Vertraulichkeitsvereinbarungen je nach Einsatzzweck zu verwenden. In diesem Fall muss klar definiert werden, welche Vereinbarung für welche Fälle notwendig ist.

Ergänzende Kontrollfragen:

- Werden Externe vor dem Zugang zu vertraulichen Informationen verpflichtet, diese vertraulich zu behandeln?
- Werden durch die verwendeten Vertraulichkeitsvereinbarungen alle wichtigen Aspekte zum Schutz von organisationsinternen Informationen berücksichtigt?

M 3.56 Schulung der Administratoren für die Nutzung von VoIP

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Telefonie stellt unabhängig von der TK-Anlage zugrunde liegenden Technologie die Kommunikationsbasis der Organisation dar. Deswegen ist es unerlässlich, dass die Administratoren ausreichend geschult sind, damit sie in der Lage sind, die benötigten Funktionen und Sicherheitsmerkmale optimal zu nutzen.

In den Schulungen sollten ausreichende Kenntnisse zu den für die Einrichtung und den Betrieb der VoIP-Komponenten notwendigen Vorgehensweisen, Werkzeugen und Techniken vermittelt werden. Dies gilt auch für herstellerspezifische Aspekte einzelner Produkte, die als VoIP-Komponenten eingesetzt werden.

Für den effizienten Einsatz von VoIP werden ausführliche Kenntnisse über Netze benötigt. Diese müssen ebenfalls in der Schulung vermittelt werden. Oft werden die VoIP-Komponenten auf Standard-IT-Systemen mit eigenständigem Betriebssystem eingesetzt. Hinweise zu diesem Schulungsbestandteil sind in den jeweiligen IT-Grundschutz-Bausteinen zu den Betriebssystemen zu finden.

Im Allgemeinen sollten in den entsprechenden Schulungen mindestens folgende Elemente enthalten sein:

  - Grundlagen zu VoIP - Kompression und Übertragung von Sprachnachrichten mit möglichen Auswirkungen wie Jitter, Delay und Echo
  - Grundlagen der eingesetzten Protokolle der Anwendungsschicht (beispielsweise RTP, SIP und H 3.23)

- Administration
  - Sicherheitsrelevante Grundlagen und Konzepte der Administration, Kenntnisse der Kommandos zu Einrichtung, Betrieb, Wartung und Fehlersuche für jede VoIP-Komponente. Eine Schulung sollte eine ausgewogene Mischung aus Theorie und Praxis darstellen.
  - Kenntnisse über die Administration der IT-Systeme, auf denen die VoIP-Komponenten betrieben werden sollen.
  - Überblick über relevante rechtliche Aspekte beim VoIP-Betrieb wie z. B. Datenschutz
  - Management der Geräte, Werkzeuge
  - Protokollierung
  - Sicherung und Verwaltung von Konfigurationsdaten
  - Angriffsszenarien (z. B. Denial of Service Angriffe, ARP-Spoofing, IP-Spoofing, DNS-Spoofing, Viren und andere Schadsoftware)
  - Grundlagen zum Thema Virtuelle Private Netze (VPN)
  - Grundlagen zum Umgang mit verschlüsselten Daten (Verschlüsselung z. B. mit SRTP oder IPSec) und Möglichkeiten zur Behandlung verschlüsselter Daten

- Netztechnik
  - Grundlagen der Strukturierung von Netzen und Dienstgüte
  - Grundlagen von IP und der darauf aufbauender Protokolle (IP-Adressierung, ICMP, TCP, UDP)
  - Virtuelle Netzsegmentierung (VLAN)
- Fehlerbehebung
  - Fehlerquellen und Ursachen
  - Mess- und Analysewerkzeuge, Werkzeuge zur automatischen Überprüfung der einzelnen Komponenten des Sicherheitsgateways auf korrekte Funktion
  - Teststrategien zur Fehlersuche

Auch wenn in einer Gruppe von Administratoren die Aufgaben verteilt sind, ist es unverzichtbar, dass alle Administratoren ein allgemeines Grundwissen besitzen. Die individuellen Schwerpunkte können davon ausgehend gezielt ausgebaut und gepflegt werden. Zu vielen Produkten gibt es von den Herstellern oder spezialisierten Anbietern ein umfangreiches Angebot an aufeinander aufbauenden und individuell vertiefenden Seminaren. Das Angebot an qualifizierten Schulungen stellt ebenfalls ein Kriterium dar, das bei der Entscheidung für einen bestimmten Hersteller berücksichtigt werden sollte.

Für Schulungsmaßnahmen sollte bereits bei der Beschaffung von IT-Komponenten ein ausreichendes Budget eingeplant und ein Schulungsplan für alle Administratoren erstellt werden.

Ergänzende Kontrollfragen:

- Steht ein ausreichendes Budget für Schulungsmaßnahmen zur Verfügung?
- Wurde ein Schulungsplan für Administratoren in Anlehnung an die erwähnten Punkte erstellt?

M 3.57 Szenarien für den Einsatz von VoIP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Für VoIP, also die Sprachübertragung über IP-Netze, gibt es unterschiedliche Anwendungsszenarien. Das Bedrohungspotenzial und die Sicherheitsanforderungen sind dementsprechend ebenfalls unterschiedlich. Im Folgenden werden derzeit typische Anwendungsfälle dargestellt.

Einsatz von VoIP im Endgeräteanschlussbereich

Das erste Anwendungsszenario besteht darin, VoIP für die interne Sprachkommunikation in Firmen- und Behördennetzen zu verwenden.

Dies umfasst, vollständig oder auch nur komponentenweise, den Einsatz von IP-Telefonen, eines LAN-basierten Telekommunikationssystems, das die Vermittlungs- und Mehrwertfunktionen übernimmt sowie die Verbindung in die Außenwelt sicherstellt, und eines IP-Netzes für die Verbindung von Endgeräten und TK-Anlage. Die Verbindung in das digitale Fernsprechnetz kann dabei über lokale Gateways oder über einen VoIP-Provider erfolgen. Bei so genannten "hybriden Anlagen" werden in herkömmliche TK-Anlagen VoIP-Baugruppen integriert, die den Anschluss von IP-Telefonen, meist proprietären Systemtelefonen, ermöglichen.

Ziel dabei ist die Integration der Daten- und Telefonienetze. Den möglichen Einsparungen an Leitungen, Netzkomponenten, Management, Administration und Wartung stehen allerdings zusätzliche Bedrohungen gegenüber wie z. B. das mit geringen Kenntnissen durchführbare Abhören der Datenverbindung, denen Rechnung zu tragen ist. Die erforderlichen Sicherheitsmaßnahmen relativieren einen Teil der Einsparpotenziale, insbesondere bei der Anpassung eines vorhandenen Datennetzes für den VoIP-Einsatz, sind jedoch zwingende Voraussetzung für den sicheren und verlässlichen Einsatz dieser Technologie.

Einsatz von VoIP zur TK-Anlagen-Kopplung

Traditionell werden TK-Anlagen überwiegend über separate Wähl- oder Standleitungen miteinander verbunden.

Eine zunehmend realisierte Anwendung von VoIP ist die Kopplung von lokalen Telekommunikationsanlagen (Trunking) über IP-Verbindungen. Dabei werden traditionelle TK-Anlagen an verschiedenen Standorten unter Nutzung eines WAN-Datennetzes gekoppelt. Die Zusammenführung von Telefonie- und Datennetz in der Standortvernetzung bietet dabei erhebliche Flexibilität, eine effizientere Bandbreitennutzung und damit auch ein Einsparpotenzial.

Einsatz von VoIP zur Internet-Telefonie

Ein weiteres Szenario ist die Sprachübertragung über öffentliche IP-Netze, vor allem über das Internet. Die zunehmend größeren Bandbreiten im Backbone- und Endanschlussbereich, die zu einer mittlerweile akzeptablen Sprachqualität führen, beschleunigen den Trend zur Internet-Telefonie im privaten Bereich.

Dabei können Softphones eingesetzt werden, die meist, ähnlich zu Messaging-Diensten, über zentrale Verzeichnisse registriert sind. Zunehmende Verbreitung finden kompakte und kostengünstige VoIP-Gateways, die es ermögli-

chen, mit herkömmlichen Telefonen (analog oder ISDN) Internet-Telefonie-Dienste zu nutzen. Es werden aber auch kostengünstige Hardphones für eine private Nutzung von den Herstellern angeboten.

Unternehmen und Behörden nutzen die Sprachübertragung über öffentliche IP-Netze dagegen derzeit kaum. Der Hauptgrund ist, dass hier keine Mechanismen zur Verfügung stehen, um eine bestimmte Sprach- oder Übertragungsqualität zu garantieren.

M 3.58 Einführung in WLAN-Grundbegriffe

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement, Administrator

WLANs können in zwei verschiedenen Architekturen betrieben werden. Im Ad-hoc-Modus kommunizieren zwei oder mehr mobile Endgeräte, die mit einer WLAN-Karte ausgestattet sind (Clients), direkt miteinander.

In den meisten Fällen wird ein WLAN im Infrastruktur-Modus betrieben, d. h. die Kommunikation der Clients erfolgt über eine zentrale Funkbrücke, den sogenannten Access Point. Über den Access Point erfolgt auch die Verbindung in kabelgebundene LAN-Segmente.

Der Infrastruktur-Modus lässt mehrere Einsatzvarianten zu:

- Mittels mehrerer Access Points können überlappende Funkzellen installiert werden, sodass beim Übergang eines Clients in die nächste Funkzelle die Funkverbindung aufrecht erhalten werden kann ("Roaming"). Auf diese Weise können große Bereiche flächendeckend versorgt werden. Die Reichweite einer Funkzelle ist extrem abhängig von den Umgebungsbedingungen und liegt im Bereich von ca. 10 bis 150 Meter.
- Zwei Access Points können auch als Brücke (Bridge) zwischen zwei leitungsgebunden LANs eingesetzt werden. Ebenso ist der Einsatz eines Access Points als Relaisstation (Repeater) zur Erhöhung der Reichweite möglich.
- Bei der Verwendung entsprechender Komponenten (Richtantennen) an den Access Points kann ein WLAN auch zur Vernetzung von Liegenschaften eingesetzt werden. Hier können laut Herstellerangaben Reichweiten im Kilometerbereich erreicht werden. Die Access Points können dabei als Relaisstation oder Brücke betrieben werden.

Im Standard IEEE 802.11 werden die Bezeichnungen Independent Basic Service Set (IBSS) für Funk-Netze im Ad-hoc-Modus und Basic Service Set (BSS) für Konstellationen im Infrastruktur-Modus mit einem Access Point verwendet. Mehrere gekoppelte BSS werden als Extended Service Set (ESS) bezeichnet, das koppelnde Netz wird Distribution System (DS) genannt.

Die in Deutschland und in fast allen Staaten Europas zugelassenen WLAN-Systeme nach IEEE 802.11, 802.11b und 802.11g nutzen das ISM-Frequenzband (Industrial-Scientific-Medical) zwischen 2,4 und 2,48 GHz, das gebührenfrei und ohne zusätzliche Genehmigung verwendet werden kann. Die Sendeleistung ist auf maximal 100 mW EIRP (Effective Isotropic Radiated Power) begrenzt.

Systeme des Standards IEEE 802.11 übertragen die Daten mit einer Rate von 1 bzw. 2 Mbit/s mittels Bandspreizverfahren, entweder mittels Frequenzsprung- (FHSS) oder Direct-Sequence- (DSSS) Verfahren. Der Vollständigkeit halber sei erwähnt, dass 802.11 auch eine Infrarot-Übertragung definiert, die bisher aber in der Praxis bedeutungslos geblieben ist.

Die Systeme nach IEEE 802.11b verwenden nur das DSSS-Verfahren. Die zu übertragenen Daten werden mit einem festen Code gespreizt, um die

Übertragung unempfindlicher gegen Störung zu machen. Der Zugriff auf den Funkkanal erfolgt, wie bei allen Systemen der 802.11 Standards, nach einem zufallsgesteuerten Verfahren, genannt Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Die Brutto-Datenübertragungsrate beträgt bei IEEE 802.11b maximal 11 Mbit/s. Die Übertragungsraten können, wie bei allen Systemen der 802.11 Standards, nicht garantiert werden, sie hängen ab von der Anzahl der Clients und der Qualität der Funkübertragungsstrecke.

Systeme des Standards IEEE 802.11g verwenden die Übertragungstechnik Orthogonal Frequency Division Multiplexing (OFDM) nach IEEE 802.11a und erlauben daher auch Datenraten von bis zu 54 Mbit/s.

Im 2,4 GHz-Frequenzbereich stehen in Deutschland 13 Frequenzkanäle mit einem Frequenzabstand von 5 MHz für die Funkübertragung nach 802.11b zur Verfügung. Bei einer Kanalbandbreite von ca. 22 MHz können jedoch nur maximal 3 Kanäle gleichzeitig überlappungsfrei genutzt werden, beispielsweise die Kanäle 2, 7 und 12.

Systeme der Standards IEEE 802.11a und 802.11h nutzen den 5 GHz-Bereich. Im Frequenzbereich von 5,15 bis 5,35 GHz und bei 5,47 bis 5,725 GHz sind in Deutschland insgesamt 19 Kanäle in einem Abstand von 20 MHz unter Auflagen freigegeben worden. Bei einer Kanalbandbreite von 20 MHz werden direkt benachbarte Kanäle hier nicht gestört. Im 5 GHz Frequenzbereich arbeiten auch militärische und zivile Radar- und Navigationsanwendungen und es dürfen hier nur Systeme eingesetzt werden, die eine dynamische Frequenzwahl und eine Anpassung der Sendeleistung unterstützen.

Überblick über Sicherheitsmechanismen

Die Sicherheitsmechanismen aller 802.11 kompatiblen Systeme sind im Standard IEEE 802.11 definiert. Die Erweiterungen a, b, g und h des Standards bieten keine zusätzlichen Sicherheitsmechanismen, nur die Erweiterung i definiert neue Sicherheitsmechanismen. Die in IEEE 802.11 definierten Mechanismen dienen ausschließlich zur Sicherung der Funkstrecke zwischen den Clients und Access Points. Darüber hinaus lässt der Standard aber auch Freiraum für proprietäre Erweiterungen.

Sämtliche Sicherheitsmechanismen des Standards IEEE 802.11, die im Folgenden dargestellt werden, sind überwindbar und bieten keinen verlässlichen Schutz für sensible Informationen.

Netzname (SSID)

- Der Standard bietet die Möglichkeit einen Netznamen (ESSID bzw. SSID: (Extended) Service Set Identity) zu vergeben. Dabei gibt es zwei Betriebsarten. Wird durch den Nutzer die Kennung "Any" angegeben, akzeptiert die WLAN-Komponente beliebige SSIDs. Im anderen Fall wird der eingetragene Name überprüft und nur Teilnehmer mit der gleichen SSID können am Netz teilnehmen. Bei der Übergabe zwischen zwei benachbarten Funkzellen dient die SSID dazu, den nächsten Access Point zu finden. Da die SSID im Klartext über das Netz gesendet wird, kann ein Angreifer sie mit einfachen Mitteln in Erfahrung bringen. Einige Access Points bieten die Möglichkeit, das Senden der SSID im Broadcast zu unterbinden. Das Unterdrücken der SSID auf diese Weise ist jedoch nicht standardkonform.

- Jede Netzkarte verfügt über eine eindeutige Hardwareadresse, die sogenannte MAC-Adresse (Media Access Control-Adresse). Prinzipiell ist es möglich, in einem WLAN MAC-Adressen zu definieren, denen es erlaubt ist, mit einem Access Point zu kommunizieren. Die Adresslisten müssen hierfür allerdings "von Hand" gepflegt werden, was sehr aufwendig ist. In vielen Einsatzszenarien ist dies nicht möglich. Das Filtern der MAC-Adressen ist nicht im Standard enthalten. Andererseits ist die Filterung von MAC-Adressen standardkonform, da die Filterung keine Auswirkungen auf die Kompatibilität der Clients hat.

MAC-Adresse

- Vertraulichkeit, Integrität und Authentizität im WLAN sollen durch das "Wired Equivalent Privacy"-Protokoll (WEP) gesichert werden. Das WEP-Protokoll basiert auf der Stromchiffre RC4, mit der Klardaten paketweise abhängig von einem Schlüssel und einem Initialisierungsvektor (IV) in Chiffratdaten umgewandelt werden. Der Schlüssel ist dabei eine Zeichenkette von wahlweise 40 oder optional 104 Bit und muss den am WLAN beteiligten Clients sowie dem Access Point vorab zur Verfügung gestellt werden. Dabei wird für das gesamte WLAN ein gemeinsamer Schlüssel verwendet. Der IV wird vom Absender gewählt und sollte für jedes übertragene Datenpaket unterschiedlich sein. Der IV wird dem verschlüsselten Datenpaket unverschlüsselt vorangestellt und über das WLAN übertragen.

  WEP verschlüsselt nur die übertragenen Nutzdaten und die Integritätschecksumme. Management- und Steuersignale (Management- und Control-Frames) werden auf der Funk-Schnittstelle jedoch nicht verschlüsselt.

WEP Verschlüsselung, Integritätsschutz und Authentisierung

Während der Entwicklung des Standards IEEE 802.11i wurde von der Wi-Fi Alliance, basierend auf dem Draft 3.0 von IEEE 802.11i, Wi-Fi Protected Access (WPA) veröffentlicht. WPA enthält bereits einige Verbesserungen der Sicherheitsmechanismen und beschreibt zum einen den Einsatz des im Wesentlichen auf dem Wired Equivalent Protocol (WEP) basierenden Temporary Key Integrity Protocol (TKIP) in Kombination mit dem Integritätsprüfungsverfahren MICHAEL zur Verschlüsselung der Datenpakete. Durch MICHAEL ist in WPA das Problem der mangelhaften Integritätsprüfung in WEP gelöst worden. TKIP und MICHAEL sind als temporäre Lösung zu verstehen, da TKIP nur optional verwendet werden kann und laut WPA-Spezifkationen nicht zwingend ist.

Im Standard IEEE 802.11i, welches bis auf einige Freiheitsgrade bei der Auswahl der EAP-Methoden dem WPA2 der Wi-Fi Alliance entspricht, wird ein anderes Verschlüsselungsverfahren fest vorgeschrieben, das CTR mode (Counter Mode) with CBC-MAC Protocol (Cipher Block Chaining Message Authentication Code, CCMP). Dieses Verfahren setzt, im Gegensatz zu RC4 in WEP und WPA, den Advanced Encryption Standard (AES) zur Verschlüsselung der Authentisierungs- und Nutzdaten ein. Bei der Authentisierung wird hierbei nicht direkt der Klartext mit AES verschlüsselt, sondern ein aus dem symmetrischen Schlüssel gebildeter Zähler. Das eigentliche Verschlüsselungsergebnis entsteht dann aus der XOR-Verknüpfung eines Blocks des Klartexts mit dem AES-verschlüsselten Zähler. Außerdem wird die Methode Cipher Block Chaining (CBC) zur Integritätssicherung der Daten verwendet. Zur Schlüsselverwaltung und -verteilung wird IEEE 802.1X vorausgesetzt.

Die in IEEE 802.11i verwendete Schlüssellänge des AES-Schlüssels beträgt 128 Bit. Dieses Verfahren ist langfristig tragbar, erfordert aber - im Gegensatz zu der TKIP-Variante - neue Hardware.

Als zusätzlicher Schutz der Authentisierung kann das Extensible Authentication Protocol (EAP) gemäß Standard IEEE 802.1X verwendet werden. EAP wird im RFC 3748 genau beschrieben. Der Benutzer meldet sich hier bei einer Authentisierungsinstanz, z. B. an einem RADIUS-Server, an und dieser prüft die Zugangsberechtigung, bevor der Sitzungsschlüssel ausgetauscht wurde. EAP unterstützt eine Reihe von Authentisierungsmethoden, so dass auch Zertifikate und Zwei-Faktor-Authentisierungen genutzt werden können.

Ergänzende Kontrollfragen:

- Wurden die Benutzer und vor allem die Administratoren in der Bedienung und zur Sicherheit von WLANs geschult?
- Wurden die Benutzer auf die Sicherheitsmechanismen der verwendeten Werkzeuge hingewiesen und in deren Nutzung geschult?

M 3.59 Schulung zum sicheren WLAN-Einsatz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement, Administrator

Beim Betrieb von WLAN-Komponenten sind eine Vielzahl von Kenntnissen sowohl über die grundlegende Funktionsweise als auch über spezielle technische Ausprägungen, aber auch über eine Vielzahl von Sicherheitsaspekten erforderlich. Daher ist es unabdingbar, dass sowohl die IT-Verantwortlichen als auch das IT-Sicherheitsmanagement über WLAN-Grundlagen informiert sind.

Schulung von Administratoren

Die Administratoren für den Betrieb von WLAN-Komponenten sollten außerdem neben theoretischen auch praktische Kenntnisse besitzen. WLAN-Schulungen für Administratoren sollten unter anderem folgende Themen behandeln:

- Überblick über Sicherheitsaspekte bei WLANs
  - Typische Gefährdungen
  - SSID, Betriebsmodi, Verbindungsaufbau, Adressfilterung, Verhinderung von Spoofing, MAC-Adress-Filterung
- Auswahl geeigneter Sicherheitsmechanismen, Authentikation und Absicherung der Kommunikation
  - WEP, WPA, WPA2, IEEE 802.11i, IEEE 802.1X
  - Schlüsselmanagement in TKIP, CCMP usw.
  - Authentisierungsmechanismen im WLAN, wie z. B. EAP, RADIUS
  - Aufspüren von WLANs
- Sicherheitsmaßnahmen für den WLAN-Betrieb
  - sicherheitsrelevante WLAN-Konfigurationsparameter
  - Systemmanagement
  - Netz-Analyse-Programme und Wireless Intrusion Detection Systeme
  - VPNs für WLANs, IPSec, DHCP
  - Zusammenspiel WLANs mit Sicherheitsgateways
  - Absicherung von WLAN-Komponenten gegen unbefugten Zugriff

Schulung von Benutzern

Aber auch die Benutzer von WLAN-Komponenten, vornehmlich von WLAN-Clients, sind zu schulen. Dabei sollten die Benutzer die Funktionsweise und die sichere Bedienung der WLAN-Komponenten kennen lernen. Benutzern muss genau erläutert werden, was die Sicherheitseinstellungen bedeuten und warum sie wichtig sind. Außerdem müssen sie auf die Gefahren hingewiesen werden, wenn diese Sicherheitseinstellungen aus Bequemlichkeit bzw. zur Reduktion von störenden Warnmeldungen umgangen oder deaktiviert werden. Durch eine gezielte Sensibilisierung der Benutzer kann eine ordnungsgemäße Bedienung der WLAN-Komponenten und deren Sicherheitseinstellungen erreicht werden.

Schulung von Werkschutz und Pförtner

Vor dem Hintergrund von Wardriving-Attacken sollte außerdem eine Sensibilisierung des Werkschutzes und der Pförtner erfolgen. So sollte der Werkschutz darauf achten, ob sich über einen längeren Zeitraum unbekannte Personen mit Notebook und eventuell sogar WLAN-Antennen vor dem Betriebsgelände aufhalten. Bei Verdachtsfällen sollte das Sicherheitsmanagement informiert werden.

Die Schulungsinhalte müssen immer entsprechend der jeweiligen Einsatzszenarien angepasst werden. Auch Schulungen mit Hilfe von webbasierten interaktiven Programmen im Intranet sind hier denkbar. Neben der reinen Schulung zu WLAN-Sicherheitsmechanismen müssen die Mitarbeiter jedoch auch die WLAN-Sicherheitsrichtlinie ihrer Organisation vorgestellt bekommen.

Ergänzende Kontrollfragen:

- Sind die Administratoren auf den Umgang mit WLAN-Komponenten vorbereitet und insbesondere in sicherheitsrelevanten Aspekten geschult?
- Sind alle Benutzer mit den Inhalten der WLAN-Sicherheitsrichtlinie vertraut?
- Sind die Benutzer mit den WLAN-Sicherheitsmechanismen vertraut und werden diese auch angewandt?
- Wurden der Werksschutz und die Pförtner sensibilisiert?

M 4 Maßnahmenkatalog Hardware und Software

M 4.28	Software-Reinstallation bei Benutzerwechsel eines tragbaren PC	
M 4.29	Einsatz eines Verschlüsselungsproduktes für tragbare PCs	
M 4.30	Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen	
M 4.31	Sicherstellung der Energieversorgung im mobilen Einsatz	
M 4.32	Physikalisches Löschen der Datenträger vor und nach Verwendung	
M 4.33	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung	
M 4.34	Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen	
M 4.35	Verifizieren der zu übertragenden Daten vor Versand	
M 4.36	Sperren bestimmter Faxempfänger-Rufnummern	
M 4.37	Sperren bestimmter Absender-Faxnummern	
M 4.38	Abschalten nicht benötigter Leistungsmerkmale	
M 4.39	Abschalten des Anrufbeantworters bei Anwesenheit	
M 4.40	Verhinderung der unautorisierten Nutzung des Rechnermikrofons	
M 4.41	Einsatz angemessener Sicherheitsprodukte für IT-Systeme	
M 4.42	Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung	
M 4.43	Faxgerät mit automatischer Eingangskuvertierung	
M 4.44	Prüfung eingehender Dateien auf Makro-Viren	**entfallen**
M 4.45	Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW	
M 4.46	Nutzung des Anmeldepasswortes unter WfW und Windows 95	
M 4.47	Protokollierung der Sicherheitsgateway-Aktivitäten	
M 4.48	Passwortschutz unter Windows NT/2000/XP	
M 4.49	Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System	
M 4.50	Strukturierte Systemverwaltung unter Windows NT	
M 4.51	Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT	

M 4.52	Geräteschutz unter Windows NT/2000/XP	
M 4.53	Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT	
M 4.54	Protokollierung unter Windows NT	
M 4.55	Sichere Installation von Windows NT	
M 4.56	Sicheres Löschen unter Windows-Betriebssystemen	
M 4.57	Deaktivieren der automatischen CD-ROM-Erkennung	
M 4.58	Freigabe von Verzeichnissen unter Windows 95	
M 4.59	Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten	
M 4.60	Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten	
M 4.61	Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten	
M 4.62	Einsatz eines D-Kanal-Filters	
M 4.63	Sicherheitstechnische Anforderungen an den Telearbeitsrechner	
M 4.64	Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen	
M 4.65	Test neuer Hard- und Software	
M 4.66	Novell Netware - Sicherer Übergang ins Jahr 2000	**entfallen**
M 4.67	Sperren und Löschen nicht benötigter Datenbank-Accounts	
M 4.68	Sicherstellung einer konsistenten Datenbankverwaltung	
M 4.69	Regelmäßiger Sicherheitscheck der Datenbank	
M 4.70	Durchführung einer Datenbanküberwachung	
M 4.71	Restriktive Handhabung von Datenbank-Links	
M 4.72	Datenbank-Verschlüsselung	
M 4.73	Festlegung von Obergrenzen für selektierbare Datensätze	
M 4.74	Vernetzte Windows 95 Rechner	
M 4.75	Schutz der Registrierung unter Windows NT/2000/XP	
M 4.76	Sichere Systemversion von Windows NT	
M 4.77	Schutz der Administratorkonten unter Windows NT	
M 4.78	Sorgfältige Durchführung von Konfigurationsänderungen	
M 4.79	Sichere Zugriffsmechanismen bei lokaler Administration	

M 4.136 Sichere Installation von Windows 2000

M 4.137 Sichere Konfiguration von Windows 2000

M 4.138 Konfiguration von Windows 2000 als Domänen-Controller

M 4.139 Konfiguration von Windows 2000 als Server

M 4.140 Sichere Konfiguration wichtiger Windows 2000 Dienste

M 4.141 Sichere Konfiguration des DDNS unter Windows 2000

M 4.142 Sichere Konfiguration des WINS unter Windows 2000

M 4.143 Sichere Konfiguration des DHCP unter Windows 2000

M 4.144 Nutzung der Windows 2000 CA

M 4.145 Sichere Konfiguration von RRAS unter Windows 2000

M 4.146 Sicherer Betrieb von Windows 2000/XP

M 4.147 Sichere Nutzung von EFS unter Windows 2000/XP

M 4.148 Überwachung eines Windows 2000/XP Systems

M 4.149 Datei- und Freigabeberechtigungen unter Windows 2000/XP

M 4.150 Konfiguration von Windows 2000 als Workstation

M 4.151 Sichere Installation von Internet-PCs

M 4.152 Sicherer Betrieb von Internet-PCs

M 4.153 Sichere Installation von Novell eDirectory

M 4.154 Sichere Installation der Novell eDirectory Clientsoftware

M 4.155 Sichere Konfiguration von Novell eDirectory

M 4.156 Sichere Konfiguration der Novell eDirectory Clientsoftware

M 4.157 Einrichten von Zugriffsberechtigungen auf Novell eDirectory

M 4.158 Einrichten des LDAP-Zugriffs auf Novell eDirectory

M 4.159 Sicherer Betrieb von Novell eDirectory

M 4.160 Überwachen von Novell eDirectory

M 4.161 Sichere Installation von Exchange/Outlook 2000

M 4.162 Sichere Konfiguration von Exchange 2000 Servern

M 4.163 Zugriffsrechte auf Exchange 2000 Objekte

M 4.164 Browser-Zugriff auf Exchange 2000

M 4.165 Sichere Konfiguration von Outlook 2000

M 4.166 Sicherer Betrieb von Exchange/Outlook 2000

M 4.167 Überwachung und Protokollierung von Exchange 2000 Systemen

M 4.168 Auswahl eines geeigneten Archivsystems

M 4.169 Verwendung geeigneter Archivmedien

M 4.170 Auswahl geeigneter Datenformate für die Archivierung von Dokumenten

M 4.171 Schutz der Integrität der Index-Datenbank von Archivsystemen

M 4.172 Protokollierung der Archivzugriffe

M 4.173 Regelmäßige Funktions- und Recoverytests bei der Archivierung

M 4.174 Vorbereitung der Installation von Windows NT/2000 für den IIS

M 4.175 Sichere Konfiguration von Windows NT/2000 für den IIS

M 4.176 Auswahl einer Authentisierungsmethode für Webangebote

M 4.177 Sicherstellung der Integrität und Authentizität von Softwarepaketen

M 4.178 Absicherung der Administrator- und Benutzerkonten beim IIS-Einsatz

M 4.179 Schutz von sicherheitskritischen Dateien beim IIS-Einsatz

M 4.180 Konfiguration der Authentisierungsmechanismen für den Zugriff auf den IIS

M 4.181 Ausführen des IIS in einem separaten Prozess

M 4.182 Überwachen des IIS-Systems

M 4.183 Sicherstellen der Verfügbarkeit und Performance des IIS

M 4.184 Deaktivieren nicht benötigter Dienste beim IIS-Einsatz

M 4.185 Absichern von virtuellen Verzeichnissen und Web-Anwendungen beim IIS-Einsatz

M 4.186 Entfernen von Beispieldateien und Administrations-Scripts des IIS

M 4.187 Entfernen der FrontPage Server-Erweiterung des IIS

M 4.188 Prüfen der Benutzereingaben beim IIS-Einsatz

M 4.189 Schutz vor unzulässigen Programmaufrufen beim IIS-Einsatz

M 4.190 Entfernen der RDS-Unterstützung des IIS

M 4.191 Überprüfung der Integrität und Authentizität der Apache-Pakete,

M 4.192 Konfiguration des Betriebssystems für einen Apache-Webserver

M 4.193 Sichere Installation eines Apache-Webservers

M 4.194 Sichere Grundkonfiguration eines Apache-Webservers

M 4.195 Konfiguration der Zugriffssteuerung beim Apache-Webserver

M 4.196 Sicherer Betrieb eines Apache-Webservers

M 4.197 Servererweiterungen für dynamische Webseiten beim Apache-Webserver

M 4.198 Installation eines Apache-Webservers in einem chroot-Käfig

M 4.199 Vermeidung gefährlicher Dateiformate

M 4.200 Umgang mit USB-Speichermedien

M 4.201 Sichere lokale Grundkonfiguration von Routern und Switches

M 4.202 Sichere Netz-Grundkonfiguration von Routern und Switches

M 4.203 Konfigurations-Checkliste für Router und Switches

M 4.204 Sichere Administration von Routern und Switches

M 4.205 Protokollierung bei Routern und Switches

M 4.206 Sicherung von Switch-Ports

M 4.207 Einsatz und Sicherung systemnaher z/OS-Terminals

M 4.208 Absichern des Start-Vorgangs von z/OS-Systemen

M 4.209 Sichere Grundkonfiguration von z/OS-Systemen

M 4.210 Sicherer Betrieb des z/OS-Betriebssystems

M 4.211 Einsatz des z/OS-Sicherheitssystems RACF

M 4.212 Absicherung von Linux für zSeries

M 4.213 Absichern des Login-Vorgangs unter z/OS

M 4.214 Datenträgerverwaltung unter z/OS-Systemen

M 4.215 Absicherung sicherheitskritischer z/OS-Dienstprogramme

M 4.274 Sichere Grundkonfiguration von Speichersystemen

M 4.275 Sicherer Betrieb eines Speichersystems

M 4.276 Planung des Einsatzes von Windows Server 2003

M 4.277 Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows Server 2003

M 4.278 Sichere Nutzung von EFS unter Windows Server 2003

M 4.279 Erweiterte Sicherheitsaspekte für Windows Server 2003

M 4.280 Sichere Basiskonfiguration von Windows Server 2003

M 4.281 Sichere Installation und Bereitstellung von Windows Server 2003

M 4.282 Sichere Konfiguration der IIS-Basis-Komponente unter Windows Server 2003

M 4.283 Sichere Migration von Windows NT 4 Server und Windows 2000 Server auf Windows Server 2003

M 4.284 Umgang mit Diensten unter Windows Server 2003

M 4.285 Deinstallation nicht benötigter Client-Funktionen von Windows Server 2003

M 4.286 Verwendung der Softwareeinschränkungsrichtlinie unter Windows Server 2003

M 4.287 Sichere Administration der VoIP-Middleware

M 4.288 Sichere Administration von VoIP-Endgeräten

M 4.289 Einschränkung der Erreichbarkeit über VoIP

M 4.290 Anforderungen an ein Sicherheitsgateway für den Einsatz von VoIP

M 4.291 Sichere Konfiguration der VoIP-Middleware

M 4.292 Protokollierung bei VoIP

M 4.293 Sicherer Betrieb von Hotspots

M 4.294 Sichere Konfiguration der Access Points

M 4.295 Sichere Konfiguration der WLAN-Clients

M 4.296 Einsatz einer geeigneten WLAN-Management-Lösung

M 4.297 Sicherer Betrieb der WLAN-Komponenten

M 4.298 Regelmäßige Audits der WLAN-Komponenten

M 4.1 Passwortschutz für IT-Systeme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Der Passwortschutz eines IT-Systems soll gewährleisten, dass nur solche Benutzer einen Zugriff auf die Daten und IT-Anwendungen erhalten, die eine entsprechende Berechtigung nachweisen. Unmittelbar nach dem Einschalten des IT-Systems muss der Berechtigungsnachweis erfolgen. Kann der Benutzer die erforderliche Berechtigung nicht nachweisen, so verhindert der Passwortschutz den Zugriff auf das IT-System.

Realisiert werden kann der Passwortschutz an einem IT-System auf verschiedene Weise:

- Die meisten BIOS-Varianten bieten die Installation eines Boot-Passwortes an. Bei Fehleingaben wird der Boot-Vorgang nicht fortgesetzt. Ein BIOS-Passwort ist nicht schwer zu überwinden, schützt aber vor Zufallstätern, sollte also zumindest überall da eingesetzt werden, wo keine besseren Zugriffsschutzmechanismen vorhanden sind (siehe auch: M 4.84 *Nutzung der BIOS-Sicherheitsmechanismen*).
- Gute Betriebssysteme enthalten bereits Zugriffsschutzmechanismen. In den meisten Fällen müssen diese aber noch aktiviert werden, beispielsweise durch die Vergabe von Passwörtern für alle Benutzer. Näheres hierzu findet sich in den betriebssystem-spezifischen Bausteinen.
- Es wird Zusatzhardware oder -software installiert, die vor dem eigentlichen Start des Rechners ein Passwort abfragt und bei falscher Passworteingabe die weitere Nutzung des IT-Systems verhindert.

Für den Umgang mit Passwörtern sind die Hinweise in M 2.11 *Regelung des Passwortgebrauchs* zu beachten, insbesondere ist das Passwort regelmäßig zu ändern.

Ergänzende Kontrollfragen:

- Ist auf den betroffenen Rechnern ein Passwortschutz installiert?
- Welche BIOS- Sicherheitsmechanismen sind aktiviert?

M 4.2 Bildschirmsperre

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Unter einer Bildschirmsperre versteht man die Möglichkeit, die auf dem Bildschirm aktuell vorhandenen Informationen zu verbergen. Eine Bildschirmsperre sollte nur durch eine erfolgreiche Benutzerauthentikation, also z. B. eine Passwortabfrage, deaktiviert werden können, damit bei einer kürzeren Abwesenheit des IT-Benutzers ein Zugriffsschutz für das IT-System gewährleistet wird.

Die Bildschirmsperre sollte sich sowohl manuell vom Benutzer aktivieren lassen, als auch nach einem vorgegebenen Inaktivitäts-Zeitraum automatisch gestartet werden. Alle Benutzer sollten dafür sensibilisiert sein, dass sie die Bildschirmsperre aktivieren, wenn sie den Arbeitsplatz für eine kurze Zeit verlassen. Bei längeren Abwesenheiten sollten Benutzer sich abmelden.

automatische Sperre bei fehlenden Benutzereingaben

Der Zeitraum, nach dem sich eine Bildschirmsperre wegen fehlender Benutzereingaben aktiviert, sollte gewisse Grenzen weder unter- noch überschreiten. Der Zeitraum sollte nicht zu knapp gewählt werden, damit die Bildschirmsperre nicht bereits nach kurzen Denkpausen anspringt. Dieser Zeitraum darf aber auf keinen Fall zu lang sein, damit die Abwesenheit des Benutzers nicht von Dritten ausgenutzt werden kann. Eine sinnvolle Vorgabe ist eine Zeitspanne von 15 Minuten. Das IT-Sicherheitsmanagement-Team sollte Vorgaben für die Einstellung der Wartezeit machen, die die Sicherheitsanforderungen der jeweiligen IT-Systeme und deren Einsatzumgebung berücksichtigen.

Passwortabfrage einschalten

Die meisten Betriebssysteme enthalten bereits Bildschirmsperren. Bei deren Nutzung muss darauf geachtet werden, die Passwortabfrage zu aktivieren.

Eine passwortunterstützte Bildschirmsperre wird von MS-Windows 3.x als Bildschirmschoner angeboten. Die Dokumentation dazu sagt jedoch: "Ist eine Non-Windows-Anwendung die aktuelle Anwendung, wird der Bildschirmschoner nicht automatisch aktiviert, unabhängig davon, ob die Anwendung in einem Fenster, von der MS-DOS-Befehlszeile oder als Symbol ausgeführt wird." Unter Windows 95 aktiviert sich der Bildschirmschoner jedoch auch bei DOS-Anwendungen. Neben MS-Windows gibt es weitere Produkte, die einen passwortunterstützenden Bildschirmschoner anbieten. Vor dem Einsatz solcher Produkte ist zu überprüfen, ob die Bildschirmsperre unter allen Applikationen funktioniert.

Unter Unix kann eine Bildschirmsperre mit Programmen wie *lock* oder - unter X-Windows - *lockscreen* erfolgen.

Ergänzende Kontrollfragen:

- Ist auf den betreffenden Rechnern eine Bildschirmsperre installiert?
- Wird die Bildschirmsperre konsequent eingesetzt?

M 4.3 Regelmäßiger Einsatz eines Anti-Viren-Programms

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Funktionsweise von Anti-Viren-Programmen

Zum Schutz vor Computer-Viren können unterschiedliche Wirkprinzipien genutzt werden. Programme, die IT-Systeme nach bekannten Viren durchsuchen, haben sich in der Vergangenheit als effektivstes und wirksamstes Mittel in der Viren-Bekämpfung erwiesen. Von Vorteil ist, dass neu erhaltene Software oder Datenträger schon vor dem ersten Einsatz geprüft werden können. Man kann daher eine Infektion mit bekannten Computer-Viren grundsätzlich vermeiden. Ein weiterer Vorteil ist, dass man durch das Anti-Viren-Programm eine genauere Information über den jeweils entdeckten Virus erhält. Die bekannten Viren sind durch Spezialisten analysiert worden, so dass man weiß, ob Schadensfunktionen vorhanden sind. Ein gutes Anti-Viren-Programm muss daher nicht nur in der Lage sein, viele Viren zu finden, sondern sie auch möglichst exakt identifizieren.

Schutz vor Makro-Viren

Nicht nur reguläre Programm-Dateien können Computer-Viren enthalten, sondern auch Dateien von Anwendungsprogrammen, die eine Makrosprache verwenden ("Makro-Viren"). Betroffen sind in der Regel die Office-Programme (wie Textverarbeitung oder Tabellenkalkulation) der meisten Hersteller. Die meisten Anwendungsprogramme bieten Einstellungsoptionen, die den Schutz vor Makro-Viren erhöhen. Beispielsweise kann beim Öffnen von Dateien die Ausführung von Makros standardmäßig verhindert werden. In den Informationen und Dokumentationen der Hersteller von Anwendungsprogrammen sollte daher gezielt nach diesem Thema gesucht und die Empfehlungen beachtet werden.

Auch wenn nahezu alle Anti-Viren-Programme Makro-Viren erkennen, sollten die folgenden Maßnahmen erwogen werden, um die Sicherheit zu erhöhen: In einer Testumgebung können Dateien mit dem jeweiligen Anwendungsprogramm gefahrlos auf Makro-Viren untersucht werden. Alternativ besteht die Möglichkeit, empfangene Dateien mit einem Editor zu bearbeiten, der die Datei in ein Format umwandelt, in dem die Makros nicht ablauffähig sind. Die empfangenen Dateien können auch mit so genannten Viewern geöffnet werden, die es kostenlos für die Darstellung der verbreitetsten Dateiformate gibt und die ebenfalls die Ausführung von Makros nicht zulassen.

Texte im RTF-Format weitergeben

Dokumente sollten nur in Formaten nach außen gegeben werden, die möglichst "ungefährlich" sind, also beispielsweise solchen, zu denen keine Makrosprache existiert und damit keine Gefahr von Makro-Viren besteht. Textdokumente sollten z. B. statt als DOC- oder SDW-Datei möglichst nur im RTF-Format nach außen gegeben werden (siehe auch M 4.134 *Wahl geeigneter Datenformate*).

Bei der Verwendung des RTF-Formats ist jedoch zu beachten, dass damit unter bestimmten Voraussetzungen der Makroviren-Schutz von Microsoft

Word umgangen werden kann. Bekannte Viren werden jedoch von aktuellen Anti-Viren-Programmen gefunden. Für RTF existiert zwar keine Makrosprache, es können jedoch Verknüpfungen mit Dokumentenvorlagen (DOT) eingebettet sein, die ihrerseits Makros enthalten können. Wird eine solche RTF-Datei geöffnet und ist die Dokumentvorlage ebenfalls im Zugriff, führt Microsoft Word in der Dokumentenvorlage eventuell enthaltene Makros ohne Rückfrage aus. Betroffen sind ungepatchte Versionen von Word 97, 98, 2000 und 2001 (Mac).

Als weitere Vorbeugung sollten Benutzer darauf hingewiesen werden, wie sie die automatische Ausführung möglicherweise vorhandener Makros verhindern können. Dies ist leider für fast alle Programme und Versionen unterschiedlich und auch nicht immer zuverlässig.

Betrieb von Computer-Anti-Viren-Programmen

Zu beachten ist, dass Anti-Viren-Programme mit der Zeit ihre Wirksamkeit verlieren, da sie nur die zu ihrem Erstellungszeitpunkt bekannten Computer-Viren berücksichtigen, neu hinzugekommene jedoch meist nicht erkennen können. Daher ist eine regelmäßige, mindestens wöchentliche (besser tägliche) Aktualisierung des Anti-Viren-Programms erforderlich.

Durch Parametrisierung lassen sich bei Anti-Viren-Programmen Einstellungen vornehmen, über die festgelegt wird, welche Dateien geprüft werden sollen und in welchem Umfang die Prüfung erfolgen soll. Hier ist es Aufgabe des IT-Sicherheitsmanagements, die geeigneten Einstellungen zu ermitteln und den Benutzern mitzuteilen bzw. als Voreinstellungen an diese weiterzugeben.

Ebenso wie andere Programme können Anti-Viren-Programme durch Aufruf (transient) oder im Hintergrund (resident) genutzt werden. Die Betriebsart des Schutzprogramms hat entscheidenden Einfluss auf die Akzeptanz bei den Benutzern und damit auf die tatsächlich erreichte Schutzfunktion.

Beim transienten Betrieb muss das Anti-Viren-Programm durch den Benutzer gestartet werden, der außerdem explizit festlegen muss, welche Datenträger durchsucht werden sollen. Hierdurch können Infektionen erst im Nachhinein festgestellt werden. Ein Viren-Schutz ist zwar grundsätzlich möglich, jedoch hängt die Wirksamkeit von der Sorgfalt der Benutzer ab.

Beim residenten Betrieb wird das Anti-Viren-Programm beim Start des Rechners in den Speicher geladen und verbleibt dort aktiv bis zum Ausschalten. Es verrichtet seine Tätigkeit, ohne dass der Benutzer dabei mitwirkt, er kann inzwischen seine eigentliche Arbeit, z. B. das Schreiben von Texten, ausführen. Der residente Betrieb wird empfohlen.

Wird ein Virus gefunden, wird die betroffene Datei für den Zugriff gesperrt, d. h. der Benutzer kann sie nicht verwenden, solange das Schutzprogramm aktiv ist. Der Einsatz speicherresidenter Anti-Viren-Programme unter Windows-Betriebssystemen ist derzeit die beste Möglichkeit, sich vor Computer-Viren zu schützen, weil jede Datei vor ihrer Nutzung (Öffnen zur Bearbeitung, Kopieren, Drucken, Entpacken usw.) geprüft und bei Viren-Befall gesperrt werden kann.

Beim Einsatz von Verschlüsselungstechniken müssen die potentiellen Auswirkungen auf den Antivirusschutz bedacht werden. Werden Dateien verschlüsselt, so können Systemkomponenten bzw. Anwendungen auf die Dateien nicht zugreifen, solange sie den entsprechenden Schlüssel nicht besitzen. Dies impliziert, dass ein Viren-Suchprogramm entweder im Kontext des Benutzers laufen oder mit dem entsprechenden kryptographischen Schlüssel ausgestattet werden muss, um eine verschlüsselte Datei auf Viren überprüfen zu können. Wird jedoch die Benutzerkennung, unter der das Viren-Suchprogramm ausgeführt wird, mit dem entsprechenden kryptographischen Schlüssel ausgestattet, entstehen Sicherheitsrisiken, die es zu vermeiden gilt. Daher wird der Einsatz eines residenten Viren-Suchprogramms empfohlen, welches die Virenprüfung im Benutzerkontext bei jedem Zugriff auf eine Datei durchführt.

Verhaltensregeln bei Auftreten eines Computer-Virus sind unter M 6.23 *Verhaltensregeln bei Auftreten eines Computer-Virus* beschrieben.

Ergänzende Kontrollfragen:

- Wann wurde die letzte Überprüfung vorgenommen? Wurde das Ergebnis dokumentiert?
- Wurden Computer-Viren gefunden? Wenn ja, so kann dies darauf hindeuten, dass unerlaubt unautorisierte Software eingesetzt wurde.
- Wann wurde das eingesetzte Anti-Viren-Programm zuletzt aktualisiert?
- Sind Maßnahmen zum Schutz vor Makro-Viren umgesetzt?

M 4.4 Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer, Administrator

Handelsübliche PCs sind heute in der Regel mit einem Diskettenlaufwerk und einem CD-/DVD-ROM-Laufwerk bzw. CD-/DVD-Writer ausgestattet. Zusätzlich besteht die Möglichkeit, über Schnittstellen externe Speichermedien anzuschließen. Ein Beispiel sind USB-Memory-Sticks, die in die USB-Schnittstelle gesteckt werden und von neueren Betriebssystemen (z. B. für Microsoft-Betriebssysteme ab Windows 2000) automatisch erkannt werden. Durch solche Laufwerke für Wechselmedien und externe Datenspeicher ergeben sich folgende potentielle Sicherheitsprobleme:

- Der PC könnte von solchen Laufwerken unkontrolliert gebootet werden.
- Es könnte unkontrolliert Software von solchen Laufwerken eingespielt werden.
- Daten könnten unberechtigt auf Wechselmedien kopiert werden.

Beim Booten von Wechselmedien oder beim Installieren von Fremdsoftware können nicht nur Sicherheitseinstellungen außer Kraft gesetzt werden, sondern der PC kann auch mit Computer-Viren und anderen Schadprogrammen infiziert werden.

Diesen Gefahren muss durch geeignete organisatorische oder technische Sicherheitsmaßnahmen entgegengewirkt werden. Hierfür bieten sich verschiedene Vorgehensweisen an, deren spezifische Vor- und Nachteile im Folgenden kurz dargestellt werden:

- **Ausbau von Laufwerken**

  Der Ausbau der Laufwerke für Wechselmedien bietet zwar den sichersten Schutz vor den oben genannten Gefährdungen, ist aber meist mit erheblichem Aufwand verbunden. Weiterhin ist zu berücksichtigen, dass der Ausbau unter Umständen die Administration und Wartung des IT-Systems behindert. Diese Lösung sollte in Betracht gezogen werden, wenn besondere Sicherheitsanforderungen bestehen.

- **Verschluss von Laufwerken**

  Für einige Laufwerksarten gibt es abschließbare Einschubvorrichtungen, mit denen die unkontrollierte Nutzung verhindert werden kann. Bei der Beschaffung sollte sichergestellt werden, dass die Laufwerksschlösser für die vorhandenen Laufwerke geeignet sind und diese nicht beschädigen können. Außerdem sollte darauf geachtet werden, dass die Schlösser herstellerseitig mit hinreichend vielen unterschiedlichen Schlüsseln angeboten werden. Nachteilig sind die Beschaffungskosten für die Laufwerksschlösser und der Aufwand für die erforderliche Schlüsselverwaltung.

- **Deaktivierung im BIOS bzw. Betriebssystem**

  Im BIOS bieten die meisten PCs Einstellmöglichkeiten dafür, von welchen Laufwerken gebootet werden kann. In Verbindung mit einem Passwort-

schutz der BIOS-Einstellungen (siehe auch M 4.84 *Nutzung der BIOS-Sicherheitsmechanismen*) kann dadurch das unkontrollierte Booten von Wechselmedien unterbunden werden. Weiterhin können die vorhandenen Laufwerke bei modernen Betriebssystemen einzeln deaktiviert werden.

Dies schützt vor unberechtigter Nutzung, z. B. Installation von Fremdsoftware oder Kopieren auf Wechselmedien.

Die Deaktivierung der Laufwerke im BIOS bzw. Betriebssystem hat den Vorteil, dass keine Hardware-Änderungen erforderlich sind. Die entsprechenden Einstellungen im Betriebssystem können gegebenenfalls sogar zentral vorgenommen werden. Wirksam ist diese Vorgehensweise jedoch nur, wenn der Benutzer nicht über die Berechtigungen im Betriebssystem verfügt, um die Deaktivierung der Laufwerke rückgängig zu machen.

- **Kontrolle der Schnittstellennutzung**

  Der Betrieb von externen Speichermedien wie USB-Memory-Sticks lässt sich nur sehr schwer verhindern, wenn die verwendete Schnittstelle auch für andere (erlaubte) Zusatzgeräte genutzt wird. So werden beispielsweise Notebooks ausgeliefert, die zum Anschluss einer Maus nur die USB-Schnittstelle zur Verfügung stellen. Dadurch ist es in der Regel nicht sinnvoll, ein "USB-Schloss" zu verwenden oder die Schnittstelle durch andere mechanische Maßnahmen zu deaktivieren.
  Die Nutzung von Schnittstellen sollte daher durch entsprechende Rechtevergabe auf Ebene des Betriebssystems oder mit Hilfe von Zusatzprogrammen geregelt werden. Alternativ kann das Hinzufügen von Geräten überwacht werden. Beim Anschluss von Datenspeichern an externen Schnittstellen werden oft vom Betriebssystem Treiber bzw. Kernelmodule geladen oder Einträge in Konfigurationsdateien (wie der Windows-Registry) erzeugt, die detektiert werden können. Einzelheiten sind produkt- und betriebssystemspezifisch und werden in einer separaten Maßnahme beschrieben (siehe auch M 4.200 *Umgang mit USB-Speichermedien*).

- **Richtlinien für die Nutzung**

  In vielen Fällen dürfen die Benutzer die eingebauten Laufwerke für Wechselmedien oder Speichermedien an externen Schnittstellen durchaus verwenden, die Nutzung ist jedoch durch entsprechende Richtlinien reglementiert. Auf technischer Ebene sollte dann lediglich das Booten von Wechselmedien im BIOS deaktiviert werden. Ausbau, Verschluss oder Deaktivierung der Laufwerke im Betriebssystem kommen nicht in Frage.

  In diesem Fall sollten die Richtlinien für die Nutzung der Laufwerke und Speichermedien so explizit wie möglich definiert werden. Beispielsweise kann ein generelles Verbot ausgesprochen werden, nur das Kopieren öffentlicher Text-Dokumente wird erlaubt. Die Richtlinien müssen allen Benutzern bekannt gemacht und die Einhaltung kontrolliert werden. Die Installation und das Starten von Programmen, die von Wechselmedien eingespielt wurden, sollte untersagt und soweit wie möglich auch technisch unterbunden werden (siehe auch M 2.9 *Nutzungsverbot nicht freigegebener Hard- und* Software).

Diese rein organisatorische Lösung sollte nur dann gewählt werden, wenn die Benutzer hin und wieder oder regelmäßig auf die Laufwerke zugreifen müssen. Anderenfalls sollte der Zugriff - wie oben beschrieben - durch technische Maßnahmen unterbunden werden.

Bei der Auswahl einer geeigneten Vorgehensweise müssen immer *alle* Laufwerke für Wechselmedien berücksichtigt werden, aber ebenso auch alle Möglichkeiten, über Vernetzung Daten auszutauschen, also insbesondere auch E-Mail und Internet-Anbindungen. Wenn der PC über eine Verbindung zum Internet verfügt, ist es nicht allein ausreichend, alle Laufwerke für Wechselmedien zu deaktivieren oder auszubauen. Besonderes Augenmerk ist auf den Schutz vor Schadprogrammen, z. B. Computer-Viren oder Trojanische Pferde, zu richten (siehe auch M 4.3 *Regelmäßiger Einsatz eines Viren-Schutzprogramms*).

Damit die Sicherheitsmaßnahmen akzeptiert und beachtet werden, müssen die Benutzer über die Gefährdung durch Laufwerke für Wechselmedien informiert und sensibilisiert werden.

Ergänzende Kontrollfragen:

- Ist der Zugriff auf Wechselmedien unterbunden oder reglementiert?
- Sind die Benutzer über alle Regelungen zum Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern informiert?
- Ist sichergestellt, dass PCs nicht unkontrolliert von Wechselmedien gebootet werden?

M 4.5 Protokollierung der TK-Administrationsarbeiten

Verantwortlich für Initiierung: TK-Anlagen-Verantwortlicher, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Alle Eingaben, die über die Wartungseingänge der TK-Anlage vorgenommen werden, sollten protokolliert werden. Dies kann entweder über einen Protokolldrucker und/oder auf anderen Speichermedien erfolgen. Auf die erzeugten Protokolldateien darf der TK-Anlagenadministrator kein Schreibrecht besitzen. Die vom Drucker erzeugten Ausdrucke sollten laufende Seitenzahlen besitzen, die einzelnen Protokollmeldungen laufende Meldungsnummern.

Das BSI hat in Zusammenarbeit mit dem Zentralverband der Elektro- und Elektronikindustrie (ZVEI) einen Katalog von Anforderungen erarbeitet, der auch eine verbesserte Protokollierung beinhaltet. Dieser Katalog soll bei der Beschaffung neuer TK-Anlagen für Bundesbehörden zum Tragen kommen. Bei vorhandenen TK-Anlagen sollte überprüft werden, inwieweit die Hersteller solche verbesserten Möglichkeiten als Update anbieten können.

Ergänzende Kontrollfragen:

- Findet eine Protokollierung statt?
- Besteht die Möglichkeit festzustellen, ob der Protokolldrucker ausgeschaltet wurde?

M 4.6 Revision der TK-Anlagenkonfiguration

Verantwortlich für Initiierung: TK-Anlagen-Verantwortlicher, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Revisor

Nach jeder Konfigurationsveränderung, z. B. der Freigabe einer Berechtigung für einen Teilnehmer, sollte diese in eine Ist-Bestandsliste eingetragen werden. Diese Liste kann per Hand oder automatisiert geführt werden. In regelmäßigen (nicht unbedingt gleichmäßigen) Abständen (z. B. alle 6 Monate) sollte diese Ist-Bestandsliste zumindest stichprobenartig mit der Realität verglichen werden. Unstimmigkeiten sind mit Hilfe der Protokolle aufzuklären. Insbesondere sollte kontrolliert werden, ob

- alle nicht vergebenen Rufnummern auch wirklich nicht eingerichtet sind,
- verbotene Berechtigungen auch nirgendwo vergeben sind,
- deaktivierte Leistungsmerkmale auch wirklich inaktiv sind,
- deaktivierte Dial-In-Funktionen auch wirklich inaktiv sind.

Das BSI hat in Zusammenarbeit mit dem Zentralverband der Elektro- und Elektronikindustrie (ZVEI) einen Katalog von Anforderungen erarbeitet, der unter anderem auch Forderungen nach einer besseren Unterstützung von Revisionstätigkeiten beinhaltet. Dieser Katalog soll bei der Beschaffung neuer TK-Anlagen für Bundesbehörden zum Tragen kommen. Bei vorhandenen TK-Anlagen sollte überprüft werden, inwieweit die Hersteller solche verbesserten Möglichkeiten als Update anbieten können.

Ergänzende Kontrollfragen:

- Ist es möglich, aus den Unterlagen heraus Angaben, beispielsweise über die Berechtigungen bestimmter Anschlüsse, zu geben?
- Wann wurde die Dokumentation das letzte Mal an der Realität überprüft?

M 4.7 Änderung voreingestellter Passwörter

Verantwortlich für Initiierung: TK-Anlagen-Verantwortlicher, IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator, Benutzer

Viele IT-Systeme, TK-Anlagen und Netzkoppelelemente (beispielsweise ISDN-Router, Sprach-Daten-Multiplexer etc.) besitzen nach der Auslieferung durch den Hersteller noch voreingestellte Standardpasswörter. Von Herstellern oder Administratoren voreingestellte Passwörter sind direkt nach der Installation, spätestens bei erstmaliger Inbetriebnahme von Hard- oder Software zu ändern. Hierbei sind die einschlägigen Regeln für Passwörter zu beachten (siehe M 2.11 *Regelung des Passwortgebrauchs*).

Achtung: Bei einigen TK-Anlagen werden vorgenommene Änderungen der Konfiguration nur im RAM abgelegt. Dies gilt auch für Passwortänderungen. Daher ist nach einer solchen Operation stets eine Datensicherung vorzunehmen und eine neue Sicherungskopie zu erstellen. Unterbleibt dies, so ist nach einem "Restart" der Anlage wieder das Standardpasswort gültig. Weiterhin sollte überprüft werden, ob nach Einrichten eines neuen Passworts das Standardpasswort tatsächlich seine Gültigkeit verloren hat und nicht weiterhin für den Systemzugang genutzt werden kann.

Ergänzende Kontrollfragen:

- Ist die Anlage noch mit einem Standardpasswort versehen?
- Wurden (beispielsweise bei TK-Anlagen) die Sicherungskopien nach der Vergabe und Speicherung des individuellen Passworts angelegt?
- Ist der Systemzugang mit dem Standardpasswort nach der Eingabe eines neuen Passworts weiterhin möglich?
- Werden die einschlägigen Regeln zum Passwortgebrauch beachtet?

M 4.8 Schutz des TK-Bedienplatzes

Verantwortlich für Initiierung: TK-Anlagen-Verantwortlicher, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Sollte die TK-Anlage mit Hilfe eines Bedien-PCs administriert werden, so ist dieser mindestens mit den für PCs üblichen Schutzmaßnahmen, siehe Baustein B 3.201 *Allgemeiner Client*, zu versehen.

Optional:

Sollte die TK-Anlage nicht über ausreichende Sicherheitsfunktionen für Rechteverwaltung und Zugangsschutz verfügen, so kann überlegt werden, marktgängige Zusatzeinrichtungen (Portcontroller) einzusetzen. Mit Hilfe solcher Geräte können sichere Identifizierungs- und Authentisierungsverfahren realisiert werden.

Ergänzende Kontrollfragen:

- Ist der Bedien-PC mit einem Passwortschutz versehen?
- Steht der Bedien-PC in einer gesicherten Umgebung?
- Wer hat Zugang zum Bedien-PC?
- Wer hat Zugriffsrechte für den Bedien-PC?

M 4.9 Einsatz der Sicherheitsmechanismen von X-Windows

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator

Release 5 der X-Window-Software bietet nur wenige Maßnahmen, um die Sicherheit bei der Übertragung von Daten zwischen dem X-Server und dem X-Client zu erhöhen, so dass der Einsatz von X-Window-Software nur in einer sicheren Umgebung empfohlen werden kann.

Befehl xhost

- **Rechnerspezifische Zugriffskontrolle:** Auf jedem X-Server gibt es eine Liste zugelassener Rechner, die mit dem Befehl *xhost* verändert werden kann. Sie muss auf jeden Fall auf die Rechner beschränkt bleiben, die einen Zugriff auf den X-Server benötigen. Es sollte auf keinen Fall ein globaler Zugriff mit *xhost* + ermöglicht werden. Dies kann erreicht werden, indem explizit Rechner in der *xhost*-Tabelle eingetragen werden. Darüber hinaus ist zu beachten, dass jeder Benutzer auf einem der zugelassenen Rechner uneingeschränkten Zugriff auf den X-Server hat. Diese Art der Zugriffskontrolle kann deshalb nur dann empfohlen werden, wenn aus zwingenden Gründen keiner der folgenden Mechanismen eingesetzt werden kann.

MIT-MAGIC-COOKIE NIS-Authentisierung

- **Benutzerspezifische Zugriffskontrolle:** Der X-Server Prozess lässt sich so konfigurieren, dass bei einem Login (z. B. mit Hilfe von *xdm*) ein Schlüssel generiert wird, der zur Authentisierung bei einer Übertragung zwischen Client und Server benutzt wird. Dieser Schlüssel (*MAGIC COOKIE*) wird im Heimatverzeichnis des Benutzers in der Datei *.Xauthority* abgelegt und kann mit Hilfe des Befehls *xauth* an den X-Client übertragen werden. Während allerdings der *MIT-MAGIC-COOKIE*-Mechanismus nur als eine Art Passwort angesehen werden muss, das bei seiner Übertragung abgehört werden kann, bietet ein in Verbindung mit *NIS* angebotener und mit einer DES-Verschlüsselung arbeitender Mechanismus mehr Sicherheit und sollte deshalb bevorzugt werden.

abgesicherter Kanal

- **Zugriffskontrolle über Secure Shell:** Die Kommunikation zwischen X-Client und X-Server kann auch über einen abgesicherten Kanal einer *ssh*-Verbindung erfolgen (siehe auch M 5.64 *Secure Shell*). Hierbei erfolgt sowohl eine rechnerbasierte als auch eine benutzerbasierte Zugriffskontrolle. Die Authentisierungs- und Nutzdaten werden verschlüsselt. Für einen sicheren Betrieb von X-Windows wird die Nutzung von Secure Shell daher empfohlen.

Abhören von Tastatureingaben

Mit einem Zusatzprogramm können unter X-Windows die Tastendrücke eines entfernten Rechners in Klarschrift übersetzt und eingesehen werden. Bei der Benutzung des Programms *xterm* kann das Weiterleiten von Tastendrücken verhindert werden, indem verhindert wird, dass *KeyPress*-Events, welche es bekommt, noch an andere Applikationen weitergeleitet werden. Dafür muss die *secure keyboard*-Option über das *xterm*-Menü eingeschaltet werden, so dass das entsprechende Fenster exklusiven Zugriff auf die Tastatur hat.

Ergänzende Kontrollfragen:

- Wird verhindert, dass Benutzer durch den Befehl *xhost* + die rechnerspezifische Zugriffskontrolle abschalten?

M 4.10 Passwortschutz für TK-Endgeräte

Verantwortlich für Initiierung: TK-Anlagen-Verantwortlicher, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Endgeräte, insbesondere Telefone, können oft mit einem Passwortschutz versehen werden. Bei aktiviertem Passwortschutz stehen Leistungsmerkmale, wie Rufumleitung, Heranholen von Rufen etc. erst nach Eingabe des Passwortes zur Verfügung. Ohne die Kenntnis des Passwortes können in der Regel nur interne Gespräche geführt werden. Um einen Missbrauch dieser Leistungsmerkmale zu verhindern, sollte von dieser Möglichkeit des Passwortschutzes immer Gebrauch gemacht werden.

Ergänzende Kontrollfragen:

- Können TK-Endgeräte mit einem Passwortschutz versehen werden?
- Sind die Benutzer über die Möglichkeit des Passwortschutzes aufgeklärt worden?
- Wenn ja, wird diese Option in der Praxis genutzt?

M 4.11 Absicherung der TK-Anlagen-Schnittstellen

Verantwortlich für Initiierung: TK-Anlagen-Verantwortlicher, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Schnittstellen einer TK-Anlage, über die Administrationstätigkeiten ausgeführt werden können, stellen schützenswerte Punkte dar. Sie sollten daher besonders abgesichert werden. Über unbenutzte oder ungesicherte Schnittstellen können von Unbefugten, etwa unter Zuhilfenahme eines Laptops, Manipulationen am System durchgeführt werden. Der Passwortschutz auf einen TK-Bedienplatz oder PC-Gateway wäre in einem solchen Fall wirkungslos. Ziel ist es also, dies zu verhindern, zumindest aber den Versuch erkennbar zu machen. Aus diesem Grund sollten die benutzten Schnittstellen gut verschraubt und ggf. zusätzlich verplombt werden. Unbenutzte Schnittstellen können durch verschraubte und verplombte Abschlusskappen gesichert werden.

Ergänzende Kontrollfragen:

- Sind alle Schnittstellen bekannt, über die die TK-Anlage konfigurierbar ist?
- Existieren an der Anlage frei zugängliche Schnittstellen?
- Sind die vorhandenen Anschlusskabel mechanisch an beiden Enden gesichert?

M 4.12 Sperren nicht benötigter TK-Leistungsmerkmale

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, TK-Anlagen-Verantwortlicher, IT-Sicherheits-management

Verantwortlich für Umsetzung: Administrator

Der Umfang der verfügbaren Leistungsmerkmale sollte auf das notwendige Minimum beschränkt werden. Die Software nicht benötigter Leistungsmerk-male sollte, wenn möglich, von der Anlage entfernt werden. Da dies in vielen Fällen nicht möglich ist, können diese Leistungsmerkmale nur gesperrt (deaktiviert) werden. Von Zeit zu Zeit sollte überprüfte werden, ob diese Leistungsmerkmale auch wirklich gesperrt sind.

Ergänzende Kontrollfragen:

- Werden freigegebene Leistungsmerkmale auf ihren tatsächlichen Bedarf geprüft?
- Werden nicht genutzte und somit offensichtlich nicht erforderliche Leistungsmerkmale gesperrt?

M 4.13 Sorgfältige Vergabe von IDs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

In Unix-Systemen werden anhand von Benutzer- und Gruppenkennungen von Prozessen und Dateien unter anderem Verursacher von Aktionen festgestellt und Rechte vergeben. Daher ist eine sorgfältige Vergabe dieser Kennungen erforderlich.

Jeder Login-Name, jede Benutzer-ID (UID) und jede Gruppen-ID (GID) darf nur einmal vorkommen. Auch nach dem Löschen eines Benutzers bzw. einer Gruppe sollen Login-Name und UID bzw. GID für eine bestimmte Zeit nicht neu vergeben werden. Bei vernetzten Systemen muss auch system-übergreifend darauf geachtet werden, dass Benutzernamen und IDs nicht mehrfach vergeben werden. Dies ist insbesondere bei der Verwendung von NFS wegen der Umsetzung der UIDs wichtig, damit keine Daten unberechtigt gelesen werden können.

Jeder Benutzer muss Mitglied mindestens einer Gruppe sein. Jede in der Datei */etc/passwd* vorkommende GID muss in der Datei */etc/group* definiert sein.

Jede Gruppe sollte nur die Benutzer enthalten, die unbedingt notwendig sind. Dieses ist insbesondere für die Systemgruppen (wie *root*, *sys*, *bin*, *adm*, *news*, *uucp*, *nuucp* oder *daemon*) wichtig.

Logins mit UID 0 (*Super-User*) dürfen außer für den Systemadministrator *root* nur für administrative Logins nach vorher festgelegten Regeln vergeben werden (siehe M 2.33 *Aufteilung der Administrationstätigkeiten unter Unix*,).

Es ist sinnvoll, für Login-Namen und UIDs bzw. GIDs Namenskonventionen festzulegen. Weiterhin sollte regelmäßig überprüft werden, ob alle UIDs plausibel sind. Sie sollten also z. B. nur aus Ziffern stehen bzw. keine ungültigen Kombinationen wie 00 oder 000 enthalten.

Die Dateien */etc/passwd* und */etc/group* sollten nicht mit Editoren bearbeitet werden, da Fehler die Systemsicherheit stark beeinträchtigen können. Es sollten ausschließlich die entsprechenden Administrationstools benutzt werden, die allerdings sehr systemspezifisch sind.

Ergänzende Kontrollfragen:

- Nach welchen Regeln werden IDs vergeben?
- Werden die Dateien */etc/passwd* und */etc/group* regelmäßig auf Konsistenz überprüft?
- Stehen im UID-Feld von */etc/passwd* wirklich Ziffern?
- Sind alle UIDs plausibel?

M 4.14 Obligatorischer Passwortschutz unter Unix

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der Passwortschutz für jeden Account auf einem Unix-Rechner stellt sicher, dass nur ein berechtigter Benutzer sich unter seinem Login-Namen einloggen kann, indem nach Eingabe des Login-Namens eine Authentisierung durch Eingabe des Passworts erfolgt.

geeignete Version von passwd verwenden

Bei der Verwendung von Passwörtern für Benutzer und Gruppen sind die unter M 2.11 *Regelung des Passwortgebrauchs* beschriebenen Regeln zu beachten. Es muss beachtet werden, dass bei einigen Systemen nur eine begrenzte Zeichenanzahl bei der Passwort-Prüfung berücksichtigt wird. Zur Realisierung dieser Maßnahmen sollten nur Programmversionen von *passwd*, die die Einhaltung dieser Regeln sicherstellen, oder administrative Maßnahmen, z. B. Shellskripts und entsprechende *cron*-Einträge, benutzt werden.

Als weitere Möglichkeit kann auch das Unix-Standard-Kommando *passwd* durch andere Passwort-Programme mit erweiterter Funktionalität ersetzt werden. Dazu gehören auch die Public-Domain-Programme *anlpasswd*, *npasswd* und *passwd+*, die bereits beim Ändern des Passwortes durch den Benutzer das neu gewählte Passwort auf seine Güte testen und zurückweisen, wenn dieses zu schwach ist. Sie sind z. B. über den FTP-Server *ftp://ftp.cert.dfn.de/pub/tools/password/* erhältlich.

Die Passwörter sollen nicht in der allgemein lesbaren Datei */etc/passwd*, sondern in einer für die Benutzer nicht lesbaren *shadow*-Passwortdatei gespeichert sein. In jedem neueren Unix-System ist diese *shadow*-Möglichkeit enthalten, aber leider nach einer Erstinstallation nicht immer aktiviert (so muss z. B. unter RedHat Linux nach der Standardinstallation die Verwendung der *shadow*-Passwortdatei mit dem Befehl *pwconv* aktiviert werden).

Benutzer-Kennungen ohne Passwort sperren

Die Datei */etc/passwd* ist regelmäßig auf Benutzer-Kennungen ohne Passwort zu untersuchen. Wird eine solche gefunden, ist der Benutzer zu sperren. Ist für Gruppen Passwortzwang vereinbart worden, so ist entsprechend die Datei */etc/group* zu prüfen. Es empfiehlt sich jedoch, für Gruppen keine Passwörter zu vergeben und für jede Gruppe nur so wenig Benutzer wie möglich einzutragen. Das Wechseln zwischen Gruppen, in denen der Benutzer eingetragen ist, wird dadurch erleichtert, und unberechtigtes Wechseln durch systematisches Ausprobieren von Passwörtern mit Hilfe entsprechender Programme ist nicht möglich.

Alle Logins, insbesondere diejenigen mit UID 0, sollten regelmäßig auf das Vorhandensein und die Güte von Passwörtern getestet werden (siehe auch M 2.11 *Regelung des Passwortgebrauchs* und M 4.26 *Regelmäßiger Sicherheitscheck des Unix-Systems*). Neben den in M 4.26 *Regelmäßiger Sicherheitscheck des Unix-Systems* beschriebenen Programmen können diese Logins auch z. B. mit

```
awk -F: '{if ($3=="0") print $1}' /etc/passwd
awk -F: '{if ($2=="") print $1}' /etc/passwd
```

ermittelt werden.

Ergänzende Kontrollfragen:

- Wird die Benutzung von Passwörtern regelmäßig kontrolliert?
- Werden die Benutzer an der Wahl von schwachen Passwörtern gehindert (z. B. mit *anlpasswd*)?
- Wie lange sind die Passwörter gültig?

M 4.15 Gesichertes Login

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Es sollte ein Login-Programm verwendet bzw. Optionen aktiviert werden, so dass die folgenden Maßnahmen durchgeführt werden können:

- Jeder Benutzer muss eine eigene Kennung und ein eigenes Passwort erhalten. Es darf kein Zugang ohne Kennung oder Passwort möglich sein. Als Passwort-Ersatz kann die Authentisierung des Benutzers auch über elektronische Signaturen, Pass-Tickets oder Ähnliches erfolgen.
- Die Anzahl erfolgloser Login-Versuche wird beschränkt. Nach jedem erfolglosen Login-Versuch vergrößert sich die Wartezeit bis zur nächsten Login-Aufforderung. Nach einer bestimmten Anzahl von Fehlversuchen wird die betroffene Benutzer-Kennung und / oder das Terminal gesperrt. Dabei ist zu bedenken, dass dadurch nicht der Administrator ausgesperrt werden darf, es muss ihm an der Konsole eine Zugangsmöglichkeit offen bleiben.
- Der Zeitpunkt des letzten erfolgreichen Logins wird dem Benutzer beim Login gemeldet.
- Erfolglose Login-Versuche werden dem Benutzer beim Login gemeldet. Eventuell sollte diese Meldung bei mehreren darauf folgenden Anmeldungen wiederholt werden.
- Der Zeitpunkt des letzten Logouts wird dem Benutzer beim Login gemeldet. Hierbei wird zwischen Logouts zu einem interaktiven Login und solchen zu einem nicht-interaktiven Login (Logout von Hintergrundprozessen) unterschieden.
- Für das Login über Netze, in denen Passwörter unverschlüsselt übertragen werden, empfiehlt sich die zusätzliche Verwendung von Einmalpasswörtern (siehe auch M 5.34 *Einsatz von Einmalpasswörtern*).

Spezielle Hinweise zur Absicherung des Login-Vorgangs unter z/OS finden sich in der Maßnahme M 4.213 *Absichern des Login-Vorgangs unter z/OS*. **z/OS**

Ergänzende Kontrollfragen:

- Sind die Benutzer darauf hingewiesen worden, den Zeitpunkt des letzten erfolgreichen Logins auf Plausibilität zu überprüfen?
- Wie häufig werden erfolglose Login-Versuche dem Benutzer gemeldet?

M 4.16 Zugangsbeschränkungen für Accounts und / oder Terminals

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Sperre außerhalb der Arbeitszeit

Der Account und / oder das Terminal eines Benutzers sollen außerhalb der offiziellen Arbeitszeit gesperrt werden. Soweit das nicht mit vertretbarem Aufwand möglich ist (zum Beispiel bei sehr unregelmäßigen oder häufig wechselnden Arbeitszeiten), sollte die Sperrung zumindest zu den Zeiten erfolgen, die grundsätzlich außerhalb der Arbeitszeit liegen.

Beschränkung auf bestimmte IT-Systeme

Falls Mitarbeiter nur an einem bestimmten Terminal oder IT-System innerhalb des Netzes arbeiten, ist die Nutzung der Benutzer-Kennung und des dazugehörenden Passwortes auf diesen Rechner zu beschränken, so dass ein Einloggen von einem anderen Rechner aus ausgeschlossen ist. Insbesondere sollte sich der Administrator nach Möglichkeit nur von der Konsole aus anmelden. Dies kann auch technisch forciert werden (siehe auch M 4.21 *Verhinderung des unautorisierten Erlangens von Administratorrechten*).

Attributvergabe auf Gerätedateien

Unter Unix ist für Terminals der jeweilige Benutzer als Eigentümer des entsprechenden Gerätetreibers einzutragen. Sobald dieser sich ausgeloggt hat, sollte automatisch wieder *root* Eigentümer werden. Nur der jeweilige Benutzer sollte hierfür Leseberechtigung haben. Falls ein Benutzer Nachrichten (z. B. mit *talk*) von anderen Systembenutzern empfangen möchte, muss er ihnen Schreibberechtigung für den Gerätetreiber einräumen. Es ist zu überprüfen, ob dies unbedingt notwendig ist.

In PC-Netzen kann die Anzahl von gleichzeitigen Anmeldungen unter einem Account von mehreren PCs aus beschränkt werden. Zum Schutz vor dem unbemerktem Eindringen von Angreifern sollte verhindert werden, dass sich ein Benutzer an mehreren PCs gleichzeitig anmelden kann.

Ergänzende Kontrollfragen:

- Wurden Zeitfenster, d. h. temporäre Zugangsbeschränkungen, für alle Accounts und Terminals eingerichtet?

M 4.17 Sperren und Löschen nicht benötigter Accounts und Terminals

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Accounts, die über einen längeren Zeitraum nicht benutzt werden, sollten gesperrt und später gelöscht werden. Wenn beim Löschen von Accounts Dateien übrig bleiben, die keinem existierenden Benutzereintrag mehr zugeordnet sind, besteht die Gefahr, dass diese Dateien später eingerichteten Benutzern unberechtigt zugeordnet werden.

"verwaiste" Dateien finden

Beim Entfernen von Benutzern sind unter Unix die entsprechenden Einträge in */etc/passwd*, */etc/group* und das Heimatverzeichnis des Benutzers zu löschen. Ebenso ist darauf zu achten, dass weitere Benutzereinträge in Dateien wie */etc/hosts*, *shadow*, u. a. gelöscht werden. Die Daten des Heimatverzeichnisses sollten vorher gesichert werden. Bei der Sperrung bzw. auf jeden Fall vor dem Löschen eines Accounts sollte der betroffene Benutzer informiert werden. Beim Löschen von Accounts ist darauf zu achten, dass auch die Dateien des Benutzers gefunden werden, die nicht in seinem Heimatverzeichnis liegen. Dies kann z. B. mit dem Programm *find* und der Option *-uid* erfolgen. Solche Dateien müssen gelöscht oder anderen Benutzern zugeordnet werden. Weiterhin ist darauf zu achten, dass laufende Prozesse und noch anstehende Aufträge gelöscht werden, z. B. unter Unix in der *crontab*.

Ebenso sollten Terminals, die über einen längeren Zeitraum nicht benutzt werden, gesperrt und später entfernt werden.

Unter Unix sind vom System vorgegebene Logins (z. B. *sys*, *bin*, *adm*, *uucp*, *nuucp*, *daemon* und *lp*), die nicht benötigt werden, zu sperren, indem in das zugehörige Passwortfeld in der Datei */etc/passwd* z. B. "LOCKED" eingetragen wird.

Wenn ein neu einzurichtender Benutzer seinen Account nur für einen begrenzten Zeitraum benötigt, sollte dieser nur befristet eingerichtet werden.

Es kann vorteilhaft sein, Accounts grundsätzlich nur befristet einzurichten und in regelmäßigen Abständen (z. B. jährlich) bei Bedarf zu verlängern.

Ist absehbar, dass ein Benutzer eines lokalen Netzes längere Zeit abwesend ist (Urlaub, Krankheit, Abordnung, ...), so sollte sein Account für diese Zeit im Netz-Server gesperrt werden, so dass das Arbeiten unter seiner Benutzer-Kennung für diese Zeit nicht mehr möglich ist. Jeder Benutzer sollte dem Netzadministrator Zeiten längerer Abwesenheit mitteilen.

Ergänzende Kontrollfragen:

- Wie wird überprüft, welche Accounts länger nicht benutzt wurden?
- Wird überprüft, welche Accounts nicht mehr benötigt werden?
- Wird der Netzadministration mitgeteilt, dass ein Benutzer des Netzes für längere Zeit abwesend sein wird?
- Wird sichergestellt, dass alle Dateien und Verzeichnisse gelöschter Accounts anderen Benutzern zugeordnet oder gelöscht werden?

M 4.18 Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um das Aktivieren des Monitor-Modus und das Booten in den Single-User-Modus zu verhindern, sollten folgende Maßnahmen ergriffen werden:

- Wenn es (abhängig von der Unix-Variante und der zugrunde liegenden Hardware) möglich ist, muss zum Schutz des Unix-Servers ein BIOS-Passwort vergeben werden. **BIOS-Passwort**
- Beim Booten in den Single-User-Modus sollte das Super-User-Passwort abgefragt werden, um Unberechtigten den Zugang zum Unix-Server zu erschweren. **Super-User-Passwort**
- Wenn Tastaturschlösser vorhanden sind, sollten diese zum Schutz der Systemkonsole benutzt werden, um den Zugang zum Monitor-Modus zu verhindern. **Tastaturschlösser**

Diese Maßnahme wird ergänzt durch die Maßnahme M 4.21 Verhinderung des unautorisierten Erlangens von Administratorrechten.

Ergänzende Kontrollfragen:

- Ist der Zugriff auf die Konsole durch Passwörter oder andere Maßnahmen geschützt?

M 4.19 Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

indirekt aufgerufene Programme prüfen

Die hier genannten Maßnahmen gelten für Dateien und Verzeichnisse, für die der Administrator zuständig ist, das heißt für solche, die entweder für alle Benutzer von Bedeutung sind oder die Administrationszwecken dienen. Es reicht nicht aus, die Rechte eines Programms zu überprüfen, es muss auch die Rechtevergabe aller Programme überprüft werden, die von diesem Programm aus aufgerufen werden (insbesondere zur Vermeidung Trojanischer Pferde).

Die Attribute aller Systemdateien sollten möglichst so gesetzt sein, dass nur der Systemadministrator Zugriff darauf hat. Verzeichnisse dürfen nur die notwendigen Privilegien für die Benutzer zur Verfügung stellen.

s-Bit vermeiden

Das s-Bit sollte nur gesetzt sein, wenn unbedingt erforderlich. Bei Shellskripts soll das s-Bit nicht gesetzt sein. Das s-Bit darf nur vom Administrator gesetzt werden, die Notwendigkeit hierfür ist zu begründen und zu dokumentieren.

In Verzeichnissen, in denen alle Benutzer Schreibrechte haben müssen (z. B. */tmp*), sollte das t-Bit (Sticky-Bit) gesetzt sein.

Integrität prüfen

Die Integrität aller bei Unix-Systemdateien und -verzeichnissen gesetzten Attribute sollte regelmäßig verifiziert werden, z. B. mit *Tripwire* (siehe auch M 4.26 *Regelmäßiger Sicherheitscheck des Unix-Systems*).

Ergänzende Kontrollfragen:

- Wird die Attributvergabe bei Unix-Systemdateien regelmäßig überprüft?
- Gibt es Listen, anhand derer diese Überprüfungen durchgeführt werden?
- Ist das s-Bit nur dort gesetzt, wo es unbedingt erforderlich ist?

M 4.20 Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Die hier genannten Maßnahmen gelten für Dateien und Verzeichnisse eines Benutzers (incl. Mail-Dateien).

Fremdzugriffe verhindern

Die Benutzer sollten die Attribute ihrer Dateien und Verzeichnisse so setzen, dass andere Benutzer nicht darauf zugreifen können. Wenn anderen Benutzern der Zugriff erlaubt werden soll, sollten entsprechende Benutzergruppen eingerichtet werden.

Für benutzerspezifische Konfigurationsdateien wie *.profile*, *.exrc*, *.login*, *.cshrc* sollte nur der jeweilige Eigentümer Rechte besitzen.

Auf Unix-Systemen haben diverse Programme benutzerspezifische Konfigurationsdateien wie *.exrc*, *.emacs* oder *.mailrc*, die nach Programmaufruf automatisch durchlaufen werden und Variablen und Optionen für den Benutzer setzen. Damit in diesen keine trojanischen Pferde installiert werden können, sollte nur der jeweilige Eigentümer Zugriffsrechte besitzen.

Die Datei *.exrc* wird gelesen, bevor die Editoren *ex* oder *vi* gestartet werden. Falls sich eine gleichnamige Datei im aktuellen Verzeichnis befindet, wird diese bei einigen Unix-Versionen ausgewertet. Alle eingesetzten Unix-Versionen müssen daraufhin überprüft werden, da damit auch die Ausführung von Betriebssystemkommandos bei jedem Editoraufruf möglich ist.

s-Bit vermeiden

Das s-Bit sollte nur gesetzt sein, wenn unbedingt erforderlich. Bei Shellskripts soll das s-Bit nicht gesetzt sein. Das s-Bit sollte nur nach Einbeziehung des Administrators gesetzt werden, die Notwendigkeit hierfür ist zu begründen und zu dokumentieren.

umask

Mit *umask* (user file creation mode mask) wird für jeden Benutzer festgelegt, welche Attribute zur Regelung der Zugriffsrechte eine von ihm neu angelegte Datei erhält. In den benutzerspezifischen Konfigurationsdateien wie */etc/profile* oder den *$HOME/.profile*-Dateien sollte *umask* = 0027 (-rw-r-----) oder *umask* = 0077 (-rw-------) eingestellt sein, damit die Dateiattribute für neu angelegte Dateien nur dem Erzeuger (und evtl. der Gruppe) Zugriffsrechte geben.

Mail-Dateien

Integrität prüfen

Die Attribute der Mail-Dateien sollten regelmäßig daraufhin überprüft werden, ob nur der jeweilige Eigentümer auf die Dateien Zugriff hat. Die Integrität der bei den Unix-Benutzerdateien und -verzeichnissen gesetzten Attribute sollte regelmäßig verifiziert werden, z. B. mit *Tripwire* (siehe auch M 4.26 *Regelmäßiger Sicherheitscheck des Unix-Systems*).

Ergänzende Kontrollfragen:

- Sind die Benutzer über die Bedeutung einer minimalen Rechtevergabe informiert?
- Werden die gesetzten *umask*-Werte regelmäßig vom Administrator überprüft?
- Ist das s-Bit nur dort gesetzt, wo es unbedingt erforderlich ist?

M 4.21 Verhinderung des unautorisierten Erlangens von Administratorrechten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Zugriffe auf su beschränken

Durch den Befehl *su* kann jeder Benutzer Super-User-Rechte erlangen, wenn er das entsprechende Passwort besitzt. Da die Anzahl fehlerhafter Versuche bei *su* nicht beschränkt ist, besteht ein erhöhtes Risiko, dass das Passwort durch systematisches Probieren mit Hilfe entsprechender Programme herausgefunden wird. Deshalb sollte *su* nur für den Super-User zugänglich sein. Alternativ könnte ein modifiziertes *su* installiert werden, bei dem die Anzahl erfolgloser Versuche beschränkt ist, sich die Wartezeit bis zur nächsten *su*-Aufrufmöglichkeit nach jedem erfolglosen Login-Versuch vergrößert und nach einer bestimmten Anzahl von Fehlversuchen die Ausführmöglichkeit und / oder das Terminal gesperrt wird. Jede Verwendung des Befehls *su* sollte protokolliert werden.

Wenn das System es zulässt, kann der Login-Name des Super-Users anders als *root* genannt werden. Als zusätzliche Super-User-Logins sollten aber nur administrative Logins (siehe M 2.33 *Aufteilung der Administrationstätigkeiten unter Unix*) geschaffen werden.

nur an der Konsole administrieren

Der Administrator darf nur von der Konsole aus arbeiten, um zu verhindern, dass bei einem Abhören der Leitung sein Passwort bekannt wird. Unter Solaris kann dies beispielsweise erreicht werden, indem die Datei */etc/default/login* entsprechend konfiguriert wird. Alternativ können Sicherheitsfunktionen verwendet werden, die das Ausspähen von Administratorpasswörtern verhindern. Beispiele für geeignete Mechanismen sind Secure Shell (siehe Maßnahme M 5.64 *Secure Shell*) und Einmalpasswörter (siehe Maßnahme M 5.34 *Einsatz von Einmalpasswörtern*).

Bei BSD-Unix kann sich *root* nur an Terminals einloggen, die in der Datei */etc/ttytab* als *secure* gekennzeichnet sind. Ist diese Option für alle Terminaleinträge entfernt, kann sich ein Administrator an einem Terminal nur mit dem Kommando *su* als *root* einloggen. Es sollte überlegt werden, eine Benutzergruppe einzurichten, auf die die Ausführung des Kommandos *su* beschränkt ist.

Konsole nicht als secure kennzeichnen

Ist bei BSD-Unix die Konsole in der Datei */etc/ttytab* als *secure* gekennzeichnet, wird kein Passwort beim Hochfahren in den Single-User-Modus abgefragt, daher muss dieser Eintrag unbedingt entfernt werden.

ftp für administrative Zugänge verbieten

Die Datei */etc/ftpusers* enthält die Login-Namen, die sich nicht per ftp anmelden dürfen. Bei ftp werden die Passwörter über eine ungeschützte Klartextverbindung übertragen. Daher sollten administrative Zugänge (*root, bin, daemon, sys, adm, lp, smtp, uucp, nuucp, etc.*) hier eingetragen werden. Bei einigen Standardinstallationen steht root nicht in dieser Datei.

s-Bit vermeiden

Wenn ein Benutzer bzw. ein Benutzer-Programm eine Super-User-Datei (Dateien mit Eigentümer root und gesetztem s-Bit) ausführt, erhält dieser Benutzer bzw. dieses Programm bei der Ausführung Super-User-Rechte. Das

ist für bestimmte Anwendungen erforderlich, kann aber unter Umständen auch missbräuchlich benutzt werden. Deshalb ist darauf zu achten, dass nur die notwendigsten Programmdateien Super-User-Dateien sind und keine weiteren Super-User-Dateien von Dritten hinzugefügt werden.

Automatisches Mounten von Geräten für austauschbare Datenträger:

automatisches Mounten vermeiden

Mit sich auf dem gemounteten Laufwerk befindenden s-Bit-Programmen kann ein Benutzer Super-User-Rechte erlangen. Automatisches Mounten sollte daher restriktiv gehandhabt werden. Manche Unix-Versionen bieten eine Option des *mount*-Befehls, der dazu führt, dass das s-Bit für das entsprechende Filesystem ignoriert wird. Bei austauschbaren Datenträgern sollte überlegt werden, diese Option anzuwenden.

Bei der Freigabe von Verzeichnissen, die von anderen Rechnern gemountet werden dürfen, sind die unter M 5.17 *Einsatz der Sicherheitsmechanismen von NFS* beschriebenen Einschränkungen zu beachten. Es sollten insbesondere keine Verzeichnisse mit *root*-Rechten und nur bei Bedarf Verzeichnisse mit Schreibrechten freigegeben werden.

Diese Maßnahme wird ergänzt durch die Maßnahme M 4.18 *Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus*.

Ergänzende Kontrollfragen:

- Ist der Befehl *su* nur für den Administrator ausführbar?
- Wird die Verwendung des Befehls *su* automatisch protokolliert?
- Wer hat Schreibzugriff auf die entsprechenden Konfigurationsdateien?

M 4.22 Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Zugriff auf Kommandos beschränken

Mit Unix-Befehlen wie *ps*, *finger*, *who, last* lassen sich Informationen über einen Benutzer (z. B. Arbeitsverhalten) ermitteln. Viele Unix-Derivate enthalten dazu noch weitere Befehle wie z. B. *listusers* unter Solaris. Es ist zu überlegen, ob das Ausführen dieser Befehle für jeden Benutzer erlaubt sein soll (Datenschutz, Ausspähen von Login-Namen und Ähnlichem.). Im Zweifelsfall sollte der Zugriff auf diese Befehle beschränkt werden.

Passwörter nicht als Kommandoparameter übergeben

Beim Aufruf von Kommandos dürfen keine sensitiven Informationen als Parameter mit eingegeben werden, wie z. B. ein Passwort, da andere Benutzer mit *ps* diese Angaben sehen können.

Die Protokolldateien wie *wtmp, utmp, wtmpx, utmpx,* etc. sollten nach Möglichkeit durch geeignete Zugriffsrechte vor unbefugtem Auslesen geschützt werden, da hieraus eine Vielzahl von Informationen über die Benutzer herausgelesen werden kann.

M 4.23 Sicherer Aufruf ausführbarer Dateien

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator, Benutzer

Ausführbare Dateien können direkt gestartet werden. Im Gegensatz hierzu können Anwendungsdaten, wie Textdateien, nur über ein entsprechendes Programm angesehen werden. Unter Windows sind ausführbare Dateien an ihrer Dateiendung (beispielsweise .exe, .com, .vbs, .bat, .cmd) und unter Unix durch Dateirechte (x-Flag) erkennbar.

Es muss sichergestellt werden, dass nur freigegebene Versionen ausführbarer Dateien und keine eventuell eingebrachten modifizierten Versionen (insbesondere Trojanische Pferde) aufgerufen werden (siehe M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*).

Ein Angreifer könnte eine ausführbare Datei soweit verändern, dass er die Privilegien des Benutzers erhält, der die Datei ausführt. Um dies zu verhindern, dürfen ausführbare Dateien nur lesbar sein. Ein Schreibzugriff darf nur Administratoren gestattet werden.

Ausführbare Dateien für die Schreibrechte benötigt werden, z. B. weil sie sich in der Entwicklung befinden, dürfen nur in separaten Bereichen verwendet werden. Dasselbe gilt für neue Software, die für einen späteren Einsatz auf einem Produktivsystem getestet werden soll. Hierfür können beispielsweise separate Testsysteme eingesetzt werden oder spezielle Benutzerkonten ohne weitere Privilegien. Nur so kann verhindert werden, dass diese Applikationen Schaden anrichten.

Auch bereits getestete Software kann die Sicherheit beeinträchtigen. Dies betrifft vor allem sehr komplexe Anwendungen wie zum Beispiel Webserver. Schon beim Start von Anwendungen muss sichergestellt werden, dass jeder Prozess nur so viele Rechte erhält wie unbedingt notwendig sind. So kann bei einem erfolgreichen Angriff der eintretende Schaden begrenzt werden. Diese Dienste dürfen, wenn möglich, nicht mit Administrator-Rechten gestartet werden. Hierfür eignen sich ebenfalls Benutzerkonten mit eingeschränkten Privilegien. Über klare Trennungen von Rechten, unter Unix oder Linux beispielsweise durch *chroot*-Umgebungen, die den eintretenden Schaden begrenzen können, muss nachgedacht werden.

Im Weiteren muss sichergestellt werden, dass nur die gewünschte, freigegebene Version ausgeführt werden kann. Ein Angreifer könnte sonst eine modifizierte Datei mit dem selben Namen in ein Verzeichnis kopieren, auf das er Schreibrechte hat. Wird beim Aufruf in den Verzeichnissen nach der Datei gesucht, könnte die modifizierte statt die gewünschte Datei ausgeführt werden.

Bei vielen Betriebssysteme werden die Verzeichnisse, in denen nach den ausführbaren Dateien gesucht werden soll, in der entsprechenden Reihenfolge in der *PATH*-Variable eingetragen. Die Anzahl der angegebenen Verzeichnisse sollte gering und überschaubar gehalten werden. Relative Verzeichnisangaben, die das jeweils aktuelle Arbeitsverzeichnis enthalten, dürfen als Angabe in der *PATH*-Variable nicht enthalten sein. Ausführbare Dateien sollen nur in dafür vorgesehenen Verzeichnissen gespeichert sein. In

den in einer *PATH*-Variable enthaltenen Verzeichnissen darf nur der jeweilige Eigentümer Schreibrechte erhalten. Dies muss regelmäßig überprüft werden.

Ergänzende Kontrollfragen:

- Werden die *PATH*-Einträge regelmäßig überprüft?
- Befinden sich ausführbare Dateien verstreut im System?
- Sind die Regelungen für ausführbare Dateien den Benutzern bekannt?
- Wird die Integrität der ausführbaren Dateien regelmäßig verifiziert?

M 4.24 Sicherstellung einer konsistenten Systemverwaltung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator

In vielen komplexen IT-Systemen, z. B. unter Unix oder in einem Netz, gibt es eine Administratorrolle, die keinerlei Beschränkungen unterliegt. Unter Unix ist das der Super-User *root,* in einem Novell-Netz der *SUPERVISOR* bzw. *admin*. Durch fehlende Beschränkungen ist die Gefahr von Fehlern oder Missbrauch besonders hoch.

nicht unter Super-User-Login arbeiten

Um Fehler zu vermeiden, soll unter dem Super-User-Login nur gearbeitet werden, wenn es notwendig ist; andere Arbeiten soll auch der Administrator nicht unter der Administrator-Kennung erledigen. Insbesondere dürfen keine Programme anderer Benutzer unter der Administrator-Kennung aufgerufen werden. Ferner sollte die routinemäßige Systemverwaltung (zum Beispiel Backup, Einrichten eines neuen Benutzers) nur menügesteuert durchgeführt werden können.

Absprache unter den Administratoren

Durch Aufgabenteilung, Regelungen und Absprache ist sicherzustellen, dass Administratoren keine inkonsistenten oder unvollständigen Eingriffe vornehmen. Zum Beispiel darf eine Datei nicht gleichzeitig von mehreren Administratoren editiert und verändert werden, da dann nur die zuletzt gespeicherte Version erhalten bleibt.

Secure Shell verwenden

Wenn die Gefahr des Abhörens von Leitungen zu Terminals besteht, sollte der Administrator nur an der Konsole arbeiten, damit keine Passwörter abgehört werden können. Bei der Administration von Unix-Systemen kann eine verschlüsselte Kommunikation mit dem Protokoll Secure Shell erfolgen. Hiermit ist eine gesicherte Administration von entfernten Arbeitsstationen aus möglich (siehe auch M 5.64 *Secure Shell*).

Für alle Administratoren sind zusätzliche Benutzer-Kennungen einzurichten, die nur über die eingeschränkten Rechte verfügen, die die Administratoren zur Aufgabenerfüllung außerhalb der Administration benötigen. Für Arbeiten, die nicht der Administration dienen, sollen die Administratoren ausschließlich diese zusätzliche Benutzer-Kennungen verwenden.

Änderungen dokumentieren

Alle durchgeführten Änderungen sollten dokumentiert werden, um diese nachvollziehbar zu machen und die Aufgabenteilung zu erleichtern (siehe auch M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*). Für die nachträgliche Überprüfung durchgeführter Administratortätigkeiten kann mit dem Unix-Befehl *script* ein Protokoll der eingebenen Befehle angefertigt werden. Dieser Befehl protokolliert die gesamte Terminal-Sitzung in einer ASCII-Datei. Solch eine Datei kann dann bei Bedarf einem elektronischen oder ausgedruckten Administrations-Journal beigefügt werden.

Ergänzende Kontrollfragen:

- Wie ist sichergestellt, dass Eingriffe des Administrators nicht zu Inkonsistenzen führen?
- Werden vor größeren Eingriffen Backups gefahren?
- Haben die Administratoren zusätzliche Benutzer-Kennungen mit eingeschränkten Rechten?
- Werden standardmäßig die zusätzlichen Benutzer-Kennungen benutzt?
- Wird ein Administrations-Journal geführt? Werden dort alle Änderungen dokumentiert?

M 4.25 Einsatz der Protokollierung im Unix-System

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Protokollmöglichkeiten des einzelnen Unix-Systems sind einzusetzen und gegebenenfalls durch Programme oder Shellskripts zu ergänzen.

Folgende Maßnahmen sollen ergriffen werden:

regelmäßige Auswertung

- Die Protokoll-Dateien müssen regelmäßig ausgewertet werden. Die Auswertung sollte nicht immer zum selben Zeitpunkt erfolgen, um zu verhindern, dass ein Angreifer diese Tatsache ausnutzt. Wenn z. B. der Administrator jeden Tag um 17.00 Uhr die Systemaktivitäten überprüft, kann ein Angreifer um 18.00 Uhr unbemerkt tätig werden.

automatische Alarmierung

- Je nach Art der protokollierten Ereignisse kann es erforderlich sein, schnellstmöglich einzugreifen. Damit der Administrator über solche Ereignisse (z. B. Protokolldatei zu groß, wichtige Serverprozesse abgebrochen, mehrfach versuchte *root*-Logins während ungewöhnlicher Tageszeiten, etc.) automatisch informiert wird, sollten halbautomatische Logfileparser für die Alarmierung eingesetzt werden (z. B. *swatch*, *logsurfer* oder *checksyslog*).
- Soweit erforderlich, sollten die Protokolldateien gesichert werden, bevor sie zu groß oder vom System gelöscht werden. Es ist zu prüfen, welche gesetzlichen oder vertraglichen Aufbewahrungsfristen beachtet werden müssen.
- Informationen aus Dateien wie *wtmp*, *utmp*, *wtmpx*, *utmpx*, etc. sollten mit Skepsis betrachtet werden, da diese Dateien leicht zu manipulieren sind.
- Die Datei-Attribute der Protokolldateien sollten so gesetzt sein, dass Unberechtigte keine Änderungen oder Auswertungen der Protokolle vornehmen können.
- Folgende Protokolldateien sollten mindestens erstellt und kontrolliert werden: Logins (auch Fehlversuche), Aufruf von *su*, Fehlerprotokollierungsdatei / Protokollierung wichtiger Vorgänge (*errorlog*), Administratortätigkeiten (insbesondere von *root* ausgeführte Befehle). Weitere Einzelheiten finden sich in M 4.106 *Aktivieren der Systemprotokollierung*.

  Der Befehl *last* zeigt Login- und Logout-Informationen wie Zeitpunkt und Terminal für jeden Benutzer an. Der Administrator sollte mit diesem Befehl regelmäßig überprüfen, ob sich Benutzer auf ungewöhnlichem Weg anmelden, z. B. über Modemleitungen oder über FTP.

dedizierter Loghost

Wenn auf vielen Systemen Protokolldaten anfallen sollten, empfiehlt sich der Einsatz eines dedizierten Loghosts, der besonders abgesichert ist. Das Weiterleiten (Forward) der Syslog-Meldungen auf diesen Loghost muss in der Syslog-Konfigurationsdatei aktiviert werden (siehe M 4.106 *Aktivieren der Systemprotokollierung)*.

Die anfallenden Protokolldaten dürfen nur benutzt werden, um die ordnungsgemäße Anwendung der IT-Systeme zu kontrollieren, nicht für andere Zwecke, insbesondere nicht zur Erstellung von Leistungsprofilen von Benutzern (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*).

Ergänzende Kontrollfragen:

- Werden die Protokolldateien regelmäßig ausgewertet?
- Ist die Protokollierung noch aktiv und ausreichender Speicherplatz vorhanden?
- Wird die Integrität der Konfigurationsdateien für die Protokollierung regelmäßig verifiziert und protokolliert (z. B. mit *Tripwire*)?
- Wie werden die Protokolldateien archiviert und gegen Manipulation und unbefugte Einsichtnahme geschützt?

M 4.26 Regelmäßiger Sicherheitscheck des Unix-Systems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Tools verwenden

Unix-Betriebssysteme bieten standardmäßig verschiedene Sicherheitseigenschaften an. Diese können jedoch nur zum Erfolg führen, wenn sie sinnvoll eingesetzt werden. Die hierfür notwendigen Einstellungen sollen mit Hilfe von Tools automatisiert überprüft werden, um

- Inkonsistenzen innerhalb eines Unix-Systems erkennen und beseitigen zu können und
- den Systemverwalter in die Lage zu versetzen, das Unix-Betriebssystem unter optimaler Ausnutzung der gegebenen Sicherheitsmechanismen zu verwalten.

Diese Prüfung kann mit im Unix-System vorhandenen Programmen, selbsterstellten Shellskripts oder Public-Domain-Programmen erfolgen. Für einige Unix-Varianten sind auch kommerzielle Programme verfügbar.

Beispiele:

- **pwck**

  Dieser Befehl gehört zu den Standard-Betriebssystemkommandos. Mit diesem Befehl nimmt man eine Konsistenzprüfung der Datei */etc/passwd* vor. Es wird überprüft, ob alle notwendigen Einträge vorgenommen wurden, ob das Login-Verzeichnis für den Benutzer existiert und ob das Login-Programm vorhanden ist. Ähnliche Funktionen beinhaltet unter Solaris der Befehl *logins*, mit dem auch Accounts ohne Passwort gefunden werden können.

- **grpck**

  Mit diesem Befehl nimmt man eine Konsistenzprüfung der Datei */etc/group* vor. Er gehört ebenfalls zu den Standard-Betriebssystemkommandos. Es wird überprüft, ob alle notwendigen Einträge vorgenommen wurden, ob alle Mitglieder einer Gruppe auch in der Benutzerpasswortdatei vorhanden sind und ob die Gruppennummer mit der dort angegebenen übereinstimmt.

- **tripwire**

  Mit diesem Programm können Integritätsprüfungen von Dateien durchgeführt werden. Dazu werden Prüfsummen über Dateien gebildet und in einer Datenbank gespeichert. *tripwire* ist in verschiedenen kostenlosen Versionen verfügbar.

- **cops**

  Dieses Public-Domain-Programm dient zur Überprüfung der Sicherheit von Unix-Systemen, z. B. werden verschiedene Systemeinstellungen, Zugriffsrechte, SUID-Dateien etc. überprüft und potentielle Sicherheitslücken aufgezeigt.

- **tiger**

  Mit diesem Public-Domain-Programm können Unix-Systeme ähnlich wie mit *cops* auf Sicherheitslücken überprüft werden.

- **SATAN**

  Mit diesem Public-Domain-Programm kann die Netz-Sicherheit analysiert werden. Es überprüft vernetzte Unix-Systeme auf bekannte, aber oftmals nicht beseitigte Schwachstellen.

- **crack**

  Mit diesem Public-Domain-Programm überprüft man, ob zu einfache, leicht erratbare Passwörter vorhanden sind.

Ergänzende Kontrollfragen:

- Werden die Durchführung und die Ergebnisse des Sicherheitschecks dokumentiert?
- Welche Schwachstellen werden durch die eingesetzten Programme und Shellskripts überprüft?

M 4.27 Zugriffsschutz am Laptop

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Jeder Laptop sollte mit einem Zugriffsschutz versehen werden, der verhindert, dass dieser unberechtigt benutzt werden kann. Bei Laptops sollte als Minimalschutz, wenn kein anderer Sicherheitsmechanismus vorhanden ist, der BIOS-Bootschutz aktiviert werden, wenn dessen Nutzung möglich ist. Erst nach Eingabe des korrekten Bootpasswortes wird der Rechner dann hochgefahren. Die im Umgang mit Passwörtern zu beachtenden Regeln sind in M 2.11 *Regelung des Passwortgebrauchs* aufgeführt worden.

Außerdem bieten nahezu alle Betriebssysteme die Möglichkeit, Anmeldepasswörter einzurichten und diese mit geeigneten Restriktionen zu versehen (z. B. Mindestlänge, Lebensdauer, etc.). Da diese Bordmittel nur eine begrenzte Sicherheit bieten, empfiehlt es sich bei Laptops, auf denen sich schnell große Mengen sensitiver Daten sammeln, zusätzliche Sicherheitshard- oder -software einzusetzen. Dazu gehören beispielsweise Chipkarten oder Token, die die Authentikation absichern.

Ist keine Passwortroutine installiert, sollte, wenn keine Verschlüsselung der Daten erfolgt, die Speicherung von schutzbedürftigen Daten auf der Festplatte verboten und deren Speicherung stattdessen nur auf mobilen Datenträgern, also z. B. Disketten oder USB-Sticks, zugelassen werden. Diese sind dann getrennt vom Laptop aufzubewahren, zum Beispiel in der Brieftasche.

Bei kurzen Arbeitsunterbrechungen muss unbedingt ein Zugriffsschutz aktiviert werden, z. B. ein Bildschirmschoner. Ist es absehbar, dass die Unterbrechung länger dauert, ist der Laptop auszuschalten.

Ergänzende Kontrollfragen:

- Ist ein angemessener Zugriffschutz für die Laptops vorhanden? Werden die Regeln für den korrekten Umgang mit dem Zugriffschutz eingehalten?
- Wird bei der Übergabe eines Laptops das Passwort gewechselt?

M 4.28 Software-Reinstallation bei Benutzerwechsel eines Laptops

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Wechselt der Benutzer eines Laptops, so muss sichergestellt sein, dass auf diesem weder schutzbedürftige Daten noch Computer-Viren vorhanden sind. Die Löschung von Daten kann durch vollständiges Überschreiben oder mit Hilfe spezieller Löschprogramme vorgenommen werden. Ein aktuelles Viren-Suchprogramm muss anschließend zum Einsatz kommen. Beide Vorgänge müssen für alle benutzten Datenträger wie Festplatte, Disketten, CDs oder USB-Sticks durchgeführt werden.

Es empfiehlt sich jedoch, die Festplatte des tragbaren PC neu zu formatieren und anschließend die erforderliche Software und Daten neu aufzuspielen. Was hierbei zu beachten ist, ist in M 4.235 *Abgleich der Datenbestände von Laptops* beschrieben.

Ergänzende Kontrollfrage:

- Wird vor der Formatierung sichergestellt, dass der vorhergehende Benutzer keinerlei Daten vom Laptop mehr benötigt?

M 4.29 Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Um zu verhindern, dass aus einem trotz aller Vorsichtsmaßnahmen gestohlenen tragbaren IT-System schutzbedürftige Daten ausgelesen werden können, sollte ein Verschlüsselungsprogramm eingesetzt werden. Mit Hilfe der marktgängigen Produkte ist es möglich, einzelne Dateien, bestimmte Bereiche oder die ganze Festplatte so zu verschlüsseln, dass nur derjenige, der über den geheimen Schlüssel verfügt, in der Lage ist, die Daten zu lesen und zu gebrauchen.

Die Sicherheit der Verschlüsselung hängt dabei von drei verschiedenen Punkten zentral ab:

- Der verwendete Verschlüsselungsalgorithmus muss so konstruiert sein, dass es ohne Kenntnis des verwendeten Schlüssels nicht möglich ist, den Klartext aus dem verschlüsselten Text zu rekonstruieren. Nicht möglich bedeutet dabei, dass der erforderliche Aufwand zum Brechen des Algorithmus bzw. zum Entschlüsseln in keinem Verhältnis steht zum dadurch erzielbaren Informationsgewinn.
- Der Schlüssel ist geeignet zu wählen. Nach Möglichkeit sollte ein Schlüssel zufällig erzeugt werden. Wenn es möglich ist, einen Schlüssel wie ein Passwort zu wählen, sollten die diesbezüglichen Regeln aus M 2.11 *Regelung des Passwortgebrauchs* beachtet werden.
- Der Verschlüsselungsalgorithmus (das Programm), der verschlüsselte Text und die Schlüssel dürfen nicht zusammen auf einem Datenträger gespeichert werden. Es bietet sich an, den Schlüssel einzeln aufzubewahren. Dies kann dadurch geschehen, dass er auf einer Pappkarte in Form einer Scheckkarte aufgeschrieben und anschließend wie eine Scheckkarte im Portemonnaie aufbewahrt wird. Die kryptographischen Schlüssel sollten auf einem auswechselbaren Datenträger wie z. B. auf Diskette, Chipkarte oder USB-Stick gespeichert werden und getrennt vom tragbaren IT-System aufbewahrt werden (z. B. in der Brieftasche).

Eine Verschlüsselung kann online oder offline vorgenommen werden. Online bedeutet, dass sämtliche Daten der Festplatte (bzw. einer Partition) verschlüsselt werden, ohne dass der Benutzer dies aktiv veranlassen muss. Eine Offline-Verschlüsselung wird explizit vom Benutzer initiiert. Er muss dann auch entscheiden, welche Dateien verschlüsselt werden sollen. Zur Auswahl und Nutzung von kryptographischen Verfahren sollte auch Baustein B 1.7 *Kryptokonzept* beachtet werden.

Für den Bereich der öffentlichen Verwaltung kann das BSI für den Einsatz auf stationären und tragbaren PCs ein Offline-Verschlüsselungsprogramm unter gewissen Randbedingungen zur Verfügung stellen, das den Sicherheitsanforderungen im Bereich des normalen Schutzbedarfs genügt.

Ergänzende Kontrollfragen:

- Werden die Benutzer im Umgang mit dem Verschlüsselungsprogramm geschult?
- Werden Daten und Schlüssel getrennt aufbewahrt?

M 4.30 Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Einige der Standardprodukte im PC-Bereich bieten eine Reihe von nützlichen IT-Sicherheitsfunktionen, deren Güte im einzelnen unterschiedlich sein kann, aber Unbefugte behindern bzw. mögliche Schäden verringern. Im folgenden seien fünf dieser Funktionen kurz erläutert:

- Passwortschutz bei Programmaufruf: das Programm kann nur gestartet werden, wenn vorher ein Passwort korrekt eingegeben wurde. Dies verhindert die unberechtigte Nutzung des Programms.
- Zugriffsschutz zu einzelnen Dateien: das Programm kann nur dann auf eine geschützte Datei zugreifen, wenn das mit dieser Datei verknüpfte Passwort korrekt eingegeben wird. Dies verhindert den unerlaubten Zugriff mittels des Programms auf bestimmte Dateien.
- Automatische Speicherung von Zwischenergebnissen: das Programm nimmt eine automatische Speicherung von Zwischenergebnissen vor, so dass ein Stromausfall nur noch die Datenänderungen betrifft, die nach dieser automatischen Speicherung eingetreten sind.
- Automatische Sicherung der Vorgängerdatei: wird eine Datei gespeichert, zu der im angegebenen Pfad eine Datei gleichen Namens existiert, so wird die zweite Datei nicht gelöscht, sondern mit einer anderen Kennung versehen. Damit wird verhindert, dass versehentlich eine Datei gleichen Namens gelöscht wird.
- Verschlüsselung von Dateien: das Programm ist in der Lage, eine Datei verschlüsselt abzuspeichern, so dass eine unbefugte Kenntnisnahme verhindert werden kann. Die Inhalte der Datei sind damit nur denjenigen zugänglich, die über den verwendeten geheimen Kryptierschlüssel verfügen.
- Automatisches Anzeigen von Makros in Dateien: diese Funktion soll das unbeabsichtigte Ausführen von Makros verhindern (Makro-Viren).

Je nach eingesetzter Software und damit vorhandenen Zusatzsicherheitsfunktionen kann der Einsatz dieser Funktionen sinnvoll sein. Für mobil eingesetzte IT-Systeme bietet sich insbesondere die Nutzung des Passwortschutzes bei Programmaufruf und die automatischen Speicherung an.

Ergänzende Kontrollfragen:

- Welche Sicherheitsfunktionen bieten die eingesetzten Softwareprodukte?
- Welche dieser Funktionen werden regelmäßig genutzt?
- Werden die Benutzer auf diese Funktionen hingewiesen?
- Werden die sicherheitsrelevanten Hinweise in Handbüchern oder Zertifizierungsreports beachtet?

M 4.31 Sicherstellung der Energieversorgung im mobilen Einsatz

Verantwortlich für Initiierung: Benutzer

Verantwortlich für Umsetzung: Benutzer

Um die Energieversorgung eines tragbaren PC oder PDAs auch im mobilen Einsatz aufrechterhalten zu können, werden üblicherweise Akkus oder Batterien eingesetzt. Je nach Kapazität des Akkus bzw. der Batterie und Bauweise des mobilen Endgerätes reicht dies für einen beschränkten Zeitraum, z. B. einige Stunden, aus. Damit nach Abfall der Betriebsspannung keine Daten in flüchtigen Speichern verloren gehen, sollten einige Randbedingungen eingehalten werden:

- Die Warnanzeigen des mobilen Endgerätes (falls vorhanden), die den Spannungsabfall anzeigen, dürfen nicht ignoriert werden. Die Warnanzeigen sollten so konfiguriert sein, dass nach der ersten Warnung noch genügend Zeit vorhanden ist, um eine Datensicherung durchzuführen.
- Falls es absehbar ist, dass der mobile Einsatz längerfristig ist, sind aufladbare Batterien vorher nachzuladen und ggf. geladene Ersatzbatterien mitzuführen.
- Gerade bei älteren Akkus sind die Gebrauchzeiten verkürzt und die Entladung gegen Ende der Kapazität kann sehr schnell erfolgen. Beim Betrieb müssen daher regelmäßige Datensicherungen durchgeführt werden, um Datenverlust zu vermeiden. Da sich solche Akkus auch im Stand-by-Modus schnell entladen können, sollte der Ladezustand regelmäßig kontrolliert und Sicherungen der Konfigurationsdaten des Laptops oder PDAs für den Notfall mitgeführt werden. Ein baldiger Austausch des Akkus gegen einen neuwertigen ist empfehlenswert, sobald solche Alterserscheinungen auftreten.
- Beim Laden sollten die Hinweise im Handbuch des mobilen IT-Systems beachtet werden, damit die Lebensdauer des Akkus nicht beeinträchtigt wird.
- Vor einer Reise bzw. bei der Übergabe eines mobilen IT-Systems ist der ausreichende Ladezustand der Akkus oder Batterien sicherzustellen. Der Ladezustand der Akkus sollte regelmäßig überprüft werden, da sich ein Akku im Laufe der Zeit entlädt, auch wenn er nicht verwendet wird.

Ladezustand regelmäßig überprüfen

- Das Ladenetzteil sollte optional mitgeführt werden.

Es empfiehlt sich darüber hinaus, während der Nutzung des mobilen IT-Systems in kurzen Abständen die verarbeiteten Daten auf einem nichtflüchtigen Medium zu speichern. Dazu können auch automatische Datensicherungen in Standardprogrammen benutzt werden.

Kurzschlüsse am Akku vermeiden

Wenn eine längere Nutzung des mobilen IT-Systems absehbar ist, z. B. bei Dienstreisen, sollte ein geladener Ersatzakku mitgeführt werden. Der Ersatzakku sollte in einer Schutzhülle verwahrt werden, da Schäden durch Überhitzung oder Brand entstehen können, wenn die Kontakte des Akkus mit

leitenden Materialien in Berührung kommen. Dies kann durch viele Gegenstände des täglichen Gebrauchs wie Schlüssel oder Ketten verursacht werden.

Jede Art IT-System sollte ausgeschaltet werden, bevor der Akku gewechselt wird, damit der Speicher nicht beschädigt wird.

Hinweis:

stationärer Einsatz

Der schlechteste Aufbewahrungsort für Akkus (vor allem Lithium-Ionen-Akkus) ist der angeschaltete Laptop im stationären Einsatz, also solange dieser ohnehin über eine Steckdose mit dem Stromnetz verbunden ist. Beim Betrieb in einer Dockingstation sollte der Akku also möglichst vorher herausgenommen werden.

Ergänzende Kontrollfrage:

- Sind die Benutzer über den optimalen Umgang mit Akkus aufgeklärt?

M 4.32 Physikalisches Löschen der Datenträger vor und nach Verwendung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Verfahrensverantwortlicher

Neben den in Maßnahme M 2.167 *Sicheres Löschen von Datenträgern* enthaltenen Hinweisen zur Löschung oder Vernichtung von Datenträgern sind für den Datenträgeraustausch folgende Punkte zu beachten:

Magnetische Datenträger, die für den Austausch bestimmt sind, sollten vor dem Beschreiben mit den zu übermittelnden Informationen physikalisch gelöscht werden. Es soll damit sichergestellt werden, dass keine Restdaten weitergegeben werden, für deren Erhalt der Empfänger keine Berechtigung besitzt.

Eine für den normalen Schutzbedarf ausreichende physikalische Löschung kann erreicht werden, indem der komplette Datenträger oder zumindest die genutzten Bereiche mit einem bestimmten Muster überschrieben werden. Möglich ist auch eine Formatierung des Datenträgers, wenn diese nicht wieder rückgängig gemacht werden kann. Es sollte vermieden werden, nur einzelne Dateien zu löschen, hierbei bleiben häufig Restinformationen erhalten, die die Rekonstruktion der gelöschten Dateien ermöglichen.

In der Regel sind die übertragenen Daten auch für den Empfänger schützenswert. Analog ist auch hier nach dem Wiedereinspielen der Daten eine physikalische Löschung des Datenträgers vorzusehen.

Auf den Einsatz von nicht-löschbaren Datenträgern (wie z. B. WORMs) ist zum Zwecke des Datenaustausches dann zu verzichten, wenn sich darauf weitere, nicht für den Empfänger bestimmte Informationen befinden, die nicht gelöscht werden können.

Ergänzende Kontrollfragen:

- Ist den für den Austausch der Datenträger Verantwortlichen das Verfahren des physikalischen Löschens bekannt?
- Stehen diesen Mitarbeitern geeignete Programme zum physikalischen Löschen bereit?
- Sind die Empfänger von schützenswerten Informationen über den Schutzwert der übermittelten Daten informiert?

M 4.33 Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Neben den in M 2.3 *Datenträgerverwaltung* dargestellten Umsetzungshinweisen sollte unmittelbar vor und unmittelbar nach einer Datenübertragung sowie beim Austausch bzw. beim Versand von Disketten oder anderen Datenträgern eine Viren-Überprüfung durchgeführt werden (siehe M 4.3 *Regelmäßiger Einsatz eines Viren-Schutzprogramms*). Dabei ist darauf zu achten, dass das eingesetzte Viren-Suchprogramm auch Makro-Viren erkennen kann.

Ein Protokoll der Absender-Überprüfung sollte dem übermittelten Datenträger beigefügt oder einer Datei, die elektronisch versandt wird, angehängt werden. Es empfiehlt sich, dieses Protokoll als Kopie zu verwahren. Der Empfänger hätte anhand dieses Protokolls einen ersten Eindruck von der Integrität der übermittelten Daten. Dies entbindet jedoch nicht von einer erneuten Virenüberprüfung. Der Absender kann andererseits bei eventuellen Beschwerden bezüglich Virenbefall der Daten plausibel machen, dass ein Befall bei ihm unwahrscheinlich war.

Ergänzende Kontrollfragen:

- Wird ein möglichst aktuelles Viren-Suchprogramm eingesetzt?
- Werden die zum Austausch vorgesehen Daten vor dem Austausch auf Viren überprüft?
- Wird ein Protokoll dieser Überprüfung an den Absender übermittelt?
- Werden empfangene Dateien und Datenträger vor dem Einspielen auf Virenbefall hin überprüft?

M 4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Werden vertrauliche Informationen oder Informationen mit hohem Integritätsanspruch übertragen und besteht eine gewisse Möglichkeit, dass diese Daten Unbefugten zur Kenntnis gelangen, von diesen manipuliert werden oder durch technische Fehler verändert werden können, sollte ein kryptographisches Verfahren zum Schutz der Daten für den Transport oder die Übermittlung in Betracht gezogen werden.

Vertraulichkeitsschutz durch Verschlüsselung

Einsatz eines sicheren Verschlüsselungsalgorithmus

Für die Übertragung vertraulicher Informationen bedarf es deren Verschlüsselung. Das entscheidende Merkmal eines Verschlüsselungsverfahrens ist die Güte des Algorithmus sowie der Schlüsselauswahl. Ein anerkannter Algorithmus, der für den normalen Schutzbedarf ausreicht, ist der Tripel-DES, der auf dem Data Encryption Standard (DES) basiert. Dieser ist leicht zu programmieren, zumal der Quell-Code in vielen Fachbüchern in der Programmiersprache C abgedruckt ist. Für den Bereich der öffentlichen Verwaltung kann das BSI für den Einsatz auf stationären und tragbaren PCs ein Offline-Verschlüsselungsprogramm (Chiasmus für Windows) unter gewissen Randbedingungen zur Verfügung stellen, dass den Sicherheitsanforderungen im Bereich des normalen Schutzbedarfs genügt. Ein Anforderungsvordruck findet sich auf der BSI-Webseite.

Zugriffsschutz auf das Verschlüsselungsprogramm

Um den Anforderungen der Vertraulichkeit der zu übertragenden Informationen zu entsprechen, müssen das IT-System des Absenders und des Empfängers den Zugriffsschutz auf das Verschlüsselungsprogramm ausreichend gewährleisten. Gegebenenfalls sollte dieses Programm auf einem auswechselbaren Datenträger gespeichert, in der Regel verschlossen aufbewahrt und nur bei Bedarf eingespielt und genutzt werden.

Integritätsschutz durch Checksummen, Verschlüsselung oder Digitaler Signaturbildung

Ist für den Datenaustausch lediglich die Integrität der zu übermittelnden Daten sicherzustellen, muss unterschieden werden, ob ein Schutz nur gegen zufällige Veränderungen, z. B. durch Übertragungsfehler, oder auch gegen Manipulationen geleistet werden soll. Sollen ausschließlich zufällige Veränderungen erkannt werden, können Checksummen-Verfahren (z. B. Cyclic Redundancy Checks) oder fehlerkorrigierende Codes zum Einsatz kommen. Schutz gegenüber Manipulationen bieten darüber hinaus Verfahren, die unter Verwendung eines symmetrischen Verschlüsselungsalgorithmus (z. B. Tripel-DES) aus der zu übermittelnden Information einen so genannten Message Authentication Code (MAC) erzeugen. Andere Verfahren bedienen sich eines asymmetrischen Verschlüsselungsalgorithmus (z. B. RSA) in Kombination mit einer Hashfunktion und erzeugen eine "Digitale Signatur". Die jeweiligen erzeugten "Fingerabdrücke" (Checksumme, fehlerkorrigierende Codes, MAC,

Digitale Signatur) werden zusammen mit der Information an den Empfänger übertragen und können von diesem überprüft werden.

sichere Schlüsselübermittlung

Für die Übermittlung oder den Austausch ggf. notwendiger Schlüssel sei hier auf Maßnahme M 2.46 *Geeignetes Schlüsselmanagement* verwiesen. Weitere Informationen zum Einsatz kryptographischer Verfahren und Produkte finden sich in Baustein B 1.7 *Kryptokonzept*.

Ergänzende Kontrollfragen:

- Werden Verschlüsselungsprogramme oder Checksummen-Verfahren zum Schutz der Vertraulichkeit oder Integrität bereitgestellt?
- Sind die für die Datenübertragung Verantwortlichen über ein ordnungsgemäßes Schlüsselmanagement informiert?
- Ist der Schutz der Vertraulichkeit/Integrität nur auf dem Transport- bzw. Übertragungsweg oder auch auf dem Empfänger- oder Absendersystem zu gewährleisten?

M 4.35 Verifizieren der zu übertragenden Daten vor Versand

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Vor dem Versenden des Datenträgers ist dieser darauf zu überprüfen, ob die gewünschten Informationen - und auch nur diese - vom Datenträger rekonstruierbar sind.

Um die korrekte Übertragung zum Datenträger zu überprüfen, kann ein Programm eingesetzt werden, dass die ursprüngliche mit der übertragenen Datei zeichenweise vergleicht (auf einem PC unter DOS z. B. mittels des Befehls *comp*).

Auch sollten alle Dateien des Datenträgers aufgelistet werden (z. B. mit *dir* unter DOS oder *ls* unter Unix), um sicherzustellen, dass nur für den Empfänger bestimmte Dateien auf diesem Datenträger enthalten sind.

Befanden sich vorher andere Daten auf diesem Datenträger, so sind diese physikalisch zu löschen (M 4.32 *Physikalisches Löschen der Datenträger vor und nach Verwendung*).

Ergänzende Kontrollfragen:

- Werden die auszutauschenden Datenträger vor dem Versenden darauf überprüft, ob die gewünschten Information vollständig vom Datenträger rekonstruierbar sind?
- Werden die auszutauschenden Datenträger vor dem Versenden üblicherweise darauf überprüft, ob nur die gewünschten Information vom Datenträger rekonstruierbar sind?

M 4.36 Sperren bestimmter Faxempfänger-Rufnummern

Verantwortlich für Initiierung: Vorgesetzte, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Fax-Verantwortlicher, Fax-Poststelle

Besteht die Notwendigkeit, das zufällige oder absichtliche Versenden von Informationen oder Unterlagen per Fax an eine nicht gewünschte Empfängerrufnummer zu verhindern, so bietet die heutige Technik dazu mindestens drei Lösungen:

Einstellung am Faxgerät oder Faxserver

Bei einigen Faxgeräten bzw. Faxservern ist es möglich, die Versendung von Faxen an bestimmte Faxempfänger-Rufnummern zu unterbinden (positiver Ausschluss) oder alternativ alle Empfängerrufnummern außer einigen ausgewählten Rufnummern zu sperren (negativer Ausschluss).

Einstellung an der TK-Anlage

Die gleiche Art der Berechtigungsvergabe kann auch in modernen TK-Anlagen erreicht werden, vorausgesetzt, das Faxgerät ist über eine solche Anlage ans Telefonnetz angeschlossen.

Benutzung einer Zusatzeinrichtung

Wenn ein Faxgerät oder die TK-Anlage eine solche Möglichkeit nicht bietet, so kann zum Beispiel vom Betreiber des öffentlichen Netzes eine Zusatzeinrichtung gemietet werden, die den Verbindungsaufbau zu bestimmten Rufnummern (positiver und negativer Ausschluss) verhindert.

Ergänzende Kontrollfragen:

- Besteht die Notwendigkeit, bestimmte Faxadressaten auszuschließen?
- Ist es vorgekommen, dass Faxsendungen an falsche Empfänger versandt wurden?

M 4.37 Sperren bestimmter Absender-Faxnummern

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Fax-Verantwortlicher, Fax-Poststelle

Damit bestimmte Faxsendungen das eigene Faxgerät nicht blockieren können, z. B. bei Überlastung durch spezielle Faxaktionen von Werbeagenturen, kann ggf. eine Sperre bestimmter Sender-Faxnummern realisiert werden.

Auswertung der Senderrufnummer durch das Faxgerät oder den Faxserver

Einige moderne Faxgeräte (Gruppe 4) sind in der Lage, die übermittelte Senderrufnummer auszuwerten und den Empfang von Faxsendungen ausgewählter Rufnummern zu verweigern. Dies gilt auch für einige Faxserver, sofern diese an das ISDN-Netz angeschlossen sind. Daneben kann auch die Faxabsenderkennung (CSID - Call Subscriber ID) zur Auswertung herangezogen werden. Nachteilig ist allerdings, dass der Faxabsender die Rufnummernübermittlung unterdrücken und die übermittelte Rufnummer sowie die Absenderkennung manipulieren kann.

Einrichtung geschlossener Benutzergruppen

Eine weitere Möglichkeit besteht darin, dass beim Telefon-Netzbetreiber kostenpflichtig eine geschlossene Benutzergruppe eingerichtet wird, wenn Empfänger und Sender an digitalen Vermittlungsstellen angeschlossen sind. Teilweise wird diese Möglichkeit auch von modernen TK-Anlagen angeboten (vergleiche auch Baustein B 3.401 *TK-Anlage*).

Ergänzende Kontrollfragen:

- Besteht die Notwendigkeit zur Sperre bestimmter Absender-Faxnummern?
- Sind dem Fax-Verantwortlichen die geschilderten Varianten von Gegenmaßnahmen bekannt?

M 4.38 Abschalten nicht benötigter Leistungsmerkmale

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Nicht benötigte Leistungsmerkmale (insbesondere die Fernabfrage) sollten nach Möglichkeit abgeschaltet werden, um vor Missbrauch und Fehlbedienung geschützt zu sein. Zur Entscheidung, ob ein Leistungsmerkmal benötigt wird, sollten auch die damit verbundenen Sicherheitsrisiken einbezogen werden.

Ergänzende Kontrollfrage:

- Werden die Benutzer explizit aufgefordert, nicht benötigte Leistungsmerkmale abzuschalten?

M 4.39 Abschalten des Anrufbeantworters bei Anwesenheit

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Benutzer

In Zeiten, in denen der Anrufbeantworter nicht benötigt wird, kann er zum Schutz gegen Missbrauch abgeschaltet oder vom Telefonnetz getrennt werden. Insbesondere in dem Fall, dass das Gerät über die Funktion der Raumüberwachung verfügt, sollte dies konsequent durchgeführt werden.

Zu beachten ist, dass sich in einigen Fällen die abgeschalteten Anrufbeantworter selbständig aktiveren, wenn die Verbindung nach einer gewissen Zeit nicht aufgebaut wird (z. B. nach 10-maligem Klingeln).

Ergänzende Kontrollfrage:

- Schaltet sich ihr Anrufbeantworter automatisch ab?

M 4.40 Verhinderung der unautorisierten Nutzung des Rechnermikrofons

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Das Mikrofon eines vernetzten Rechners kann von denjenigen benutzt werden, die Zugriffsrechte auf die entsprechende Gerätedatei (unter Unix zum Beispiel */dev/audio*) haben. Unter Windows NT bestimmen die Zugriffsrechte auf die entsprechenden Schlüssel der Registrierung (*HKEY_LOCAL_MACHINE\HARDWARE*.), wer das Rechnermikrofon aktivieren kann. Diese Rechte sind daher sorgfältig zu vergeben. Der Zugriff auf die Gerätedatei sollte nur möglich sein, solange jemand an dem IT-System arbeitet. Wenn die Benutzung eines vorhandenen Mikrofons generell verhindert werden soll, muss es - wenn möglich - ausgeschaltet oder physikalisch vom Gerät getrennt werden.

Zugriffsrechte setzen

Falls das Mikrofon in den Rechner integriert ist und nur durch Software ein- und ausgeschaltet werden kann, müssen die Zugriffsrechte so gesetzt sein, dass es kein Unbefugter benutzen kann. Dies kann z. B. erfolgen, indem unter Unix allen Benutzern die Leserechte auf die Gerätedatei */dev/audio* bzw. unter Windows NT die Zugriffsrechte auf die entsprechenden Schlüssel der Registrierung entzogen werden. Dadurch ist ausgeschlossen, dass ein normaler Benutzer das Mikrofon benutzen kann, er kann aber weiterhin Audio-Dateien abspielen.

sicheres Deaktivieren

Bei IT-Systemen mit Mikrofon ist zu prüfen, ob Zugriffsrechte und Eigentümer bei einem Zugriff auf die Gerätedatei verändert werden. Falls dies der Fall ist oder falls gewünscht ist, dass jeder Benutzer das Mikrofon benutzen kann und es nicht nur in Einzelfällen durch den Systemadministrator freigegeben werden soll, muss der Administrator ein Kommando zur Verfügung stellen, das

- nur aktiviert werden kann, wenn jemand an dem IT-System angemeldet ist,
- nur durch diesen Benutzer aktiviert werden kann und
- die Zugriffsberechtigungen dem Benutzer nach dem Abmelden wieder entzieht.

physikalisches Trennen

Solange der Zugriff auf das Mikrofon durch kein sicheres Kommando geregelt wird, muss das Mikrofon physikalisch vom Rechner oder der Rechner vom Netz getrennt werden.

Rechner mit eingebautem Mikrofon sollten während einer vertraulichen Besprechung aus dem Raum entfernt werden oder zumindest ausgeschaltet werden. Bei einem Laptop sollten alle evtl. vorhandenen Verbindungen zu Kommunikationsnetzen, beispielsweise ISDN, die nicht benötigt werden, getrennt werden. In den meisten Fällen ist es hierzu am einfachsten, das entsprechende Kabel auszustecken.

Ergänzende Kontrollfragen:

- Kann das Rechnermikrofon ausgeschaltet oder physikalisch vom Rechner getrennt werden?
- Wer hat Zugriff auf die Mikrofon-Gerätedatei bzw. auf die Teile der Registrierung, die die Manipulation von Hardware-Einstellungen erlauben?

M 4.41 Einsatz angemessener Sicherheitsprodukte für IT-Systeme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Datenschutzbeauftragter, Verantwortliche der einzelnen IT-Anwendungen

Verantwortlich für Umsetzung: Beschaffungsstelle, Administrator

Je nachdem, welche Sicherheitsanforderungen an ein IT-System gestellt werden, reichen eventuell die vorhandenen Sicherheitsfunktionalitäten nicht aus, so dass zusätzlich geeignete Sicherheitsprodukte eingesetzt werden sollten. Typische Beispiele dafür sind Zugangskontrolle, Zugriffsrechteverwaltung und -prüfung, Protokollierung oder Verschlüsselung.

Bei IT-Systemen muss beispielsweise sichergestellt werden, dass

- nur autorisierte Personen das IT-System benutzen können (siehe auch BDSG, Zugangskontrolle). Hierfür sind geeignete Authentisierungsmechanismen auszuwählen.
- die Benutzer auf die Daten nur in der Weise zugreifen können, die sie zur Aufgabenerfüllung benötigen. Hierbei unterstützen geeignete Benutzertrennung und Rechtevergabe.
- Unregelmäßigkeiten und Manipulationsversuche erkennbar werden. Hierbei helfen Protokollierungsfunktionen, Verschlüsselung und digitale Signatur.
- Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle). Hierbei unterstützen beispielsweise Backup-Programme.

Reichen die Protokollierungsmöglichkeiten des IT-Systems nicht aus, um eine ausreichende Beweissicherung zu gewährleisten, so müssen diese nachgerüstet werden. Hierzu gibt es auch verschiedene Gesetze, die dies erfordern. Beispielsweise ist nach BDSG, bei der Eingabekontrolle "zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind".

Ist es mit dem IT-System nicht möglich, den Administrator daran zu hindern, auf bestimmte Daten zuzugreifen oder zumindest diesen Zugriff zu protokollieren und zu kontrollieren, dann kann z. B. mit einer Verschlüsselung der Daten verhindert werden, dass der Administrator diese Daten im Klartext liest, wenn er nicht im Besitz des zugehörigen Schlüssels ist.

Empfohlene Mindestfunktionalitäten:

IT-Systeme sollten mindestens die folgenden Sicherheitseigenschaften besitzen. Wenn diese nicht im Standardumfang vorhanden sind, sollten diese über zusätzliche Sicherheitsprodukte nachgerüstet werden.

- *Identifikation und Authentisierung*: Es sollte eine Sperre des Systems nach einer vorgegebenen Anzahl fehlerhafter Authentisierungsversuche statt finden, die nur ein Administrator zurücksetzen kann. Wird ein

Passwort verwendet, sollte das Passwort mindestens acht Stellen umfassen und darf nicht unverschlüsselt im System gespeichert werden.

- *Rechteverwaltung und -kontrolle*: Es sollte eine Rechteverwaltung und -kontrolle auf Festplatten und Dateien vorhanden sein, wobei zumindest zwischen lesendem und schreibendem Zugriff unterschieden werden soll. Für Benutzer sollte kein Systemzugriff auf Betriebssystemebene möglich sein.
- *Rollentrennung zwischen Administrator und Benutzer*: Es sollte eine klare Trennung zwischen Administrator und Benutzer möglich sein, wobei nur der Administrator Rechte zuweisen oder entziehen können sollte.
- *Protokollierung* der Vorgänge Anmelden, Abmelden und Rechteverletzung sollte möglich sein.
- *Automatische Bildschirmsperre*: Nach zeitweiser Inaktivität der Tastatur oder Maus sollte eine Bildschirmsperre automatisch aktiv werden. Diese sollte sich auch direkt aktivieren lassen. Der erneute Zugriff auf das IT-System darf erst nach erfolgreicher Identifikation und Authentisierung wieder möglich sein.
- *Boot-Schutz* soll verhindern, dass der Rechner unbefugt von anderen Medien gebootet werden kann.

Sollte ein oder mehrere dieser Sicherheitsfunktionalitäten nicht vom Betriebssystem unterstützt werden, so müssen ersatzweise geeignete zusätzliche Sicherheitsprodukte eingesetzt werden.

Zusätzliche Forderungen an Sicherheitsprodukte:

- *Benutzerfreundliche Oberfläche* zur Erhöhung der Akzeptanz.
- Aussagekräftige und nachvollziehbare Dokumentation für Administrator und Benutzer.

Wünschenswerte Zusatzfunktionalität von Sicherheitsprodukten:

- *Rollentrennung zwischen Administrator, Revisor und Benutzer;* nur der Administrator kann Rechte zuweisen oder entziehen und nur der Revisor hat Zugriff auf die Protokolldaten,
- *Protokollierung* von Administrationstätigkeiten,
- *Unterstützung der Protokollauswertung* durch konfigurierbare Filterfunktionen,
- *Verschlüsselung* der Datenbestände mit einem geeigneten Verschlüsselungsalgorithmus und in einer Weise, dass ein Datenverlust bei Fehlfunktion (Stromausfall, Abbruch des Vorgangs) systemseitig abgefangen wird.

Die Realisierung dieser Funktionalität kann sowohl in Hardware wie auch in Software erfolgen. Bei der Neubeschaffung eines Produktes sollte Maßnahme M 2.66 *Beachtung des Beitrags der Zertifizierung für die Beschaffung* berücksichtigt werden.

Übergangslösung:

Sollte es nicht möglich sein, kurzfristig ein geeignetes Sicherheitsprodukt zu beschaffen, sind andere geeignete Sicherheitsmaßnahmen zu ergreifen. Diese sind dann typischerweise organisatorischer Natur und müssen von den Benutzern konsequent eingehalten werden. Wenn ein IT-System beispielsweise keine Bildschirmsperre hat, muss dieses in den kurzen Phasen, wo es nicht benutzt wird, ein- oder weggeschlossen werden.

Ergänzende Kontrollfragen:

- Wurde vor der Beschaffung von IT-Systemen überprüft, ob diese angemessen Sicherheitsfunktionalitäten bieten?

M 4.42 Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Datenschutzbeauftragter, Verantwortliche der einzelnen IT-Anwendungen

Verantwortlich für Umsetzung: Anwendungsentwickler

Mehrere Gründe können zu der Notwendigkeit führen, dass innerhalb der Anwendungsprogramme selbst Sicherheitsfunktionalitäten wie eine Zugangskontrolle, eine Zugriffsrechteverwaltung und -prüfung oder eine Protokollierung implementiert werden müssen:

- Reichen die Protokollierungsmöglichkeiten des IT-Systems einschließlich zusätzlich eingesetzter IT-Sicherheitsprodukte nicht aus, um eine ausreichende Beweissicherung zu gewährleisten, so müssen diese Protokollelemente im Anwendungsprogramm implementiert werden. (Beispiel: BDSG, Anlage zum § 9, Eingabekontrolle: "zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind".)
- Reicht die Granularität der Zugriffsrechte des IT-Systems einschließlich zusätzlich eingesetzter Sicherheitsprodukte nicht aus, um einen ordnungsgemäßen Betrieb zu gewährleisten, so muss eine Zugriffsrechteverwaltung und -kontrolle im Anwendungsprogramm implementiert werden. (Beispiel: eine Datenbank mit einer gemeinsamen Datenbasis. Vorausgesetzt sei, dass je nach Funktion des Benutzers nur Zugriffe auf bestimmte Felder zulässig sind.)
- Ist es mit dem IT-System einschließlich zusätzlich eingesetzter IT-Sicherheitsprodukte nicht möglich, den Administrator daran zu hindern, auf bestimmte Daten zuzugreifen oder zumindest diesen Zugriff zu protokollieren und zu kontrollieren, dann muss dies bei Bedarf durch zusätzliche Sicherheitsfunktionen im Anwendungsprogramm implementiert werden. Zum Beispiel kann mit einer Verschlüsselung der Daten verhindert werden, dass der Administrator diese Daten im Klartext liest, wenn er nicht im Besitz des zugehörigen Schlüssels ist.

Diese zusätzlichen Anforderungen an IT-Anwendungen müssen schon in der Planung und Entwicklung berücksichtigt werden, da eine nachträgliche Implementation meist aus Kostengründen nicht mehr möglich ist.

Ergänzende Kontrollfrage:

- Wird bei der Entwicklung neuer IT-Anwendungen systematisch festgestellt, welche Sicherheitsfunktionen die Anwendung bereitstellen muss?

M 4.43 Faxgerät mit automatischer Eingangskuvertierung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Beschaffer

Faxgeräte mit automatischer Eingangskuvertierung verhindern, dass eingegangene Faxe unberechtigt entnommen und unberechtigt gelesen werden. Eingehende Faxe werden so geknickt, dass nur das Faxvorblatt sichtbar bleibt, und dann in einem Klarsichtumschlag eingeschweißt. Danach fällt der Umschlag in ein verschließbares Fach im Faxgerät. Zugriff auf die Umschläge hat normalerweise nur der Berechtigte, der den Schlüssel zu diesem Fach besitzt. Eine unbefugte Kenntnisnahme ist vor Zustellung des Fax nur durch gewaltsames Öffnen des Faches oder Aufreißen des verschweißten Umschlages möglich und wird daher zumindest bemerkt.

Ergänzende Kontrollfrage:

- Ist die Anschaffung eines derartigen Gerätes sinnvoll?

M 4.44 Prüfung eingehender Dateien auf Makro-Viren

Diese Maßnahme ist mit Version 2005 entfallen.

M 4.45 Einrichtung einer sicheren Peer-to-Peer-Umgebung unter WfW

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Für jeden Rechner unter WfW sollte der Administrator die Peer-to-Peer-Funktionalitäten einzeln zulassen oder sperren und damit die WfW-Umgebung benutzerspezifisch einschränken. Dafür benötigt er das Administrationswerkzeug ADMINCFG.EXE.

Nach dem Aufruf von ADMINCFG.EXE muss zunächst die Sicherheitskonfigurationsdatei WFWSYS.CFG geöffnet werden, in der die Sicherheitseinstellungen des jeweiligen WfW-Rechners gespeichert sind. ADMINCFG.EXE kann dabei nicht nach verschiedenen Benutzern auf einem WfW-Rechner unterscheiden.

Selbst wenn die Umgebung nicht eingeschränkt werden soll, ist die Sicherheitskonfigurationsdatei WFWSYS.CFG mit einem Passwortschutz zu versehen. Wird das Administrationswerkzeug ADMINCFG.EXE dazu lokal installiert, ist es anschließend wieder zu entfernen.

Mit Hilfe des Administrationswerkzeugs ADMINCFG.EXE können unter Sicherheitsgesichtspunkten folgende Konfigurationen für den Rechner vorgenommen werden:

Die **Freigabeoptionen** sind festzulegen:

- Wenn der Rechner nicht für die Freigabe von Verzeichnissen vorgesehen ist, ist die Option *Dateifreigabe deaktivieren* einzustellen. Die entsprechenden Funktionen stehen dann im Dateimanager nicht mehr zur Verfügung, es ist aber weiter möglich, sich mit Verzeichnissen anderer Rechner zu verbinden.
- Wenn der Rechner nicht für die Freigabe von Druckern vorgesehen ist, ist die Option *Druckerfreigabe deaktivieren* einzustellen.
- Wenn der Rechner nicht für Netz-DDE-Freigabe (z. B. Telefonieren unter WfW, Datenaustausch über die Ablagemappe) vorgesehen ist, ist die Option *Netz-DDE-Freigabe deaktivieren* einzustellen.

Die **Kennwortoptionen** sind festzulegen:

- Bei aktiviertem Kennwort-Caching werden in einer Datei alle WfW-Netzverbindungen mit zugehörigen Passwörtern gespeichert, wenn dies vom Benutzer beim jeweiligen Verbindungsaufbau gewünscht wird. Wiederholte Passworteingaben sind dann später nicht mehr erforderlich. Die Option *Kennwort-Caching deaktivieren* sollte eingestellt werden, zumindest immer dann, wenn der WfW-Rechner nicht über einen ausreichenden Zugangsschutz (z. B. BIOS-Passwort) verfügt.
- *Kennworte in Freigabe-Dialogfeldern lesbar anzeigen* darf nicht aktiviert sein, da sonst bei der Passwort-Eingabe dieses im Klartext auf dem Bildschirm erscheint.

- *Ablauf des Anmeldekennwortes* sollte auf den in der Sicherheitsstrategie vorgegebenen Zeitraum eingestellt werden.
- *Minimale Kennwortlänge* muss auf mindestens 6 eingestellt werden.
- *Alphanumerische Kennworte erzwingen* sollte eingestellt werden. Buchstaben-Zahlen-Kombinationen werden damit obligatorisch.

Die **Administrator-Einstellungen** sind festzulegen:

- Der Administrator muss ein Passwort für die erstellte Konfigurationsdatei WFWSYS.CFG festlegen, das nur ihm und seinem Stellvertreter bekannt sein darf. Dieses Passwort ist sicher zu hinterlegen (siehe M 2.22 *Hinterlegen des Passwortes*).
- Über *Optionen aktualisieren* können voreingestellte Sicherheitsprofile von einem Server übernommen werden. Darüber hinaus kann auch eingestellt werden, dass beim Start eines Clients die Sicherheitskonfigurationsdatei des Servers überprüft und bei Änderungen die lokale aktualisiert wird. Dies erleichtert dem Administrator die zentrale Administration des WfW-Netzes, das einfache Hinzufügen weiterer WfW-Rechner und das Wechseln des Passwortes für die Konfigurationsdatei.

Der Administrator muss darüber hinaus beim Einrichtung eines WfW-Rechners auch die weiteren Punkte beachten:

- Die Voreinstellung *Beim Start wieder freigeben* ist in den Freigabeoberflächen (Datei- und Druckmanager) zu deaktivieren.
- Die Voreinstellung *Kennwort in der Kennwortliste speichern* ist in den Verbindungsoberflächen (Datei- und Druckmanager) zu deaktivieren.
- In der Programmgruppe *Systemsteuerung* unter *Netzwerk* sollte gemäß der Namenskonvention der Computername, der Name der Arbeitsgruppe und der Standard-Anmeldename voreingestellt werden.
- Das WfW-Protokoll ist zu aktivieren (in der Programmgruppe *Systemsteuerung* unter *Netzwerk*). Dabei sollten sämtliche Ereignisse aufgezeichnet und die Protokolldatei ausreichend groß, beispielsweise 32 KByte, angelegt werden.
- In der Programmgruppe *Systemsteuerung* unter *Netzwerk* sollte über die Schaltfläche *Start* voreingestellt werden, ob eigene Anwendungen des Rechners oder Zugriffe anderer mit Priorität bedient werden. Ist der Zugriff anderer nachrangig, sollte die Priorität zugunsten schnellerer Ausführung gewählt werden.
- Beim Einsatz von *Schedule+* ist darauf zu achten, dass das standardmäßig vergebene Recht, offene oder besetzte Zeitblöcke einzusehen, für alle nicht berechtigten WfW-Benutzer deaktiviert wird. Jeder Teilnehmer am selben Post-Office ist sonst in der Lage, das zeitliche Arrangement der individuellen Termine einzusehen.

WfW bietet die Möglichkeit, Sicherheitsprofile auf einem "Server" zu hinterlegen, die die einzelnen Clients im WfW-Netz zur Aktualisierung abrufen. Dadurch ist es möglich, die Sicherheitseinstellungen über das Netz zu

administrieren. Um den administrativen Aufwand zu minimieren, sollte diese Möglichkeit genutzt werden.

Wird ein Post-Office eingerichtet, dass von mehreren Benutzern zur Kommunikation oder zur gemeinsamen Terminplanung genutzt werden soll, ist in Erwägung zu ziehen, von diesem eine Datensicherung in angemessenen Zeiträumen anzulegen. Dies ist notwendig, um einem versehentlichen oder absichtlichen Löschen des Post-Office entgegenzuwirken, da dies unter WfW nicht sicher verhindert wird.

Optionen und Einstellungen dokumentieren

Die festgelegten Freigabeoptionen, Kennwortoptionen und Administrator-Einstellungen sollten nachvollziehbar dokumentiert werden. Dies kann auch in elektronischer Form erfolgen, wenn sichergestellt ist, dass auch bei nicht funktionierenden Peer-to-Peer-Diensten auf die Dokumentation zugegriffen werden kann. Die Dokumentation muss bei Änderungen an den Optionen und Einstellungen entsprechend aktualisiert werden.

Ergänzende Kontrollfragen:

- Werden die Sicherheitseinstellungen über das Netz administriert?
- Werden die vorgenommenen Einstellungen in geeigneter Form dokumentiert?

M 4.46 Nutzung des Anmeldepasswortes unter WfW und Windows 95

Verantwortlich für Initiierung: Administrator

Verantwortlich für Umsetzung: Benutzer

Meldet sich ein neuer Benutzer an einem Rechner unter WfW oder Windows 95 an, wird er gefragt, ob er eine Kennwortliste ([*anmeldename*].*pwl*) unter seinem Anmeldenamen anlegen möchte. In dieser Liste werden dann alle diejenigen Passwörter festgehalten, die von diesem Benutzer beim Verbinden mit Ressourcen anderer mitgeteilt werden müssen. Dies geschieht allerdings nur dann, wenn dieses "Caching" von Passwörtern auf diesem Rechner explizit erlaubt ist und der Benutzer es im Einzelfall auch wünscht.

Das Anmeldepasswort dient einzig und allein dem Schutz dieser Kennwortliste. Nur bei korrekter Eingabe des zum Anmeldenamen gehörigen Passwortes wird diese entschlüsselt und steht zur Verfügung.

Insbesondere wenn ein WfW- oder Windows 95-Rechner von mehreren Benutzern eingesetzt wird, wird ein Schutz der gespeicherten Kennwörter gegenüber den Benutzern desselben Rechners nur durch ein individuelles Anmeldepasswort gewährleistet.

Das jeweilige Passwort ist geeignet auszuwählen, regelmäßig zu wechseln und sicher zu hinterlegen (siehe M 2.11 *Regelung des Passwortgebrauchs* und M 2.22 *Hinterlegen des Passwortes*).

Hinweise:

Werden vom Benutzer keine Passwörter in der Kennwortliste gespeichert, ist auch kein Anmeldepasswort unter WfW notwendig. Wird also Passwort-Caching grundsätzlich vom Administrator mittels ADMINCFG.EXE unter WfW bzw. über die Systemrichtlinien unter Windows 95 deaktiviert, so ist das Anmeldepasswort überflüssig. Selbst Maskerade auf dem PC kann mit diesem Authentisierungsmechanismus nicht verhindert werden, da jede Kennwortliste umbenannt, der ursprüngliche Anmeldename erneut genutzt und anschließend die ursprüngliche Kennwortliste wieder zurückbenannt werden kann.

Wird allerdings Passwort-Caching erlaubt und auch genutzt, muss der Administrator mittels ADMINCFG.EXE unter WfW bzw. über die Systemrichtlinien unter Windows 95 die Mindestlänge des Anmeldepasswortes auf 6 setzen. Damit ist die Eingabe des Passwortes beim Anmelden unter WfW und Windows 95 obligatorisch und kann nicht deaktiviert werden. In Ausnahmefällen, z. B. wenn der Rechner nur von einem Benutzer genutzt wird und ein ausreichender Zugangsschutz (BIOS-Passwort, Bildschirmsperre, usw.) besteht, kann das Anmeldepasswort deaktiviert werden. Eine Deaktivierung ist möglich, wenn die Mindestlänge des Passwortes auf Null gesetzt wird.

Werden vom Benutzer versehentlich Passwörter in der Kennwortliste gespeichert, ist die Datei [*anmeldename*].*pwl* zu löschen.

Ergänzende Kontrollfrage:

- Wird den WfW- bzw. Windows 95 Benutzern mitgeteilt, dass neben dem Passwortschutz am PC (z. B. BIOS-Passwort) zusätzlich das Anmeldepasswort für den Schutz der individuellen Kennwortliste unter WfW bzw. Windows 95 notwendig ist?

M 4.47 Protokollierung der Sicherheitsgateway-Aktivitäten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Es muss festgelegt werden, welche Ereignisse protokolliert werden und wer die Protokolle auswertet. Die Protokollierung muss den jeweils geltenden rechtlichen Bestimmungen entsprechen. Für Protokolldaten ist in Deutschland insbesondere die Zweckbindung nach § 14 des BDSG zu beachten.

Für den Einsatz der Protokollierung am Sicherheitsgateway sollten die folgenden Punkte beachtet werden:

- Es muss möglich sein, die Protokolldaten (beispielsweise IP-Adressen) eindeutig einzelnen Rechnern (oder Personen) zuzuordnen. Dabei müssen jedoch die jeweils zutreffenden gesetzlichen Regelungen zum Datenschutz beachtet werden.
- Die Protokolldaten sollten nicht nur auf den einzelnen Komponenten des Sicherheitsgateways, sondern zusätzlich auch auf einem zentralen Protokollierungsserver (Loghost) gespeichert werden, so dass die Gefahr des Datenverlustes durch einen Hacker-Angriff oder durch einen Systemausfall verringert wird.
- Die Übertragung der Protokollinformationen von den Komponenten zum Loghost muss über eine gesicherte Verbindung erfolgen, damit die Protokollinformationen vor ihrer endgültigen Speicherung nicht verändert werden können.
- Wenn bei der Übertragung zum Loghost nicht-vertrauenswürdige Netze passiert werden müssen, so müssen die Daten verschlüsselt werden.
- Die Größe des freien Speicherplatzes auf dem verwendeten Medium sollte regelmäßig kontrolliert werden.
- Bei einem Ausfall der Protokollierung (z. B. aufgrund fehlenden Speicherplatzes auf der Festplatte) sollten alle Funktionen, die Protokolldaten generieren, gesperrt werden. Idealerweise sollte das Sicherheitsgateway jeglichen Verkehr blockieren und eine entsprechende Meldung an den Administrator weitergeben.
- Die Protokolldaten sollten auf einem WORM-Medium ("Write Once, Read Many") gespeichert werden.
- Art und Umfang der Protokollierung sollten sich an der Sensibilität der zu verarbeitenden Daten sowie am Verwendungszweck orientieren.
- Spezielle, einstellbare Ereignisse, wie z. B. wiederholte fehlerhafte Passworteingaben für eine Benutzer-Kennung oder unzulässige Verbindungsversuche, müssen bei der Protokollierung hervorgehoben werden und sollten zu einer unverzüglichen Warnung des Firewall-Administrators führen.
- Die einzelnen Komponenten sollten eine Zeitsynchronisation durchführen, um eine Korrelation der Daten zu ermöglichen. Siehe dazu auch M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*.

Bei kleinen Netzen, in denen nur ein einfaches Sicherheitsgateway eingesetzt wird, kann gegebenenfalls auf einen zusätzlichen Loghost verzichtet werden.

Umfang der Protokollierung am Paketfilter

Abgewiesene Pakete protokollieren!

Die Protokollierung am Paketfilter sollte zumindest alle Pakete erfassen, die auf Grund einer Paketfilterregel abgewiesen werden.

Je nach Sicherheitsanforderungen sind eventuell zusätzliche Klassen von Paketen interessant:

- "Ungewöhnliche" Pakete, beispielsweise mit einer fehlerhaften Kombination aus TCP-Flags oder Pakete mit fehlerhaften Header-Informationen.

  Solche Pakete sollten zwar ohnehin durch eine entsprechende Paketfilterregel abgewiesen und aus diesem Grund bereits von der Protokollierung erfasst werden, aber es wird trotzdem empfohlen, solche Pakete gesondert zu protokollieren, da sie beispielsweise Indizien für sogenannte "Stealth Scans" sein können. Außerdem kann eine Häufung fehlerhafter Pakete auf technische Probleme im Netz hindeuten.

- Bei verbindungsorientierten (beispielsweise TCP-basierten) Protokollen kann es sinnvoll sein, auch akzeptierte Pakete zu protokollieren, die zu einem Verbindungsaufbau gehören (beispielsweise TCP-Pakete, die zum 3-Wege-Handshake gehören), sowie eventuell zusätzlich Pakete, die zum Abbau einer bestehenden Verbindung gehören.

- Bei verbindungslosen Protokollen, über die keine großen Datenmengen übertragen werden (beispielsweise UDP-basierte Protokolle wie DNS) kann es unter Umständen sinnvoll sein, alle Pakete zu protokollieren.

Welche zusätzlichen Klassen von Paketen protokolliert werden hängt in erster Linie vom Schutzbedarf des vertrauenswürdigen Netzes ab. Allerdings bringt die Protokollierung alleine keinen Sicherheitsgewinn, sondern die Informationen müssen auch nach entsprechenden Kriterien ausgewertet werden.

Von den Paketen, für die eine Protokollierung gewünscht wird, sollten mindestens die folgenden Informationen protokolliert werden:

- Quell- und Ziel-IP-Adresse
- Quell- und Zielport oder ICMP-Typ
- Datum und Zeit
- zutreffende Regel des Paketfilters

Wird zusätzlich ein ALG verwendet, so kann auf die Protokollierung der akzeptierten Pakete verzichtet werden, da der Proxy in diesem Fall meist ausreichende Verbindungsinformationen protokolliert.

Umfang der Protokollierung am Application-Level-Gateway

Auf dem ALG alle Verbindungen protokollieren

Auf dem ALG, der durch den äußeren Paketfilter vor der großen Masse unzulässiger Pakete geschützt wird, sollten für jeden (erfolgreichen oder versuchten) Verbindungsaufbau die folgenden Daten protokolliert werden:

- Quell- und Ziel-IP-Adresse
- Quell- und Zielport
- Dienst
- Datum und Zeit
- Verbindungsdauer
- eventuell Authentisierungsdaten oder ausschließlich Tatsache des Fehlschlagens einer Authentisierung

Es muss möglich sein, für bestimmte Benutzer die Protokollierung abzuschalten, damit nicht wegen einer zu großen Anzahl von Protokolleinträgen wichtige Informationen übersehen werden. Diese Auswahl kann z. B. anhand des Rechteprofils einzelner Benutzer getroffen werden.

Für die einzelnen Protokolle werden darüber hinaus die folgenden Einstellungen empfohlen:

DNS

- Ablehnung von Anfragen
- Zulassen von Anfragen
- von anderen Rechnern initiierte ("ausgehende") Zonen-Transfers
- vom ALG initiierte ("eingehende") Zonen-Transfers

Zonen-Transfers werden in der Regel vom Betreiber des DNS-Server verhindert, so dass auf diese Überprüfungen auch verzichtet werden kann.

FTP

- Ziel-Adresse (URL)
- Abgelehnte PORT-Befehle
- Name der übertragenen Datei
- Menge der übertragenen Daten
- Statusnachricht

HTTP

- Ziel-Adresse (URL)
- Menge der übertragenen Daten
- Verbindungsmethode (z. B. GET, POST, CONNECT)
- Hinweis auf angewandte Filterkriterien
- Statusnachricht

NNTP

- Ziel-Adresse (URL)
- Menge der übertragenen Daten
- Statusnachricht

SMTP

- E-Mail-Adresse des Absenders und des Empfängers der E-Mail
- Menge der übertragenen Daten
- Hinweis auf angewandte Filterkriterien
- Statusnachricht über Erfolg oder Misserfolg der Weiterleitung

Bei folgenden Modulen braucht keine gesonderte Protokollierung erfolgen:

Modul	**Begründung für Wegfall der Protokollierung**
HTTPS	Wird "in Reihe" mit einem HTTP-Proxy geschaltet, der bereits protokolliert.
Wartungsmodul	Relevante Protokolldaten fallen nicht an.
IDS	Protokolldaten werden auf dem IDS gesondert geliefert. Diese sollten nicht zentral gespeichert werden, um eine Umgehung von Modulen des Sicherheitsgateways zu unterbinden.

Tabelle: Module ohne gesonderte Protokollierung

Die Protokollierung wird stark vereinfacht, wenn die Software die freie Konfigurierbarkeit der "logging facility" (d.h. eine Kennzeichnung der einzelnen Log-Einträge) ermöglicht. Dadurch ist es möglich, jedem Dienst eine eindeutige Kennung zuzuordnen, anhand derer der Loghost die Protokolldaten auf verschiedene Dateien verteilen kann.

Werden die Protokolldaten über das Netz zu einem zentralen Loghost geschickt, so muss darauf geachtet werden, dass die Log-Einträge verschiedener Rechner und Dienste so gekennzeichnet werden, dass sie eindeutig zugeordnet werden können. Zusätzlich ist es sinnvoll, wenn alle Dienste ihre Protokolldaten fortlaufend nummerieren. Dadurch kann der Verlust bzw. die Manipulation von Protokolldaten erkannt werden.

Auswertung der Protokolldaten

Die Auswertung von Protokolldaten kann mit speziellen Tools unterstützt werden ("logfile analyzer"). Diese stellen die Protokolldateien auf unterschiedliche Weise dar, wobei sich die meisten Tools regulärer Ausdrücke bedienen, um relevante Daten aus den Protokolldateien zu extrahieren. Obwohl Listen mit sinnvollen regulären Ausdrücken zum Zwecke der Protokolldatenauswertung existieren, sind im Einzelfall meist Anpassungen notwendig.

Beispiele für verschiedene Ausgaben der Protokolldateien sind:

- Gruppierung und Markierung zusammengehörender Protokolldaten (z. B. LogSurfer)
- Anzeige relevanter Protokolldaten, wobei irrelevante Daten mittels regulärer Ausdrücke ausgeblendet werden können. Auf diese Weise könnten beispielsweise diejenigen Protokolldaten ausgeblendet werden, die eine erfolgreiche Operation (z. B. GET bei HTTP) dokumentieren (z. B. checksyslog).

- Anzeige von Angriffen. Die Analyse der Protokolldaten muss dabei in Echtzeit vorgenommen werden.
- Statistische Analyse der Protokolldaten (z. B. wie oft trat welche Meldung auf).

Neben der reinen Darstellung relevanter Protokolldaten existieren Tools, die abhängig von einer erkannten Auffälligkeit Aktionen (z. B. Ausführen eines Befehls) ermöglichen.

Auffällige Protokolleinträge sind beispielsweise:

- Gehäuft auftretende Anfragen an Ports, auf denen keine Dienste laufen
- Nicht erfolgreiche Zugriffsversuche auf Komponenten des Sicherheitsgateways
- Aus dem nicht-vertrauenswürdigen Netz eintreffende Pakete mit IP-Adressen des vertrauenswürdigen Netzes (Hinweis auf IP-Spoofing)
- Verdächtige, ausgehende Verbindungen von Servern aus dem vertrauenswürdigen Netz. Diese können ein Anzeichen dafür sein, dass nach einem erfolgreichen Einbruch der Angreifer Daten aus dem vertrauenswürdigen Netz nach außen kopiert oder von außen Dateien nachlädt, die er für seine weiteren Aktivitäten braucht.

Regelmäßige Auswertung

Die Protokolldateien müssen regelmäßig ausgewertet werden und es sollte festgelegt werden, welche Auswertungen mindestens erfolgen sollen. Darüber hinaus sollten zumindest grobe Richtlinien dafür festgelegt werden, welche Schritte unternommen werden, wenn bei der Auswertung auffällige Einträge festgestellt werden.

Ergänzende Kontrollfragen:

- Welche Informationen werden an den Paketfiltern protokolliert?
- Falls ein ALG eingesetzt wird: Welche Informationen werden vom ALG für die verschiedenen Dienste protokolliert?
- In welchen Abständen und nach welchen Kriterien werden die Protokolle ausgewertet?

M 4.48 Passwortschutz unter NT-basierten Windows-Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der Zugang zu einem Windows NT/2000/XP/Server 2003 System muss für jeden Benutzer durch ein Passwort geschützt und die automatische Anmeldung deaktiviert sein. Benutzerkonten ohne Passwort dürfen nicht existieren, da sie eine Schwachstelle im System darstellen. Es ist wichtig, dass auch die Benutzer die Schutzfunktion der Passwörter kennen, denn die Mitarbeit der Benutzer trägt selbstverständlich zur Sicherheit des gesamten Systems bei. Grundlage für die weiteren Empfehlungen in dieser Maßnahme ist M 2.11 *Regelung des Passwortgebrauchs*.

individuelles Anfangspasswort vergeben

Die Einrichtung eines neuen Benutzers und die Definition eines Passwortes erfolgt unter Windows NT mit Hilfe des Dienstprogramms Benutzer-Manager über das Kommando *Neuer Benutzer*. Unter Windows 2000/XP/Server 2003 ist dazu für Stand-alone Rechner das Snap-in *Lokale Benutzer und Gruppen* der *Microsoft Management Console* (MMC) zu benutzen. Für in Active-Directory-Domänen angesiedelte Rechner erfolgt das Anlegen neuer Benutzer über das MMC Snap-in *Active Directory Benutzer und Computer*. In jedem Fall ist dazu in den Feldern *Kennwort* und *Kennwortbestätigung* ein Anfangspasswort einzugeben. Die Groß- und Kleinschreibung muss beachtet werden. Dabei sollte ein sinnvolles individuelles Anfangspasswort vergeben werden, das dem Benutzer mitgeteilt wird. Dies ist auch beim Zurücksetzen des Passwortes durch den Administrator zu beachten. Die immer gleiche Wahl des Anfangspasswortes oder die Verwendung des Benutzernamens als Passwort eröffnet eine Sicherheitslücke, die mit geringem Aufwand vermieden werden kann.

Die Option *Benutzer muss Kennwort bei der nächsten Anmeldung ändern* sollte bei allen neuen Konten gesetzt sein, damit das Anmeldepasswort nicht beibehalten wird. Dagegen sollte die Option *Benutzer kann Kennwort nicht ändern* nur in Ausnahmefällen verwendet werden, etwa für vordefinierte Konten im Schulungsbetrieb. Die Option *Kennwort läuft nie ab* sollte nur für Benutzerkonten, denen mit Hilfe der Systemsteuerungsoption *Dienste* ein Dienst zugewiesen wird (zum Beispiel das MS Exchange Dienstkonto) verwendet werden. Diese Option setzt die Einstellung *Maximales Kennwortalter* in den Richtlinien für Konten außer Kraft und verhindert, dass das Passwort abläuft.

Passwort-Richtlinien

Für Windows NT können über den Benutzer-Manager Richtlinien für Benutzerkonten, Benutzerrechte und für die Systemüberwachung festgelegt werden. Unter Windows 2000/XP/Server 2003 erfolgt das Festlegen der Richtlinien entweder durch das MMC Snap-in *Lokale Sicherheitseinstellungen* oder durch das Snap-in *Gruppenrichtlinien*. Die Parameter und Werte finden sich in den Snap-ins unter *Sicherheitseinstellungen* | *Kontorichtlinien*. Dabei können und sollen die Einstellungen der Gruppenrichtlinien für Rechner, die einer Domäne angeschlossen sind, auch über das Active Directory verteilt und

durchgesetzt werden (siehe M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000* und M 2.326 *Planung der Windows XP Gruppenrichtlinien*). Ab Windows 2000 ist für Kontorichtlinien eine Sicherheitsvorlage zu erstellen (siehe auch M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003*).

Die Anforderungen an Passwörter unter Windows NT/2000/XP/Server 2003 sollten dokumentiert werden, gegebenenfalls in Form einer Sicherheitsrichtlinie. Die Dokumentation bzw. Richtlinie sollte die Einstellungen der folgenden Tabelle umfassen. Die letzte Spalte enthält Mindest-Empfehlungen für normalen Schutzbedarf:

Windows NT	Windows 2000/XP/2003	
Maximales Kennwortalter		90 Tage
Minimales Kennwortalter		1 Tag
Minimale Kennwortlänge		8 Zeichen
Kennwortzyklus	Kennwortchronik erzwingen	6 Kennwörter
Konto sperren | Sperren nach	Kontosperrungsschwelle	3 Versuche
Konto sperren | Konto zurücksetzen nach	Zurücksetzungsdauer des Kontosperrungszählers	30 Minuten
Dauer der Sperrung	Kontosperrdauer	60 Minuten
Benutzer muss sich anmelden, um Kennwort zu ändern	n/v	Deaktiviert
n/v	Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
n/v	Kennwörter für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern	Deaktiviert

Tabelle: Übersicht der Mindest-Empfehlungen zu Kennwort-Einstellungen

Bei der Festlegung der Einstellungen sind einige systemspezifische Sicherheitsaspekte zu berücksichtigen, die im Folgenden erläutert werden.

2-stellige Passwortlänge

Die minimale Passwortlänge für besonders schützenswerte Konten (z. B. Dienstkonten) sollte mehr als 14 Zeichen betragen (Dies funktioniert allerdings nicht unter Windows NT 4.0, hier sollten solche Passwörter daher in kürzeren Abständen geändert werden). Hohe Passwortlängen sind bei steigender Rechenleistung der effektivste Schutz gegen Brute-Force-Angriffe.

Die Passworthistorie sollte grundsätzlich eingeschaltet sein und wenigstens 6 Passwörter umfassen. Die Gültigkeitsdauer des Passwortes sollte auf einen Zeitraum von maximal 6 Monaten begrenzt sein. Durch Festlegung eines Wertes für das *Minimale Kennwortalter* kann verhindert werden, dass Benutzer ihr Passwort mehrfach hintereinander ändern, um so die Historienprüfung zu umgehen. Das *Minimale Kennwortalter* sollte jedoch nicht größer als 1 Tag gewählt werden, um dem Benutzer jederzeit eine Passwortänderung zu ermöglichen.

Hinweis: Unter Windows NT 3.51 und NT 4.0 darf bei *Minimales Kennwortalter* nicht der Parameter *Sofortige Änderungen erlauben* gewählt werden, da sonst die Prüfung der Passworthistorie abgeschaltet wird.

Benutzerkonten nach mehreren Fehlversuchen sperren

Benutzerkonten sollten nach wiederholten ungültigen Passworteingaben gesperrt werden, um Versuche zu erschweren, die Passwörter der Benutzer zu erraten (Brute-Force-Angriffe). Mit den Werten aus der Tabelle erfolgt eine Sperrung nach drei ungültigen Anmeldeversuchen, die innerhalb von 29 Minuten unternommen wurden. Hatte ein Benutzer nur zwei ungültige Anmeldeversuche unternommen, erhält er 30 Minuten nach dem letzten Versuch wieder drei neue Anmeldeversuche.

In der Regel sollte eine Kontosperre nur durch einen Administrator aufgehoben werden können. Mit der Einstellung *Kontosperrdauer* wird das Konto nach einem begrenzten Zeitraum automatisch wieder entsperrt. Der Zeitraum darf nicht kürzer als die *Zurücksetzungsdauer des Kontosperrungszählers* sein und sollte keinesfalls 30 Minuten unterschreiten. Prinzipiell verringert eine automatische Entsperrung stark die Sicherheit. Falls der Aufwand für die Benutzerbetreuung und der mögliche Produktivitätsausfall durch gesperrte Benutzerkonten dies rechtfertigen, dann muss hierfür ein geeigneter, möglichst hoher Wert als Kompromiss gefunden werden. Bei besonders schützenswerten Konten sollte diese Funktion aber immer deaktiviert werden.

Administratorkonto von der Kontosperre ausnehmen

Es ist zu beachten, dass das vordefinierte Administratorkonto von dieser automatischen Sperrung ausgenommen ist, um ein völliges Verriegeln des Systems zu vermeiden.

Unter Windows NT4.0 sollte von der Option *Benutzer muss sich anmelden, um Kennwort zu ändern* kein Gebrauch gemacht werden. Insbesondere mit der Einstellung *Benutzer muss Kennwort bei der nächsten Anmeldung ändern* führt diese Einstellung dazu, dass neue Benutzer keinen Zugang zum Rechner erhalten.

Eine Passwort-Richtlinie pro Active-Directory-Forrest

Werden Passwort-Richtlinien auf Domänenebene eingestellt, ist keine weitere Differenzierung der Passwort-Anforderungen für Domänenkonten möglich. Nur lokale Konten einzelner Mitgliedsserver können mit eigenen Richtlinien versehen werden. Wenn Betriebsbereiche mit unterschiedlichen Passwort-Anforderungen zwingend erforderlich sind, kann dies nur durch mehrere Active-Directory-Forrests umgesetzt werden. Der Aufwand hierfür ist nur selten gerechtfertigt, daher muss beim Festlegen der Passwort-Anforderungen ein Kompromiss für alle Betriebsbereiche (Dienstkonten, administrative Konten, allgemeine Benutzerkonten, Benutzerkonten von leitenden Personen, Benutzerkonten für die Personalvertretung usw.) gefunden werden.

Ergänzende Kontrollfragen:

- Sind die Vorgaben für die Benutzerkonten-Richtlinien dokumentiert?
- Werden die Einstellungen im Benutzer-Manager regelmäßig kontrolliert?

M 4.49 Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Windows NT/2000/XP kann nur dann sicher betrieben werden, wenn vom Systemstart an gewährleistet ist, dass eine geschlossene Sicherheitsumgebung aufgebaut wird, also dass keine Wege an den Sicherheitsfunktionen des Betriebssystems vorbei bestehen. Dies erfordert, dass sich alle durch Windows NT/2000/XP schützbaren Ressourcen unter der Kontrolle des Betriebssystems befinden. Außerdem darf es auch keine Möglichkeit geben, fremde Systeme oder offene Systemumgebungen zu starten, die den durch Windows NT/2000/XP gebotenen Schutz unterlaufen können. Dazu sind die folgenden Aspekte zu beachten:

NTFS verwenden

- Alle vorhandenen Festplattenpartitionen müssen mit dem Dateisystem NTFS formatiert sein. Partitionen, die mit den Dateisystemen FAT12, FAT16, VFAT, FAT32 oder HPFS formatiert sind, können nicht gegen Zugriffe der Benutzer geschützt werden. Dies bedeutet einerseits, dass die auf ihnen abgelegten Daten beliebigen Zugriffen aller Benutzer ausgesetzt sind, und andererseits können diese Partitionen zum unkontrollierten Datenaustausch zwischen Benutzern missbraucht werden.

Diskettenlaufwerke sperren

- Ein ähnliches Risiko stellen Diskettenlaufwerke dar, da Disketten unter Windows NT/2000/XP nur mit dem Dateisystem FAT bzw. VFAT formatiert werden können. Aus diesem Grund sind Diskettenlaufwerke an allen Rechnern, die nicht unter strikter physischer Kontrolle stehen, grundsätzlich zu sperren (siehe M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*). Auf Windows NT/2000/XP Clients können die Diskettenlaufwerke auch durch Deaktivieren über die Systemsteuerungsoption *Geräte* bzw. *Computerverwaltung/Geräte-Manager*, Gerät *Floppy*, die Diskettenlaufwerke für unprivilegierte Benutzer außer Betrieb gesetzt werden. Hiervon sollte auf Windows NT/2000 Servern abgesehen werden (siehe hierzu M 4.52 *Geräteschutz unter NT-basierten Windows-Systemen*).

- Verfügt der Rechner über ein offenes Diskettenlaufwerk oder ist es möglich, von einem vorhandenen CD-ROM-Laufwerk zu booten, so besteht die Gefahr, dass der Rechner mit einem anderen Betriebssystem als Windows NT/2000/XP gestartet wird. Die gleiche Gefährdung ergibt sich, wenn der Rechner von einem USB-Speichermedium gestartet werden kann oder auf einer lokalen Festplatte andere Betriebssysteme installiert sind. Dann kann der Anwender mit verschiedenen Programmen die Sicherheitsmechanismen von Windows NT/2000/XP umgehen. Inzwischen gibt es mehrere Programme, mit denen man Dateien, die unter NTFS geschützt sind, von einer DOS-Umgebung oder einer Linux-Umgebung lesen und zum Teil auch ändern kann. Sowohl unter dem Betriebssystem MS-DOS als auch unter dem Betriebssystem Linux werden die vom Dateisystem NTFS gesetzten Sicherheitsattribute ignoriert. Der Anwender hat daher von MS-DOS bzw. von Linux aus Zugriff auf alle Dateien des Rechners. Aus diesem Grund dürfen neben Windows NT/2000/XP keine weiteren Betriebssysteme auf der Festplatte installiert sein. Außerdem ist der Boot-Vorgang durch eine mit einem BIOS-Passwort geschützte Einstellung des BIOS so abzusichern, dass das System nicht von einem eventuell vorhandenen Diskettenlaufwerk, von einem CD-/DVD-ROM-Laufwerk oder von einem USB-Speichermedium aus gestartet werden kann (siehe M 4.1 *Passwortschutz für IT-Systeme*).

BOOT.INI schützen

- Im Rahmen einer Neuinstallation von Windows NT/2000/XP hat man die Möglichkeit, die bestehende Installation des Betriebssystems zu aktualisieren oder eine neue Version parallel zu installieren. Bei der parallelen Installation wird die bestehende Dateistruktur nicht verändert, doch wird das vordefinierte Administratorkonto mit einem neuen Passwort neu angelegt. Dieser "neue" Administrator hat dann vollen Zugriff auf alle Ressourcen des Rechners und damit auch auf alle Daten und Programme. Um diese Möglichkeit der Neuinstallation zu verhindern, dürfen Benutzer nicht in der Lage sein, die Datei *BOOT.INI* im Wurzelverzeichnis der ersten Platte zu verändern (siehe M 4.53 *Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT*, M 4.149 *Datei- und Freigabeberechtigungen unter Windows 2000/XP*, M 4.247 *Restriktive Berechtigungsvergabe unter Windows XP*).
- Mit Hilfe der Installationsprogramme kann für Windows NT/2000 auch eine Notfalldiskette (siehe M 6.42 *Erstellung von Rettungsdisketten für Windows NT*, M 6.77 *Erstellung von Rettungsdisketten für Windows 2000*) erzeugt und mit dieser dann eine Systemrekonstruktion durchgeführt werden. Dabei wird der Zugriffsschutz der NTFS-Partition des Betriebssystems aufgehoben. Es ist aus diesem Grund unbedingt erforderlich, die Installationsprogramme, eine eventuell schon vorhandene Notfalldiskette und die Setup-Disketten so zu verwahren, dass sie gegen unbefugten Zugriff geschützt sind. Schutz gegen diese spezifische Bedrohung bietet auch die Sicherung der Diskettenlaufwerke (siehe M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*) und die Absicherung des Boot-Vorgangs durch die entsprechende Einstellung des BIOS (siehe oben).

- Für die Systemrekonstruktion unter Windows XP wird die Wiederherstellungskonsole (Recovery Console) verwendet. Der Mechanismus der Notfalldisketten steht nicht mehr zur Verfügung. Die Wiederherstellungskonsole kann entweder von der Installations-CD bzw. den Installations-Disketten gestartet oder in das System integriert werden, so dass es beim Systemstart als eine der Boot-Optionen angeboten wird. Da die Wiederherstellungskonsole ein mächtiges Werkzeug ist, muss ihr Einsatz durch die entsprechende Einstellung des BIOS bzw. im allgemeinen durch die Definition der Wiederherstellungskonsole-Richtlinien (siehe M 4.244 *Sichere Windows XP Systemkonfiguration*) eingeschränkt werden.

Unter Windows NT/2000/XP ist das lokale Anmelden auf dem Server nur für Benutzer möglich, denen das Benutzerrecht *Lokale Anmeldung* gegeben wurde. Diese Benutzer sind auf die ihnen zugewiesenen Rechte und Berechtigungen eingeschränkt. Um einen Missbrauch der Möglichkeiten zum Anmelden auf dem Server zu vermeiden, sind die Benutzerrechte und die Zuordnungen zu Benutzergruppen entsprechend restriktiv vorzusehen (siehe Maßnahmen M 2.93 *Planung des Windows NT Netzes* und M 4.50 *Strukturierte Systemverwaltung unter Windows NT*). Unter Windows 2000/XP erfolgt die Verwaltung der Benutzerrechte über die lokalen Sicherheitseinstellungen bzw. über Gruppenrichtlinien (siehe M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000*, M 2.326 *Planung der Windows XP Gruppenrichtlinien*).

Ergänzende Kontrollfragen:

- Ist sichergestellt, dass Benutzer den Computer nicht von Disketten-, CD-ROM-Laufwerken oder USB-Speichermedien booten können?
- Ist die Datei *BOOT.INI* im Wurzelverzeichnis der ersten Platte vor Veränderungen geschützt?

M 4.50 Strukturierte Systemverwaltung unter Windows NT

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Benutzergruppen sind unter Windows NT Zusammenstellungen von Benutzerkonten. Wenn ein Benutzerkonto zu einer Gruppe hinzugefügt wird, erhält der betreffende Benutzer alle Rechte und Berechtigungen, die der Gruppe erteilt wurden. So kann man leicht bestimmte Benutzer mit gemeinsamen Möglichkeiten ausstatten. Nach Möglichkeit sollten die Rollen der Mitarbeiter auf Gruppen abgebildet und diesen Gruppen entsprechend ihren Bedürfnissen die Zugriffsrechte zugeteilt werden.

Die Verwendung von Gruppen an Stelle der Zuweisung von Rechten und Berechtigungen an einzelne Benutzer erleichtert die Administration und trägt durch größere Transparenz zur Erhöhung der Systemsicherheit bei. Auch bei einer geringen Anzahl von Mitarbeitern sollten Gruppen gebildet werden. Hierdurch muss bei einer Erweiterung keine grundsätzliche Umstrukturierung der Rechtestrukturen durchgeführt werden.

Rechte und Berechtigungen sind additiv, d. h. für einen Benutzer, der Mitglied in mehreren Gruppen ist, gilt in Bezug auf eine Ressource die jeweils weitestgehende Zugriffsberechtigung. Es gibt allerdings eine **Ausnahme:** Ist ein Benutzer Mitglied einer Gruppe, der auf eine Ressource die Zugriffsberechtigung "Kein Zugriff" zugeteilt wurde, so kann der Benutzer auf diese Ressource nicht zugreifen, auch dann nicht, wenn er Mitglied einer anderen Gruppe ist, der auf diese Ressource die Zugriffsberechtigung "Vollzugriff" erteilt wurde (siehe auch M 4.53 *Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT*).

Beispiel:

Benutzer Meier ist Mitglied der Gruppen "A" und "B". Der Gruppe "A" wurde auf ein Verzeichnis "Rechnung" die Zugriffsberechtigung "Lesen", der Gruppe "B" wurden auf dieses Verzeichnis die Zugriffsberechtigungen "Lesen und Schreiben" zugewiesen. Der Benutzer Meier hat damit auf das Verzeichnis "Rechnung" die Zugriffsberechtigungen "Lesen und Schreiben".

Das Benutzergruppenkonzept von Windows NT unterscheidet zwischen globalen und lokalen Gruppen.

Lokale Gruppen

Die Gruppe wird "lokal" genannt, weil ihr Berechtigungen und Rechte nur für den Rechner erteilt werden können, auf dem sie definiert wurde. Auf Rechnern unter dem Betriebssystem Windows NT (d. h. sowohl Servern als auch Workstations), die keiner Domäne angehören, gibt es nur lokale Gruppen. Um die Vergabe von Rechten und Berechtigungen zu strukturieren, wird auf solchen Rechnern ausschließlich dieser Gruppentyp benutzt.

Gehört ein Rechner unter Windows NT einer Domäne an, so sind lokale Gruppen ebenfalls verfügbar. Sie können dann Benutzerkonten aus dem eige-

nen Rechner und Benutzerkonten und globale Gruppen aus der eigenen Domäne und aus vertrauten Domänen beinhalten.

Lokale Gruppen können keine Berechtigungen auf Ressourcen anderer Domänen erhalten. Es ist nicht möglich, eine lokale Gruppe zum Mitglied einer anderen lokalen Gruppe zu machen. Lokale Gruppen werden im Benutzermanager durch ein Gruppensymbol mit einem Computer dargestellt.

Globale Gruppen

Wenn ein Rechner, auf dem Windows NT ausgeführt wird, einer Domäne angehört, gibt es einen weiteren Gruppentyp, dem der Zugriff auf die Arbeitsstation ermöglicht werden kann. Es handelt sich um die "Globale Gruppe", die an mehreren Orten verwendet werden kann: in der eigenen Domäne, auf Servern, auf Arbeitsstationen der Domäne und in vertrauten Domänen. Wenn eine Arbeitsstation einer Domäne angehört, bedeutet dies, dass den globalen Gruppen der Domäne und der vertrauten Domänen Berechtigungen und Rechte für die Arbeitsstation sowie die Zugehörigkeit zu lokalen Gruppen der Arbeitsstation erteilt werden können. Eine globale Gruppe kann nur Benutzerkonten der eigenen Domäne enthalten.

Globale Gruppen können nur auf dem primären Domänencontroller definiert werden. Es ist nicht möglich, dass andere Gruppen Mitglied einer globalen Gruppe werden. Globale Gruppen werden im Benutzermanager durch ein Gruppensymbol mit einem Globus dargestellt.

Zusammenfassend empfiehlt sich folgendes Vorgehen zur strukturierten Systemverwaltung:

Rechte und Berechtigungen werden *lokalen* Gruppen zugewiesen. Benutzer werden Mitglied in *globalen* Gruppen, und die *globalen* Gruppen werden Mitglied in *lokalen* Gruppen.

Neben der Unterscheidung in lokale und globale Gruppen gibt es auch noch die Unterscheidung zwischen vordefinierten Benutzergruppen, besonderen Gruppen und frei definierten Benutzergruppen:

Vordefinierte Benutzergruppen

Welche Aktionen ein Benutzer durchführen kann, hängt von den Gruppenmitgliedschaften seines Benutzerkontos ab. Es sind mehrere Gruppen in Windows NT vordefiniert, und standardmäßig wird jeder Gruppe ein bestimmter Satz von Benutzerrechten erteilt. Bei Bedarf können mit dem Benutzermanager zusätzliche Gruppen erstellt und definiert werden, mit denen den ihnen zugewiesenen Benutzern der Zugriff auf individuell zusammengestellte Ressourcen ermöglicht wird.

Zusätzlich zu den Rechten werden einigen der vordefinierten lokalen Gruppen vordefinierte Funktionen zugeteilt. Rechte und Zugriffsberechtigungen können den Gruppen und Benutzerkonten direkt erteilt und ihnen entzogen werden. Dagegen sind die vordefinierten Funktionen nicht direkt verwaltungsfähig. Vordefinierte Funktionen können für einen Benutzer nur bereitgestellt werden, wenn der Benutzer zum Mitglied einer geeigneten lokalen Gruppe ernannt wird.

Auf Rechnern, die unter dem Betriebssystem Windows NT als Mitgliedsserver (Server ohne Domänencontroller-Funktionalität) oder als Workstation konfiguriert sind, werden folgende lokale Gruppen standardmäßig bei der Installation eingerichtet:

- Administratoren
- Sicherungs-Operatoren
- Hauptbenutzer
- Replikations-Operatoren
- Benutzer
- Gäste

Die Rechte und Funktionen, die unter Windows NT auf Workstations und Servern, die nicht als Domänencontroller konfiguriert sind, bestimmten vordefinierten lokalen Gruppen erteilt werden, sind in der folgenden Tabelle angegeben:

	Adminstratoren	Hauptnutzer	Benutzer	Gäste	Jeder	Sicherungs-Operatoren
Lokale Anmeldung	■	■	■	■	■	■
Zugriff auf diesen Computer im Netz	■	■			■	
Übernehmen des Besitzes an Dateien und Objekten	■					
Verwaltung von Überwachungs- und Sicherheitsprotokollen	■					
Ändern der Systemzeit	■	■				
System herunterfahren	■	■	■		■	■
Herunterfahren von einem Fernsystem aus	■	■				
Sichern von Daten und Verzeichnissen	■					■
Wiederherstellen von Diensten und Verzeichnissen	■					■

Tabelle: Rechte und Funktionen unter Windows NT auf Workstations und Servern

	Adminstratoren	Hauptnutzer	Benutzer	Gäste	Jeder	Sicherungs-Operatoren
Erzeugung und Verwaltung von Benutzerkonten	■	■				
Erzeugung und Verwaltung lokaler Gruppen	■	■	■			
Erteilung von Benutzerrechten	■					
Sperrung der Arbeitsstation	■	■			■	
Zugriff auf eine gesperrte Arbeitsstation	■					
Formatierung der Festplatte	■					
Erzeugung gemeinsamer Gruppen	■	■				
Speicherung lokaler Profile	■	■	■			■
Freigabe von Verzeichnissen	■	■				
Freigabe von Druckern	■	■				
Laden und Entfernen von Gerätetreibern	■	■				

Tabelle: Fortsetzung der Tabelle Rechte und Funktionen unter Windows NT auf Workstations und Servern

Auf Servern, die unter dem Betriebssystem Windows NT als Domänen-controller konfiguriert sind, werden folgende lokale Gruppen standardmäßig bei der Installation eingerichtet:

- Administratoren
- Sicherungs-Operatoren
- Server-Operatoren
- Konten-Operatoren
- Druck-Operatoren
- Replikations-Operatoren

- Benutzer
- Gäste

Außerdem werden in dieser Konfiguration folgende globale Gruppen bei der Installation angelegt:

- Domänen-Admins
- Domänen-Benutzer
- Domänen-Gäste

Die Rechte und Funktionen, die unter Windows NT auf Domänencontrollern bestimmten vordefinierten lokalen Gruppen erteilt werden, sind in der folgenden Tabelle angegeben:

	Adminstratoren	Server-Operatoren	Konten-Operatoren	Druck-Operatoren	Sicherungs-Operatoren	Jeder	Benutzer	Gäste
Lokale Anmeldung	■	■	■	■	■			
Zugriff auf diesen Computer vom Netz	■					■		
Übernehmen des Besitzes an Dateien und Objekten	■							
Verwalten von Überwachungs- und Sicherheitsprotokollen	■							
Ändern der Systemzeit	■	■						
System herunterfahren	■	■	■	■	■			
Herunterfahren von einem Fernsystem aus	■	■						
Hinzufügen von Arbeitsstationen zur Domäne	■							
Sichern von Dateien und Verzeichnissen	■	■			■			
Wiederherstellen von Dateien und Verzeichnissen	■	■			■			

Tabelle: Rechte und Funktionen unter Windows NT auf Domänencontrollern

	Adminstratoren	Server-Operatoren	Konten-Operatoren	Druck-Operatoren	Sicherungs-Operatoren	Jeder	Benutzer	Gäste
Erzeugung und Verwaltung von Benutzerkonten	■		■					
Erzeugung und Verwaltung globaler Gruppen	■		■					
Erzeugung und Verwaltung lokaler Gruppen	■		■				■	
Erteilung von Benutzerrechten	■							
Sperren des Servers	■	■				■		
Zugriff auf einen gesperrten Server	■							
Formatierung der Server-Festplatte	■	■						
Erzeugung gemeinsamer Gruppen	■	■						
Speicherung lokaler Profile	■	■	■	■	■			
Freigabe von Verzeichnissen	■	■						
Freigabe von Druckern	■	■		■				
Laden und Entfernen von Gerätetreibern	■							

Tabelle: Fortsetzung der Tabelle Rechte und Funktionen unter Windows NT auf Domänencontrollern

Hinweis: Die oben beschriebenen Rechte, die unter Windows NT standardmäßig vergeben sind, sind alle einzeln daraufhin zu überprüfen, ob sie mit der festgelegten Sicherheitsstrategie vereinbar sind (siehe M 2.91 *Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz*). So sollte beispielsweise das Recht "Zugriff auf diesen Computer vom Netz" der Gruppe "Jeder" entzogen werden. Ob es ersatzweise der Gruppe "Benutzer" zugestanden wird, ist im einzelnen zu klären.

Die folgenden vordefinierten Gruppen stehen unter Windows NT zur Verfügung:

- *Administratoren* - Die Gruppe "*Administratoren*" ist die mächtigste Gruppe in Windows NT. Die Mitglieder dieser Gruppe verwalten die Gesamtkonfiguration des Systems. Das vordefinierte Benutzerkonto "Administrator" ist Mitglied der Gruppe "*Administratoren*". Falls ein Rechner einer Domäne angehört, ist die Gruppe "*Domänen-Admins*" standardmäßig Mitglied der Gruppe "*Administratoren*" dieses Rechners.

Hinweis: Benutzerkonten dieser Gruppe sollten nur zu Systemverwaltungsarbeiten verwendet werden, die die volle Kontrolle über das System erfordern. Arbeiten, die unter eingeschränkten Rechten durchgeführt werden können, sollten nach Möglichkeit von Benutzerkonten aus erledigt werden, die einer der anderen Gruppen angehören, um die Gefährdung des Systems durch Arbeiten mit unbeschränkten Rechten zu reduzieren. Insbesondere sollte für jeden Administrator zur Erledigung der täglichen Routinearbeiten jeweils ein Benutzerkonto angelegt werden, das nur der Gruppe "Benutzer" oder einer bzw. mehreren frei definierten Gruppen angehört. Die Anzahl der Benutzerkonten in der Gruppe "Administratoren" sollte so gering wie möglich gehalten werden.

Administratoren sind der normalen Zugriffskontrolle unterworfen und besitzen nicht automatisch Zugriff auf jede Datei. Bei Bedarf kann ein Administrator den Besitz einer Datei übernehmen und dadurch auf sie zugreifen. Der Administrator kann die Datei jedoch in diesem Fall nicht wieder an den ursprünglichen Besitzer zurückgeben, da Windows NT hierzu keine Funktion bereitstellt.

- *Domänen-Admins* - Die globale Gruppe der "*Domänen-Admins*" ist Mitglied der lokalen Gruppe der Administratoren für die betreffende Domäne und der lokalen Gruppen der Administratoren jedes Rechners in der Domäne, so dass die Domänen-Administratoren die Domänencontroller, alle Server und alle anderen Rechner in der Domäne verwalten können. Das vordefinierte Administratorkonto des Domänencontrollers ist Mitglied der Gruppe "*Domänen-Admins*".
- *Hauptbenutzer* - Die unter Windows NT Workstation definierte lokale Gruppe "*Hauptbenutzer*" stellt den Benutzerkonten ihrer Mitglieder eingeschränkte administrative Funktionen bereit. Ein Hauptbenutzer kann Verzeichnisse im Netz freigeben, die interne Uhr des Computers einstellen, Drucker installieren, freigeben und verwalten sowie allgemeine Programmgruppen erstellen. Sie können Benutzerkonten und Gruppen erstellen und die von ihnen erstellten Benutzerkonten und Gruppen ändern und löschen, und sie können für die Gruppen "*Hauptbenutzer*", "*Benutzer*" und "*Gäste*" Mitglieder entfernen bzw. hinzufügen.

  Hauptbenutzer können jedoch nicht die Gruppen "*Administratoren*", "*Domänen-Admins*", "*Konten-Operatoren*", "*Sicherungs-Operatoren*", "*Druck-Operatoren*" und "*Server-Operatoren*" verändern oder löschen, und sie können auch keine Benutzerkonten von Administratoren verändern oder löschen.

  Hinweis: Diese Gruppe sollte verwendet werden, um Untersystemverwalter zu definieren, die den Systemverwalter von gewissen Routineaufgaben, insbesondere in der Verwaltung der Benutzerkonten, entlasten, ohne jedoch dazu die volle Kontrolle über das System zu erhalten.
- *Konten-Operatoren* - Die auf Domänencontrollern definierte lokale Gruppe "*Konten-Operatoren*" entspricht weitgehend der unter Windows NT Workstation definierten Gruppe "*Hauptbenutzer*".

- *Benutzer* - Die Zugehörigkeit zur lokalen Gruppe "*Benutzer*" bietet die Funktionen, die ein Benutzer zur Durchführung der alltäglichen Aufgaben benötigt. Mit Ausnahme der vordefinierten Administrator- und Gastkonten gehören alle Benutzerkonten der Arbeitsstation der Gruppe "*Benutzer*" an. Wird ein neues Benutzerkonto hinzugefügt, so wird es automatisch Mitglied dieser Gruppe. Falls ein Rechner einer Domäne angehört, ist die Gruppe der Domänen-Benutzer standardmäßig Mitglied der Gruppe "*Benutzer*" dieses Rechners.

  Hinweis: Normalerweise sollten alle Benutzer, die keine erweiterten Rechte benötigen, nur dieser vordefinierten Gruppe sowie geeigneten frei definierten Gruppen angehören, die die Organisationsstruktur widerspiegeln. Zuordnungen zu den anderen vordefinierten Gruppen sollten nur in begründeten Einzelfällen vorgenommen werden. Dies bedeutet auch, dass Benutzer keine Administratorrechte auf ihren Arbeitsplatzrechnern erhalten sollten.

- *Domänen-Benutzer* - Die globale Gruppe der "*Domänen-Benutzer*" enthält ursprünglich das eingebaute Konto des Administrators für die betreffende Domäne. Beim Anlegen neuer Konten werden diese automatisch in die Gruppe der "*Domänen-Benutzer*" eingetragen. Diese Gruppe ist standardmäßig Mitglied der lokalen Gruppe "*Benutzer*" für die betreffende Domäne und der lokalen Gruppen der "*Benutzer*" jedes Rechners in der Domäne, so dass die "*Domänen-Benutzer*" normalen Zugang und normale Rechte und Berechtigungen bezüglich aller Rechner in der Domäne haben.

- *Gäste* - Die lokale Gruppe "*Gäste*" ermöglicht es dem gelegentlichen oder einmaligen Benutzer, sich anzumelden und mit eingeschränktem Funktionsumfang zu arbeiten. Das vordefinierte Gastbenutzerkonto ist Mitglied der Gruppe "*Gäste*". Die der Gruppe "*Benutzer*" erteilten Ressourcenberechtigungen können der Gruppe "*Gäste*" vorenthalten werden, so dass die Möglichkeiten der Mitglieder dieser Gruppe geeignet eingeschränkt werden können.

  Hinweis: Nach Möglichkeit sollten dieser Gruppe außer dem vordefinierten Gastkonto keine weiteren Benutzerkonten angehören, und das vordefinierte Gastkonto sollte gesperrt sein (siehe M 4.55 *Sichere Installation von Windows NT*). Außerdem sollte es vorsorglich mit einem Passwort versehen werden, um unbefugten Zugriffen vorzubeugen, falls es kurzfristig entsperrt werden sollte.

- *Domänen-Gäste* - Die globale Gruppe der "*Domänen-Gäste*" enthält ursprünglich das eingebaute Gastbenutzerkonto für die betreffende Domäne. Diese Gruppe ist Mitglied der lokalen Gruppe der Gäste für die betreffende Domäne.

- *Sicherungs-Operatoren* - Die Mitglieder der lokalen Gruppe "*Sicherungs-Operatoren*", die standardmäßig auf allen Rechnern unter Windows NT definiert ist, können Dateien und Verzeichnisse sichern und wiederherstellen.

Hinweis: Datensicherungen und die Wiederherstellung gesicherter Daten sollten von einem Mitglied dieser Gruppe durchgeführt werden. Es ist hierzu nicht erforderlich, ein Administratorkonto zu verwenden.

- *Druck-Operatoren* - Die Mitglieder der auf Domänencontrollern definierten lokalen Gruppe "*Druck-Operatoren*" können Drucker auf den Domänencontrollern verwalten. Sie können sich auch auf diesen Servern anmelden und sie herunterfahren.

  Hinweis: Die Verwaltung von Druckern sollte von Mitgliedern dieser Gruppe durchgeführt werden, um die unnötige Nutzung von Administratorkonten zu vermeiden.

- *Server-Operatoren* - Die Mitglieder der auf Domänencontrollern definierten lokalen Gruppe "*Server-Operatoren*" können die Drucker- und Netzfreigaben auf dem jeweiligen Domänencontroller verwalten. Weiterhin können sie Dateien und Verzeichnisse sichern und wiederherstellen, den Domänencontroller sperren und freigeben, die Festplatten des Domänencontrollers formatieren und die Systemzeit verändern. Schließlich können sie sich auch auf dem Domänencontroller anmelden und ihn herunterfahren.

  Hinweis: Routinearbeiten zur Steuerung der Domänencontroller sollten von Mitgliedern dieser Gruppe durchgeführt werden, soweit sie mit den Rechten dieser Gruppe ausgeführt werden können. Nur Arbeiten, die die völlige Kontrolle über das System erfordern, sollten von Administratorkonten aus durchgeführt werden.

- *Replikations-Operator* - Die auf Rechnern unter Windows NT definierte lokale Gruppe "*Replikations-Operator*" unterstützt die Funktionen der Verzeichnisreproduktion. Der Gruppe "*Replikations-Operator*" sollte als einziges Mitglied ein Domänenbenutzerkonto angehören, das zum Anmelden des Replikationsdienstes der Arbeitsstation dient.

  Hinweis: Dieser Gruppe sollten keine Konten von Benutzern hinzugefügt werden, und das dort vorhandene Benutzerkonto sollte nicht über die Rechte "*Lokale Anmeldung*" und "*Zugriff auf diesen Computer vom Netz*" verfügen.

Besondere Gruppen

Zusätzlich zu den oben erwähnten vordefinierten Gruppen erstellt Windows NT einige spezielle, interne Gruppen, die vom Benutzermanager nicht angezeigt werden. Sie werden jedoch in manchen Fällen in der Gruppenliste angezeigt, beispielsweise beim Zuweisen von Berechtigungen zu Verzeichnissen, Dateien, freigegebenen Netzverzeichnissen oder Druckern.

- *Jeder* - Jeder, der am Computer arbeitet. Dazu zählen alle lokalen und Fernbenutzer (d. h. die Gruppen "*INTERAKTIV*" und "*NETZWERK*" zusammengenommen). Sie können auf das Netz zugreifen, sich mit den freigegebenen Netzverzeichnissen der Arbeitsstation verbinden und den Drucker der Arbeitsstation verwenden.

- *INTERAKTIV* - Jeder, der am Computer lokal arbeitet.

- *NETZWERK* - Alle Benutzer, die über das Netz mit diesem Computer verbunden sind.
- *SYSTEM* - Das Betriebssystem.
- *ERSTELLER-BESITZER* - Der Benutzer, der folgendes erstellt hat oder besitzt: ein Verzeichnis, eine Datei in einem Verzeichnis, einen Drucker oder ein Dokument, das zu einem Drucker gesendet wurde.

Frei definierte Benutzergruppen:

Mit Hilfe von frei definierten Benutzergruppen ist es möglich, die Organisationsstruktur einer Institution auf die Rechtestruktur abzubilden. So kann für jede Organisationseinheit, also z. B. für jedes Referat bzw. für jede Abteilung, eine Gruppe gebildet werden, in der die Benutzer der jeweiligen Organisationseinheit zusammengefasst sind. Den Gruppen werden dann die notwendigen Berechtigungen auf Ressourcen zugewiesen. Werden innerhalb der Institution für vorübergehende Aufgaben Projektgruppen gebildet, so können auch diese durch Zusammenfassung der Projektgruppenmitglieder in einer entsprechenden frei definierten Gruppe abgebildet werden.

Bei der Erstellung von frei definierten Benutzergruppen auf dem primären Domänencontroller ist festzulegen, ob diese vom Typ lokal oder global sind.

Ergänzende Kontrollfragen:

- Wurde eine Strategie zur Verteilung der Benutzer auf die vordefinierten Gruppen entsprechend den von diesen Benutzern benötigten Rechten festgelegt?
- Ist diese Strategie dokumentiert?
- Wird regelmäßig kontrolliert, ob die Zuordnung der Benutzer zu den Gruppen noch mit den aktuellen Aufgaben dieser Benutzer übereinstimmt?

M 4.51 Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Benutzerprofile dienen der Speicherung von benutzerspezifischen Einstellungen der Benutzerumgebung. Dies ist u. a. der Inhalt von Programmgruppen, die Netzwerk- und Druckerverbindungen und die farbliche Darstellung des Bildschirms. Weiterhin können über Benutzerprofile die Möglichkeiten der Benutzer, mit Windows NT zu arbeiten, in verschiedener Hinsicht eingeschränkt werden. Die Verwaltung der Profile erfolgt mit dem Benutzerprofil-Editor (UPEDIT.EXE unter Windows NT 3.51 bzw. POLEDIT.EXE unter Windows NT 4.0).

Benutzerprofile können für verschiedene Einsatzzwecke erstellt werden:

- um bei Single-User-Systemen nach einer erneuten Anmeldung die ursprünglich festgelegten Einstellungen wiederherzustellen,
- um bei Multi-User-Systemen für jeden Benutzer eigene Einstellungen festzulegen,
- damit bei server-gespeicherten Benutzerprofilen jeder Benutzer von jeder NT-Workstation aus dieselbe Oberfläche erhält,
- um einheitliche Benutzerumgebungen zentral vorzugeben (sowohl bei Stand-alone-Systemen als auch bei vernetzten),
- um eine eingeschränkte Benutzerumgebung einzurichten, beispielweise um zu verhindern, dass Benutzer Änderungen an Desktop-Einstellungen vornehmen, oder den Zugriff auf die Systemsteuerung einzuschränken.

Grundsätzlich muss zwischen lokalen und server-gespeicherten Benutzerprofilen unterschieden werden. Lokale Benutzerprofile werden nur auf dem lokalem IT-System abgelegt, während server-gespeicherte Benutzerprofile zentral auf dem NT-Server verwaltet werden.

Fällt bei Verwendung von server-gespeicherten Benutzerprofilen der Server aus, dann wird auf die lokale Kopie zurückgegriffen.

Daneben muss zwischen persönlichen und verbindlichen Benutzerprofilen unterschieden werden. Persönliche Benutzerprofile sind vom Benutzer beliebig änderbar, verbindliche werden vom Administrator vorgegeben.

Verbindliche Profile bleiben von einer Sitzung zur nächsten erhalten, während einer Sitzung durchgeführte Veränderungen gehen beim Abmelden verloren. Diese Profile werden in dem Verzeichnis abgelegt, der im Profileintrag des betreffenden Kontos angegeben ist, und sie tragen unter der Version 3.51 von Windows NT die Dateinamenserweiterung *.MAN*. Ab Version 4.0 wird ein Profil dadurch als verbindliches Profil gekennzeichnet, dass die Datei *NTUSER.DAT* in *NTUSER.MAN* umbenannt wird.

Persönliche Profile, die auf einem Server abgelegt werden, können verwendet werden, um Benutzern unabhängig von der Arbeitsstation, von der aus sie

sich anmelden, dieselbe Umgebung zur Verfügung zu stellen. Persönliche Profile werden in dem Verzeichnis abgelegt, der im Profileintrag des betreffenden Kontos angegeben ist, und sie tragen unter Version 3.51 die Dateinamenserweiterung *.USR*.

Unter Version 3.51 werden die Benutzerprofile im Verzeichnis *%SystemRoot%\system32\config* in den Benutzern zugeordneten Dateien abgelegt. Dabei werden die folgenden Einstellungen im Benutzerprofil abgelegt:

- *Programm Manager:* alle vom Benutzer einstellbaren Optionen einschließlich Programmgruppen, Programme und ihre Eigenschaften, sowie alle abspeicherbaren Einstellungen
- *Dateimanager:* alle vom Benutzer wählbaren Einstellungen einschließlich der Netz-Verbindungen
- *Kommandomodus:* alle vom Benutzer wählbaren Einstellungen
- *Druck Manager:* netzweite Druckerverbindungen sowie alle abspeicherbaren Einstellungen
- *Systemsteuerung:* alle Einstellungen für Farben, Maus, Desktop, Zeiger, Tastatur, Ländereinstellungen und Klänge sowie die Einträge zur Benutzerumgebung im Element "System"
- *Zubehör:* alle benutzerspezifischen Einstellungen der Anwendungen
- *Fremdanwendungen:* alle Einstellungen, die von diesen Anwendungen als benutzerspezifische Optionen unterstützt werden
- *Anmerkungen bei der online Hilfe:* alle dort eingetragenen Anmerkungen des betreffenden Benutzers

Ab Version 4.0 werden Benutzerprofile als Verzeichnisbaum unter dem Unterverzeichnis *Profiles* des Windows-Verzeichnisses *%SystemRoot%*, also im allgemeinen *\WINNT\Profiles*, als Verzeichnis mit dem Namen des Benutzers, z. B. *\WINNT\Profiles\Schmidt*, abgelegt. Dabei wird die gesamte Struktur der Arbeitsoberfläche und insbesondere die Struktur der einzelnen Programmgruppen dort abgelegt. Die folgenden Unterverzeichnisse können dabei vorhanden sein:

- *Anwendungsdaten:* Anwendungsspezifische Daten
- *Desktop:* Elemente der Arbeitsoberfläche einschließlich der direkt auf der Arbeitsoberfläche abgelegten Dateien und Shortcuts
- *Druckumgebung:* Shortcuts zu den Einträgen in den Druckerordnern
- *Favoriten:* Shortcuts zu Programmeinträgen und Ordnern mit Favoriten
- *Netzwerkumgebung:* Shortcuts zu den Einträgen der Netzumgebung
- *Persönlich:* Shortcuts zu den Einträgen in den privaten Programmgruppen
- *Recent:* Shortcuts zu den zuletzt verwendeten Dokumenten

- *SendTo:* Shortcuts zu den Einträgen, die im Kontextmenü als Ziele von Sende-Operationen, wie etwa zu einem Diskettenlaufwerk, verwendet werden können
- *Startmenü:* Struktur des gesamten Startmenüs einschließlich aller Shortcuts zu Programmen und Programmgruppen
- *Vorlagen:* Shortcuts zu Dokumentenvorlagen

Sonstige Einstellungen, wie etwa der Verweis auf das als Hintergrund der Arbeitsoberfläche verwendete Bild oder andere benutzerspezifische Einstellungen der Systemsteuerung, werden im Ordner *Profiles* in der Datei *NTUSER.DAT* abgelegt.

Die folgenden Optionen können unter Version 3.51 verwendet werden, um die Möglichkeiten der Benutzer mit Windows NT zu arbeiten in verschiedener Hinsicht einzuschränken:

- *Einstellungen für Programm Manager*: Hier kann festgelegt werden, ob Programme über "Datei - Ausführen" gestartet werden dürfen, die aktuellen Einstellungen gespeichert werden dürfen und ob allgemeine Programmgruppen angezeigt werden. Außerdem kann die Autostartgruppe festgelegt werden.
- *Einstellungen für Programmgruppen*: Hier kann der Zugriff auf bestimmte Programmgruppen gesperrt werden und für ungesperrte Programmgruppen verschiedene Änderungsbefugnisse vergeben werden.
- Den Benutzern kann das Verbinden bzw. Trennen von Netzdruckern über den Druckmanager erlaubt oder verboten werden.
- Es kann erzwungen werden, dass die Ausführung des Anmeldeskriptes abgewartet wird, bevor der Programm-Manager gestartet wird. Diese Option sollte immer aktiviert sein, damit die im Anmeldeskript vorgesehenen Aktionen auf jeden Fall durchgeführt werden.

Ab der Version 4.0 können die folgenden Einschränkungen mit Hilfe des Systemrichtlinien-Editors festgelegt werden:

- *Systemsteuerung:* Hier kann der Zugriff auf die Systemsteuerungsoption "*Anzeige*" beschränkt werden. Wenn diese Option gewählt wurde, können noch zusätzlich die Registerkarten "*Hintergrund*", "*Bildschirmschoner*", "*Darstellung*" und "*Einstellungen*" einzeln ausgeblendet werden, und die Option "*Anzeige*" kann auch als Ganzes deaktiviert werden.

  Normalen Benutzern sollte der Zugriff auf die Systemsteuerung entzogen werden, da unbeabsichtigte Änderungen an den Systemeinstellungen Probleme verursachen können. Wenn zusätzlich der Zugriff auf die Systemsteuerungsoption "*Anzeige*" bzw. die Registerkarte "*Bildschirmschoner*" entzogen wird, kann verhindert werden, dass Benutzer die Bildschirmsperre deaktivieren. Dann muss der Administrator natürlich beim Einrichten von Benutzern die Bildschirmsperre aktivieren.
- *Shell:* Hier können folgende Einschränkungen festgelegt werden:
  - Befehl "*Ausführen*" entfernen

  - Ordner unter Einstellungen im Menü "*Start*" entfernen
  - "*Task-Leiste*" unter Einstellungen im Menü "*Start*" entfernen
  - Befehl "*Suchen*" entfernen
  - Laufwerke im Fenster "*Arbeitsplatz*" ausblenden
  - Netzwerkumgebung ausblenden
  - Kein Symbol "*Gesamtes Netzwerk*" in der Netzwerkumgebung
  - Keine Arbeitsgruppen-Computer in Netzwerkumgebung
  - Alle Desktop-Elemente ausblenden
  - Befehl "Beenden" deaktivieren
  - Keine Einstellungen beim Beenden speichern
- *System:* Hier können folgende Einschränkungen festgelegt werden:
  - Programme zum Bearbeiten der Registrierung deaktivieren
  - Nur zugelassene Anwendungen für Windows ausführen

  Für normale Benutzer sollte kein Zugriff auf die Registrierung möglich sein, da Änderungen an der Registrierung schwerwiegende Probleme verursachen können.

  Die meisten Benutzer müssen mit dem IT-System nur bestimmte Aufgabe wahrnehmen und benötigen dem entsprechend nur bestimmte Anwendungen. Daher sollte ihr Zugriff auch auf diese Anwendungen, wie z. B. ein Textverarbeitungsprogramm, eingeschränkt werden.
- *Windows NT Shell:* Hier können folgende Einschränkungen festgelegt werden:
  - Nur erlaubte Shell-Erweiterungen verwenden
  - Allgemeine Programmgruppen vom Menü "*Start*" entfernen

Unter Windows NT können sehr differenzierte Benutzerprofile erstellt werden. Diese sollten entsprechend der Sicherheitspolitik der Behörde bzw. des Unternehmens erarbeitet werden. Dies kann zeitaufwendig sein, da für verschiedene Benutzergruppen auch jeweils auf diese zurechtgeschnittene Benutzerprofile erstellt werden sollten. Alle Benutzerprofile müssen vorher darauf getestet werden, ob diese weder Lücken offen lassen noch die Benutzer an ihrer Aufgabenerfüllung hindern. Es ist auch zu bedenken, dass zu weitgehende Einschränkungen nicht nur zur Unzufriedenheit der Benutzer bis hin zur völligen Ablehnung des Systems führen können, sondern auch den Administratoren viel Arbeit verursachen können, wenn diese ständig Benutzerwünsche umsetzen müssen, wie z. B. eine andere Schriftgröße einstellen.

Die Windows NT Umgebung wird durch die Werte des aktuellen Benutzerprofils festgelegt, selbst wenn der aktuelle Benutzer weder über ein vorgeschriebenes noch über ein persönliches Profil verfügt oder auch wenn aktuell

niemand angemeldet ist. Das User Default Profil wird unter den folgenden Bedingungen geladen:

- wenn der aktuelle Benutzer über kein eigenes (vorgeschriebenes oder persönliches) Profil verfügt und sich noch nie auf dem aktuellen Rechner angemeldet hat;
- wenn ein Benutzer sich auf dem Gastkonto anmeldet.

Im ersten Fall werden die aktuellen Werte der Benutzerumgebung beim Abmelden in ein neu erstelltes lokales persönliches Profil abgespeichert, im zweiten Fall gehen sie beim Abmelden verloren.

Wenn niemand angemeldet ist, werden die aktuellen Werte für den Bildschirmhintergrund und andere Umgebungsvariablen durch das System Default Profil bestimmt.

Ergänzende Kontrollfrage:

- Ist das Gastkonto, sofern es nicht gesperrt ist, durch ein Profil auf die minimal erforderliche Funktionalität eingeschränkt?

M 4.52 Geräteschutz unter NT-basierten Windows-Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Normalerweise erlaubt Windows NT/2000/XP/Server 2003 allen Programmen den Zugriff auf Disketten und CD/DVD-ROMs/RWs. Es ist empfehlenswert, diesen Zugriff auf den gerade interaktiv angemeldeten Benutzer zu beschränken, indem die Geräte diesem Benutzer beim Anmelden exklusiv zugeordnet werden.

Im folgenden wird beschrieben, wie der Zugriff auf Disketten- und CD-ROM-Laufwerke eingeschränkt werden kann. Der Zugriff auf andere Laufwerke für auswechselbare Datenträger sollte auf vergleichbare Weise eingeschränkt werden.

Der Zugriff auf Diskettenlaufwerke sollte unter Windows NT 4.0 eingeschränkt werden, indem der Wert *AllocateFloppies* im Schlüssel *SOFTWARE \ Microsoft \ Windows NT \ Current Version \ Winlogon* des Bereiches *HKEY_LOCAL_MACHINE* der Registrierung auf den Wert *REG_Zeichenfolge = 1* gesetzt wird. Hinweis: Der Typ *REG_Zeichenfolge*, wie er in dem Programm *Regedit.exe* verwandt wird, entspricht dem Typ *REG_SZ* im Programm *Regedt32.exe*.

Analog sollte der Zugriff auf CD-ROM-Laufwerke bei Bedarf eingeschränkt werden, indem der Wert *AllocateCdRoms* im Schlüssel *SOFTWARE \ Microsoft \ Windows NT \ Current Version \ Winlogon* des Bereiches *HKEY_LOCAL_MACHINE* der Registrierung auf den Wert *REG_Zeichenfolge = 1* gesetzt wird.

Unter Windows 2000/XP/Server 2003 erfolgt die Konfiguration über die lokalen Sicherheitseinstellungen bzw. über eine Gruppenrichtlinie. Die relevanten Parameter sind unter *Computerkonfiguration / Windows-Einstellungen / Sicherheitseinstellungen / Lokale Richtlinien / Sicherheitsoptionen* zu finden und lauten unter Windows 2000:

- Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken
- Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken

Unter Windows XP/Server 2003 lauten sie wie folgt:

- Geräte: Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken
- Geräte: Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken

Beide Optionen sind zu aktivieren.

Hinweis: Da die Geräte beim Abmelden wieder für den allgemeinen Zugriff freigegeben werden, müssen die Datenträger vor dem Abmelden aus den Geräten entfernt werden.

Sofern Diskettenlaufwerke vollständig abgeschaltet werden sollen, kann dies auch dadurch geschehen, dass in der Systemsteuerungsoption *Geräte* unter Windows NT bzw. *Computerverwaltung/Gerätemanager* unter Windows 2000/XP/Server 2003 das Laden des Treiberprogramms dadurch unterbunden wird, dass dem Gerät *Floppy* die Startart *Deaktiviert* zugewiesen wird. Nach dem nächsten Systemstart steht dann das Diskettenlaufwerk überhaupt nicht mehr zur Verfügung, und es kann nur von einem Administrator durch Zuweisen der Startart *System* wieder nutzbar gemacht werden.

Auf Servern sollte das Laden des Treiberprogramms für das Diskettenlaufwerk nicht unterbunden werden. Sofern das Diskettenlaufwerk doch einmal gebraucht wird, z. B. zum Zwecke der Administration, muss dem Gerät *Floppy* die Startart *System* zugewiesen werden und der Server muss heruntergefahren werden, da der Treiber erst beim Neustart wieder geladen wird. Dies kann zu Störungen des Betriebes führen. Server müssen in einer gesicherten Umgebung aufgestellt werden.

Weiterhin erlaubt Windows NT/2000/XP/Server 2003 allen Benutzern den Zugriff auf Bandlaufwerke, so dass jeder Benutzer den Inhalt jedes Bandes lesen und schreiben kann. Normalerweise bringt dies keine Probleme mit sich, da zu einem gegebenen Zeitpunkt jeweils nur ein Benutzer interaktiv angemeldet ist. Sofern dieser jedoch ein Programm laufen lässt, das auch nach dem Abmelden noch auf das Bandlaufwerk zugreift, so kann dieses Programm möglicherweise auf ein Band zugreifen, das der nächste Benutzer auflegt, der sich anmeldet. Aus diesem Grund sollten Rechner, die sich nicht in einer kontrollierten Umgebung befinden und auf denen vertrauliche Daten verarbeitet werden, neu gestartet werden, ehe das Bandlaufwerk genutzt wird.

Hinweis: Der Einsatz von selbstladenden Bandgeräten, die mehrere Bänder aus einem Reservoir laden können, darf nur unter sehr genau kontrollierten Randbedingungen zugelassen werden. In der Regel sollten derartige Geräte nur zur Datensicherung an einem Server installiert werden. Der interaktive Zugriff normaler Benutzer auf diesen Server ist nicht zulässig (siehe auch M 6.32 *Regelmäßige Datensicherung*).

Weitere Empfehlungen zum geeigneten Umgang mit Laufwerken für Wechselmedien finden sich in der Maßnahme M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*.

Ergänzende Kontrollfragen:

- Wird die Einstellung der Schlüssel *AllocateFloppies* und *AllocateCdRoms* in der Registrierung regelmäßig kontrolliert?
- Wird die Einstellung der Parameter Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken und Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken in den Sicherheitseinstellungen bzw. Gruppenrichtlinien regelmäßig kontrolliert?

M 4.53 Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

In Windows NT wird zwischen den Zugriffsberechtigungen auf Freigabeebene und den Zugriffsberechtigungen auf Datei- und Verzeichnisebene, die im folgenden auch NTFS-Berechtigungen genannt werden, unterschieden. Die Zugriffsberechtigungen auf Freigabeebene (Shares) werden in M 2.94 *Freigabe von Verzeichnissen unter Windows NT* betrachtet.

Zugriffsberechtigungen auf Datei- und Verzeichnisebene stehen im Gegensatz zu den Freigabeberechtigungen (Share-Berechtigungen) nur auf Datenträgern mit dem Dateisystem NTFS zur Verfügung. Sie werden in der Regel vom Ersteller oder Besitzer eines Objektes (Verzeichnis oder Datei) vergeben. Auf Servern erfolgt dies meistens durch den Administrator. Die Festlegung von NTFS-Berechtigungen erfolgt unter Windows NT 4.0 typischerweise mittels des Windows NT Explorers oder über das Desktop-Symbol "Arbeitsplatz". Im Kontextmenü des entsprechenden Verzeichnisses bzw. der entsprechenden Datei ist der Menüpunkt "Eigenschaften"/"Sicherheit" auszuwählen. Dadurch gelangt man zu folgender Zugriffskontrolliste:

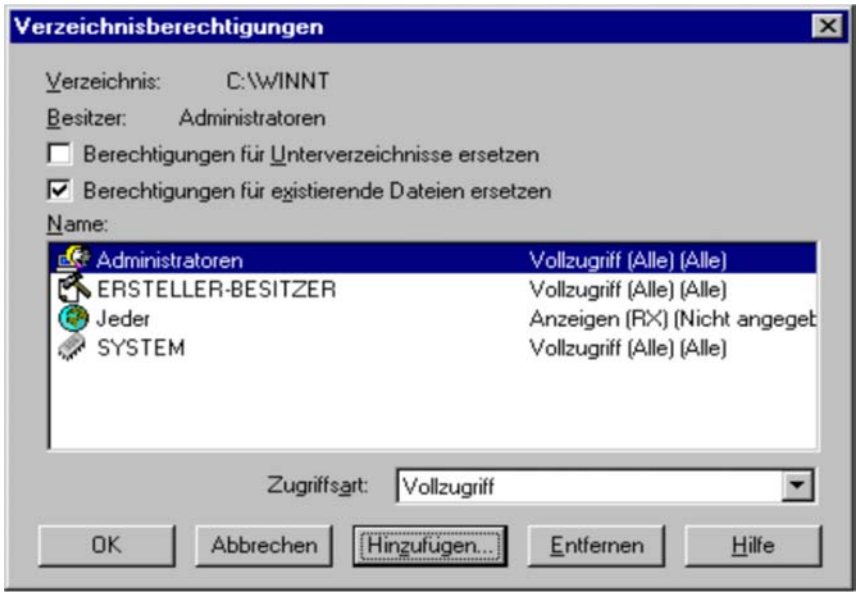


Abb.: Verzeichnisberechtigungen - Zugriffskontrolliste

Die entsprechende Zugriffskontrolliste findet sich unter Windows NT 3.51 im Dateimanager unter "Sicherheit"/"Berechtigungen". In diese Zugriffskontrolliste können bestehende Benutzergruppen und Benutzer aufgenommen und hier können jeder Benutzergruppe und jedem Benutzer Berechtigungen zugewiesen und entzogen werden. Auch ist es möglich, Benutzergruppen und Benutzer aus der Zugriffskontrolliste zu entfernen. Durch Aktivieren der Option "Berechtigungen für existierende Dateien ersetzen" können die für das Verzeichnis festgesetzten Berechtigungen auf alle Dateien dieses Verzeichnisses übertragen werden. Wird die Option "Berechtigungen für Unterver-

zeichnisse ersetzen" gewählt, werden die eingestellten Berechtigungen zudem auf alle Unterverzeichnisse übertragen. Auf diese Weise lassen sich leicht einheitliche Rechtestrukturen realisieren.

NTFS-Berechtigungen werden zunächst beim lokalen Zugriff wirksam. Müssen z. B. mehrere Benutzer an einem Computer arbeiten, so ist es möglich, durch Vergabe entsprechender Datei- und Verzeichnisberechtigungen sicherzustellen, dass jeder Benutzer nur Zugriff auf seine Daten hat.

Auch beim Zugriff über das Netz werden NTFS-Berechtigungen wirksam. Voraussetzung für den Netzzugriff ist aber, dass das Verzeichnis, auf das zugegriffen werden soll oder in dem sich das gewünschte Unterverzeichnis oder die gewünschte Datei befindet, zuvor freigegeben und mit einer entsprechenden Freigabeberechtigung versehen wurde (s. M 2.94 *Freigabe von Verzeichnissen unter Windows NT*). Im Zusammenspiel zwischen Freigabeberechtigung und NTFS-Berechtigung ist zu beachten, dass die jeweils restriktivere Berechtigung maßgebend ist. NTFS-Berechtigungen lassen sich feiner abstufen als Freigabeberechtigungen. Es ist insbesondere möglich, für jedes Unterverzeichnis und für jede Datei gesonderte NTFS-Berechtigungen zu vergeben. Von daher ist es auch möglich, Freigaben mit der Freigabeberechtigung "Vollzugriff" für die Gruppe der Benutzer bzw. Domänen-Benutzer zu versehen und die effektiven Zugriffsrechte über die NTFS-Berechtigungen zu vergeben.

Die NTFS-Berechtigungen werden unterschieden in spezifische (auch individuelle) Berechtigungen und vordefinierte Standardberechtigungen, die Kombinationen der spezifischen Zugriffsberechtigungen darstellen.

Es gibt folgende individuellen Berechtigungen:

R Lesen

W Schreiben

X Ausführen

D Löschen

P Berechtigungen ändern

O Besitz übernehmen

Aus diesen Einzelberechtigungen sind unter Windows NT vorgegebene Standardberechtigungen kombiniert worden:

Standardberechtigung	*Einzelberechtigungen*
Kein Zugriff	-
Lesen	RX
Ändern	RWXD
Anzeigen	RX
Hinzufügen	WX
Hinzufügen und Lesen	RWX
Vollzugriff	RWXDPO

Tabelle: Vorgegebene Standardberechtigungen unter Windows NT

Der Besitzer einer Datei bzw. eines Verzeichnisses hat in jedem Fall das Recht, Berechtigungen für die Datei bzw. das Verzeichnis zu vergeben und zu entziehen. Jeder, der ein Verzeichnis oder eine Datei erstellt, wird automatisch Besitzer dieser Ressource. Der Besitz an einem Verzeichnis bzw. an einer Datei kann durch "Besitz übernehmen" (P) an andere Benutzer übertragen werden. Der Besitz an einem Verzeichnis oder einer Datei geht allerdings erst durch die Besitzübernahme durch den Empfänger auf diesen über. Es ist im Gegensatz zu anderen Betriebssystemen nicht möglich, Dateien und Verzeichnisse zu verschenken. Unabhängig von den Eintragungen in der Zugriffskontrolliste können Administratoren in jedem Fall den Besitz an Dateien und Verzeichnissen übernehmen.

Hinweis:

Benutzer sollten möglichst nie die Berechtigung "*Vollzugriff*" vergeben, sondern höchstens die Berechtigung "*Ändern*", damit ihnen nicht der Besitz entzogen werden kann und sie immer die Hoheit über die Rechtevergabe behalten.

Alle Benutzer müssen darauf aufmerksam gemacht werden, regelmäßig mit dem Dateimanager oder dem Explorer zu überprüfen, ob sie noch Besitzer ihrer Verzeichnisse und Dateien sind. Dies ist der einzige Weg, mit dem Benutzer erkennen könne, ob von Ihnen gesetzte Zugriffsrechte umgangen worden sind.

Die in den folgenden Abschnitten genannten Maßnahmen gelten hauptsächlich für Dateien und Verzeichnisse, für die der Administrator zuständig ist, das heißt für solche, die entweder für alle Benutzer von Bedeutung sind oder die Administrationszwecken dienen. Es reicht nicht aus, die Rechte eines Programms zu überprüfen, es muss auch die Rechtevergabe aller Programme überprüft werden, die von diesem Programm aus aufgerufen werden (insbesondere zur Vermeidung Trojanischer Pferde).

Die Attribute aller Systemdateien sollten möglichst so gesetzt sein, dass nur der Systemadministrator Zugriff darauf hat. Verzeichnisse dürfen nur die notwendigen Privilegien für die Benutzer zur Verfügung stellen.

Verzeichnisse des Betriebssystems und der Anwendungsprogramme

Die Dateien und Verzeichnisse des Betriebssystems selbst müssen gegen unzulässige Zugriffe hinreichend geschützt werden. Die standardmäßig vorgesehenen Zugriffsrechte sollten unmittelbar nach der Installation des Systems auf schärfere Formen der Zugriffskontrolle auf die betreffenden Dateien und Verzeichnisse (das Windows-Verzeichnis, *%SystemRoot%*, z. B. *\WINNT*, das Windows-Systemverzeichnis *%SystemRoot%\SYSTEM32* und eventuelle weitere Programmverzeichnisse, z. B. *\MsOffice* und *\Programme*, und alle Unterverzeichnisse) eingestellt werden.

Dabei ist jedoch zu beachten, dass manche Programme, insbesondere 16-Bit Programme, aber auch z. B. MS Winword 7.0, im Windows-Verzeichnis und/oder im Programmverzeichnis Initialisierungs- und Konfigurationsdateien anlegen. Sollen solche Programme genutzt werden, so kann es erforderlich

werden, den Benutzern das Zugriffsrecht "Ändern" auf die betreffenden Verzeichnisse und Dateien zu geben.

Nur Administratoren dürfen auf diese Dateien und Verzeichnisse schreibenden Zugriff haben. Für alle anderen Benutzer ist der Zugriff so einzuschränken, dass sie dort nur lesenden und ausführenden Zugriff (RX) haben:

Benutzer(gruppe)	*Zugriffsrecht*
SYSTEM	Vollzugriff
Administratoren	Vollzugriff
Benutzer	Lesen

Tabelle: Zugriffsrechte auf das Betriebssystem und die Anwenderprogramme

Ggf. kann der Zugriff auf ausführbare Dateien (.EXE-, COM- und BAT-Dateien) noch weiter eingeschränkt werden, so dass nur ausführender Zugriff (X) auf diese Dateien möglich ist. In ähnlicher Weise sind die für den Systemstart kritischen Dateien *\BOOT.INI*, *\NTDETECT.COM*, *\NTLDR*, *\AUTOEXEC.BAT* und *\CONFIG.SYS* gegen unbefugte Veränderung durch unprivilegierte Benutzer zu schützen.

Dabei sollte allerdings - am besten in einer Testumgebung - überprüft werden, ob alle Anwendungsprogramme bei dieser restriktiven Einstellung noch lauffähig sind, oder ob einzelne Zugriffskontrollen doch um weitere Zugriffsmöglichkeiten ergänzt werden müssen, um beispielsweise die Abspeicherung temporärer Dateien oder von Konfigurationsinformationen in einem Programmverzeichnis zu erlauben. Generell sollte jedoch der Zugriff auf die Programmdateien selbst (.EXE-Dateien) und auf dynamische Bibliotheken (.DLL-Dateien) für die Gruppe "Jeder" auf lesenden Zugriff beschränkt werden, zumal diese Maßnahme auch einen gewissen Schutz gegen die Verbreitung von Viren bietet.

Temporäre Dateien

Temporäre Dateien, die von verschiedenen Anwendungsprogramme zum Auslagern und Zwischenspeichern von Daten verwendet werden, werden unter Windows NT im Verzeichnis *%TEMP%* (in der Regel *C:\TEMP*) abgelegt. Alle Anwender benötigen für dieses Verzeichnis auch das Recht, hier Dateien abzulegen, doch muss gleichzeitig verhindert werden, dass Benutzer auf temporäre Dateien anderer Benutzer Zugriff erhalten. Die Zugriffsrechte für das Verzeichnis sollten daher auf folgenden Wert geändert werden

Benutzer(gruppe)	Zugriffsrecht
SYSTEM	Vollzugriff
Administratoren	Vollzugriff
Ersteller/Besitzer	Ändern
Benutzer	Hinzufügen

Tabelle: Zugriffsrechte bei temporären Dateien

Registrierung

Die Registrierung von Windows NT befindet sich im Unterverzeichnis *CONFIG* des Windows-Systemverzeichnisses *%SystemRoot%\SYSTEM32*, d. h. im allgemeinen im Verzeichnis *C:\WINNT\SYSTEM32\CONFIG*. Auf dieses Verzeichnis muss der Anwender Zugriff haben, da die Registrierung automatisch durch Einstellungen des Benutzers in Anwendungsprogrammen geändert wird. Kann der Benutzer nicht auf dieses Verzeichnis zugreifen, führt das zu Systemfehlern oder zu einem Absturz des Systems. Die auf dieses Verzeichnis gesetzten Standardrechte, die möglichst nicht verändert werden sollten, sind unter Version 3.51:

Benutzer(gruppe)	Zugriffsrecht
SYSTEM	Vollzugriff
Administratoren	Vollzugriff
Ersteller/Besitzer	Ändern
Benutzer	Anzeigen

Tabelle: Zugriffsrechte bei der Registrierung bei Windows NT, Version 3.51

Ab Version 4.0 sind die Standardrechte:

Benutzer(gruppe)	Zugriffsrecht
SYSTEM	Vollzugriff
Administratoren	Vollzugriff
Ersteller/Besitzer	Vollzugriff
Jeder	Anzeigen

Tabelle: Zugriffsrechte bei der Registrierung ab Version 4.0

Die Gruppe "*Jeder*" sollte allerdings durch die Gruppe "*Benutzer*" ersetzt werden. Nur wenn Gäste auf dieses Verzeichnis Zugriff haben, muss die Gruppe "*Jeder*" das Recht "Anzeigen" haben.

Bei der Installation legt Windows NT das Verzeichnis *%SystemRoot%\REPAIR* an, um dort Konfigurationsinformationen abzu-

speichern, die für eine ggf. notwendige Reparatur einer bestehenden Installation benötigt werden. Diese Dateien werden mit Hilfe des Dienstprogramms *RDISK* aktualisiert (siehe auch M 6.42 *Erstellung von Rettungsdisketten für Windows NT*). Da da mit Hilfe dieser Dateien und entsprechender Schadsoftware Sicherheitsfunktionalitäten von Windows NT außer Kraft gesetz werden können, sollten die Rechte auf das Verzeichnis mit allen darin befindlichen Dateien wie folgt gesetzt werden:

Benutzer(gruppe)	Zugriffsrecht
System	Vollzugriff
Administratoren	Vollzugriff

Tabelle: Zugriffsrechte auf Verzeichnisse

Profile

Zum Abspeichern der Daten, die die Benutzeroberfläche und Einträge im Menü START ab der Version 4.0 beschreiben, legt Windows NT für jeden Benutzer vom System ein eigenes Profilverzeichnis im Unterverzeichnis *Profiles* des Windows-Verzeichnisses *%SystemRoot%* (in der Regel *C:\WINNT\PROFILE*) an. Unter der Version 3.51 werden Profile in Unterverzeichnissen des Systemverzeichnisses *%SystemRoot%\SYSTEM32\CONFIG* bzw. in für die einzelnen Benutzer explizit angegebenen Verzeichnissen abgespeichert.

Auf diese Verzeichnisse muss der Benutzer vollen Zugriff haben, sofern er seine Benutzeroberfläche selbst verändern können soll. Dies ist jedoch nicht immer gewünscht (siehe M 4.51 *Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT*). Beim ersten Anmelden des Benutzers wird sein Benutzerprofil automatisch vom System erzeugt. Die Standard-Zugriffsrechte für das Verzeichnis sehen wie folgt aus:

Benutzer(gruppe)	Zugriffsrecht
SYSTEM	Vollzugriff
Administratoren	Vollzugriff
betreffender Benutzer	Vollzugriff

Tabelle: Zugriffsrechte bei Profilverzeichnissen

Neben dem Profilverzeichnis für den einzelnen Benutzer gibt es noch ein Verzeichnis für alle Benutzer (*All Users*) und ein Verzeichnis als Vorlage für neue Benutzer (*Default User*). Schreibenden Zugriff auf diese Verzeichnisse sollte nur Systemverwalter haben. Die Zugriffsrechte sollten wie folgt gesetzt werden:

Benutzer(gruppe)	Zugriffsrecht
SYSTEM	Vollzugriff
Administratoren	Vollzugriff
Benutzer	Lesen

Tabelle: Zugriffsrechte in den Verzeichnissen *All Users* und *Default User*

Diese Einstellungen sollten nur verändert werden, wenn man dem Anwender das Recht nehmen möchte, seine Benutzeroberfläche zu verändern.

Benutzer-Verzeichnisse

Die Verzeichnisse für die Daten der einzelnen Benutzer sollten in der Regel so geschützt werden, dass nur die betreffenden Benutzer auf ihre Dateien zugreifen können. Andere Benutzer, auch Administratoren benötigen in der Regel keinen Zugriff auf die Daten eines Benutzers, es sei denn, dass dieser selbst explizit zusätzliche Zugriffsrechte vergibt. Damit ist in den meisten Fällen die folgende Voreinstellung für die Zugriffsrechte auf Benutzerverzeichnisse ausreichend:

Benutzer(gruppe)	Zugriffsrecht
SYSTEM	Vollzugriff
betreffender Benutzer	Vollzugriff

Tabelle: Benutzer-Verzeichniss-Zugriffsrechte

Benutzer, die einzelne Dateien oder Verzeichnisse anderen Benutzern zugänglich machen wollen, sollten hierfür Verzeichnisse außerhalb ihres Basis-Verzeichnisses einrichten. Ebenso sollten für Projektgruppen, die gemeinsam an bestimmten Dateien arbeiten, spezielle Verzeichnisse eingerichtet werden. Die Zugriffsrechte auf solche Verzeichnisse sollten auch wiederum explizit auf die Benutzer in diesen Gruppen beschränkt werden.

Sperren der Zugriffsrechte für Gäste

Bei den oben beschriebenen Zugriffskontrolllisten ist davon ausgegangen worden, dass keine Benutzer der Gruppe "*Gäste*" zugelassen sind. Deswegen ist die Gruppe "*Jeder*" durch die Gruppe "*Benutzer*" zu ersetzen. Mit dieser Maßnahme wird Gästen effektiv jede Möglichkeit zur Arbeit mit dem System und zum Zugriff auf Daten entzogen. Da dies jedoch unter Umständen dazu führen kann, dass bestimmte Anwendungssoftware nicht mehr korrekt läuft, sollte eine derartige Änderung zuerst an einem Testsystem vorgenommen und hinsichtlich ihrer Auswirkungen überprüft werden, ehe sie allgemein umgesetzt wird.

Ergänzende Kontrollfragen:

- Wird die Attributvergabe bei Systemdateien und der Registrierung regelmäßig überprüft?
- Werden die Einstellungen der Benutzerprofile regelmäßig überprüft?
- Gibt es Listen, anhand derer diese Überprüfungen durchgeführt werden?

M 4.54 Protokollierung unter Windows NT

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die für die Protokollierung sicherheitsrelevanter Ereignisse festgelegten Regelungen können mit Hilfe der Option "*Richtlinien*" des Benutzer-Managers umgesetzt werden, wobei für den normalen Schutzbedarf geeignete Regelungen im allgemeinen denen der folgenden Abbildung entsprechen:

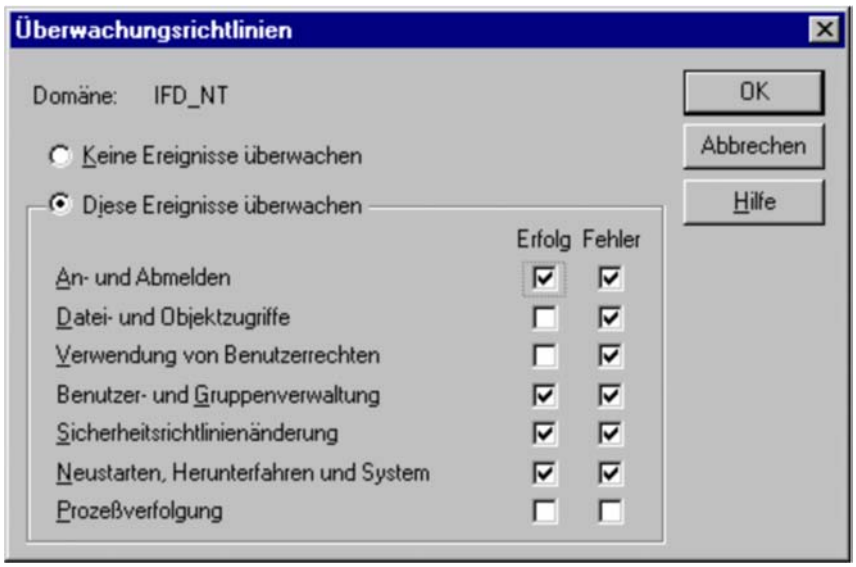


Abbildung: Überwachungsrichtlinien

Sofern auf einem Rechner Daten mit höheren Schutzanforderungen gespeichert und/oder verarbeitet werden, sollten zusätzlich noch erfolgreiche und abgewiesene Datei- und Objektzugriffe aufgezeichnet werden. Dabei sollte sich diese Aufzeichnung auf die Dateien, die besonders schutzwürdige Informationen enthalten, sowie auf die zur Verarbeitung dieser Dateien benötigten Programme beschränken, damit die Protokolldatei nicht so umfangreich wird, dass sie nicht mehr mit tragbarem Aufwand auswertbar ist.

Bei höheren Sicherheitsanforderungen sollten auch Zugriffe und Zugriffsversuche auf die Registrierung, zumindest für die Schlüssel *HKEY_LOCAL_MACHINE* und *HKEY_USERS*, aufgezeichnet werden. Dabei empfiehlt es sich, alle abgewiesenen Versuche aufzuzeichnen und von den erfolgreichen zumindest die folgenden, die zu Veränderungen der Registrierung führen können:

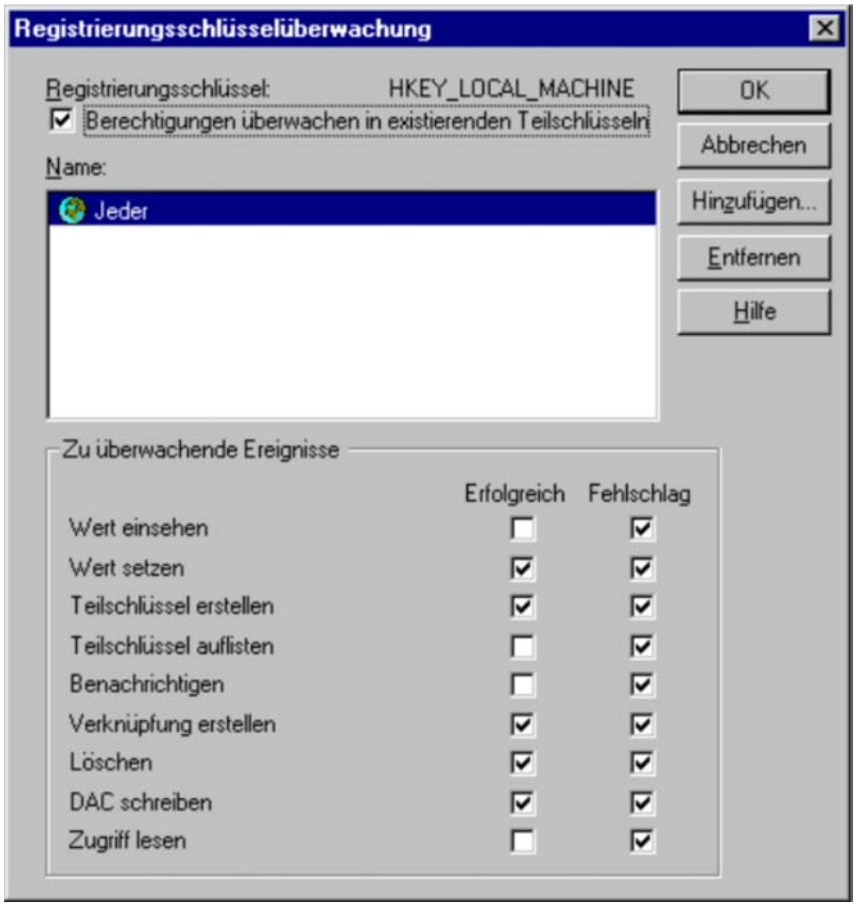


Abbildung: Registrierungsschlüsselüberwachung

Dabei ist zu beachten, dass Zugriffe auf die Registrierung nur dann aufgezeichnet werden, wenn bei den allgemeinen Überwachungsrichtlinien die Überwachung der Datei- und Objektzugriffe aktiviert ist.

Bei der Überwachung der Zugriffe auf die Registrierung fallen erhebliche Mengen an Protokolldaten an, die auch ausgewertet werden müssen. Zudem wirkt sich die Protokollierung dieser Ereignisse u. U. negativ auf die Systemperformance aus. Es bietet sich unter Berücksichtigung der Sicherheitsanforderungen ggf. das folgende alternative Vorgehen an: Abgewiesene Zugriffsversuche auf die Schlüssel *HKEY_LOCAL_MACHINE* und *HKEY_USERS* werden so protokolliert, wie zuvor beschrieben. Die erfolgreichen Zugriffe auf diese Schlüssel werden nicht protokolliert. Vielmehr wird ein geeignetes Integritätssicherungsprogramm eingesetzt. So können Veränderungen an diesen Schlüsseln leicht erkannt werden. Der Nachteil dieser Methode ist aber, dass der Urheber von Veränderungen nicht erkannt werden kann.

Die Protokolldatei sollte durch Festlegung entsprechender Vorgaben mit dem Dienstprogramm *Ereignisanzeige* so groß angelegt werden, dass alle innerhalb eines vorgegebenen Zeitraums (beispielsweise in einer Woche) anfallenden Einträge mit Sicherheit abgespeichert werden können. Dabei sollte ein

Sicherheitsspielraum vorgesehen werden, so dass in der Regel maximal nur etwa 30 % der Protokolldatei gefüllt werden. Nach Ablauf des vorgesehenen Zeitraums ist die Protokolldatei jeweils zu analysieren, zu archivieren und dann zu leeren, um Platz für neue Einträge zu schaffen.

Um Systemausfälle durch Vollschreiben der Protokolldatei zu vermeiden, sollte normalerweise eine der Optionen "*Überschreiben falls notwendig*" oder "*Überschreiben älter als x Tage*", wobei für *x* die Länge des vorgesehenen Archivierungszyklus, z. B. 30 Tage, angegeben wird, gewählt werden:

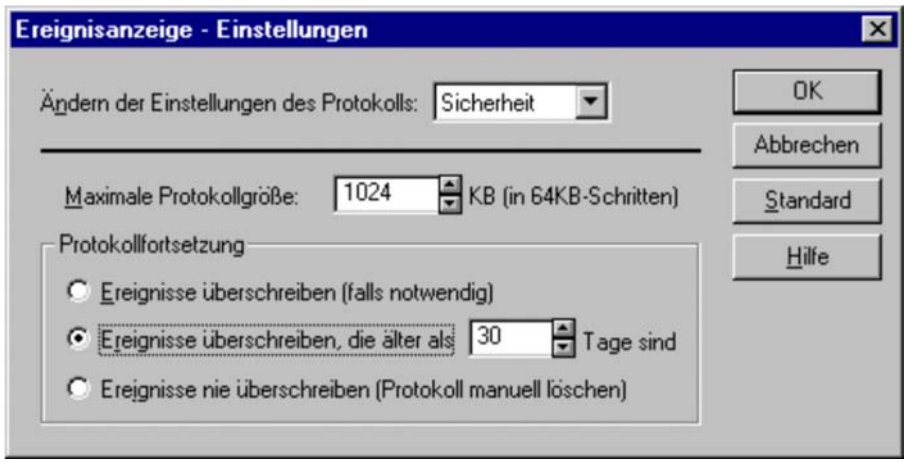


Abbildung: Ereignisanzeige - Einstellungen

Für Systeme, für die erhöhte Sicherheitsanforderungen bestehen, sollte statt dessen die Option "*Nie überschreiben (Protokoll manuell löschen)*" gewählt werden, was allerdings zum Systemstillstand bei Überlauf des Logs führt und dann einen entsprechenden Aufwand verursacht.

Die Auswertung der Protokolle erfolgt mit dem Verwaltungsprogramm *Ereignisanzeige*, das durch Auswahl geeigneter Filterregeln die gezielte Auswertung sicherheitskritischer Vorgänge ermöglicht:

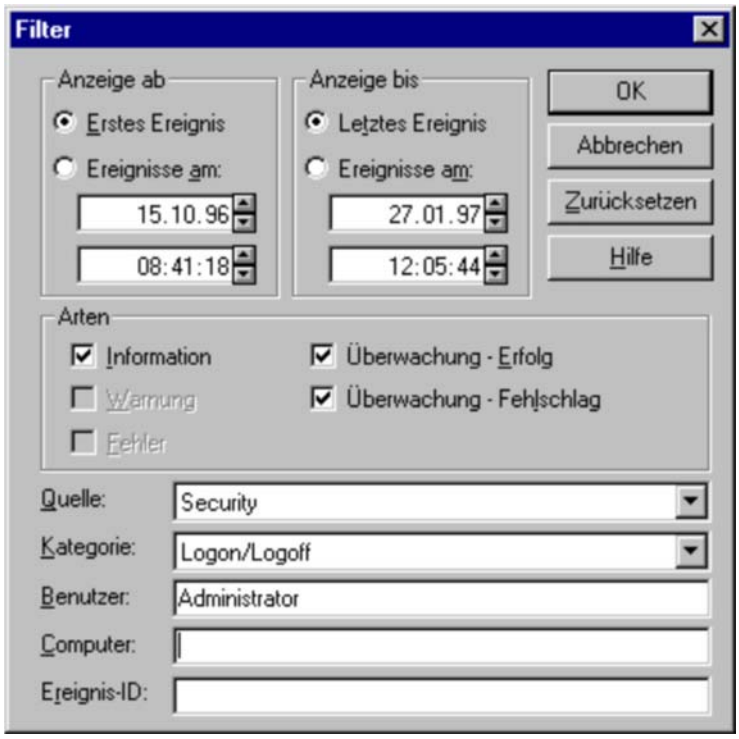


Abbildung: Filter

Die Auswertung des Sicherheitsprotokolls sollte einer geeigneten, allgemein verbindlichen Vorgabe folgen (siehe M 2.64 *Kontrolle der Protokolldateien* und M 2.92 *Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz*).

Ergänzende Kontrollfragen:

- Werden die aufgezeichneten Protokolle regelmäßig geprüft?
- Werden die möglichen Konsequenzen sicherheitskritischer Protokolleinträge analysiert?

M 4.55 Sichere Installation von Windows NT

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Vor der Installation von Windows NT sollten einige Überlegungen getroffen werden, die im folgenden kurz dargestellt werden.

Sichere Systemversion

Schon bei der Beschaffung muss entschieden werden, ob Windows NT in der englischen oder in der deutschen Version zum Einsatz kommen soll. Außerdem muss Windows NT, um sicher zu sein, wenigstens in der Version 3.51 mit dem jeweils aktuellen Service Pack betrieben werden (siehe auch M 4.76 *Sichere Systemversion von Windows NT*). Sofern eine ältere Windows NT Installation vorhanden ist, sollte diese nach Möglichkeit auf die Version 4 oder zumindest auf die Version 3.51 aktualisiert werden.

Partitionen und Dateisysteme

Windows NT unterstützt neben dem eigenen Dateisystem NTFS auch das DOS-Dateisystem FAT und das OS/2-Dateisystem HPFS. Ein Großteil der sicherheitsrelevanten Einstellungen ist allerdings nur unter NTFS gültig. Bei der Installation von Windows NT ist daher zu beachten, dass keine HPFS- oder DOS-Partitionen angelegt werden, da für diese kein Zugriffsschutz gilt, so dass derartige Partitionen zum Unterlaufen des Schutzes von Windows NT missbraucht werden können. Statt dessen müssen alle Partitionen mit dem NTFS-Dateisystem formatiert oder, sofern frühere Daten beibehalten werden sollen, zu diesem Dateisystem konvertiert werden.

Allerdings ist die Unterstützung des FAT-Dateisystems für Disketten notwendig, da das NTFS-Dateisystem aufgrund seiner Größe nicht auf Disketten untergebracht werden kann. Daher sollte der Zugriff auf Diskettenlaufwerke beschränkt werden (siehe M 4.52 *Geräteschutz unter Windows NT/2000/XP*).

Konfiguration des Anmelde-Vorgangs

Normalerweise zeigt Windows NT beim Anmelden den Namen des letzten Benutzers an, der sich am betreffenden Rechner eingeloggt hat. Diese Anzeige sollte durch Eintrag/Veränderung des Wertes "*DontDisplayLastUserName*" im Schlüssel "*SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon*" des Bereiches *HKEY_LOCAL_MACHINE* der Registrierung auf den Wert *REG_SZ = "1"* verhindert werden.

Um unberechtigte Benutzer vor einem unzulässigen Zugriff auf das System zu warnen, sollte vor dem eigentlichen Anmelde-Vorgang ein Fenster mit einem geeigneten Text angezeigt werden. Dies wird durch Eingabe geeigneter Texte in die beiden Einträge "*LegalNoticeCaption*" und "*LegalNoticeText*" im Schlüssel "*SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon*" des Bereiches *HKEY_LOCAL_MACHINE* der Registrierung erreicht.

Die betreffenden Änderungen können mit Hilfe des Registrierungs-Editors (des Programms REGEDT32.EXE im Windows-Systemverzeichnis *%SystemRoot%\SYSTEM32*) vorgenommen werden. Dabei ist besondere

Vorsicht anzuwenden, da fehlerhafte Einstellungen in der Registrierung dazu führen können, dass das System nicht mehr lauffähig ist. Ab der Version 4.0 von Windows NT können diese Werte mit Hilfe des Systemrichtlinien-Editors zentral für die einzelnen Arbeitsstationen vorgegeben werden.

Laden von Subsystemen

Die optionalen Subsysteme POSIX und OS/2 sollten nur dann installiert bleiben, wenn sie zur Durchführung von Anwendungen auch tatsächlich benötigt werden. Sofern dies nicht der Fall ist, sollte auf ihre Installation verzichtet werden, oder die Systeme sollten, falls diese schon erfolgt ist, wieder gelöscht werden. Dazu sind dann die Unterverzeichnisse *POSIX* bzw. *OS2* des Windows-Systemverzeichnisses *%SystemRoot%\SYSTEM32* mit ihren eventuellen Unterverzeichnissen zu löschen. Weiterhin sind die folgenden Programme und ladbaren Bibliotheken im Windows-Verzeichnis *%SystemRoot%\SYSTEM32* zu löschen:

- OS/2: OS2.EXE
  OS2SRV.EXE
  OS2SS.EXE
- POSIX: PSXDLL.DLL
  PAX.EXE
  POSIX.EXE
  PSXSS.EXE

Außerdem sind folgende Einträge im Teilschlüssel *\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems* im Bereich *HKEY_LOCAL_MACHINE* der Registrierung zu löschen:

- OS/2: Eintrag "Os2" mit dem Wert %SystemRoot%\system32\os2ss.exe

- POSIX: Eintrag "Posix" mit dem Wert %SystemRoot%\system32\psxss.exe

Starten von Diensten

Sofern Dienste, die keine Standarddienste von Windows NT sind, konfiguriert werden sollen, sollte bei Festlegung der Startart dieser Dienste (mit der Systemsteuerungsoption "*Dienste*") nach Möglichkeit ein eigenes Benutzerkonto zum Start jedes dieser Dienste vorgesehen werden, um die Befugnisse des betreffenden Dienstes geeignet einschränken zu können. Das dabei verwendete Benutzerkonto muss über das Recht "*Als Dienst starten*" verfügen, und es sollte außer für diesen Dienst nicht verwendet werden, also insbesondere auch kein Login von Benutzern zulassen. Dienste, die nicht auf diese Weise einem speziellen Benutzerkonto zugeordnet wurden, laufen im Kontext der speziellen Benutzergruppe *SYSTEM* (siehe M 4.50 *Strukturierte Systemverwaltung unter Windows NT*), also mit den größtmöglichen Zugriffsberechtigungen.

Geräteschutz

Sofern der Computer über Diskettenlaufwerke, CD-ROM-Laufwerke und/oder Bandlaufwerke verfügt, sollten diese nach Möglichkeit spezifisch

geschützt werden, wie in der Maßnahme M 4.52 *Geräteschutz unter Windows NT/2000/XP* beschrieben.

Notfalldiskette

Bei der Installation bietet Windows NT an, eine Notfalldiskette mit den wichtigsten Konfigurationsinformationen zu erzeugen. Von dieser Möglichkeit sollte Gebrauch gemacht werden, und die Diskette sollte bei Änderungen am System jeweils aktualisiert werden (siehe M 6.42 *Erstellung von Rettungsdisketten für Windows NT*). Dabei empfiehlt es sich, die Aktualisierung der Notfalldiskette jeweils nach dem nächsten Systemstart vorzunehmen, wenn also sichergestellt ist, dass sich das geänderte System noch starten lässt.

Vordefinierte Benutzerkonten

Das vordefinierte **Administratorkonto** ist Mitglied der vordefinierten Gruppe "Administratoren". Es erhält die Rechte und Berechtigungen, die dieser Gruppe erteilt wurden. Das Administratorkonto wird von der Person verwendet, welche die Gesamtkonfiguration der Arbeitsstation oder des Servers verwaltet. Der Administrator besitzt mehr Kontrollmöglichkeiten über den Windows NT Computer als jeder andere Benutzer. Daher ist dieses Konto besonders zu schützen (siehe M 4.77 *Schutz der Administratorkonten unter Windows NT*). Das vordefinierte **Gastkonto** ist Mitglied der Gruppe "Gäste". Es erhält die Rechte und Berechtigungen, die dieser Gruppe erteilt wurden. Beispielsweise kann sich ein Benutzer beim Gastkonto anmelden, Dateien erstellen und diese wieder löschen sowie Dateien lesen, für die ein Administrator den Gästen die Leseerlaubnis erteilt. Das Gastkonto wird als Service für Benutzer eingerichtet, die gelegentlich oder nur einmal den Rechner benutzen, so dass diese sich anmelden und mit eingeschränktem Funktionsumfang arbeiten können. Das Gastkonto ist bei der Installation von Windows NT 4.0 zunächst gesperrt, und es wird mit einem leeren Kennwort installiert. Das Gastkonto ist auf jeden Fall mit einem sicheren Passwort zu versehen, und die Sperre sollte nicht aufgehoben werden, wenn es keine schwerwiegenden Gründe für seine Benutzung gibt. Das vordefinierte Gastkonto kann umbenannt, aber nicht gelöscht werden. Es sollte unmittelbar nach der Installation umbenannt werden.

Das **Erstbenutzerkonto** wird für den ersten Benutzer einer Arbeitsstation eingerichtet. Da es Mitglied der Gruppe "Administratoren" ist, kann die Arbeitsstation mit dem Erstbenutzerkonto vollständig verwaltet werden. Das Erstbenutzerkonto wird bei der Installation von Windows NT erstellt, wenn die Arbeitsstation zu einer Arbeitsgruppe hinzugefügt wird oder wenn sie nicht für den Netzbetrieb konfiguriert wurde. Das System fordert zur Eingabe eines Benutzernamens und eines Kennworts auf. Wenn der Rechner bei der Installation von Windows NT zu einer Domäne hinzugefügt wird, wird das Erstbenutzerkonto nicht erstellt, weil erwartet wird, dass sich der Benutzer unter Verwendung eines Kontos von der Domäne anmeldet.

Hinweis: Sofern Windows NT bei der Installation ein Erstbenutzerkonto einrichtet, sollte dieses als Konto zur Systemverwaltung verwendet werden.

Installation im Netz

Weiterhin ist zu beachten, dass alle Clients bei der Konfiguration ihrer Netzsoftware als Mitglieder einer der vorher definierten Domänen (und nicht als Mitglieder von Arbeitsgruppen) konfiguriert werden. Falls auf ihnen Benutzerkonten benötigt werden, müssen diese immer als domänenweite Konten und nicht als lokale Konten definiert werden, um die Entstehung unüberschaubarer Rechtestrukturen zu vermeiden.

Zur Vereinfachung der Installation einer größeren Anzahl von Clients sollten vorher Skripten definiert werden, die eine automatische Installation und Konfiguration dieser Clients ermöglichen. Software aller Art sollte zentral auf einem Server bereitgestellt und von dort aus auf dem entsprechenden Rechner installiert werden.

Ergänzende Kontrollfragen:

- Welchen Benutzern wurde die Zugangskontrollinformation (Benutzername, Passwort) zu den vordefinierten Benutzerkonten mitgeteilt?
- Wird regelmäßig kontrolliert, ob das Gastkonto noch gesperrt ist, bzw. wenn es genutzt werden muss, werden die der Gruppe "Gäste" erteilten Zugriffsrechte und die Gruppenzuordnung des Gastkontos regelmäßig überprüft?

M 4.56 Sicheres Löschen unter Windows-Betriebssystemen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Benutzer, Administrator

Windows NT/2000/XP/Server 2003

Das Windows Dateisystem NTFS legt in einer Master Dateitabelle (MFT) alle Dateiinformationen wie Namen, Pfad und Attribute ab. Diese Angaben werden nicht verschlüsselt. Programme, die direkt auf die Festplatte zugreifen können, können unter Umgehung der Sicherheitsmechanismen von Windows NT/2000/XP/Server 2003 auf alle Dateien beliebig zugreifen. Dies gilt insbesondere für Programme, die unter einem anderen Betriebssystem als Windows auf demselben Rechner laufen.

Beim Löschen einer Datei unter dem Dateisystem NTFS wird diese nicht physikalisch gelöscht oder überschrieben, sondern lediglich dem Zugriff entzogen, wobei jedoch unter Windows NTFS - im Gegensatz zu der Situation bei MS-DOS - sichergestellt ist, dass ein Zugriff auf diese gelöschten Daten, etwa mit einem Rekonstruktionsprogramm oder unter Verwendung direkter Plattenzugriffe, nicht mehr möglich ist. Dennoch können gelöschte Dateien unter anderen Betriebssystemen als Windows mit Programmen, die direkt auf die Festplatte zugreifen können, wieder hergestellt werden.

Aus diesen Gründen muss Windows als einziges Betriebssystem installiert sein, und es muss verhindert werden, dass andere Betriebssysteme gestartet werden können (siehe auch M 4.52 *Geräteschutz unter NT-basierten Windows-Systemen* und M 4.55 *Sichere Installation von Windows NT*).

Papierkorb unter Windows

Unter Windows werden Dateien beim Löschen, sofern der Benutzer nicht ausdrücklich ein direktes Löschen verlangt, zunächst in einen benutzerspezifischen Bereich, den sogenannten "Papierkorb", verlagert. Aus diesem Bereich werden sie erst dann entfernt, wenn der von gelöschten Dateien belegte Speicherplatz die für das betreffende Plattenlaufwerk vorgegebene Größe überschreitet oder wenn der Benutzer explizit den Papierkorb leert. Der Inhalt des Papierkorbs sollte daher regelmäßig gelöscht werden, damit die Festplatte nicht zu voll wird und der Benutzer nicht den Überblick verliert. Die maximale Größe des für den Papierkorb reservierten Speicherplatzes kann auch unter "*Eigenschaften*" des Icons "Papierkorb" auf einen geeigneten kleineren Wert, z. B. 2 MByte, eingestellt werden. Dateien mit sensitivem Inhalt sollten nicht in den Papierkorb verschoben werden, sondern explizit gelöscht werden, indem beim Löschen die Umschalttaste gedrückt wird.

Unter Windows besteht zudem die Möglichkeit aus dem Papierkorb gelöschte Dateien durch Hilfsprogramme zu rekonstruieren. Dateien mit besonders sensitivem Inhalt sollten daher vollständig überschrieben werden statt sie in den Papierkorb zu verschieben (siehe M 2.3 *Datenträgerverwaltung*).

Windows XP/Server 2003 bietet die Möglichkeit an, die Dateien direkt und nicht über den Papierkorb zu löschen. Direktes Löschen von Dateien kann in Eigenschaften des Papierkorbs (*Dateien sofort löschen*) oder durch das Aktivieren der Richtlinie *Benutzerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Windows Explorer* | *Gelöschte Dateien nicht in Papierkorb verschieben* erzwungen werden. Hierauf sollten die Benutzer hingewiesen werden.

Unter Windows XP/Server 2003 ist es möglich, den gesamten freien Plattenplatz eines Datenträgers oder eines Unterverzeichnisses mit dem Kommando *cipher.exe /w* zu überschreiben. *cipher.exe* macht insgesamt drei Schreibdurchgänge und überschreibt den freigegebenen Platz im ersten Durchgang mit 0x0, im zweiten mit 0xF und im dritten mit pseudo-zufälligen Daten. Bei der Benutzung dieses Kommandos soll jedoch berücksichtigt werden, dass die Inhalte kleiner Dateien (unter 4 KB), die gelöscht wurden, unüberschrieben bleiben können, wenn sie direkt in der Master File Table (MFT) und nicht in separaten Datenträger-Clustern abgelegt sind. Das Verfahren ist auch geeignet, um verschlüsselte Dateien von unverschlüsselt zwischengespeicherten Datenresten zu bereinigen.

Damit Dateien tatsächlich unwiederbringlich gelöscht werden, sollten spezielle Löschprogramme eingesetzt werden, mit denen alle Restinformationen zu dieser Datei auf dem Datenträger überschrieben werden.

Ergänzende Kontrollfragen:

- Ist die Größe des Papierkorbs auf einen sinnvollen Wert eingestellt?
- Sind alle Benutzer darüber informiert, dass über den Papierkorb gelöschte Dateien nicht zuverlässig gelöscht sind?

M 4.57 Deaktivieren der automatischen CD-ROM-Erkennung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Unter Windows können CD-ROMs automatisch erkannt und bearbeitet werden. Dadurch können auch auf der CD-ROM gespeicherte Programme automatisch auf dem Rechner ausgeführt werden. Die automatische CD-ROM-Erkennung sollte daher *permanent* unterbunden werden.

Unter Windows 95 ist dafür auf der Registerkarte GERÄTEMANAGER unter der Systemsteuerungsoption SYSTEM für die CD-ROM die Eigenschaft *Automatische Benachrichtigung beim Wechsel* zu deaktivieren.

Unter Windows NT 4.0 und Windows 2000 ist für die permanente Deaktivierung der automatischen CD-ROM-Erkennung in der Registrierung der Eintrag *Autorun* im Schlüssel *SYSTEM \ CurrentControlSet \ Services \ CD-ROM* im Bereich *HKEY_LOCAL_MACHINE* auf den Wert *REG_WORD = 0* zu setzen. Unter Windows XP kann dies auch durch das Setzen der Richtlinie *Computerkonfiguration | Administrative Vorlagen | System | Autoplay deaktivieren* auf den Wert *Alle Laufwerke* erfolgen. Die Deaktivierung der automatischen CD-ROM-Erkennung kann auch auf Benutzerbasis erfolgen (Richtlinie *Benutzerkonfiguration | Administrative Vorlagen | System | Autoplay deaktivieren*). Die Richtlinien können sowohl in lokalen als auch Active Directory-basierten Gruppenrichtlinien definiert werden.

Falls die automatische CD-ROM-Erkennung nicht generell deaktiviert wird, sollte dies dokumentiert werden. Im Einzelfall kann die automatische CD-ROM-Erkennung *für jede CD-ROM einzeln* durch Drücken der Shift-Taste beim Einlegen verhindert werden. Erfahrungsgemäß wird dies in der Praxis allerdings selten gemacht.

Ergänzende Kontrollfragen:

- Ist die automatische CD-ROM-Erkennung ausgeschaltet?
- Sind die Benutzer informiert, wie sie die automatische CD-ROM-Erkennung temporär verhindern können?

M 4.58 Freigabe von Verzeichnissen unter Windows 95

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Für jeden Rechner unter Windows 95 muss entschieden werden, ob die Peer-to-Peer-Funktionalitäten benötigt werden, um sie dann einzeln zuzulassen oder zu sperren. Dafür kann über die Systemrichtlinien über die Menüpunkte *Systemsteuerung / Netzwerk / Datei- und Druckerfreigabe* die Datei- und Druckerfreigabe einzeln zugelassen oder gesperrt werden. Anschließend muss dem Benutzer der Zugriff auf diese Registerkarte entzogen werden.

Wenn die Dateifreigabe deaktiviert ist, stehen die entsprechenden Funktionen im Dateimanager bzw. Explorer nicht mehr zur Verfügung, es ist aber weiter möglich, sich mit Verzeichnissen anderer Rechner zu verbinden.

Der Administrator muss darüber hinaus beim Einrichtung eines WfW-Rechners auch die weiteren Punkte beachten:

- Unter Windows 95 ist durch die Systemrichtlinien sicherzustellen, dass die Benutzer weder Rechner- noch Benutzernamen selbstständig ändern können.
- Die Voreinstellung "Kennwort in der Kennwortliste speichern" ist in den Verbindungsoberflächen zu deaktivieren.
- Rechner- noch Benutzernamen sollten gemäß den Organisationsvorgaben vergeben werden. Durch die Systemrichtlinien ist sicherzustellen, dass die Benutzer weder Rechner- noch Benutzernamen selbstständig ändern können.
- Beim Einsatz von Schedule+ ist darauf zu achten, dass das standardmäßig vergebene Recht, offene oder besetzte Zeitblöcke einzusehen, für alle nicht berechtigten WfW-Benutzer deaktiviert wird. Jeder Teilnehmer am selben Post-Office ist sonst in der Lage, das zeitliche Arrangement der individuellen Termine einzusehen.

Wird ein Post-Office eingerichtet, dass von mehreren Benutzern zur Kommunikation oder zur gemeinsamen Terminplanung genutzt werden soll, ist in Erwägung zu ziehen, von diesem eine Datensicherung in angemessenen Zeiträumen anzulegen. Dies ist notwendig, um einem versehentlichen oder absichtlichen Löschen des Post-Office entgegenzuwirken, da dies unter WfW nicht sicher verhindert wird.

Unter Windows 95 ist es möglich, eine Remote-Administration einzurichten, die Administratoren ermöglicht, über das Netz auf die einzelnen Workstations zuzugreifen. Vor Aktivierung dieser Option ist abzuklären, ob dies mit den Sicherheitszielen der Organisation vereinbar ist.

Durch die Aktivierung der Remote-Administration besteht die Gefahr, dass

- jemand Kennung und Passwort für die Remote-Administration ausprobieren kann, oder

- ein Administrator jederzeit unbemerkt auf Benutzerrechner zugreifen kann.

Falls diese Eigenschaft zur Erleichterung der Workstation-Betreuung gewünscht ist, ist zu überlegen, ob ein Adminstrator für alle von ihm betreuten Workstations dasselbe Administrator-Passwort verwenden soll. Dies lässt sich zwar leichter merken, führt aber dazu, dass ein Angreifer auf alle Workstations zugreifen kann, wenn er dieses eine Passwort herausgefunden hat.

Ergänzende Kontrollfragen:

- Ist dokumentiert, welche Verzeichnisse auf welchen Rechnern für den Netzzugriff freigegeben sind?
- Werden die vorhandenen Freigaben an Veränderungen im Einsatzumfeld angepasst?
- Ist dokumentiert, auf welchen Rechnern Remote-Administration eingerichtet ist?

M 4.59 Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Moderne ISDN-Karten sowie deren Kommunikationssoftware bzw. das in das Karten-RAM geladene Betriebssystem besitzen zahlreiche, über die reinen ISDN-Funktionalitäten hinausgehende Leistungsmerkmale. Solche"Komfort-Funktionalitäten", welche teilweise auch bei ausgeschaltetem IT-System angesprochen werden können, sind:

- der Empfang und Versand von Faxen,
- Funktionen eines digitalen Anrufbeantworters,
- das Abhören eingegangener Aufzeichnungen des digitalen Anrufbeantworters,
- das Telefonieren über ein im Lieferumfang der Karte enthaltenes Mikrofon bzw. einen enthaltenen Hörer.

Soweit es möglich ist, sollten nicht benötigte Karten-Funktionalitäten deaktiviert werden, am besten durch das Entfernen des jeweiligen Softwaremoduls. Lassen sich Karten-Funktionalitäten lediglich durch Parameter konfigurieren, so muss die korrekte Einstellung der Parameter regelmäßig geprüft werden.

Ergänzende Kontrollfragen:

- Werden die zur Verfügung stehenden Funktionalitäten auf ihren tatsächlichen Bedarf geprüft?
- Werden nicht genutzte und somit offensichtlich nicht erforderliche Funktionen gesperrt?

M 4.60 Deaktivieren nicht benötigter ISDN-Router-Funktionalitäten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Neben Servicefunktionen bzw. der Fernwartung (siehe M 2.108 *Verzicht auf Fernwartung der ISDN-Netzkoppelelemente*) können auch Funktionen der Router-Betriebssysteme zu Sicherheitslücken führen. Beispielsweise ist das Aufrufen einer Telnet-Sitzung auf dem Router und das sich anschließende Manipulieren der Management Information Base möglich, wenn dieser mit einem Unix-Betriebssystem ausgestattet ist.

Soweit es möglich ist, sind diese nicht benötigten Funktionalitäten zu deaktivieren, am besten durch das Entfernen des jeweiligen Softwaremoduls. Lassen sich Karten-Funktionalitäten lediglich durch Parameter konfigurieren, so muss die korrekte Einstellung der Parameter regelmäßig geprüft werden.

Ergänzende Kontrollfragen:

- Werden die zur Verfügung stehenden Funktionalitäten auf ihren tatsächlichen Bedarf geprüft?
- Werden nicht genutzte und somit offensichtlich nicht erforderliche Funktionen gesperrt?

M 4.61 Nutzung vorhandener Sicherheitsmechanismen der ISDN-Komponenten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Sind gemäß Maßnahme M 2.106 *Auswahl geeigneter ISDN-Karten in der Beschaffung* ISDN-Karten mit Sicherheitsfunktionalitäten für das IT-System oder den Router, wie

- Fähigkeit zur Durchführung einer Authentisierung über PAP und CHAP (Password Authentikation Protocol und Challenge Handshake Authentication Protocol, RFC 1994),
- Einsatz eines Verschlüsselungsverfahrens (symmetrisch/asymmetrisch) in Hard- oder Software,
- Möglichkeit der Auswertung von CLIP-Rufnummern (Calling Line Identification Presentation) zur Authentisierung,
- Möglichkeit des Führens einer Rufnummerntabelle für das Durchführen eines Call-Backs und
- Möglichkeit der Protokollierung nicht erfolgreicher Verbindungsaufbauten (Ablehnung aufgrund falscher Rufnummern- oder PAP/CHAP-Authentisierung),

beschafft worden, sollten diese auch geeignet genutzt werden, wie es die Maßnahmen M 5.48 *Authentisierung mittels CLIP/COLP*, M 5.49 *Callback basierend auf CLIP/COLP*, M 5.50 *Authentisierung mittels PAP/CHAP* und M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen* beschreiben. Voraussetzung hierfür ist, dass alle Kommunikationspartner mit ISDN-Karten, die möglichst gleiche Sicherheitsfunktionalitäten aufweisen, ausgestattet werden.

Ergänzende Kontrollfrage:

- Sind die Sicherheitsmechanismen der ISDN-Komponenten eingeschaltet?

M 4.62 Einsatz eines D-Kanal-Filters

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Beschaffungsstelle

Ein D-Kanal-Filter wird zwischen ISDN-Anschluss (S2M oder S0) und ISDN-Endgerät oder ISDN-TK-Anlage geschaltet. Zum ISDN-Anschluss verhält es sich wie ein ISDN-Endgerät und zum ISDN-Endgerät wie ein ISDN-Anschluss. Der D-Kanal-Filter überwacht den ISDN-D-Kanal auf unzulässige Protokollaktionen und ist damit in der Lage, Manipulationsversuche über den D-Kanal zu detektieren und zu verhindern. Der Einsatz des D-Kanal-Filters ist insbesondere dann sinnvoll, wenn mit qualifizierten Angriffen über Remote-Zugriffe (zum Beispiel bei Fernwartung und -administration) zu rechnen ist.

D-Kanal-Filter schränken weiterhin Leistungsmerkmale und Dienste für Rufnummern bestimmter Kommunikationspartner in der Weise ein, dass es unter konkreten Betriebszuständen nicht zu einem Missbrauch bzw. zur Gefährdung der ISDN-Endeinrichtung kommen kann. Versuche, unberechtigt Leistungsmerkmale und Dienste zu nutzen, werden von D-Kanal-Filtern mit einem Verbindungsabbau (Disconnect, Release) beantwortet und protokolliert.

Weitere Informationen zu dieser vom BSI initiierten Technologie können unter der IT-Grundschutz-Hotline nachgefragt werden.

Ergänzende Kontrollfragen:

- Wird der D-Kanal-Filter eingeschaltet?

M 4.63 Sicherheitstechnische Anforderungen an den Telearbeitsrechner

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Die sicherheitstechnischen Anforderungen an den Telearbeitsrechner richten sich nach dem Schutzbedarf der zu bearbeitenden Daten am Telearbeitsplatz und der Daten, auf die der Telearbeiter über den Kommunikationsrechner der Institution zugreifen kann. Je höher der Schutzbedarf, desto mehr Maßnahmen müssen ergriffen werden, um diesen Schutz zu gewährleisten. Allgemeine Sicherheitsziele für den Telearbeitsrechner sind:

- Der Telearbeitsrechner darf nur von autorisierten Personen benutzt werden können.

  Damit wird sichergestellt, dass nur autorisierte Personen die Daten und Programme, die im Telearbeitsrechner gespeichert sind bzw. auf die über den Kommunikationsrechner zugegriffen werden kann, nutzen können. Autorisierte Personen sind der Administrator des Telearbeitsrechners und der Telearbeiter nebst seines Stellvertreters.

- Der Telearbeitsrechner darf nur für autorisierte Zwecke benutzt werden.

  Damit wird unterstützt, dass der Telearbeiter den Rechner nicht unautorisiert benutzt oder verändert. Dies beugt Schäden durch Fehlbedienung und Missbrauch vor.

- Schäden aufgrund eines Diebstahls oder Defektes des Telearbeitsrechners müssen tolerabel sein.

  Telearbeitsrechner werden üblicherweise in einer wenig gesicherten Umgebung eingesetzt, so dass mit Diebstahl zu rechnen ist. Dabei tritt ein Verlust der Verfügbarkeit und ggf. der Vertraulichkeit der gespeicherten Daten ein. Dennoch müssen die Schäden gering bleiben.

- Versuchte oder erfolgte Manipulationen am Telearbeitsrechner sollen für den Telearbeiter erkennbar sein.

  Damit wird sichergestellt, dass der Telearbeitsrechner in einem integren Zustand verbleibt, auch wenn Manipulationsversuche nicht ausgeschlossen werden können.

Für einen Telearbeitsrechner sind folgende Funktionalitäten sinnvoll:

- Der Telearbeitsrechner muss über einen **Identifizierungs- und Authentisierungsmechanismus** verfügen. Insbesondere ist sicherzustellen, dass

  - sicherheitskritische Parameter, wie Passwort, Benutzer-Kennung, usw., sicher verwaltet werden. Passwörter dürfen nie unverschlüsselt auf dem Telearbeitsrechner gespeichert werden.

  - das Zugangsverfahren definiert auf Fehleingaben reagiert. Erfolgt zum Beispiel dreimal hintereinander eine fehlerhafte

Authentisierung, ist der Zugang zum Telearbeitsrechner zu sperren oder alternativ sind die zeitlichen Abstände, nach denen ein weiterer Zugangsversuch erlaubt wird, sukzessiv zu vergrößern.

- das Setzen bestimmter Minimalvorgaben für die sicherheitskritischen Parameter möglich ist. So sollte die Mindestlänge eines Passwortes sechs Zeichen betragen.
- nach zeitweiser Inaktivität der Tastatur oder Maus automatisch eine Bildschirmsperre aktiviert wird, die erst nach erneuter Identifikation und Authentisierung deaktiviert werden kann.

- Der Telearbeitsrechner muss über eine **Zugriffskontrolle** verfügen. Insbesondere ist sicherzustellen, dass
  - der Telearbeitsrechner verschiedene Benutzer unterscheiden kann. Es muss möglich sein, mindestens zwei getrennte Rollen auf dem Telearbeitsrechner einzurichten, nämlich Administrator und Benutzer.
  - mittels einer differenzierten Rechtestruktur (lesen, schreiben, ausführen, ...) der Zugriff auf Dateien und Programme regelbar ist.
- Soll der Telearbeitsrechner über eine **Protokollierung** verfügen, können folgende Anforderungen sinnvoll sein:
  - Der Mindestumfang, den der Telearbeitsrechner protokollieren soll, sollte parametrisierbar sein. Beispielsweise sollten folgende Aktionen inklusive der aufgetretenen Fehlerfälle protokollierbar sein:
    - bei Authentisierung: Benutzer-Kennung, Datum und Uhrzeit, Erfolg, usw.
    - bei der Zugriffskontrolle: Benutzer-Kennung, Datum und Uhrzeit, Erfolg, Art des Zugriffs, was wurde wie geändert, gelesen, geschrieben, usw.
    - Durchführung von Administratortätigkeiten,
    - Auftreten von funktionalen Fehlern.
  - Die Protokollierung darf von Unberechtigten nicht deaktivierbar sein. Die Protokolle selbst dürfen für Unberechtigte weder lesbar noch modifizierbar sein.
  - Die Protokollierung muss übersichtlich, vollständig und korrekt sein.
- Soll der Telearbeitsrechner über eine **Protokollauswertung** verfügen, können folgende Anforderungen sinnvoll sein:
  - Eine Auswertefunktion muss nach den bei der Protokollierung geforderten Datenarten unterscheiden können (z. B. "Filtern aller unberechtigten Zugriffe auf alle Ressourcen in einem vorgegebenen Zeitraum").

Die Auswertefunktion muss auswertbare ("lesbare") Berichte erzeugen, so dass keine sicherheitskritischen Aktivitäten übersehen werden.

- Der Telearbeitsrechner sollte über Funktionen zur **Datensicherung** verfügen. Diese sollten u. a. folgende Anforderungen erfüllen:
  - Das Datensicherungsprogramm muss benutzerfreundlich und schnell arbeiten. Es sollte automatisierbar sein.
  - Es muss konfigurierbar sein, welche Daten wann gesichert werden.
  - Es muss eine Option zum Einspielen beliebiger Datensicherungen existieren.
  - Die Funktion muss das Sichern von mehreren Generationen ermöglichen.
  - Datensicherungen von Zwischenergebnissen aus der laufenden Anwendung sollen möglich sein.
- Soll der Telearbeitsrechner über eine **Verschlüsselungskomponente** verfügen, ist zunächst zu überlegen, welche Funktionalität benötigt wird: die Verschlüsselung ausgewählter Daten (offline) oder automatisch der gesamten Festplatte (online). Dies setzt voraus, dass ein geeigneter Verschlüsselungsalgorithmus eingesetzt wird und dass ein Datenverlust bei Fehlfunktion (Stromausfall, Abbruch der Verschlüsselung) systemseitig abgefangen wird. Darüber hinaus sind folgende Anforderungen sinnvoll:
  - Der implementierte Verschlüsselungsalgorithmus sollte - beim Einsatz in Behörden - vom BSI anerkannt sein. Hier empfiehlt sich eine individuelle Beratung durch das BSI. Außerhalb der Behörden ist bei mittlerem Schutzbedarf der DES, bei hohem Schutzbedarf der Triple-DES geeignet.
  - Das Schlüsselmanagement muss mit der Funktionalität des Telearbeitsrechners harmonieren. Dabei sind insbesondere grundsätzliche Unterschiede der Algorithmen zu berücksichtigen: Symmetrische Verfahren benutzen einen geheim zu haltenden Schlüssel für die Ent- und Verschlüsselung, asymmetrische Verfahren benutzen einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten (geheim zu haltenden) für die Entschlüsselung.
  - Der Telearbeitsrechner muss die sicherheitskritischen Parameter wie Schlüssel sicher verwalten. So dürfen Schlüssel (auch mittlerweile nicht mehr benutzte) nie ungeschützt, das heißt auslesbar, auf dem Telearbeitsrechner abgelegt werden.
- Soll der Telearbeitsrechner über Mechanismen zur **Integritätsprüfung** verfügen, sind folgende Anforderungen sinnvoll:
  - Es sollten Verfahren zur Integritätsprüfung eingesetzt werden, die absichtliche Manipulationen am Telearbeitsrechner bzw. den darauf gespeicherten Daten sowie ein unbefugtes Einspielen von Programmen zuverlässig aufdecken können.

  - Bei der Datenübertragung müssen Mechanismen eingesetzt werden, mit denen absichtliche Manipulationen an den Adressfeldern und den Nutzdaten erkannt werden können. Daneben darf die bloße Kenntnis der eingesetzten Algorithmen ohne spezielle Zusatzkenntnisse nicht ausreichen, um unerkannte Manipulationen an den obengenannten Daten vornehmen zu können.

- Der Telearbeitsrechner sollte über einen **Boot-Schutz** verfügen, um zu verhindern, dass unbefugt von auswechselbaren Datenträgern, z. B. von Diskette oder CD, gebootet werden kann.
- Es sollte möglich sein, die **Benutzerumgebung** des Telearbeitsrechners **einzuschränken**. Damit soll der Administrator festlegen können, welche Programme der Telearbeiter ausführen kann, welche Peripheriegeräte nutzbar sind und welche Änderungen der Telearbeiter am System vornehmen darf. Darüber hinaus sollte der Telearbeiter Einstellungen, die für den sicheren Betrieb notwendig sind, nicht unautorisiert ändern und nicht unerlaubt Fremdsoftware aufspielen können.
- Auf dem Telearbeitsrechner muss ein **Computer-Viren-Prüfprogramm** installiert sein, um regelmäßig den Rechner auf Computer-Viren überprüfen zu können. Vor dem Einspielen von Daten von auswechselbaren Datenträgern, vor der Weitergabe von Datenträgern bzw. beim Senden und Empfangen von Daten muss ein Virencheck durchgeführt werden. Da an Telearbeitsrechnern der Datenaustausch mit externen IT-Systemen eine wesentliche Rolle spielt und da Einzelprüfungen sehr zeitaufwendig und umständlich sind und daher häufig unterlassen werden, sollte bei einem Telearbeitsrechner bevorzugt ein residenter Virenscanner installiert sein.
- Wenn der Telearbeitsrechner über **Fernwartung** administriert werden soll, ist sicherzustellen, dass die Fernadministration nur autorisiert durchgeführt werden kann. Bei der Fernwartung muss eine Authentikation des Fernwartungspersonals, die Verschlüsselung der übertragenen Daten und eine Protokollierung der Administrationsvorgänge gewährleistet sein.
- Die Software auf einem Telearbeitsrechner sollte **benutzerfreundlich** sein. Sie sollte leicht bedienbar, verständlich und gut erlernbar sein, da Telearbeiter stärker auf sich alleine gestellt sind als andere Mitarbeiter. Insbesondere sollte den Benutzern aussagekräftige und nachvollziehbare Dokumentationen des Betriebssystems und aller installierten Programme zur Verfügung gestellt werden.

Aus den obigen Funktionalitäten sind diejenigen auszuwählen, die aufgrund der Sicherheitsanforderungen an den Telearbeitsrechner benötigt werden. Anhand dieser Funktionalitäten muss dann ein geeignetes Betriebssystem als Plattform ausgewählt werden. Wenn dieses nicht alle benötigten Funktionalitäten unterstützt, müssen dazu Zusatzprodukte eingesetzt werden. Dabei sollten möglichst alle Telearbeitsrechner einer Institution gleich ausgestattet sein, um die Betreuung und Wartung zu erleichtern. Zur sicherheitstechnischen Eignungsprüfung sollte Baustein B 1.10 *Standardsoftware* beachtet werden.

Das Gesamtsystem ist durch die Administratoren so zu konfigurieren, dass maximale Sicherheit erreicht werden kann.

Ergänzende Kontrollfragen:

- Bietet das ausgewählte Betriebssystem des Telearbeitsrechners die notwendige Funktionalität? Sind Zusatz-Sicherheitsprodukte notwendig?
- Welche der zusätzlich empfohlenen Maßnahmen sind realisiert?
- Akzeptieren die Telearbeiter die ergriffenen Sicherheitsmaßnahmen?

M 4.64 Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Vor dem Versenden einer Datei per E-Mail oder Datenträgeraustausch bzw. vor dem Veröffentlichen einer Datei auf einem Webserver sollte diese daraufhin überprüft werden, ob sie Restinformationen enthält, die nicht zur Veröffentlichung bestimmt sind. Solche Restinformationen können verschiedenen Ursprungs sein und dementsprechend unterschiedlich können auch die Aktionen sein, die dagegen zu unternehmen sind. Die häufigsten Ursachen für solche Restinformationen sind im Folgenden beschrieben.

Generell sollte Standard-Software wie z. B. für Textverarbeitung oder Tabellenkalkulation darauf überprüft werden, welche Zusatzinformationen in damit erstellten Dateien gespeichert werden. Dabei werden einige dieser Informationen mit, andere ohne Wissen des Benutzers gespeichert.

Vor der Weitergabe von Dateien sollten diese zumindest stichprobenartig auf unerwünschte Zusatzinformationen überprüft werden. Dazu sollte ein anderer Editor benutzt werden als der, mit dem die Datei erstellt wurde.

Dabei ist darauf zu achten, dass nicht alle Restinformationen einfach gelöscht werden können, ohne das Dateiformat zu zerstören. Wenn z. B. aus einer Textverarbeitungsdatei einige Bytes gelöscht werden, erkennt das Textverarbeitungsprogramm unter Umständen das Dateiformat nicht mehr. Um Restinformationen zu beseitigen,

- kann die Datei in einem anderen Dateiformat abgespeichert werden, z. B. als "Nur-Text" oder als HTML,
- können die Nutzdaten in eine zweite Instanz derselben Standard-Software kopiert werden, wobei auf dem IT-System keine andere Applikation laufen sollte. Dies empfiehlt sich insbesondere bei Dateien mit einer größeren Änderungshistorie.

Um der Weitergabe von Informationen vorzubeugen, die ursprünglich mit Wissen der Ersteller eingebracht worden sind, wie z. B. als "verborgen" formatierter Text, dessen Vorhandensein dann aber vergessen wurde, kann es sinnvoll sein, die Datei ausdrucken. Dabei sollten dann alle Optionen aktiviert werden, die beim Drucken versteckte Informationen mitausgeben.

Restinformationen/Slack-Bytes

Beim Datenträgeraustausch kann sogenannter Slack-Space ein Problem darstellen. Jedes Betriebssystem hat eine kleinste physikalische Speichereinheit mit festgelegter Größe. Unter DOS ist dies ein Sektor und umfasst 512 Byte. Bei Unix-Systemen ist dies ein Block, die Größe eines Blocks hängt dabei von der eingesetzten Unix-Variante ab. Unter DOS werden die einzelnen Sektoren einer Partition logisch zu Zuordnungseinheiten (Cluster) zusammengefasst. Wieviele Sektoren einen Cluster bilden, hängt von der Größe der Partition ab. Wird eine Datei geöffnet, werden ihr ein oder mehrere Cluster zugeordnet.

Die letzte Zuordnungseinheit wird dabei nicht vollständig benutzt, wenn die Dateigröße der zu speichernden Datei nicht zufällig ein Vielfaches der Clustergröße ist.

Dies verbraucht Speicherplatz. Der durchschnittliche Speicherplatzverbrauch hierdurch steigt mit der Clustergröße. Da diese wiederum mit der Partitionsgröße steigt, sollten Partitionen nicht zu groß sein. Hierzu ein Beispiel: Bei einer Partitionsgröße zwischen 1024 und 2047 MB hat ein einzelner Cluster 32 KB. Damit gehen durchschnittlich bei jeder Datei 16 KB Speicherplatz verloren.

Ein anderes Problem hierbei ist, dass (bei DOS-basierten Betriebssystemen) die restlichen Bytes des letzten Clusters bzw. Blocks mit zufällig im Hauptspeicher stehenden Bytes aufgefüllt werden, sogenannten Slack-Bytes. Diese können sinnlose Einträge, Informationen über die Dateistruktur, aber auch Passwörter enthalten. Auch bei einem Kopiervorgang von einem Datenträger auf den anderen kann die Datei je nach Clustergröße mit Slack-Bytes aufgefüllt werden.

Vor der Weitergabe von Dateien sollte sichergestellt werden, dass diese keine Slack-Bytes mehr enthalten. Dies kann mit Hilfe eines geeigneten Editors (z. B. Hex-Editor) überprüft werden.

Daneben haben viele Windows-Applikationen das Problem, dass das jeweilige Programm bei der Bearbeitung einer Datei den in Anspruch genommenen Speicherplatz nicht durchgehend mit Applikationsdaten überschreibt, sondern dass Lücken entstehen können, die ebenfalls alte Datenbestände des IT-Systems enthalten.

Verborgener Text / Kommentare

Eine Datei kann Textpassagen enthalten, die als "versteckt" oder "verborgen" formatiert sind. Einige Programme bieten auch die Möglichkeit an, Kommentare hinzuzufügen, die auf dem Ausdruck und oft auch am Bildschirm ausgeblendet sind. Solche Textpassagen können Bemerkungen enthalten, die nicht für den Empfänger bestimmt sind. Daher müssen in Dateien, bevor sie an Externe weitergegeben werden, solche Zusatzinformationen gelöscht werden.

Änderungsmarkierungen

Bei der Bearbeitung von Dateien kann es sinnvoll sein, hierbei Änderungsmarkierungen zu verwenden. Da diese auf dem Ausdruck und am Bildschirm ausgeblendet werden können, muss vor der Weitergabe von Dateien ebenfalls überprüft werden, ob diese Änderungsmarkierungen enthalten.

Versionsführung

In praktisch allen aktuellen Office-Suites gibt es die Möglichkeit, verschiedene Versionen eines Dokumentes in **einer** Datei zu speichern. Dies dient dazu, um bei Bedarf auf frühere Überarbeitungsstände zurückgreifen zu können. Dies kann aber sehr schnell zu riesigen Dateien führen, z. B. wenn Graphiken mitgeführt werden. Auf keinen Fall sollte die Option "Version beim Schließen automatisch speichern" gewählt werden, da hier bei jedem Schließen einer Datei die komplette Vorgängerversion zusätzlich gespeichert wird.

Dateieigenschaften

Als Dateieigenschaften oder Datei-Info werden in der Datei Informationen gespeichert, die bei späteren Suchen helfen sollen, Dateien wieder zu finden. Dabei können je nach Applikation Informationen wie Titel, Verzeichnisstrukturen, Versionsstände, Bearbeiter (nicht nur der Unterschreibende), Kommentare, Bearbeitungszeit, letztes Druckdatum, Dokumentnamen und -beschreibungen enthalten sein. Einige dieser Informationen werden von den Programmen selber angelegt und können nicht durch den Bearbeiter beeinflusst werden. Andere Informationen müssen manuell eingegeben werden. Vor der Weitergabe einer Datei an Externe ist zu überprüfen, welche zusätzlichen Informationen dieser Art die Datei enthält.

Schnellspeicherung

Textverarbeitungsprogramme nutzen die Option der Schnellspeicherung, um nur die Veränderungen seit der letzten Sicherung und nicht das gesamte Dokument speichern zu müssen. Dieser Vorgang nimmt somit weniger Zeit in Anspruch als ein vollständiger Speichervorgang. Ein vollständiger Speichervorgang erfordert jedoch weniger Festplattenspeicher als eine Schnellspeicherung. Der entscheidende Nachteil ist jedoch, dass die Datei unter Umständen Textfragmente enthalten kann, die durch die Überarbeitung hätten beseitigt werden sollen. Grundsätzlich sollten daher Schnellspeicherungsoptionen abgeschaltet werden.

Entscheidet sich der Benutzer trotzdem für die Schnellspeicheroption, sollte er bei folgenden Situationen immer einen vollständigen Speichervorgang durchführen:

- wenn die Bearbeitung eines Dokuments abgeschlossen ist,
- bevor eine weitere Anwendung ausgeführt wird, die viel Speicherplatz in Anspruch nimmt,
- bevor der Dokumenttext in eine andere Anwendung übertragen wird,
- bevor das Dokument in ein anderes Dateiformat konvertiert wird und
- bevor das Dokument per E-Mail oder Datenträgeraustausch versandt wird.

Ergänzende Kontrollfragen:

- Wurden die Benutzer über die möglichen Gefährdungen durch Restinformationen in Dateien informiert?
- Wurden die Benutzer über die möglichen Gefährdungen durch den Einsatz von Schnellspeicheroptionen aufgeklärt?

M 4.65 Test neuer Hard- und Software

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Vor dem Einsatz neuer Hardware-Komponenten oder neuer Software müssen diese auf speziellen Testsystemen kontrolliert werden. Neben der Lauffähigkeit des Produktes ist dabei insbesondere zu überprüfen, dass der Einsatz neuer Komponeten keine negativen Auswirkungen auf die laufenden IT-Systeme hat. Da vor erfolgreichen Tests Schadfunktionen nicht ausgeschlossen werden können und da bei Tests Fehler provoziert werden, sind immer **vom Produktionsbetrieb isolierte** Testsysteme zu verwenden.

Der Einsatz isolierter Testsysteme ist auch erforderlich, um selbstextrahierende Dateien, die z. B. per E-Mail empfangen wurden, auf Schadfunktionen zu prüfen.

Generelle Verfahrensweisen für die Software-Abnahme und -Freigabe inklusive des Testens sind in Baustein B 1.10 *Standardsoftware* beschrieben. Erst nach bestandenem Test dürfen neue Komponenten für die Installation auf Produktionssystemen freigegeben werden.

Ergänzende Kontrollfragen:

- Ist neue Hard- bzw. Software vor dem Einsatz getestet worden?
- Ist neue Software auf Computer-Viren geprüft worden?

M 4.66 Novell Netware - Sicherer Übergang ins Jahr 2000

Diese Maßnahme ist mit Version 2004 entfallen.

M 4.67 Sperren und Löschen nicht benötigter Datenbank-Accounts

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Wenn ein neu einzurichtender Benutzer seinen Datenbank-Account nur für einen befristeten Zeitraum benötigt, sollte dieser auch nur befristet eingerichtet werden, falls die Datenbank eine solche Möglichkeit zur Verfügung stellt. Es kann vorteilhaft sein, Accounts grundsätzlich nur befristet einzurichten und in regelmäßigen Abständen (z. B. jährlich) bei Bedarf zu verlängern.

Darüberhinaus sollte die Datenbankadministration schnellstmöglichst über das endgültige Ausscheiden eines Benutzers informiert werden. Spätestens am letzten Arbeitstag des Benutzers ist dessen Account zu sperren.

Auch wenn Benutzer in ein anderes Aufgabengebiet, einen anderen Zuständigkeitsbereich oder andere Projekte wechseln, müssen die dafür nicht mehr benötigten Datenbank-Accounts gesperrt oder die Zugriffsrechte entsprechend angepasst werden.

Weiterhin sollte regelmäßig geprüft werden, ob vorhandene Datenbank-Accounts tatsächlich benötigt werden. Insbesondere sollten hierbei auch nicht benötigte Standard-Accounts gesperrt werden.

Ergänzende Kontrollfragen:

- Existieren organisatorische Regelungen für befristete Datenbank-Accounts, insbesondere dann, wenn das Datenbanksystem das Einrichten solcher Accounts nicht unterstützt?
- Wird regelmäßig geprüft, welche Datenbank-Accounts nicht mehr benötigt werden?
- Wird der Datenbankadministration mitgeteilt, wenn Benutzer der Datenbank ausgeschieden sind?

M 4.68 Sicherstellung einer konsistenten Datenbankverwaltung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator

Die Datenbankverwaltung steht im Zentrum des Betriebskonzepts eines Datenbanksystems (DBS), auf dessen Grundlage unter anderem die konsistente Datenbankverwaltung sichergestellt werden soll. Im Betriebskonzept müssen alle für den Betrieb des DBS wichtigen Prozesse mit fest definierten Ausgangspunkten, Durchführungsreihenfolgen und Zielen sowie die zur Durchführung der Prozesse berechtigten Rollen mit ihren Rechten und Pflichten definiert sein.

Im weiteren Verlauf des Projekts müssen darüber hinaus den definierten Rollen reale Personen zugeordnet werden.

In der Rollenbeschreibung werden die Aufgaben, Zugriffsrechte und Befugnisse der Rollen beschrieben, die zur Durchführung bestimmter Funktionen notwendig sind (siehe auch M 2.132 *Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen*). Im Datenbank-Managementsystem (DBMS) sind die definierten Rollen als Benutzergruppen einzurichten, denen die rollenspezifische Rechte zuzuordnen sind. Den Benutzergruppen werden gemäß Rollenprofil die zuständigen Benutzer über ihre Benutzerkennung zugeordnet.

Besonders zu beachten sind nachfolgende Hinweise:

- Der Systemadministrator ist ein spezieller Benutzer in der Rechteverwaltung des Datenbanksystems, der bereits nach der Installation des DBMS zur Verfügung steht. Dieser Benutzer unterliegt prinzipiell keinerlei Beschränkungen bei der Nutzung des Datenbanksystems, wodurch ein Risiko für Fehler oder Missbrauch besteht. Diese Kennung darf nur von dem kleinen Kreis der System-Administratoren für explizit festgelegte Administrationsaufgaben, wie die Einrichtung von Datenbank-Administratoren für einzelne Datenbanken genutzt werden.
- Die Benutzergruppen der Datenbank-Administratoren für einzelne Datenbanken und somit auch die jeweils zugeordneten Benutzer unterliegen prinzipiell keinerlei Beschränkungen bei Nutzung und Manipulation der Datenbanken in ihrem Zuständigkeitsbereich, wodurch ein generelles Gefahrenpotential besteht. Die Rechte, die für diese Aufgaben notwendig sind, müssen daher wie der Personenkreis, der mit diesen Rechten ausgestattet wird, klar definiert und dokumentiert sein.
- In vielen Fällen arbeiten die Administratoren auch als Benutzer auf einer Datenbank, da sie neben ihrer Administratorentätigkeit Benutzeraufgaben wahrnehmen oder die Datenbank für die Ablage und Verwaltung von Dokumentationen im Administrationsumfeld nutzen. In diesem Fall ist für sie, neben der Administratorenkennung, eine normale Benutzerkennung anzulegen, die für solche Arbeiten mit der Datenbank genutzt wird. Die Administratorenkennung darf nur für Administrationstätigkeiten genutzt werden.

- Die Zuordnung eines Benutzers zu mehreren Benutzergruppen sollte genau geplant werden, da der Benutzer die Summe der Berechtigungen aller Benutzergruppen erhält, denen er zugeordnet ist.

Zusätzlich sollte durch eine klare Aufgabenteilung, verbindliche Regelungen sowie Absprachen zwischen den Administratoren sichergestellt werden, dass Administratoren keine inkonsistenten oder unvollständigen Eingriffe vornehmen. Dabei sollten folgende Bedingungen erfüllt sein:

- Die Art und Weise der Durchführung von Änderungen sowie deren Dokumentation ist festzulegen.
- Art, Umfang und Grund der Änderungen sind zu beschreiben.
- Änderungen an Datenbankobjekten oder Daten sind prinzipiell durch den Verantwortlichen der IT-Anwendung genehmigungspflichtig. Handelt es sich dabei um ein zentrales Datenbankobjekt, so erfordert eine Änderung die Zustimmung aller Verantwortlichen der betroffenen IT-Anwendungen.
- Der Zeitpunkt der geplanten Änderungen ist festzulegen und bekannt zu geben.
- Vor der Durchführung von Änderungen muss die Datenbank komplett gesichert werden.
- Für den laufenden Betrieb sollte ein Kontrollintervall festgelegt werden, in dem die Dokumente/Protokolle auf Aktualität und Korrektheit überprüft werden (siehe auch M 4.69 *Regelmäßiger Sicherheitscheck der Datenbank*).

Um Gefährdungen der Datenbankintegrität und Inkonsistenzen einzelner Datensätze zu vermeiden, sollten alle Datenbankobjekte einer Anwendung unter die ausschließliche Verwaltung einer eigens für die jeweilige Anwendung eingerichteten Benutzergruppe gestellt werden. Dieser Benutzergruppe dürfen ausschließlich Anwender zugeordnet werden, die direkte Zugriffsrechte auf die Datenbankobjekte der betreffenden Anwendung zu ihrer Aufgabenerfüllung benötigen. Außerdem sollte der für die jeweilige Anwendung zuständige Datenbankadministrator Mitglied dieser Benutzergruppe sein.

Ergänzende Kontrollfragen:

- Welche Maßnahmen werden ergriffen, um Eingriffe des Datenbankadministrators, die zu Inkonsistenzen führen können, zu verhindern?
- Haben alle Datenbankadministratoren eine zusätzliche Benutzer-Kennung mit eingeschränkten Rechten?
- Werden für die Datenbankobjekte einer Anwendung spezielle Benutzer-Gruppen eingerichtet?
- Sind die Vorgaben zur Administration und Nutzung der Datenbank in einem Betriebskonzept festgelegt?

M 4.69 Regelmäßiger Sicherheitscheck der Datenbank

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der Datenbankadministrator sollte regelmäßig, jedoch mindestens einmal monatlich einen Sicherheitscheck des Datenbanksystems (DBS) durchführen, der durch das Betriebskonzept geregelt sein sollte. In Abhängigkeit der Prüfungsergebnisse sollten entsprechende Maßnahmen ergriffen werden, um Abweichungen von den Vorgaben des Betriebskonzepts abzustellen. Diese Maßnahmen und die Zuständigkeiten für die Umsetzung sollten ebenfalls im Betriebskonzept festgelegt sein.

Folgende Aspekte sollten im Rahmen des Sicherheitschecks mindestens überprüft werden, wobei die mit (*) markierten Punkte meist durch entsprechende Skripte automatisiert werden können:

- Werden die im Betriebskonzept vorgegebenen Nachweise (z. B. Dokumentation von Änderungen) korrekt erstellt?
- Sind die erforderlichen und geplanten Sicherungs- und Sicherheitsmechanismen aktiv und greifen sie auch?
- Gibt es Datenbank-Benutzer mit leicht zu ermittelndem oder keinem Passwort? (*)
- Gibt es Benutzer, die die ihnen zugewiesenen Rechte nicht mehr für ihre Aufgabenerfüllung benötigen?
- Wer darf bzw. kann außer dem Datenbank-Administrator auf die Dateien der Datenbank-Software bzw. auf die Dateien der Datenbank auf Betriebssystemebene zugreifen? (*)
- Wer hat außer dem Datenbank-Administrator Zugriff auf die System-Tabellen der Datenbanken?
- Wer darf mit einem interaktiven SQL-Editor auf die Datenbank zugreifen?
- Welche Benutzer-Kennungen haben modifizierende Zugriffsrechte auf die Datenbankobjekte der Anwendungen? (*)
- Welche Benutzer-Kennungen haben lesende und / oder modifizierende Zugriffsrechte auf die Daten der Anwendungen? (*)
- Welche Benutzer besitzen die gleichen Rechte wie der Datenbank-Administrator? (*)
- Verfügt das Datenbanksystem über ausreichend freie Ressourcen? (*)

Ergänzende Kontrollfragen:

- Wann wurde der letzte Sicherheitscheck durchgeführt?
- Werden die Durchführung und die Ergebnisse der Sicherheitschecks dokumentiert?
- Werden nach der Aufdeckung von Sicherheitslücken Maßnahmen zur Beseitigung eingeleitet?

M 4.70 Durchführung einer Datenbanküberwachung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um die Verfügbarkeit, die Datenbankintegrität und die Vertraulichkeit der Daten gewährleisten zu können, ist eine regelmäßige und in angemessen definierten Überwachungszeiträumen durchzuführende Datenbanküberwachung erforderlich. Dabei zu beachtende Aspekte, die im folgenden kurz erläutert werden, sind unter anderen die Datenfragmentierung innerhalb der Datenbank, das aktuelle Datenvolumen und dessen Veränderung hinsichtlich der vorhandenen Ressourcen (Füllgrad) sowie die Auslastung der Datenbank.

Datenfragmentierung

Die Datenbank ist in regelmäßigen Zeitabständen hinsichtlich einer möglichen Fragmentierung zu überprüfen, um gegebenenfalls Maßnahmen, wie z. B. eine Reorganisation der Datenbank, planen und durchführen zu können.

Die Speicherplatzverwaltung in einem Datenbankmanagementsystem (DBMS) geschieht in der Regel in Form von Blöcken fester Größe, d. h. eine Veränderung (meist Vergrößerung) des Speicherplatzes erfolgt nur in Blöcken. Datensätze werden dabei auf eine minimale Anzahl von Blöcken verteilt abgespeichert. Prinzipiell werden Daten hinzugefügt, indem zuerst freie Blöcke belegt und wenn nötig zusätzlich neue Blöcke angelegt werden. Beim Löschen werden die zugehörigen Blöcke wieder freigegeben und stehen für neue Daten zur Verfügung.

Im Laufe der Zeit entsteht durch Datenveränderungen im Speicherbereich eine Abfolge von belegten und unbelegten Blöcken sowie eine immer größere Anzahl unvollständig belegter Blöcke. Darüberhinaus werden die Datensätze physikalisch weit über die Speichermedien verteilt. Diese Fragmentierung erhöht nicht nur den Speicherbedarf, sondern verlangsamt auch Datenbankoperationen, da Datensätze und freier Speicherplatz erst über einen größeren Speicherbereich gesucht werden müssen.

Sollte die Fragmentierung der Datenbank aufgrund der oben genannten Gründe eine festgelegte Grenze überschreiten, muss eine Reorganisation durchgeführt werden. Datenbank-Hersteller und Drittanbieter stellen zur Unterstützung dieser Aufgaben Administrations- und Hilfsprogramme zur Verfügung.

Datenvolumen und Füllgrad

Um einer zu starken bzw. zu raschen Fragmentierung vorzubeugen, erlauben einige Datenbankmanagementsysteme durch Definition bestimmter Parameter bereits beim Anlegen der Tabellen, eine bestimmte Menge zusammenhängender Blöcke zu reservieren. Damit steigt bei gleichem Datenvolumen der Füllgrad.

Die Datenbankdateien sollten regelmäßig hinsichtlich ihres Datenvolumen und Füllgrades überwacht werden. Dabei wird regelmäßig überprüft, ob sich das Datenvolumen zusammen mit dem Füllgrad im vorgegebenen Rahmen verändert. Ist das Wachstum größer als erwartet, kann es unter Umständen zu Speicherengpässen kommen. Aus den Beobachtungen sollten Maßnahmen, wie z. B. eine Erweiterung der Speicherkapazitäten, abgeleitet werden.

Beispiel:

Bei einer Oracle-Datenbank wird jeder Tabelle eine feste Anzahl von Extents (im Sprachgebrauch von Oracle: logische Größeneinheit) zugeordnet. Die Daten einer Tabelle werden in mindestens einem Extent abgelegt. Sobald die Kapazität eines Extents ausgeschöpft ist, legt das DBMS automatisch ein weiteres Extent an. Beim Erstellen einer Tabelle können dabei folgende Werte definiert werden:

- Größe des ersten und nachfolgenden Extents in Bytes
- Wachstum aller weiteren Extents in Prozent, wobei diese Zahl in Relation zur Größe des zweiten Extents steht
- Maximale Anzahl an Extents, die für die Tabelle angelegt werden dürfen
- Reservierte Blöcke für spätere Änderungen in Prozent

Wenn durch Anlage weiterer Extents der freie Speicherbereich innerhalb eines Tablespaces (siehe Beispiel in G 2.39 *Mangelhafte Konzeption eines DBMS*) zu gering wird, muss ein neuer Tablespace hinzugefügt werden. Eine Verringerung der Anzahl der Tablespaces ist nur durch vollständige Reorganisation möglich.

Auslastung

Darüber hinaus ist die Auslastung der Datenbank regelmäßig zu prüfen, insbesondere im Hinblick auf die eingestellten Obergrenzen (siehe M 4.73 *Festlegung von Obergrenzen für selektierbare Datensätze*).

Welche Informationen für eine konkrete Datenbanküberwachung relevant sind, hängt von deren spezieller Funktionsweise, also von der eingesetzten Datenbank-Standardsoftware ab. Dementsprechend sind auch individuelle Maßnahmen einzuleiten, die die Datenbankkonfiguration dahingehend modifizieren, dass sie den Anforderungen hinsichtlich Zugriffsgeschwindigkeiten, durchzuführender Transaktionen usw. gerecht wird.

Eine Automatisierung der Datenbanküberwachung kann in vielen Fällen mit Hilfe von Skripten durchgeführt werden. Eine Voraussetzung ist allerdings, dass die Informationen in auswertbarer Form von der eingesetzten Datenbank-Software zur Verfügung gestellt werden.

Ergänzende Kontrollfragen:

- Werden die Datenbankdateien, wichtige Tabellen und die Auslastung der Datenbank regelmäßig überprüft?
- Sind die Überwachungszeiträume angemessen definiert?

M 4.71 Restriktive Handhabung von Datenbank-Links

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Über Datenbank-Links (DB-Links) besteht die Möglichkeit, von einer Datenbank innerhalb eines DBMS aus auf die Daten einer anderen Datenbank, gegebenenfalls in einem anderen DBMS, zuzugreifen. Um einen angemessenen Schutz der Daten zu gewährleisten, sollte diese Technik nur im Rahmen eines entsprechenden Berechtigungskonzepts angewendet werden. In diesem Konzept muss unter anderem die Kontrolle der Berechtigungen eines Benutzers bei der Verwendung von DB-Links geregelt werden.

So kann festgelegt werden, dass ein Benutzer prinzipiell die Möglichkeit erhält, auf eine fremde Datenbank zuzugreifen, wenn dort die gleiche Benutzer-Kennung existiert, mit der sich der Benutzer an der lokalen Datenbank anmeldet. Einen weitergehenderen Schutz erhält man durch die Möglichkeit, einen DB-Link mit expliziter Angabe einer Benutzer-Kennung und eines Passwortes zu erstellen.

Nachfolgende Aspekte sollten im Hinblick auf DB-Links in einem Berechtigungskonzept geregelt werden:

- Im allgemeinen sollte nur der Administrator das Recht besitzen, mittels der entsprechenden CREATE-Kommandos DB-Links zu erstellen. Insbesondere gilt dies für DB-Links, die von allen Datenbankbenutzern genutzt werden dürfen (sogenannte PUBLIC DB-Links). Die Berechtigung zur Erstellung von DB-Links sollte dagegen für normale Benutzer-Kennungen nicht vergeben werden.
- Die Anzahl von parallel nutzbaren DB-Links eines Benutzers sollte begrenzt werden, um die Belastung der Datenbank-Server unter Kontrolle halten zu können (siehe M 4.73 *Festlegung von Obergrenzen für selektierbare Datensätze*). Ansonsten kann ein Angreifer dies ausnutzen, um den Durchsatz der Datenbank-Server zu reduzieren oder diese sogar vollständig zu überlasten.
- Eine Dokumentation der vom Administrator angelegten DB-Links ist unabdingbar. Die Dokumentation sollte neben der Verbindungsart (über eine spezielle Benutzer-Kennung oder unter der Voraussetzung, dass die jeweilige aktuelle Datenbank-Kennung ebenfalls für die verbundene Datenbank angelegt wurde) auch beinhalten, welcher Benutzerkreis in der Lage ist, den entsprechenden DB-Link zu nutzen.

Ergänzende Kontrollfragen:

- Wird auf die Verwendung von PUBLIC DB-Links verzichtet?
- Enthält das Datenbank-Konzept Vorgaben für den Einsatz von DB-Links?
- Welche Benutzerkennungen sind berechtigt, DB-Links zu erstellen?

M 4.72 Datenbank-Verschlüsselung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Anwendungsentwickler

In Abhängigkeit von der Art der in einer Datenbank gespeicherten Informationen und den sich daraus ergebenden Anforderungen an deren Vertraulichkeit und Integrität kann es notwendig werden, diese Daten zu verschlüsseln. Dabei kann zwischen einer Online- und einer Offline-Verschlüsselung unterschieden werden:

- Bei einer Online-Verschlüsselung werden die Daten während des laufenden Betriebs ver- und entschlüsselt, ohne dass die betroffenen Benutzer davon etwas merken. Dafür können Tools eingesetzt werden, mit denen entweder auf Betriebssystemebene die gesamte Festplatte verschlüsselt wird, oder solche, mit denen nur die Anwendungsdaten der Datenbank verschlüsselt werden.
- Bei einer Offline-Verschlüsselung werden die Daten erst nach ihrer Bearbeitung verschlüsselt und vor ihrer Weiterverarbeitung wieder entschlüsselt. Dies wird im allgemeinen mit Tools durchgeführt, die nicht in das Datenbanksystem integriert sind, und kann insbesondere für Datensicherungen oder Datenübertragungen sinnvoll sein. Dabei ist zu beachten, dass genügend Platz auf der Festplatte vorhanden ist, da die Ver- bzw. Entschlüsselung nur dann erfolgreich ausgeführt werden kann, wenn auf der Festplatte genügend Platz für das Original und die verschlüsselte Version der Datenbank verfügbar ist.

Darüber hinaus besteht die Möglichkeit, Daten weiterhin im Klartext in der Datenbank abzuspeichern, beim Zugriff über ein Netz jedoch eine verschlüsselte Datenübertragung zu realisieren. Dies kann z. B. durch die *Secure Network Services* der Oracle SQL*Net Produktfamilie durchgeführt werden.

Welche Daten mit welchem Verfahren zu verschlüsseln sind, ist am besten bereits bei der Auswahl der Datenbank-Standardsoftware festzustellen (siehe M 2.124 *Geeignete Auswahl einer Datenbank-Software*). Dabei sollten die Anforderungen hinsichtlich der Verschlüsselung von Datenbeständen mit den entsprechenden Leistungsmerkmalen der Datenbank-Software verglichen werden. Als Mindestanforderung sollte sie in jedem Fall sicherstellen, dass die Passwörter der Benutzer-Kennungen der Datenbank verschlüsselt abgelegt sind.

Falls die Anforderungen durch keine der am Markt verfügbaren Datenbank-Standardsoftware abgedeckt werden können, sollte man den Einsatz von Zusatzprodukten prüfen, um die entsprechende Sicherheitslücke zu schließen. Falls auch keine Zusatzprodukte erhältlich sind, muss ein Konzept für die Umsetzung einer Verschlüsselungsstrategie erstellt werden, das im Unternehmen bzw. in der Behörde umgesetzt wird.

Ergänzende Kontrollfragen:

- Werden von der Datenbank oder durch Zusatzprodukte geeignete Techniken zur Verschlüsselung bereitgestellt?
- Sind die Verantwortlichen über ein ordnungsgemäßes Schlüsselmanagement informiert?

M 4.73 Festlegung von Obergrenzen für selektierbare Datensätze

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Anwendungsentwickler

Um den Zugriff auf ein Datenbanksystem besser kontrollieren zu können und um die Performance zu verbessern, sollten Obergrenzen für bestimmte Parameter von Datenbank-Systemen festgelegt werden.

Zudem kann durch diese Maßnahme die Wahrscheinlichkeit bestimmter Arten von Denial-of-Service-Attacken (siehe G 5.65 *Verhinderung der Dienste eines Datenbanksystems*) verringert werden.

Beispiele sind:

- die Festlegung von Obergrenzen für Datensätze, die im Rahmen eines Datenzugriffs selektiert werden können
- die maximale Anzahl von Anmeldungen pro Benutzer-Kennung
- der maximale Anspruch auf CPU-Zeit pro Anmeldung
- die Gesamtdauer einer Datenbankverbindung
- die maximal zulässige inaktive Zeit während einer Anmeldung

Dabei sind vor allem folgende Hinweise zu beachten:

Festlegung von Obergrenzen für selektierbare Datensätze

Insbesondere wenn große Datenmengen in einer Datenbank abgelegt wurden, sollte eine maximale Anzahl von Datensätzen definiert werden, die im Rahmen eines Datenzugriffs selektiert werden können.

Existieren solche Obergrenzen nicht, kann ein Benutzer gezielt oder unbeabsichtigt beliebig umfangreiche Selektierungen durchführen. Dies behindert nicht nur den einzelnen Benutzer in seiner Arbeit, sondern führt unter Umständen auch bei allen anderen Benutzern der Datenbank zu langen Wartezeiten. Werden die Datensätze dabei selektiert um sie zu modifizieren, sind sie solange für alle anderen Benutzer gesperrt, bis die Transaktion beendet ist.

Die Obergrenzen müssen im Rahmen der Anwendungen definiert werden, die auf die Datenbank zugreifen. Dabei müssen geeignete Kontrollen bzw. Sperren realisiert werden, die die Einhaltung der Obergrenzen überwachen. Stellt eine Anwendung Suchfunktionalitäten bereit, so sollte die uneingeschränkte Suche generell abgelehnt und die Eingabe von Suchkriterien gefordert werden.

Sollte zwischen Anwendungsprogramm und Datenbank eine große Distanz liegen (z. B. Anbindung über Internet) sollten Ergebnisse in Blöcken ausgetauscht werden, für die ebenfalls Obergrenzen festzulegen sind.

Beispiel:

Ein Anwendungsprogramm greift über eine Internetverbindung auf eine Datenbank zu. Die vom Anwendungsprogramm an die Datenbank übergebenen Abfragen liefern potentiell sehr große Datenmengen zurück. Um nicht Gefahr zu laufen, durch zu große Ergebnisblöcke die Übertragung an die Anwendung

zu verlangsamen, wird auf der Datenbank die Abfrage in einer Prozedur gekapselt. Diese Prozedur überträgt bei jedem Aufruf eine festgelegte Menge von Daten (beispielsweise 5 Datensätze), bis alle Ergebnisse vollständig übertragen sind. Die Anwendung schickt in einer Schleife Anfragen an das DBMS und setzt die erhaltenen Teilergebnisse wieder zusammen oder kann eventuell auch schon Teilergebnisse anzeigen.

Festlegung von Ressourcenbeschränkungen

Eine weitere Möglichkeit, die von einigen Herstellern angeboten wird, ist die Festlegung von Ressourcenbeschränkungen in Bezug auf die Benutzung einer Datenbank.

Beispiele:

Mit folgendem Kommando wird in einer Oracle-Datenbank für die Datenbankkennung "Meier" der temporäre Tablespace "Temp" auf 100 MB begrenzt:

```
ALTER USER Meier TEMPORARY TABLESPACE Temp QUOTA
100M ON Temp;
```

Mit dem nachfolgenden Befehl wird ein Profil "Tester" erstellt, das die Anzahl der Sessions, die maximale CPU-Zeit pro Session, die maximale Zeit einer Datenbankverbindung und die maximale Leerlaufzeit (IDLE) begrenzt. Dieses Profil kann dann einzelnen Benutzern zugeordnet werden.

```
CREATE PROFILE Tester LIMIT
SESSIONS PER USER       2,
CPU _PER_SESSION        6000,
IDLE_TIME               30,
CONNECT_TIME            500;
```

Eine Ingres-Datenbank erlaubt beispielsweise für Benutzer und Gruppen das Setzen von Grenzen für die maximale Ein- und Ausgabe je Abfrage oder für die Anzahl von Sätzen pro Abfrage.

Weiterhin kann die Anzahl der Benutzer beschränkt werden, die gleichzeitig auf die Datenbank zugreifen dürfen. Je nach Lizenzmodell kann durch deren Begrenzung mittels Parametereinstellungen im DBMS unter Umständen auch gewährleistet werden, dass die maximal zur Verfügung stehende Zahl an Lizenzen für die Datenbank-Software nicht überschritten wird.

Außerdem verursachen viele parallel zugreifende Benutzer eine hohe Arbeitslast, der der Datenbank-Server eventuell nicht gewachsen ist. Hierdurch verlängert sich die durchschnittliche Dauer einer Transaktion. Ist in diesem Fall eine Erweiterung der Ressourcen des Datenbanksystems nicht möglich oder nicht gewünscht, schafft hier eine Begrenzung der maximal möglichen parallelen Benutzerzugriffe ebenfalls Abhilfe.

Auf der anderen Seite kann eine Begrenzung der maximal möglichen parallelen Benutzerzugriffe auch zu starken Einbußen bei der Performance für

die Benutzer führen. Diese Funktionalität sollte deshalb nur nach genauer Prüfung oder temporär, beispielsweise in einmalig auftretenden Spitzenzeiten, eingesetzt werden.

Wenn die Zahl der Datenbankbenutzer zunimmt und absehbar ist, dass die aktuellen Ressourcen zukünftig die Anforderungen an die Performance nicht mehr erfüllen können oder dass mehr Lizenzen benötigt werden, ist eine entsprechende Erweiterung vorzusehen und zu planen.

Die absehbaren Anforderungen sollten bereits während der Auswahl einer Datenbank-Standardsoftware geklärt werden, um gegebenenfalls ein Konzept zur Umsetzung der Ressourcenbeschränkungen zu erstellen (siehe M 2.124 *Geeignete Auswahl einer Datenbank-Software*).

Ergänzende Kontrollfragen:

- Wird die Einhaltung von Obergrenzen in den Anwendungen kontrolliert und umgesetzt?
- Wird eine uneingeschränkte Suche in den Anwendungen prinzipiell unterbunden?
- Wurden die Anforderungen an eine Ressourcenbeschränkung der Datenbank formuliert und dokumentiert?

M 4.74 Vernetzte Windows 95 Rechner

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Administrator

Werden Windows 95 Rechner in einem Netz betrieben (Novell Netware oder Windows NT), so sollte die Möglichkeit genutzt werden, die jeweiligen Systemrichtlinien auf Netzservern zu speichern und diese dort zentral zu verwalten.

Mit Hilfe der SYSTEMSTEUERUNG unter NETZWERK wird hierbei die primäre Netzwerkanmeldung, d. h. der Pfad für die Systemrichtlinien festgelegt. Standardmäßig werden die Benutzerprofile auf einem Novell Netware Server unter SYS:PUBLIC abgelegt. Erfolgt die primäre Netzanmeldung an einem Windows NT Rechner, so werden die Benutzerprofile standardmäßig unter NETLOGON (*%SystemRoot%\SYSTEM32\REPL\IMPORT\SCRIPTS*) abgelegt.

Die Aktivierung der Benutzerprofile wird mit Hilfe der SYSTEMSTEUERUNG-KENNWÖRTER-BENUTZERPROFILE sichergestellt.

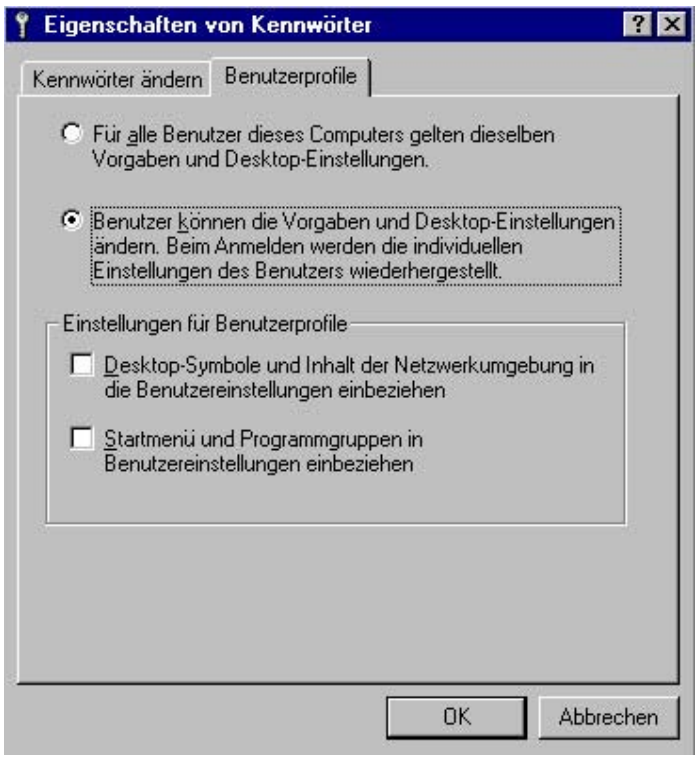


Abbildung: Eigenschaften von Kennwörtern

Weiterhin sollte zudem der Betrieb von Windows 95 ohne Netzwerkanmeldung gesperrt werden um eine Umgehung der Systemrichtlinien auf lokaler Basis zu verhindern. Hierzu sollte mit Hilfe von *POLEDIT.EXE* unter lokaler Computer-Netzwerk-Anmeldung die Option *NETZWERKBESTÄTIGUNG FÜR WINDOWS ZUGRIFF FORDERN* aktiviert werden.

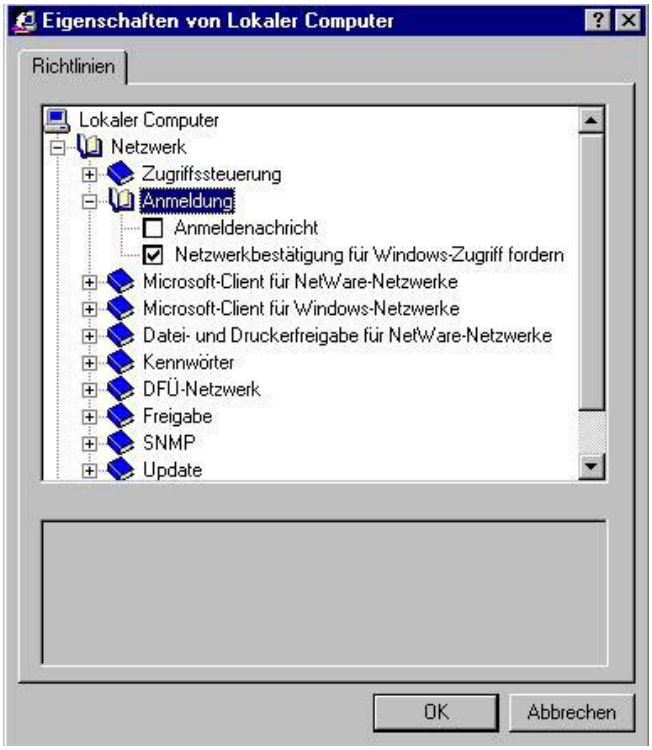


Abbildung: Eigenschaften von Lokaler Computer

Gruppenrichtlinien werden unter Windows 95 über SYSTEMSTEUERUNG-SOFTWARE-WINDOWS-SETUP installiert und befinden sich standardmäßig in dem Verzeichnis

ADMIN\APPTOOLS\POLEDIT\GROUPPOL.INF.

Die Namen der jeweiligen Benutzergruppen müssen hierbei den eingerichteten Benutzergruppen unter Novell Netware bzw. Windows NT entsprechen.

Um den ordnungsgemäßen IT-Betrieb sicherzustellen, sollte zusätzlich beachtet werden, dass das Programm *POLEDIT.EXE* nicht auf dem lokalen Windows 95 Rechner installiert werden darf, da mit diesem Programm die gültigen Systemrichtlinien von jederman dauerhaft verändert werden können.

Ebenso sollte in der Datei MSDOS.SYS der Wert BootKeys verändert werden (BootKeys=1) um den Start von Windows 95 im "abgesicherten Modus" zu unterbinden. Dies verhindert, dass die Systemrichtlinien nicht zur Anwendung kommen.

Das BIOS des Computers sollte zudem einen Systemboot über Diskette verhindern, sowie das Diskettenlaufwerk mit einem Schloss versperrt werden, um Einsatz von unautorisierter Software zu erschweren.

M 4.75 Schutz der Registrierung unter Windows NT/2000/XP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Zugriffsrechte auf Registry-Dateien

In der Registrierung eines Windows NT/2000/XP Systems werden alle wichtigen Konfigurations- und Initialisierungsinformationen gespeichert. Dort wird u. a. auch die SAM-Datenbank verwaltet, die die Benutzer- und Computerkonten enthält. Beim Einsatz von Windows 2000/XP gilt dies insbesondere für Rechner, die keiner Domäne angeschlossen sind, oder Domänen-Rechner, auf denen auch lokale Konten benutzt werden.

Zugriffsrechte auf Registry-Einträge

Die Registrierung eines Windows NT/2000/XP Systems besteht aus mehreren Dateien, die sich in dem Verzeichnis *%SystemRoot%\SYSTEM32\Config* befinden. Aus diesem Grund sollten die Zugriffsrechte auf dieses Verzeichnis und die darin enthaltenen Dateien so gesetzt werden, wie dies in M 4.53 *Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT*, M 4.149 *Datei- und Freigabeberechtigungen unter Windows 2000/XP* und M 4.247 *Restriktive Berechtigungsvergabe unter Windows XP* vorgeschlagen wird.

Zur Erhöhung des Schutzes sollten unmittelbar nach der Installation von Windows NT die folgenden sicherheitsrelevanten Teile der Registrierung durch expliziten Eintrag von Zugriffsrechten mit Hilfe des Registrierungs-Editors besonders geschützt werden. Dies erfolgt mit Hilfe des Programms *REGEDT32.EXE* im Windows-Systemverzeichnis *%SystemRoot% \ SYSTEM32*. Die Einstellungen sollten so erfolgen, dass die Gruppe *Jeder* für diese Teile nur über die Zugriffsrechte *Wert einsehen*, *Teilschlüssel auflisten*, *Benachrichtigen* und *Zugriff lesen* verfügt:

- im Bereich HKEY_LOCAL_MACHINE:
  \Software\Windows3.1MigrationStatus (mit allen Unterschlüsseln)
  \Software\Microsoft\RPC (mit allen Unterschlüsseln)
  \Software\Microsoft\Windows NT\CurrentVersion
  unter dem Schlüssel \Software\Microsoft\Windows NT\CurrentVersion\:
  + Profile List
  + AeDebug
  + Compatibility
  + Drivers
  + Embedding
  + Fonts
  + FontSubstitutes
  + GRE_Initialize
  + MCI
  + MCI Extensions
  + Port (mit allen Unterschlüsseln)
  + WOW (mit allen Unterschlüsseln)
- im Bereich HKEY_CLASSES_ROOT:

  \HKEY_CLASSES_ROOT (mit allen Unterschlüsseln)

Die entsprechenden Einstellungen für Zugriffsrechte auf die Registrierung unter Windows XP sind in der Maßnahme M 4.247 *Restriktive Berechtigungsvergabe unter Windows XP* zu finden.

Einstellungen testen

Dabei ist sorgfältig vorzugehen, da fehlerhafte Einstellungen in der Registrierung dazu führen können, dass das System nicht mehr lauffähig ist und nach dem nächsten Starten eventuell nicht mehr bootet. Die hier genannten Einstellungen sollten daher zunächst auf ein Testsystem angewendet und auf ihre Lauffähigkeit in der aktuellen Umgebung kritisch geprüft werden, ehe sie allgemein eingesetzt werden.

Netzzugriff auf die Registrierung

Sofern diese Funktionalität nicht unbedingt gebraucht wird, sollte auch der Zugriff über das Netz auf die Registrierung gesperrt werden. Dies ist ab der Version 4.0 möglich, indem der Eintrag *winreg* im Schlüssel *\System\CurrentControlSet\Control\SecurePipeServers* im Bereich *HKEY_LOCAL_MACHINE* auf den Wert *REG_DWORD = 1* gesetzt wird.

In der Version 3.x besteht die Möglichkeit der expliziten Sperrung von Netzzugriffen auf die Registrierung nicht. Hier kann man sich damit behelfen, dass die Zugriffsberechtigung für *Jeder* auf die Wurzel des Bereiches *HKEY_LOCAL_MACHINE* (**nicht** jedoch auf die darunter liegenden Schlüssel!) entfernt wird, so dass nur noch Administratoren auf diesen Bereich Zugriff haben. Diese Änderung ist unbedingt auf einem Testsystem zu überprüfen, da sie zur Folge haben kann, dass einige Anwendungen nicht mehr lauffähig sind. Es ist zu beachten, dass diese Änderung nur bis zum nächsten Systemstart bestehen bleibt.

M 4.76 Sichere Systemversion von Windows NT

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator, Beschaffer

Auswahl der Sprachversion

Vor der Beschaffung des Betriebssystems Windows NT muss entschieden werden, ob die englische oder die deutsche Version beschafft werden soll. Es ist nicht möglich, eine eindeutige Empfehlung abzugeben. Daher soll hier nur aufgezeigt werden, welche spezifischen Vor- und Nachteile die Entscheidung für die eine oder andere Version mit sich bringt.

Die englische Version von Windows NT ist stärker verbreitet als die deutsche Version. Dies führt dazu, dass Tools, Service Packs und Hot Fixes für die englische Version schneller verfügbar sind. Es gibt auch Tools, die nur mit der englischen Version von Windows NT einsetzbar sind. Es ist auch möglich, die englische Version von Windows NT so zu konfigurieren, dass Fehlermeldungen in deutscher Sprache ausgegeben werden.

Andererseits ergibt sich die gleiche Situation hinsichtlich der Verfügbarkeit bei den Schadprogrammen. Auch diese werden für die englische Version schneller entwickelt und sind teilweise für die deutsche Version überhaupt nicht verfügbar.

Auswahl des jeweils aktuellen Service Packs

Windows NT kann nur dann sicher betrieben werden, wenn mindestens die Version 3.51 oder die Version 4.0 installiert ist. Weiterhin wird die Installation des jeweils aktuellen Service Packs empfohlen. Vor dem Einsatz im Wirkbetrieb sollte jedoch getestet werden, ob das Service Pack mit allen Komponenten in der vorliegenden Umgebung problemlos zusammenarbeitet. Eventuell müssen neben der Installation des Service Packs weitere Updates an Hardware- oder Software-Komponenten vorgenommen werden. Für die Windows NT Version 3.51 ist bei Drucklegung das Service Pack 5 und für Windows NT Version 4.0 das Service Pack 6a verfügbar. Die installierte Systemversion und das ggf. installierte Service Pack werden beim Systemstart angezeigt.

Installation von Hot Fixes

Außerdem werden durch Microsoft so genannte Hot Fixes zur Verfügung gestellt, die Updates zu dem jeweils aktuellen Service Pack darstellen. Die jeweils aktuellen Hot Fixes sollten ebenfalls installiert werden, soweit sie Funktionen des installierten Systems betreffen. Hot Fixes werden als Reaktion auf aufgetretene Probleme kurzfristig erstellt. Dies bedingt auch, dass sie nicht so ausgetestet sind, wie die Service Packs. Deshalb sollten auf einem System auch nur die wirklich erforderlichen Hot Fixes installiert werden. Der Systemverwalter muss sich regelmäßig darüber informieren, welches Service Pack und welche Hot Fixes für sein System aktuell sind.

Erneutes Einspielen bei Änderungen der Systemkonfiguration

Die einmalige Installation eines Service Packs oder eines Hot Fixes reicht nicht für die Sicherstellung der Systemintegrität. Jede Änderung der Systemkonfiguration, die einen Zugriff auf die Installations-CD-ROM erforderlich macht oder bei der neue Gerätetreiber installiert werden müssen, bedingt eine erneute Installation des aktuellen Service Packs und der notwendigen Hot Fixes. Wird dies unterlassen, besteht die Gefahr, dass Systemdateien, die aus dem jeweiligen Service Pack oder dem Hot Fix stammen, durch eine ältere

Version ersetzt werden, was im schlimmsten Fall dazu führen kann, dass ein Windows NT System nicht mehr in Betrieb genommen werden kann.

Nach der Installation eines Service Packs oder eines Hot Fixes sollten die Notfalldisketten aktualisiert werden (siehe M 6.42 *Erstellung von Rettungsdisketten für Windows NT*). Außerdem sollte die Sicherheitskonfiguration des betroffenen Rechners überprüft werden.

M 4.77 Schutz der Administratorkonten unter Windows NT

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator

Bei jeder Installation eines jeden Windows NT Systems wird ein Administratorkonto angelegt. Auf Windows NT Rechnern, die als Workstation oder als Server ohne Domänencontrollerfunktion installiert werden, ist dieses vordefinierte Administratorkonto Mitglied der Gruppe "Administratoren". Auf Servern, die unter dem Betriebssystem Windows NT als Primäre Domänencontroller installiert werden, wird das vordefinierte Administratorkonto bei der Installation Mitglied der Gruppen "Administratoren", "Domänen-Admins" und "Domänen-Benutzer". Es ist weiterhin möglich, beliebige auf einem Windows NT Rechner definierte Benutzerkonten den Gruppen "Administratoren" oder "Domänen-Admins" hinzuzufügen.

Das vordefinierte Administratorkonto und die nach der Installation den Gruppen "Administratoren" bzw. "Domänen-Admins" hinzugefügten Benutzerkonten erhalten die Rechte und Berechtigungen, die der oder den Gruppen erteilt wurden, in denen sie Mitglied sind. Diese Konten werden von den Personen verwendet, welche die Gesamtkonfiguration der Arbeitsstation oder des Servers verwalten. Administratoren besitzen mehr Kontrollmöglichkeiten über den Windows NT Computer als jeder andere Benutzer.

Das vordefinierte Administratorkonto unterscheidet sich aber in wesentlichen Punkten von allen anderen Konten unter Windows NT: Es kann nicht gelöscht werden und es ist von der automatischen Sperre bei wiederholten Anmeldeversuchen mit falschem Passwort ausgenommen. Außerdem kann es auf Windows NT Workstations und auf Windows NT Servern ohne Domänencontrollerfunktionalität nicht aus der Gruppe "Administratoren" entfernt werden. Auf Windows NT Domänencontrollern ist es nicht möglich, das vordefinierte Administratorkonto sowohl aus der Gruppe "Administratoren" als auch aus der Gruppe "Domänen-Admins" zu entfernen. Die Entfernung aus einer dieser beiden Gruppen ist aber möglich. Damit wird verhindert, dass ein Administrator zeitweise oder vollständig aus dem System ausgesperrt wird. Andererseits führt dieser Mechanismus zu einem erhöhten Einbruchsrisiko. An dieser Stelle muss ausdrücklich darauf hingewiesen werden, dass alle nachträglich angelegten Benutzerkonten, die durch Aufnahme in die Gruppen "Administratoren" bzw. "Domänen-Admins" Administratorrechte erlangt haben, selbstverständlich durch andere Administratoren gesperrt und gelöscht bzw. aus den o. g. Gruppen wieder entfernt werden können. Auch ist die automatische Sperre bei wiederholten Anmeldeversuchen mit falschem Passwort wirksam, sofern diese in den Kontenrichtlinien definiert wurde.

Auf **allen Windows NT Computern** sollte das vordefinierte Administratorkonto auf einen nicht leicht erratbaren Namen umbenannt werden. Es sollte bereits bei der Installation mit einem sicheren Passwort (siehe M 2.11 *Regelung des Passwortgebrauchs*) versehen werden. Das Passwort sollte möglichst die maximale Länge von 14 Zeichen ausnutzen und ist sicher zu hinterlegen. Es ist sinnvoll, für die tägliche Administration nicht das vor-

definierte Administratorkonto zu benutzen, sondern Benutzerkonten, die der Gruppe "Administratoren" oder "Domänen-Admins" hinzugefügt wurden. Die Passwortlänge dieser Konten sollte mindestens 8 Zeichen betragen. Das vordefinierte Administratorkonto sollte lediglich für den Fall benutzt werden, dass ein Zugriff über die nachträglich angelegten Konten mit Administratorrechten nicht möglich ist, z. B. weil diese Konten wegen wiederholten Anmeldeversuchen mit falschem Passwort gesperrt sind.

Auch ist es sinnvoll, danach ein neues Konto mit dem Namen "Administrator" anzulegen, dieses mit einem Passwort zu versehen, es zu deaktivieren und dieses Konto nur in der Gruppe "Gäste" aufzunehmen. Diesem Konto dürfen keine besonderen Systemrechte zugewiesen werden, da es lediglich dazu dient, einen potentiellen Angreifer auf eine falsche Spur zu führen.

Weiterhin sollte das Sicherheitsprotokoll regelmäßig auf Anmeldeversuche mit Konten, die über Administratorrechte verfügen, überprüft werden (siehe M 4.54 *Protokollierung unter Windows NT*).

Es existiert eine spezielle Schadsoftware, mit der ein lokal angemeldeter Benutzer der Gruppe "Administratoren" beliebige Benutzerkonten hinzufügen kann. Um dies zu verhindern, sollte auf allen Computern unter dem Betriebssystem Windows NT 4.0 mit dem Service Pack 3 der Hot Fix "getadmin-fix" installiert werden, der durch Microsoft kostenlos zur Verfügung gestellt wird. Nach der Installation des Service Packs 4 ist es nicht mehr erforderlich, den o. g. Hotfix zu installieren.

Um ein Extrahieren des Administratorpasswortes zu verhindern, sollten außerdem die Rechte auf die Verzeichnisse *%SystemRoot%\SYSTEM32\Config* und *%SystemRoot%\SYSTEM32\Repair* so gesetzt werden, wie dies in M 4.53 *Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT* vorgeschlagen wird. Auch müssen Notstartdisketten und evtl. vorhandene Bandsicherungen unter Verschluss gehalten werden.

Abhängig vom Schutzbedarf der Daten, die mit **Windows NT Workstations** verarbeitet werden, ist zu entscheiden, ob für alle lokalen Administratorenkonten das gleiche Passwort benutzt wird. Eine generelle Empfehlung kann nicht gegeben werden, es sollte jedoch bei einer Entscheidung zugunsten des gleichen Passwortes für alle Workstations bedacht werden, dass ein Angreifer im Falle der Kompromittierung dieses Passwortes auf allen betroffenen Workstations Administratorrechte hat.

Bei **Windows NT Servern** sollten noch folgende weitere Maßnahmen getroffen werden. Es sollten die Administratorenkonten auf den verschiedenen Servern nicht alle mit dem gleichen Passwort versehen werden. Weiterhin sollte möglichst nicht über das Netz fernadministriert werden. Dies wird erreicht, indem der Gruppe "Administratoren" das Recht "*Zugriff auf diesen Computer vom Netz*" entzogen wird. Wo auf eine Fernadministration z. B. aufgrund räumlicher Gegebenheiten nicht verzichtet werden kann, sollten die Angriffsmöglichkeiten, die sich dadurch eröffnen, so gering wie möglich gehalten werden. Dazu gehört, dass eine Anmeldung über das Netz für Benutzerkonten mit Administratorrechten nur über in den Kontenrichtlinien festgelegte Rechner, die unter dem Betriebssystem Windows NT betrieben

werden, erlaubt wird. Diese Rechner sollten möglichst in gesicherten Bereichen aufgestellt werden. Auf diesen Rechnern sollte zwingend die LAN-Manager-Kompatibilität abgeschaltet werden, um so zu vermeiden, dass Passwörter von Benutzerkonten mit Administratorrechten unverschlüsselt bzw. nur schwach verschlüsselt über das Netz gesendet werden. Dazu ist es erforderlich, bei einem Windows NT 4.0 mit Service Pack 3 den Hot Fix "lm-fix" zu installieren. Sofern auf dem System bereits das Service Pack 4 installiert wurde, ist eine Installation des v. g. Hot Fix nicht notwendig. In jedem Fall ist aber in der Registrierung der folgende Schlüssel zu ergänzen: *HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\Lsa* um den Eintrag "*LMCompatibilityLevel*" vom Typ "REG_DWORD" und dem Wert "2".

Ein so modifizierter Windows NT Rechner ist danach nicht mehr in der Lage, auf Ressourcen zuzugreifen, die sich auf Rechnern befinden, die das Windows NT Authentisierungsschema nicht beherrschen. Dies sind u. a. alle Rechner, die unter dem Betriebssystem Windows 95 betrieben werden.

Auf **Domänencontrollern** reicht es nicht aus, der Gruppe "Administratoren" das Recht "*Zugriff auf diesen Computer vom Netz*" zu entziehen, weil auf Domänencontrollern das vordefinierte Administratorkonto automatisch Mitglied in den Gruppen "Domänen-Admins" und "Domänen-Benutzer" geworden ist. Das vordefinierte Administratorkonto sollte daher aus der Gruppe der "Domänen-Admins" entfernt werden. Dies ist möglich, solange dieses Konto Mitglied der Gruppe "Administratoren" bleibt. Außerdem sollte das vordefinierte Administratorkonto aus der Gruppe "Domänen-Benutzer" entfernt werden. Dies ist allerdings nicht ohne weiteres möglich, da es die primäre Gruppe dieses Kontos ist. Es muss daher eine beliebige globale Gruppe angelegt werden, die nicht über das Recht "*Zugriff auf diesen Computer vom Netz*" verfügt. Das vordefinierte Administratorkonto ist dieser Gruppe hinzuzufügen und es ist einzustellen, dass dies nunmehr die primäre Gruppe des Kontos sein soll. Erst danach kann das vordefinierte Administratorkonto aus der Gruppe "Domänen-Benutzer" entfernt werden.

M 4.78 Sorgfältige Durchführung von Konfigurationsänderungen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator

Die Durchführung von Änderungen an einem IT-System im Echtbetrieb ist immer als kritisch einzustufen und entsprechend sorgfältig muss hierbei vorgegangen werden.

Bevor mit Änderungen am System begonnen wird, muss als erstes die alte Konfiguration gesichert werden, sodass sie schnell verfügbar ist, wenn Probleme mit der neuen Konfiguration auftreten.

Bei vernetzten IT-Systemen müssen die Benutzer rechtzeitig über die Durchführung von Wartungsarbeiten informiert werden, damit sie zum einen ihre Planung auf eine zeitweise Systemabschaltung einrichten können, und damit sie zum anderen nach Änderungen auftretende Probleme richtig zuordnen können.

Die Konfigurationsänderungen sollten immer nur schrittweise durchgeführt werden. Zwischendurch sollte immer wieder überprüft werden, ob die Änderungen korrekt durchgeführt wurden und das IT-System sowie die betroffenen Applikationen noch lauffähig sind.

Bei Änderungen an Systemdateien ist anschließend ein Neustart durchzuführen, um zu überprüfen, ob sich das IT-System korrekt starten lässt. Für Problemfälle sind alle für einen Notstart benötigten Datenträger vorrätig zu halten, z. B. Boot-Disketten, Start-CD-ROM.

Komplexere Konfigurationsänderungen sollten möglichst nicht in den Originaldateien vorgenommen werden, sondern in Kopien. Alle durchgeführten Änderungen sollten von einem Kollegen überprüft werden, bevor sie in den Echtbetrieb übernommen werden.

Bei IT-Systemen mit hohen Verfügbarkeitsanforderungen ist auf Ersatzsysteme zurückzugreifen bzw. zumindest ein eingeschränkter IT-Betrieb zu gewährleisten. Das Vorgehen kann sich dabei idealerweise nach dem Notfall-Handbuch richten.

Die durchgeführten Konfigurationsänderungen sollten Schritt für Schritt notiert werden, sodass bei auftretenden Problemen das IT-System durch sukzessive Rücknahme der Änderungen wieder in einen lauffähigen Zustand gebracht werden kann (siehe auch M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*).

Ergänzende Kontrollfragen:

- Werden Systemveränderungen schrittweise dokumentiert?
- Lassen sich die Änderungen nachträglich rückgängig machen?

M 4.79 Sichere Zugriffsmechanismen bei lokaler Administration

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Bei einigen aktiven Komponenten kann über einen lokalen Zugriff die Administration der Komponenten erfolgen. Solch ein lokaler Zugriff ist zumeist über einen seriellen Anschluss (üblicherweise eine V.24 bzw. EIA-232-E Schnittstelle) realisiert. Für einen sicheren lokalen Zugriff sind die folgenden Maßnahmen zu beachten:

- Die aktiven Netzkomponenten und ihre Peripheriegeräte, wie z. B. angeschlossene Terminals, müssen sicher aufgestellt werden (siehe M 1.29 *Geeignete Aufstellung eines IT-Systems*),
- der lokale Zugriff zur Administration der lokalen Komponenten muss softwaretechnisch und/oder mechanisch gesperrt werden,
- eine eventuell vorhandenes Standardpasswort des lokalen Zugriffs muss sofort nach Inbetriebnahme geändert werden (zur Auswahl des neuen Passwortes siehe M 2.11 *Regelung des Passwortgebrauchs*),
- die Sicherheitseigenschaften dauerhaft angeschlossener Terminals oder Rechner, wie z. B. automatische Bildschirmsperre oder Auto-Logout, sind zu aktivieren (siehe M 5.11 *Server-Konsole sperren*).

Eine lokale Administration bietet folgende Vorteile:

- Die Gefahr des Abhörens von Passwörtern wird reduziert.
- Auch bei einem Ausfall des Netzsegmentes, in dem sich die aktive Komponente befindet, oder bei einem Ausfall des gesamten Netzes ist eine Administration weiterhin möglich.

Eine lokale Administration bietet allerdings auch folgende Nachteile:

- Aktive Netzkomponenten können im allgemeinen so konfiguriert werden, dass eine lokale oder eine zentrale Administration der aktiven Netzkomponenten möglich ist. Für die Auswahl der Konfigurationsmethode kann jedoch keine generelle Empfehlung gegeben werden. Zu berücksichtigen ist jedoch, dass bei der Konfiguration für eine ausschließlich lokale Administration keine zentrale Administration der aktiven Netzkomponenten mehr möglich ist. Diese muss dann immer vor Ort direkt an den entsprechenden Komponenten vorgenommen werden. In diesem Fall erhöht sich auch die Reaktionszeit im Störungsfall, da unter Umständen längere Wege bis zum Standort der Komponente zurückzulegen sind.
- Der lokale Zugriff ist durch die Realisierung über eine V.24 bzw. EIA-232-E Schnittstelle im allgemeinen langsamer als ein Fernzugriff über das Netz.

Ergänzende Kontrollfragen:

- Sind die Standardpaßwörter für den lokalen Zugriff gegen sichere ausgetauscht worden?

M 4.80 Sichere Zugriffsmechanismen bei Fernadministration

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Einige aktive Netzkomponenten können über einen Netzzugriff fernadministriert oder überwacht werden. Der Zugriff erfolgt entweder über verbindungsorientierte oder verbindungslose Protokolle. Hierzu gehören:

- Protokolle zur reinen Datenübertragung, beispielsweise um neue Firmware-Versionen oder Konfigurationsdateien zu übertragen, z. B. *FTP*, *TFTP* (von letzterem wird prinzipiell abgeraten) oder *RCP* (siehe auch M 6.52 *Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten*),
- Protokolle zur interaktiven Kommunikation, z. B. *Telnet*,
- Protokolle für das Netzmanagement, z. B. *SNMP* oder *CMIP*.

Bei allen Zugriffsarten ist dafür Sorge zu tragen, dass kein unautorisierter Zugriff erfolgen kann.

Hierzu sind die Standardpasswörter bzw. Community-Namen der Netzkomponenten gegen sichere Passwörter bzw. Community-Namen auszutauschen (siehe M 4.82 *Sichere Konfiguration der aktiven Netzkomponenten*). Die Kopplung von Community-Namen und Passwort betrifft bei vielen aktiven Netzkomponenten die Protokolle FTP, Telnet, SNMP und CMIP. Einige Komponenten bieten auch die Möglichkeit, den Zugriff auf der Basis von MAC- oder IP-Adressen zu beschränken. Soweit möglich, sollte diese Option genutzt werden, um den Zugriff nur von dedizierten Managementstationen aus zu gestatten.

Protokolle zur Datenübertragung (TFTP, FTP, RCP) sollten nur von der Netzkomponente selbst initiiert werden können. Dies trifft insbesondere für nicht authentisierende Protokolle wie TFTP zu. Für interaktive Kommunikationsprotokolle (Telnet) sollte die Auto-Logout-Option der Netzkomponente aktiviert werden.

Bei den meisten der genannten Protokollen ist zu beachten, dass die Übertragung der Passwörter bzw. Community-Namen im Klartext erfolgt, also prinzipiell abgehört werden kann (siehe hierzu M 5.61 *Geeignete physikalische Segmentierung* und M 5.62 *Geeignete logische Segmentierung*)

Beispiel: Die bei SNMP standardmäßig voreingestellten Community-Namen "public" und "private" sollten gegen andere Namen ausgetauscht werden.

Ergänzende Kontrollfragen:

- Wurden alle Standardpasswörter und Community-Namen gegen sichere selbstgewählte ausgetauscht?
- Können Datenübertragungen nur von den Netzkomponenten aus initiiert werden?

M 4.81 Audit und Protokollierung der Aktivitäten im Netz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Revisor

Eine angemessene Durchführung von Protokollierung, Audit und Revision ist ein wesentlicher Faktor der Netzsicherheit.

Eine *Protokollierung* innerhalb eines Netzmanagementsystems oder an bestimmten aktiven Netzkomponenten erlaubt es, gewisse (im allgemeinen zu definierende) Zustände für eine spätere Auswertung abzuspeichern. Typische Fälle, die protokolliert werden können, sind z. B. die übertragenen fehlerhaften Pakete an einer Netzkomponente, ein unautorisierter Zugriff auf eine Netzkomponente oder die Performance eines Netzes zu bestimmten Zeiten. Eine Auswertung solcher Protokolle mit geeigneten Hilfsmitteln erlaubt beispielsweise einen Rückschluss, ob die Bandbreite des Netzes den derzeitigen Anforderungen genügt, oder die Erkennung von systematischen Angriffen auf das Netz.

Unter einem *Audit* wird die Verwendung eines Dienstes verstanden, der insbesondere sicherheitskritische Ereignisse betrachtet. Dies kann online oder offline erfolgen. Bei einem Online-Audit werden die Ereignisse mit Hilfe eines Tools (z. B. einem Netzmanagementsystem) in Echtzeit betrachtet und ausgewertet. Bei einem Offline-Audit werden die Daten protokolliert oder aus einer bestehenden Protokolldatei extrahiert. Zu den mit Hilfe eines Offline-Audits überwachten Faktoren gehören häufig auch Daten über Nutzungszeiten und angefallene Kosten.

Bei der *Revision* werden die beim (Offline-) Audit gesammelten Daten von einem oder mehreren unabhängigen Mitarbeitern (4-Augen-Prinzip) überprüft, um Unregelmäßigkeiten beim Betrieb der IT-Systeme aufzudecken und die Arbeit der Administratoren zu kontrollieren.

Die mit einem Netzmanagement-System möglichen Protokollierungs- und Audit-Funktionen sind in einem sinnvollen Umfang zu aktivieren. Neben Performance-Messungen zur Überwachung der Netzlast sind dabei insbesondere die Ereignisse (Events) auszuwerten, die von einem Netzmanagement-System generiert werden, oder spezifische Datensammler (z. B. RMON-Probes) einzusetzen, mit denen sicherheitskritische Ereignisse überwacht und ausgewertet werden können.

Bei der Protokollierung fallen zumeist sehr viele Einträge an, sodass diese nur mit Hilfe eines Werkzeuges sinnvoll ausgewertet werden können. Beim Audit liegt die Fokussierung auf der Überwachung von sicherheitskritischen Ereignissen. Zusätzlich werden beim Audit häufig auch Daten über Nutzungszeiträume und anfallende Kosten erhoben.

Dabei sind für ein Audit insbesondere folgende Vorkommnisse von Interesse:

- Daten über die Betriebsdauer von IT-Systemen (wann wurde welches IT-System ein- bzw. wieder ausgeschaltet?),

- Zugriffe auf aktive Netzkomponenten (wer hat sich wann angemeldet?),
- sicherheitskritische Zugriffe auf Netzkomponenten und Netzmanagement-Komponenten mit oder ohne Erfolg,
- Verteilung der Netzlast über die Betriebsdauer eines Tages oder eines Monats und die allgemeine Performance des Netzes.

Weiterhin sollten folgende Vorkommnisse protokolliert werden:

- Hardware-Fehlfunktionen, die zu einem Ausfall eines IT-Systems führen können,
- Unzulässige Änderungen der IP-Adresse eines IT-Systems (in einem TCP/IP-Umfeld).

Ein Audit kann sowohl online als auch offline betrieben werden. Bei einem Online-Audit werden entsprechend kategorisierte Ereignisse direkt dem Auditor mitgeteilt, der ggf. sofort Maßnahmen einleiten kann. Dafür müssen Ereignisse in geeignete Kategorien eingeteilt werden, damit der zuständige Administrator oder Auditor auf wichtige Ereignisse sofort reagieren kann und nicht unter einer Flut von Informationen den Überblick verliert. Ist Rollentrennung notwendig? Bei einem Offline-Audit werden die Daten aus den Protokolldateien oder speziellen Auditdateien mit Hilfe eines Werkzeuges für Auditzwecke aufbereitet und durch den Auditor überprüft. Im letzteren Fall können Maßnahmen zur Einhaltung oder Wiederherstellung der Sicherheit nur zeitverzögert eingeleitet werden. Im allgemeinen wird eine Mischform aus Online- und Offline-Audit empfohlen. Dabei werden für das Online-Audit die sicherheitskritischen Ereignisse gefiltert und dem Auditor sofort zur Kenntnis gebracht. Zusätzlich werden weniger kritische Ereignisse offline ausgewertet.

Für Protokollierung und Audit können die Standard-Managementprotokolle, wie z. B. SNMP und das darauf aufsetzende RMON, aber auch spezifische Protokolle des eingesetzten Netzmanagement-Produkt verwendet werden.

Auf keinen Fall dürfen Benutzer-Passwörter im Rahmen eines Audits oder einer Protokollierung gesammelt werden! Dadurch wird ein hohes Sicherheitsrisiko erzeugt, falls es zu einem unberechtigten Zugriff auf diese Informationen kommt. Auch falsch eingegebene Passwörter sollten nicht protokolliert werden, da sie sich von den gültigen Passwörtern meist nur um ein Zeichen bzw. um eine Vertauschung zweier Zeichen unterscheiden.

Es muss weiterhin festgelegt werden, wer die Protokolle und Audit-Daten auswertet. Hierbei muss eine angemessene Trennung zwischen Ereignisverursacher und -auswerter (z. B. Administrator und Auditor) vorgenommen werden. Weiterhin ist darauf zu achten, dass die datenschutzrechtlichen Bestimmungen eingehalten werden. Für alle erhobenen Daten ist insbesondere die Zweckbindung nach § 14 BDSG zu beachten.

Die Protokoll- oder Auditdateien müssen regelmäßig ausgewertet werden. Sie können sehr schnell sehr umfangreich werden. Um die Protokoll- oder Auditdateien auf ein auswertbares Maß zu beschränken, sollten die Auswertungsintervalle daher angemessen, aber dennoch so kurz gewählt werden, dass eine sinnvolle Auswertung möglich ist.

Ergänzende Kontrollfragen:

- Werden die aufgezeichneten Protokoll- und Auditdaten regelmäßig kontrolliert?
- Werden die möglichen Konsequenzen sicherheitskritischer Ereignisse analysiert?
- Werden die Benutzer-Passwörter protokolliert?

M 4.82 Sichere Konfiguration der aktiven Netzkomponenten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Neben der Sicherheit von Serversystemen und Endgeräten wird die eigentliche Netzinfrastruktur mit den aktiven Netzkomponenten in vielen Fällen vernachlässigt. Gerade zentrale aktive Netzkomponenten müssen jedoch sorgfältig konfiguriert werden. Denn während durch eine fehlerhafte Konfiguration eines Serversystems nur diejenigen Benutzer betroffen sind, die die entsprechenden Dienste dieses Systems nutzen, können bei einer Fehlkonfiguration eines Routers größere Teilnetze bzw. sogar das gesamte Netz ausfallen oder Daten unbemerkt kompromittiert werden.

Im Rahmen des Netzkonzeptes (siehe M 2.141 *Entwicklung eines Netzkonzeptes*) sollte auch die sichere Konfiguration der aktiven Netzkomponenten festgelegt werden. Dabei gilt es insbesondere folgendes zu beachten:

- Für Router und Layer-3-Switching muss ausgewählt werden, welche Protokolle weitergeleitet und welche nicht durchgelassen werden. Dies kann durch die Implementation geeigneter Filterregeln geschehen.
- Es muss festgelegt werden, welche IT-Systeme in welcher Richtung über die Router kommunizieren. Auch dies kann durch Filterregeln realisiert werden.
- Sofern dies von den aktiven Netzkomponenten unterstützt wird, sollte festgelegt werden, welche IT-Systeme Zugriff auf die Ports der Switches und Hubs des lokalen Netzes haben. Hierzu wird die MAC-Adresse des zugreifenden IT-Systems ausgewertet und auf ihre Berechtigung hin überprüft.

Für aktive Netzkomponenten mit Routing-Funktionalität ist außerdem ein geeigneter Schutz der Routing-Updates erforderlich. Diese sind zur Aktualisierung der Routing-Tabellen erforderlich, um eine dynamische Anpassung an die aktuellen Gegebenheiten des lokalen Netzes zu erreichen. Dabei kann man zwei verschiedene Sicherheitsmechanismen unterscheiden:

- Passwörter

  Die Verwendung von Passwörtern schützt die so konfigurierten Router vor der Annahme von Routing-Updates durch Router, die nicht über das entsprechende Passwort verfügen. Hierdurch können also Router davor geschützt werden, falsche oder ungültige Routing-Updates anzunehmen.Der Vorteil von Passwörtern gegenüber den anderen Schutzmechanismen ist ihr geringer Overhead, der nur wenig Bandbreite und Rechenzeit benötigt.

- Kryptographische Prüfsummen

  Prüfsummen schützen vor der unbemerkten Veränderung von gültigen Routing-Updates auf dem Weg durch das Netz. Zusammen mit einer

Sequenznummer oder einem eindeutigen Bezeichner kann eine Prüfsumme auch vor dem Wiedereinspielen alter Routing-Updates schützen.

Die Auswahl eines geeigneten Routing-Protokolls ist die Voraussetzung für einen angemessenen Schutz der Routing-Updates. RIP-2 (Routing Information Protocol Version 2, RFC 1723) und OSPF (Open Shortest Path First, RFC 1583) unterstützen Passwörter in ihrer Basis-Spezifikation und können durch Erweiterungen auch kryptographische Prüfsummen nach dem MD5 (Message Digest 5) Verfahren verwenden.

Ergänzende Kontrollfragen:

- Wurde bei der Erstellung des Netzkonzeptes die sichere Konfiguration der aktiven Netzkomponenten berücksichtigt?
- Wird ein geeignetes Routing-Protokoll eingesetzt?
- Wie werden die Routing-Updates geschützt?

M 4.83 Update/Upgrade von Soft- und Hardware im Netzbereich

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Durch ein Update von Software können Schwachstellen beseitigt oder Funktionen erweitert werden. Dies betrifft beispielsweise die Betriebssoftware von aktiven Netzkomponenten wie z. B. Switches oder Router, aber auch eine Netzmanagement-Software. Ein Update ist insbesondere dann notwendig, wenn Schwachstellen bekannt werden, die Auswirkungen auf den sicheren Betrieb des Netzes haben, wenn Fehlfunktionen wiederholt auftauchen oder eine funktionale Erweiterung aus sicherheitstechnischen oder fachlichen Erfordernissen notwendig wird.

Auch ein Upgrade von Hardware kann in bestimmten Fällen sinnvoll sein, wenn z. B. eine neue Version eines Switches eine höhere Transfer- und Filterrate bietet. Durch diese Maßnahmen kann der Grad der Verfügbarkeit, der Integrität und der Vertraulichkeit unter Umständen erhöht werden.

Bevor jedoch ein Upgrade oder ein Update vorgenommen wird, muss die Funktionalität, die Interoperabilität und die Zuverlässigkeit der neuen Komponenten genau geprüft werden. Dies geschieht am sinnvollsten in einem physikalisch separaten Testnetz, bevor das Update oder Upgrade in den produktiven Einsatz übernommen wird (siehe M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen)*.

Ergänzende Kontrollfrage:

- Werden die Updates bzw. Upgrades vor einem produktiven Einsatz auf die Interoperabilität mit den bereits vorhandenen Komponenten überprüft?

M 4.84 Nutzung der BIOS-Sicherheitsmechanismen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Moderne BIOS-Varianten bieten eine Vielzahl von Sicherheitsmechanismen an, mit denen sich die Benutzer oder die Systemadministration vertraut machen sollten. Auf keinen Fall sollten aber ungeschulte Benutzer BIOS-Einträge verändern, da hierdurch schwerwiegende Schäden verursacht werden können.

- Passwortschutz: Bei den meisten BIOS-Varianten kann ein Passwortschutz aktiviert werden. Dieser kann verhältnismäßig einfach überwunden werden, sollte aber auf jeden Fall benutzt werden, wenn keine anderen Zugriffsschutzmechanismen zur Verfügung stehen. Meist kann ausgewählt werden, ob das Passwort vor jedem Rechnerstart oder nur vor Zugriffen auf die BIOS-Einstellungen überprüft werden soll. Teilweise können sogar verschiedene Passwörter für diese Prüfungen benutzt werden. Um zu verhindern, dass Unbefugte die BIOS-Einstellungen ändern, sollte das Setup- oder Adminstrator-Passwort immer aktiviert werden.

  Mit einigen (leider wenigen) BIOS-Varianten kann zusätzlich der Zugriff auf die Diskettenlaufwerke durch ein Passwort geschützt werden. Dies sollte benutzt werden, um das unbefugte Aufspielen von Software oder das unbemerkte Kopieren von Daten zu verhindern.

- Boot-Reihenfolge: Die Boot-Reihenfolge sollte so eingestellt sein, dass immer als erstes von der Festplatte gebootet wird. Beispielsweise sollte also "C,A" eingestellt werden. Dies schützt vor der Infektion mit Boot-Viren, falls versehentlich eine Diskette im Laufwerksschacht vergessen wird, spart Zeit und schont das Diskettenlaufwerk.

  Die Umstellung der Boot-Reihenfolge soll verhindern, dass der Boot-Vorgang von einem externen Datenträger erfolgt. Hiermit soll gewährleistet werden, dass während des Boot-Vorgangs nicht auf eine im Diskettenlaufwerk eingelegte Diskette zugegriffen wird, wodurch ein Boot-Virus den PC infizieren könnte (siehe G 5.23 *Computer-Viren*). Je nach verwendetem BIOS und Betriebssystem muss auch das Booten von anderen austauschbaren Datenträgern wie CD-ROMs verhindert werden.

  Ohne eine Umstellung der Boot-Reihenfolge können auch weitere Sicherheitsmaßnahmen wie Zugriffsschutzmechanismen (siehe M 4.1 *Passwortschutz für IT-Systeme*) umgangen werden. Ein Beispiel hierfür ist das Starten eines anderen Betriebssystems, so dass gesetzte Sicherheitsattribute ignoriert werden (siehe M 4.49 *Absicherung des Boot-Vorgangs für ein Windows NT/2000/XP System*).

  Generell sollte die Wirksamkeit der Umstellung der Boot-Reihenfolge durch einen Boot-Versuch geprüft werden, da einige Controller die interne Reihenfolge außer Betrieb nehmen und eine getrennte Einstellung erfordern.

- Virenschutz, Virus-Warnfunktion: Wird diese Funktion aktiviert, verlangt der Rechner vor einer Veränderung des Boot-Sektors bzw. des MBR (Master Boot Record) eine Bestätigung, ob diese durchgeführt werden darf.

Ergänzende Kontrollfrage:

- Welche BIOS- Sicherheitsmechanismen sind aktiviert?

M 4.85 Geeignetes Schnittstellendesign bei Kryptomodulen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Ein Kryptomodul sollte so beschaffen und konfigurierbar sein, dass der gesamte Informationsfluss von und zu dem Modul oder gar ein unmittelbarer physikalischer Zugriff auf den Datenbestand des Moduls kontrolliert bzw. eingeschränkt werden kann. Je nach Anwendungsfall bzw. Schutzbedarf empfiehlt sich die Verwendung von physikalisch getrennten Ein- und Ausgabeports. In jedem Fall sollten die Modulschnittstellen so aufgebaut sein, dass die einzelnen Datenkanäle logisch voneinander verschieden sind, obwohl sie möglicherweise einen gemeinsamen Ein- oder Ausgangsport teilen. Im Zusammenhang mit dem Schlüsselmanagement des Kryptomoduls muss gewährleistet sein, dass die Ausgabekanäle von der internen Schlüsselgenerierung bzw. dem Eingabeport für die manuelle Schlüsseleingabe zumindest logisch getrennt sind. In vielen Fällen werden zum Anschluss einer externen Versorgungsspannung bzw. eines externen Versorgungstakts und zur ausschließlichen Verwendung von Reparatur- oder Wartungsaufgaben separate Schnittstellen zur Verfügung stehen. Aus der Perspektive des Kryptomoduls ist daher die folgende Aufteilung und Verwendung zweckmäßig:

- Dateneingabeschnittstelle, die all diejenigen Eingabedaten des Kryptomoduls führt, die im Modul weiterverarbeitet oder bearbeitet werden (z. B. kryptographische Schlüssel, Authentisierungsinformationen, Statusinformationen von anderen Kryptomodulen, Klartextdaten etc.).
- Datenausgabeschnittstelle, die all diejenigen Daten des Kryptomoduls führt, die vom Modul an dessen Umgebung gelangen sollen (z. B. verschlüsselte Daten, Authentisierungsinformationen, Steuerinformationen für andere Kryptomodule, etc.).
- Steuereingabeschnittstelle, die sämtliche Steuerbefehle, -signale und -daten zur Ablaufsteuerung und Einstellung der Betriebsweise des Moduls führt.
- Statusausgabeschnittstelle, die alle Signale, Anzeigen und Daten an die Umgebung abführt, um den inneren Sicherheitszustand des Kryptomoduls anzuzeigen.

Und schließlich

- Maintenance-Schnittstelle, die ausschließlich Wartungs- und/oder Reparaturzwecken dient.

Die Dokumentation für eine Kryptokomponente sollte eine Beschreibung sämtlicher Komponenten enthalten (Hard-, Firm- und/oder Software).

Ferner sollte die Dokumentation die komplette Spezifikation der Modulschnittstellen beinhalten zuzüglich der physikalischen oder logischen Ports, manuellen oder logischen Steuereinheiten, physikalischen oder logischen Anzeigeelementen sowie deren physikalischen, logischen oder elektrischen

Eigenschaften. Wenn eine Kryptokomponente eine Maintenance-Schnittstelle enthält, sollte die Dokumentation auch die vollständige Spezifikation der durchzuführenden Wartungsprozesse zur Verfügung stellen. Alle physikalischen und logischen Ein- und Ausgabekanäle innerhalb des Moduls müssen explizit offengelegt sein. Neben der konkreten Einbindung der Kryptokomponente in eine vorgesehene Einsatzumgebung ist auch die Bedienung und Benutzung der Kryptokomponente zu beschreiben.

Die Dokumentation sollte weiterhin eine Zusammenstellung der Sicherheitsfunktionalität enthalten und womöglich die Abhängigkeit von Hard-, Firm- oder Software aufzeigen, die je nach Konzeption der Kryptokomponente nicht unmittelbar zum Lieferumfang der Kryptokomponente gehören.

Die Dokumentation über die Modulschnittstellen sind vom Modulhersteller zur Verfügung zu stellen. Die Dokumentation wird beispielsweise von einem Administrator benötigt, der beabsichtigt, das Kryptomodul in seine Systemumgebung zu integrieren, oder von einem Evaluator, der eine Sicherheitsbeurteilung des Kryptomoduls vornehmen möchte.

Ergänzende Kontrollfragen:

- Welche Informationen liegen zu den Krypto-Modulschnittstellen vor?
- Sind die Informationen ausreichend?

M 4.86 Sichere Rollenteilung und Konfiguration der Kryptomodule

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Viele kryptographische Sicherheitskomponenten bieten die Möglichkeit, dass mehrere Nutzerrollen sowie die zugehörigen Handlungen, die durch das autorisierte Personal ausgeführt werden können, unterschieden werden können. Abhängig vom Schutzbedarf sind hierzu Zugriffskontroll- und Authentisierungsmechanismen erforderlich, um verifizieren zu können, ob ein Nutzer zur Ausführung des gewünschten Dienstes auch tatsächlich autorisiert ist. In Bezug auf die unterschiedlichen Rollen bietet sich folgende Unterteilung an:

- Benutzerrolle, der die Benutzung und Verwendung der Sicherheitskomponente obliegt (z. B. Endteilnehmer, Benutzer).
- Operatorrolle, die für die Installation und das Kryptomanagement verantwortlich ist (z. B. Sicherheitsadministrator).

Und zumindest eine

- Maintenance-Rolle, die für Wartungs- und Reparaturarbeiten zuständig ist (z. B. Wartungstechniker, Revisor).

Bei Kryptokomponenten, bei denen die Benutzer- und die Administratorrolle getrennt werden kann, sollte diese Möglichkeit auch genutzt werden und durch die Administration Grundeinstellungen vorgegeben werden, wie z. B. Passwortlänge oder Schlüssellänge, sodass die Benutzer nicht aus Bequemlichkeit oder Unkenntnis unsichere Einstellungen wählen können.

Neben den unterschiedlichen Rollen gilt es entsprechend auch die verschiedenen Handlungen bzw. die von der Sicherheitskomponente bereitgestellten Dienste zu unterscheiden. Ein Kryptomodul sollte zumindest folgende Dienste zur Verfügung stellen:

- Statusanzeige zur Ausgabe des momentanen Status der Kryptokomponente,
- Selbsttest zur Initialisierung und Durchführung von selbständigen Selbsttests,
- Bypass zur Aktivierung und Deaktivierung eines Bypass mittels dessen durch das Kryptomodul Klarinformationen bzw. ungesicherte Daten transportiert werden.

Zur erforderlichen Authentisierung des Personals gegenüber der Sicherheitskomponente bieten sich eine Vielzahl von unterschiedlichen Techniken an: Passwort, PIN, kryptographische Schlüssel, biometrische Merkmale etc. Die Kryptokomponente sollte so konfiguriert sein, dass bei jedem Rollenwechsel oder bei Inaktivität nach einer bestimmten Zeitdauer die Authentisierungsinformationen erneut eingegeben werden müssen. Ferner empfiehlt sich an dieser Stelle eine Beschränkung der Authentisierungsversuche (z. B. indem der Fehlbedienungszähler auf 3 gesetzt wird).

Ergänzende Kontrollfrage:

- Sind die Kryptomodule sicher konfiguriert?

M 4.87 Physikalische Sicherheit von Kryptomodulen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Wie in M 2.165 *Auswahl eines geeigneten kryptographischen Produktes* beschrieben, können Kryptomodule in Software, Firmware oder Hardware realisiert sein. Firmware- bzw. Hardware-Produkte werden insbesondere dann gewählt, wenn das Kryptomodul besonders manipulationsresistent sein soll.

Unter diesem Gesichtspunkt sollte das Kryptomodul unter Verwendung von physikalischen Sicherheitsmaßnahmen oder unter Ausnutzung entsprechender Materialeigenschaften so konstruiert sein, dass ein unautorisierter physikalischer Zugriff auf Modulinhalte erfolgreich verhindert werden kann. Dies soll möglichen technischen Manipulationen oder sonstigen Beeinträchtigungen im laufenden Betrieb vorbeugen. In Abhängigkeit von der Sicherheitsstufe des Kryptomoduls sind hierzu beispielsweise die Verwendung von Passivierungsmaterialien, geeignete Tamperschutzmaßnahmen oder mechanische Schlösser in Betracht zu ziehen. Eine automatische Notlöschung, die eine aktive Löschung oder die Vernichtung aller im Klartext enthaltenen sensitiven Schlüsseldaten und -parameter bewerkstelligen kann, innerhalb des Kryptomoduls nach identifizierten Angriffsversuchen, zählt ebenfalls in diese Maßnahmenkategorie.

Mit dem Einsatz von diversen Sensoren und Überwachungseinrichtungen lässt sich sicherstellen, dass das Kryptomodul - was Spannungsversorgung, Taktung, Temperatur, mechanische Beanspruchung, elektromagnetische Beeinträchtigung etc. anbelangt - in seinem vorgesehenen Arbeitsbereich betrieben wird.

Zur Aufrechterhaltung seiner beabsichtigten Funktionalität sollte das Kryptomodul Selbsttests initiieren und durchführen können. Diese Tests können sich auf folgende Bereiche erstrecken: Algorithmentests, Software und Firmwaretests, Funktionstests, statistische Zufallstests, Konsistenztests, Bedingungstests sowie Schlüsselgenerierungs- und -ladetests. Im Anschluss an ein negatives Testergebnis sollte dem Benutzer des Kryptomoduls eine entsprechende Fehlermeldung signalisiert und ein entsprechender Fehlerzustand eingenommen werden. Erst nach Behebung der Fehlerursache(n) darf eine Freischaltung aus diesem Fehlerzustand möglich sein.

Beim Einsatz von Softwareprodukten muss die physikalische Sicherheit des Kryptomoduls durch das jeweilige IT-System bzw. dessen Einsatzumgebung geleistet werden. Sicherheitstechnische Anforderungen an solche IT-Systeme können den systemspezifischen Bausteinen entnommen werden.

Eine Softwarelösung sollte Selbsttests durchführen können, um Modifikationen durch Trojanische Pferde oder Coputer-Viren erkennen zu können.

M 4.88 Anforderungen an die Betriebssystem-Sicherheit beim Einsatz von Kryptomodulen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Beim Einsatz von Kryptomodulen spielt deren Einbindung ins bzw. Abhängigkeit vom jeweiligen Betriebssystem des Hostsystems eine wesentliche Rolle. Das Zusammenwirken von Betriebssystem und Kryptomodul muss gewährleisten, dass

- das Kryptomodul nicht abgeschaltet oder umgangen werden kann (z. B. durch Manipulation oder Austausch von Treibern),
- die angewendeten oder gespeicherten Schlüssel nicht kompromittiert werden können (z. B. durch Auslesen von RAM-Bereichen),
- die zu schützenden Daten **nur** mit Wissen und unter Kontrolle des Anwenders auch unverschlüsselt auf Datenträgern abgespeichert werden können bzw. das informationsverarbeitende System verlassen (z. B. bei Netzanbindung),
- Manipulationsversuche am Kryptomodul erkannt werden.

Je nach Art des Kryptomoduls (Hardware- oder Software-Realisierung, Einbindungsstrategie in die IT-Komponente etc.), den Einsatzbedingungen und dem Schutzbedarf der zu sichernden Daten können sich unterschiedlich starke Anforderungen bzgl. der Betriebssystem-Sicherheit ergeben. Bei in Software realisierten Kryptomodulen ist der Einsatz eines sicheren Betriebssystems besonders wichtig. Kommerzielle PC-Betriebssysteme sind in der Regel derart komplex und kurzen Innovationszyklen unterworfen, dass die Daten- bzw. Systemsicherheit kaum nachweisbar oder beweisbar ist. Eine Ausnahme können proprietäre oder für spezielle Anwendungen optimierte Betriebssysteme bilden (z. B. spezielle Betriebssysteme in Kryptogeräten). Daher ist es beim Einsatz von kryptographischen Produkten auf Standard-Betriebssystemen wie z. B. zur Dateiverschlüsselung oder zur E-Mail-Absicherung wichtig, dass alle Standardsicherheitsmaßnahmen für dieses Betriebssystem umgesetzt sind. Die sicherheitstechnischen Anforderungen an diese IT-Systeme können den jeweiligen systemspezifischen Bausteinen entnommen werden, so etwa für Clients oder Server in Schicht 3.

In Hardware realisierte Kryptomodule können so konstruiert sein, dass sie Mängel der Betriebssystem-Sicherheit kompensieren oder vollständig ausräumen. Hier liegt die Verantwortung zur Erfüllung der o. g. Anforderungen allein beim Kryptomodul. Es muss z. B. erkennen können, ob unverschlüsselte Daten berechtigt oder unberechtigt am Modul vorbei auf Datenträger oder andere Geräteschnittstellen geschrieben werden. Der Anwender muss in Übereinstimmung mit der für sein Umfeld individuell erstellten Sicherheitspolitik entscheiden, welche Kombination Betriebssystem / Kryptomodul erforderlich ist.

M 4.89 Abstrahlsicherheit

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Jedes elektronische Gerät strahlt mehr oder weniger starke elektromagnetische Wellen ab. Diese Abstrahlung ist als Störstrahlung bekannt und ihre maximal zulässige Stärke ist im Allgemeinen gesetzlich geregelt, in Deutschland ist dies das Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG). Bei Geräten, die Informationen verarbeiten (PC, Drucker, Faxgerät, Modem, usw.) kann diese Störstrahlung auch die gerade verarbeiteten Informationen mit sich führen. Derartige informationstragende Abstrahlung wird bloßstellende Abstrahlung genannt. Wird die bloßstellende Abstrahlung in einiger Entfernung, z. B. in einem Nachbarhaus oder auch in einem in der Nähe abgestellten Fahrzeug empfangen, kann daraus die Information rekonstruiert werden. Die Vertraulichkeit der Daten ist damit in Frage gestellt. Die Grenzwerte des EMVG reichen im allgemeinen nicht aus, um das Abhören der bloßstellenden Abstrahlung zu verhindern. Hierzu müssen in aller Regel zusätzliche Maßnahmen getroffen werden.

Bloßstellende Abstrahlung kann einen Raum auf unterschiedliche Weise verlassen:

- In Form von elektromagnetischen Wellen, die sich wie Rundfunkwellen durch den freien Raum ausbreiten.
- Als leitungsgebundene Abstrahlung entlang metallischer Leiter (Kabel, Klimakanäle, Heizungsrohre).
- Durch Überkoppeln von einem Datenkabel in parallel hierzu verlegte Kabel. Auf dem Parallelkabel breitet sich die Abstrahlung aus und kann von diesem noch in großer Entfernung abgegriffen werden.
- Als akustische Abstrahlung, z. B. bei Druckern. Die Detailinformationen des Druckvorgangs breiten sich über Schall beziehungsweise Ultraschall aus und können mit Mikrofonen aufgenommen werden.
- In Form von akustischer Überkopplung auf andere Geräte. Die Schallwandlung in elektrische Signale erfolgt dabei durch schallempfindliche Geräteteile, die unter bestimmten Voraussetzungen ähnlich wie ein "Mikrofon" arbeiten können. Die weitere Ausbreitung erfolgt dann entlang metallischer Leiter oder auch in Form elektromagnetischer Raumstrahlung.
- Bloßstellende Abstrahlung kann auch durch eine äußere Manipulation von Geräten verursacht werden. Wird z. B. ein Gerät mit Hochfrequenzenergie bestrahlt, können die im Gerät ablaufenden elektrischen Vorgänge die eingestrahlten Wellen so beeinflussen, dass diese nun die verarbeitete Information mit sich tragen.

In allen Fällen hat die Installation, also die Verkabelung der Geräte untereinander und mit dem Stromversorgungsnetz, einen wesentlichen Einfluss auf die Ausbreitung und damit auch auf die Reichweite der Abstrahlung.

Vom BSI werden Schutzmaßnahmen entwickelt, welche die Gefährdung ohne wesentliche Kostensteigerung wirksam reduzieren. Dazu gehören:

- Zonenmodell

  Das Zonenmodell berücksichtigt die Ausbreitungsbedingungen für bloßstellende Abstrahlung bei den jeweiligen Gebäude- und Geländeverhältnissen. Dabei wird die Abschwächung der Abstrahlung auf ihrem Weg vom verursachenden IT-Gerät zum potentiellen Empfänger messtechnisch erfasst. Abhängig von den Gegebenheiten am Einsatzort können gegebenenfalls Geräte eingesetzt werden, an denen nur geringfügige oder gar keine Sonderentstörmaßnahmen durchgeführt wurden.

- Quellenentstörung

  Die Quellenentstörung bewährt sich besonders bei der Neuentwicklung von IT-Produkten. Hier wird die bloßstellende Abstrahlung bereits am Entstehungsort innerhalb des Gerätes unterdrückt oder so verändert, dass sie nicht mehr auswertbar ist. Durch diese Methode kann z. B. auch der Einsatz kostengünstiger Kunststoffgehäuse möglich werden, mit vernachlässigbar geringen Auswirkungen auf den Serienpreis.

- Kurzmessverfahren

  Die Erarbeitung von Kurzmessverfahren und Manipulationsprüfverfahren erlaubt, auch nach Wartung, Reparatur oder möglichen unberechtigten Zugriffen die Abstrahlsicherheit mit geringem Aufwand sicherzustellen.

- Einsatz abstrahlarmer bzw. abstrahlgeschützter Geräte

  Hersteller von PC-Bildschirmen werben häufig mit dem Begriff "abstrahlarm" nach MPR II, TCO oder SSI. Diese Richtlinien berücksichtigen jedoch ausschließlich mögliche gesundheitsschädliche Auswirkungen der Gerätestrahlung. Die Messverfahren und Grenzwerte für die Strahlung sind daher für den Nachweis bloßstellender Abstrahlung ungeeignet und ermöglichen wie auch Messungen zur elektromagnetischen Verträglichkeit (EMV) keine Bewertung der Sicherheit gegen unberechtigtes Mitlesen der Daten.

  Daneben werden aber auch speziell abstrahlgeschützte IT-Systeme angeboten. Ein detailliertes Prüfkonzept des BSI dient zur abgestuften Prüfung von IT-Geräten bzw. -Systemen. Grundgedanke dieses Konzeptes ist es, den Umfang der Schutzmaßnahmen so gut wie möglich an die vom Anwender angenommene Bedrohungslage anzupassen, um so bei minimiertem Kostenaufwand ein Optimum an Abstrahlsicherheit zu erzielen. Ursprünglich wurde das Prüfkonzept des BSI zum Schutz staatlicher Verschlusssachen entwickelt, der Einsatz kann aber auch in der Privatwirtschaft sinnvoll sein, wenn Daten mit hohem Schutzbedarf bezüglich Vertraulichkeit geschützt werden sollen. So kann z. B. in vielen Fällen ein nach dem Zonenmodell geprüftes und für den Einsatz in den Zonen 1-3 zugelassenes Gerät (sog. "Zone 1-Gerät") bereits einen hinreichenden Schutz gegen unberechtigtes Abhören vertraulicher Daten infolge bloßstellender Abstrahlung bieten. Ein Einsatz von kostengünstigen Zone 1-Geräten wird daher vom BSI bei dem genannten Schutzbedarf empfohlen.

  Ob ein Hersteller abstrahlgeschützte Geräte gemäß dieser sog. "TEMPEST"-Kriterien in seinem Lieferprogramm anbietet, sollte durch eine Rückfrage beim Hersteller, beim BSI bzw. durch Einsicht in die offi-

zielle Produktübersicht BSI 7206, welche auf der Internetseite des BSI unter dem Stichwort *Publikationen* verfügbar ist, geklärt werden. Dabei gehört zu der Aussage, dass für ein Gerät eine TEMPEST-Zulassung vorliegt, immer auch die Aussage des Zulassungsgrades (z. B. zugelassen für den Einsatz in den Zonen 1-3 gemäß Zonenmodell).

Weitere Informationen erhalten Sie unter:

Tel.: +49 (0) 1888 9582-5637

E-Mail: Referat222@bsi.bund.de

M 4.90 Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Das OSI-Referenzmodell nach ISO

Kryptographische Verfahren können auf den verschiedenen Schichten des ISO/OSI-Referenzmodells implementiert werden. Dieses Modell, welches in Maßnahme M 5.13 *Geeigneter Einsatz von Elementen zur Netzkopplung* dieses Handbuchs kurz erläutert wird, definiert vier transportorientierte Schichten und drei anwendungsorientierte Schichten. Instanzen einer Schicht in verschiedenen Systemen kommunizieren über Protokolle miteinander. Jede Schicht bietet der nächst höheren Schicht ihre Dienste an. Das kann neben den üblichen Kommunikationsdiensten auch ein Sicherheitsdienst sein. Welcher Sicherheitsdienst in welcher Schicht des Schichtenmodells plaziert werden sollte und welche Mechanismen dazu genutzt werden können, ist im Teil 2 der ISO 7498 (Security Architecture) beschrieben.

Auch wenn konkrete Kommunikationssysteme, Referenzmodelle oder Protokolle sich nicht immer konform zum ISO-Referenzmodell verhalten, so hilft die Kenntnis des ISO-Referenzmodells bei der Beurteilung von Sicherheitsfunktionen von Produkten und erleichtert damit auch die systematische Erstellung "sicherer" Gesamtsysteme.

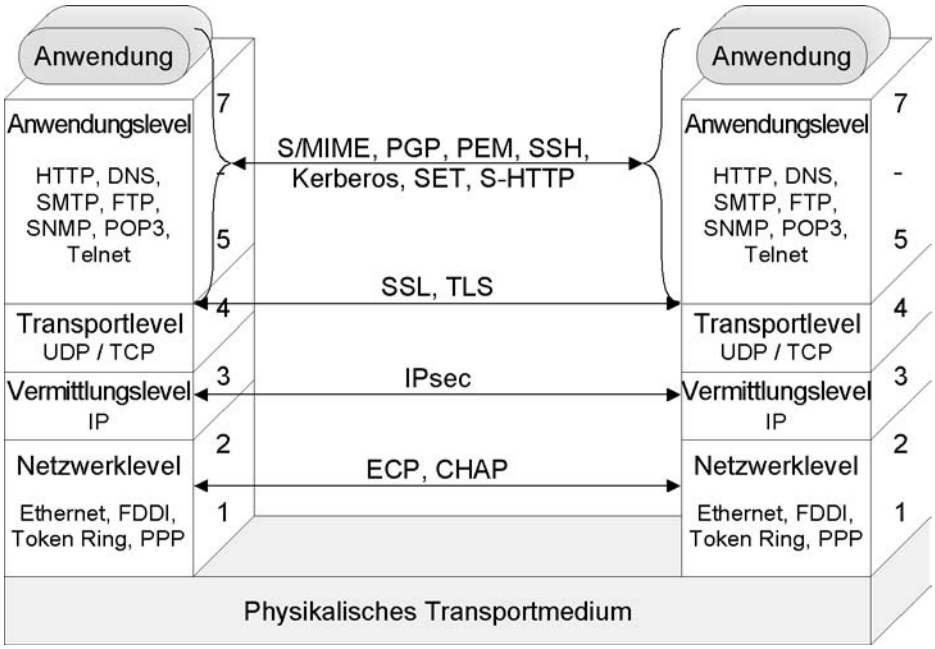


Abbildung: Beurteilung von Sicherheitsfunktionen von Produkten mit Hilfe der Kenntnis des ISO-Referenzmodells

Im folgenden soll erläutert werden, welche Vor- bzw. Nachteile mit dem Einsatz von kryptographischen Verfahren auf den jeweiligen Schichten verbunden sind.

Kryptographische Verfahren werden zur Sicherung verschiedener bei der Kommunikation anfallender Informationen eingesetzt, also um Informationen zu verschlüsseln, mit kryptographischen Prüfsummen zu versehen oder zu signieren. Zum einen können die vom Benutzer zu übermittelnden Daten gesichert werden, zum anderen aber auch Informationen, die sich beim Informationsaustausch implizit ergeben (z. B. Verkehrsflussinformationen).

Sicherheitsbeziehungen können für verschiedene Sicherheitsdienste in verschiedenen OSI-Schichten gleichzeitig existieren. Oberhalb der Schicht, in der ein Sicherheitsdienst realisiert ist, liegen die Informationen (bezüglich dieses Dienstes) ungesichert vor. Kryptographische Mechanismen (Verschlüsselung, digitale Signatur, kryptographische Prüfsummen) liefern Beiträge zur Realisierung wichtiger Sicherheitsdienste (Authentizität, Vertraulichkeit, Integrität, Kommunikations- und Datenursprungsnachweise).

Hierzu wird zunächst ein Überblick über die Gesichtspunkte gegeben, die für oder gegen den Einsatz von kryptographischen Verfahren auf den verschiedenen OSI-Schichten sprechen:

Verwendung von kryptographischen Verfahren auf			
oberen Schichten:		**unteren Schichten:**	
+:	sinnvoll, wenn die Anwendungsdaten nahe der Anwendung geschützt werden sollen bzw. der "unsichere Kanal" möglichst kurz gehalten werden soll	+:	sinnvoll für die Kopplung zweier Netze, die als sicher gelten, über eine unsichere Verbindung, z. B. Kopplung zweier Liegenschaften über öffentliche Netze
+:	auf jeden Fall immer dann, wenn die Daten nicht auf den tieferen Schichten geschützt werden	+:	zur Sicherung eines Netzes gegen unbefugte Zugriffe
+:	sinnvoll bei vielen, wechselnden Kommunikationspartnern an verschiedenen Standorten	+:	immer dann, wenn Verkehrsflussinformationen geschützt werden sollen, z. B. Adressinformationen
+:	Benutzer können sie nach eigenen Anforderungen einsetzen	+:	alle höherliegenden Header- und die Benutzerinformationen sind verschlüsselt
+:	Absicherung näher am Benutzer und für diesen erkennbarer	+:	transparent für Benutzer, geringeres Fehlbedienungsrisiko
-:	höhlen Absicherung durch Firewalls aus	+:	einfacheres Schlüsselmanagement
-:	werden häufig fehlbedient	-:	Schutz nur bis in die Schicht, in der die Sicherheitsprotokolle realisiert sind
-:	basiert häufig auf Software, kryptographische Schlüssel und Algorithmen sind einfacher manipulierbar	-:	häufig Hardware, also teuer und unflexibel
-:	höhere Abhängigkeit vom Betriebssystem bzw. darunter liegender Hardware	-:	bietet häufig keine Ende-zu-Ende Sicherheit

Tabelle: Verwendung von kryptographischen Verfahren auf die OSI-Schichten

Ein einfaches Schlüsselmanagement ergibt sich i.d.R. dann, wenn Gruppenschlüssel verwendet werden können, z. B. beim Aufbau von sicheren Teilnetzen (VPNs), bei denen die Zugänge mit Kryptogeräten versehen werden.

Kryptographische Produkte für die unteren Schichten liegen im Anschaffungspreis meist deutlich über solchen für obere Schichten, dafür werden allerdings auch weniger benötigt. Außerdem ist der Administrations- und Implementierungsaufwand meist niedriger, da Sicherheitsdienste nicht in verschiedensten Anwendungen implementiert werden müssen. Auch "exotische" Anwendungen - ohne eigene Sicherheitsfunktionalität - können dadurch gesichert Daten austauschen.

In vielen Fällen bietet sich auch eine Kombination von kryptographischen Diensten auf verschiedenen Schichten an. Dies hängt von den jeweiligen Sicherheitsanforderungen und den Einsatzbedingungen ab, wie Kosten, Performance und inwieweit entsprechende Komponenten erhältlich sind. Entscheidende Faktoren sind auch die angenommenen Gefährdungen, gegen die die implementierten Sicherheitsdienste wirken sollen, sowie die zugrunde liegende Systemarchitektur.

Sicherheits-Endgeräte <-> Sicherheits-Koppelelemente

Sicherheitssysteme können als Endgerät bzw. Teil eines Endgeräts oder als Koppelelement bzw. Teil eines Koppelelements ausgelegt sein. Koppelelemente sind z. B. aktive Netzkomponenten wie Router oder Gateways.

Im Unterschied zu Endgeräten weisen Sicherheits-Koppelelemente gewöhnlich zwei Netzschnittstellen auf, die auf einer für dieses System typischen Schicht über ein Kryptomodul (Hard- oder Software) gekoppelt sind. Eine Schnittstelle ist mit dem "sicheren" Netz verbunden (z. B. Hausnetz), die andere Schnittstelle mit einem als "unsicher" bewerteten Netz (z. B. öffentliche Netze).

Sicherheits-Endgeräte haben den Vorteil, dass die Sicherheitsmechanismen gut an die Anforderungen der Anwendung angepasst werden können. Typische SicherheitsEndgeräte sind Kryptotelefone, Kryptofaxgeräte oder hard-/softwarebasierte Sicherheitslösungen für PCs. Sicherheits-Endgeräte bieten i.d.R. Lösungen für einzelne Arbeitsplätze. Teilweise unterstützen diese Lösungen lediglich einen Dienst. Die Grenzen sind hier jedoch fließend (Telefonie über Internet-PC, Kryptotelefon mit Dateneingang). In Endgeräten ist im Gegensatz zum Koppelelement die Wahl der Sicherheitsschicht nicht eingeschränkt, da Endgeräte grundsätzlich vollständig sind, also über 7 Schichten verfügen.

Sicherheits-Koppelelemente sind häufig derart leistungsfähig konstruiert, dass sie größere Arbeitseinheiten bis hin zu ganzen Liegenschaften absichern können. Dabei versuchen die Hersteller solcher Systeme möglichst viele Dienste bzw. übergeordnete Protokolle zu unterstützen, damit eine universelle Verwendung möglich ist. Auch die weitgehende Unabhängigkeit von den Betriebssystemen der Endgeräte liefert einen Beitrag zur universellen Einsatzbarkeit von Koppelelementen. Natürlich können auch einzelne Endgeräte

durch Sicherheits-Koppelelemente abgesichert werden. Jedoch führt die höhere Leistungsfähigkeit der Geräte häufig zu höheren Kosten. Bei Koppelelementen handelt es sich definitionsgemäß um unvollständige OSI-Systeme. Daher ist auch die Implementierung von Sicherheitsdiensten auf die Schichten beschränkt, die das Koppelelement aufweist.

Auch Mischformen sind im Einsatz. Das setzt voraus, dass Sicherheits-Endgeräte und Sicherheits-Koppelelemente aufeinander abgestimmt sind, insbesondere bezüglich der verwendeten Sicherheitsmechanismen und Sicherheitsparameter (z. B. kryptographische Schlüssel).

Nutzer-, Steuer- und Managementinformationen

Ein Anwender ist hauptsächlich an der Übermittlung von Nutzerinformationen an entfernte Anwender interessiert. Je nach konkretem Referenzmodell (z. B. ISDN) werden aber zwischen den Systemen (Endgeräte, Koppelelemente) zudem Steuer-, Signalisier- und Managementinformationen zwecks Aufbau/Abbau von Verbindungen, Aushandeln von Dienstgüteparametern, Konfiguration und Überwachung des Netzes durch Netzbetreiber, usw. übertragen.

Das jeweilige Netz hat dabei die Aufgabe, Benutzerinformationen unverändert und unausgewertet zu übertragen, d. h. Benutzerinformationen müssen nur von den Endgeräten interpretiert werden können. Damit lassen sich diese Informationen unabhängig von der übrigen Netzinfrastruktur sichern, notfalls sogar unter Verwendung proprietärer Sicherheitsfunktionen (geschlossene Benutzergruppe). Steuer-, Signalisier- und Managementinformationen der Transportschichten müssen von Netzelementen des Netzbetreibers ausgewertet, geändert oder erzeugt werden können. Damit entziehen sich diese Informationen einer vom Netzbetreiber unabhängigen Sicherung (z. B. Verschlüsselung) weitgehend. Die Sicherung dieser Informationen erfordert neben entsprechenden Standards die vertrauensvolle Zusammenarbeit mit dem Netzbetreiber. Bedrohungen können sich dadurch ergeben, dass Sicherheitsfunktionen von Produkten falsch eingeschätzt werden. Bei der Auswahl von Kryptogeräten ist genau zu prüfen, welche Informationsanteile gesichert oder gefiltert werden. Ebenso ist im Umkehrschluss zu überprüfen, welche Informationen trotz des Einsatzes von Kryptogeräten ungesichert bleiben und in wieweit dies zu tolerieren ist.

Beispiel: Beim ISDN erfolgt die Übertragung der Benutzerinformationen in der Regel über die B-Kanäle. Aber auch der D-Kanal, welcher primär für die Signalisierung genutzt wird, kann zur Übertragung paketierter Daten verwendet werden. Ist das Ziel die Sicherung aller Benutzerdaten, so reicht im Fall der Übertragung von paketierten Daten über den D-Kanal die Absicherung der B-Kanäle offensichtlich nicht aus.

Sicherheit in leitungsvermittelten Netzen

Bei leitungsvermittelten Netzen werden durch den Verbindungsaufbau Kanäle definierter Bandbreite eingerichtet, die den Kommunikationspartnern exklusiv zur Verfügung stehen. Nach Einrichten der Verbindung erfolgt die Übertragung der Nutzdaten, anschließend der Verbindungsabbau. Der Netzbetreiber kann Festverbindungen einrichten, bei denen dann der durch den Teil-

nehmer gewöhnlich durchzuführende Verbindungsauf- und -abbau entfällt. Ein Beispiel für ein leitungsvermitteltes Netz ist ISDN.

Durch den Verbindungsaufbau werden Nutzdatenkanäle auf OSI-Schicht 1 zwischen den Kommunikationspartnern eingerichtet, die beim ISDN B-Kanäle heißen. Um die Vertraulichkeit der übertragenen Nutzdaten zu gewährleisten, kann dieser Kanal verschlüsselt werden. Soll darüber hinaus der Signalisierungskanal abgesichert werden, bei N-ISDN also der D-Kanal (Schicht 1-3), so muss bedacht werden, dass als Gegenstellen eines Endgeräts sowohl das Endgerät des Kommunikationspartners als auch Vermittlungsstellen des Netzbetreibers auftreten können. Der D-Kanal wird normalerweise nicht verschlüsselt, da hierzu besondere Anforderungen an den Netzbetreiber zu stellen wären. In diesem Fall sollte man die Überwachung und Filterung des D-Kanals vorsehen (siehe auch M 4.62 *Einsatz eines D-Kanal-Filters*).

Leitungsverschlüssler: Als Sonderfall muss die Verschlüsselung synchroner vollduplex Festverbindungen gesehen werden, da in diesem Fall die Vertraulichkeit - auch des Verkehrsflusses - gewährleistet werden kann. Stehen keine Daten zur Übertragung an, werden Fülldaten verschlüsselt, sodass auf der Leitung immer ein kontinuierliches "Rauschen" zu sehen ist. Der Leitungsverschlüssler stellt eine Alternative zur Verlegung geschützter Leitungen dar.

Sicherheit in paketvermittelten Netzen

Bei paketvermittelten Netzen ist zwischen verbindungsorientierter und verbindungsloser Paketvermittlung zu unterscheiden. Bei der verbindungsorientierten Paketvermittlung wird während der Verbindungsaufbauphase eine virtuelle Verbindung eingerichtet, wodurch der Datenpfad durch das Paketnetz im Anschluss festgelegt ist. Datenpakete werden nach dem Verbindungsaufbau auf Basis der zugeordneten virtuellen Kanalnummer auf dem selben Pfad durch das Netz geroutet. Sende- und/oder Empfängeradressen sind hierzu nicht mehr erforderlich. Ein Beispiel hierfür ist das X.25-Netz.

Bei verbindungsloser Paketvermittlung gibt es keine Verbindungsauf und -abbauphasen. Datenpakete werden - unter anderem ausgestattet mit Quell- und Zieladresse - einzeln vermittelt. Dies ist typisch für LAN-Datenverkehr.

Die Wahl der Schicht, in der die Sicherheitsmechanismen wirken, bestimmt, welche Informationsanteile gesichert werden. Je niedriger die gewählte Sicherheitsschicht, desto umfangreicher die Informationssicherung. Beim Durchlauf der Benutzerdaten durch die Instanzen der Schichten 7 bis 1 (Sender) werden den Daten zusätzliche Steuerinformationen hinzufügt. Geht es also nicht nur um die Sicherung von Benutzerdaten, sondern auch um die Sicherung des Verkehrsflusses, so bietet sich die Wahl einer niedrigen OSI-Schicht an. Andererseits gilt: je niedriger die gewählte OSI-Schicht, desto weniger Koppelelemente (Repeater, Bridge, Switch, Router, Gateway) lassen sich transparent überwinden.

Koppelelement	höchste Schicht des Koppelelements
Repeater	1
Bridge, Layer-2-Switch	2
Router, Layer-3-Switch, X.25-Packet Handler	3
Gateway	7

Tabelle: Gegenüberstellung: Koppelelement - ISO-Schicht

Sollen Sicherheitsdienste über Koppelelemente hinweg wirken, dann sind sie in einer Schicht zu implementieren, die oberhalb der höchsten (Teil-) Schicht der Koppelelemente liegt. Dadurch wird sichergestellt, dass die Übermittlungseinrichtungen die gesicherten Informationen unverarbeitet/ uninterpretiert weiterleiten können.

Beispiele und Folgen fehlerhafter Netzkonfigurationen:

Beispiel 1: Sämtliche Endgeräte zweier über Router und öffentliche Kommunikationsnetze gekoppelter LANs sollen zur Gewährleistung der Vertraulichkeit - insbesondere im Bereich öffentlicher Kommunikationsnetze - mit Schicht-2-Verschlüsselungskomponenten ausgestattet werden. Der Router muss zur Weiterleitung der LAN-Datenpakete über das öffentliche Netz die Adressen der Schicht 3 auswerten. Da sämtliche Schicht-3-Daten jedoch durch die Schicht-2-Verschlüsselung verborgen sind, kann die Auswertung der Schicht-3-Adressen nicht erfolgreich durchgeführt werden. Dadurch wird die Datenübertragung verhindert. Zur Abhilfe müssen hier die Verschlüsselungskomponenten für Schicht 3 (obere Teilschicht) oder höher eingesetzt werden.

Beispiel 2: Ein Großteil des Schriftverkehrs einer Institution soll zukünftig elektronisch über X.400 (Schicht 7) abgewickelt werden. Zur Sicherung der Datenintegrität plant die Institution den Einsatz von Schicht-4-Kryptokomponenten in den Endgeräten (hier PCs). Zum Zweck der Sicherung werden die Datenpakete beim Sender auf Schicht 4 mit kryptographischen Prüfsummen versehen, welche von der zugehörigen Schicht-4-Kryptokomponente des Empfängers geprüft wird. Nur Datenpakete mit korrekten Prüfsummen sollen zugestellt werden. Falls aber nicht alle MTAs (Message Transfer Agents, also die Vermittler für elektronische Mitteilungen auf Schicht 7) ebenfalls mit interoperablen Kryptokomponenten ausgestattet sind, können die MTAs ohne Kryptokomponente keine gültigen Prüfsummen erzeugen, so dass nachfolgende MTAs oder Endgeräte mit Kryptokomponente die Daten laut Vorgabe verwerfen müssen.

Aber selbst wenn sämtliche genutzten MTAs ebenso wie die Endgeräte mit interoperablen Kryptokomponenten und Sicherheitsparametern ausgestattet sind, ist die Datenintegrität nicht sichergestellt. Dann kann die abschnittsweise Sicherung der Daten zwar gewährleistet sein, eine Verfälschung der Daten innerhalb der MTAs ist jedoch unbemerkt möglich. Ferner könnten (je nach Protokoll) einzelne Schicht-4-Datenpakete verloren gehen, was zu Lücken in der Gesamtnachricht führt, deren Unversehrtheit eigentlich gesichert werden sollte. Eine Abhilfe ist hier die Integritätssicherung der Daten auf Schicht 7.

Wie die Beispiele zeigen, ist genau zu untersuchen, welche Netztopologie vorliegt und welche Netzbereiche wie gesichert werden müssen, damit eine angepasste Lösung mit den gewünschten (Sicherheits-)Merkmalen gefunden werden kann.

Abschnittsweise Sicherheit <-> Ende-zu-Ende-Sicherheit

Benutzer von Kommunikationssystemen erwarten häufig, dass Sicherheitsdienste durchgängig erbracht werden (Ende-zu-Ende-Sicherheit), also von der Eingabe der Information (Daten, Sprache, Bilder, Text) am Endgerät A bis zur Ausgabe der Information an einem entfernten Endgerät B. Ist kein durchgehender Sicherheitsdienst gewährleistet, so existieren - abgesehen von den beteiligten Endgeräten - weitere Systeme, auf denen die Informationen ungesichert vorliegen. Existiert beispielsweise keine Ende-zu-Ende-Verschlüsselung zur Sicherung der Vertraulichkeit einer Kommunikationsbeziehung zwischen zwei Teilnehmern, so liegen die Daten in mindestens einem weiteren Netzelement unverschlüsselt vor. Solche Netzelemente müssen lokalisiert und durch zusätzliche Maßnahmen abgesichert werden. Personal, welches Zugriff auf insbesondere solche ungesicherten Netzelemente hat (z. B. Administrator), muss entsprechend vertrauenswürdig sein. Sicherheitsdienste werden in diesem Fall nicht durchgängig, sondern abschnittsweise erbracht. Auf die angemessene Sicherung aller relevanten Abschnitte ist zu achten.

Mehrfache Sicherung auf verschiedenen OSI-Schichten

Gegen eine Mehrfachsicherung der zu übertragenden Informationen auf verschiedenen OSI-Schichten ist nichts einzuwenden, wenn gewisse Regeln befolgt werden, die bei standardkonformen Produkten jedoch implizit gewährleistet sind. Insbesondere bei der Verschlüsselung sind die aus der Schule bekannten Klammerregeln anzuwenden. So entspricht das Verschlüsseln dem Öffnen einer Klammer, das Entschlüsseln dem Schließen einer Klammer. Innerhalb der Klammer können nun wiederum weitere Sicherheitsmechanismen zur Anwendung kommen.

Nachteilig kann sich die Mehrfachsicherung dadurch auswirken, dass der Datendurchsatz aufgrund zusätzlicher Operationen reduziert wird oder dass sich die übertragbare Nutzdatenmenge dadurch vermindert, dass zusätzliche Daten zur Erhöhung der Redundanz (z. B. kryptographische Prüfsummen) übertragen werden müssen. Auch durch Daten, die vor der Übermittlung über Kryptosysteme gesichert werden, z. B. digital signierte Dokumente, ergibt sich implizit eine Mehrfachsicherung. Dadurch erhöht sich die Sicherheit der Datenübertragung hinsichtlich der verwendeten Sicherheitsdienste.

Oft lässt sich die Sicherheit des Gesamtsystems erst durch die Kombination mehrerer Sicherheitsprotokolle oder Sicherheitsprodukte erreichen. Sind z. B. anwendungsnahe Sicherheitslösungen verfügbar, deren vertrauenswürdige Implementierung jedoch nicht (von unabhängiger Seite) überprüft wurde (z. B. Evaluierung nach ITSEC, CC) und existieren gleichzeitig vertrauenswürdige transportorientierte Sicherheitsprodukte zur Absicherung unsicherer Netzabschnitte zwischen entfernten Liegenschaften, so kann durch die Kombination der Maßnahmen u. U. eine den Anforderungen genügende Gesamt-Sicherheitslösung geschaffen werden. Nachteilig wirken sich dabei meist der erhöhte Administrationsaufwand und/oder erhöhte Anschaffungskosten aus.

M 4.91 Sichere Installation eines Systemmanagement-systems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Installation eines Systemmanagementsystems erfordert eine umfangreiche und sorgfältige Planung. Nach erfolgter Systemanalyse (siehe M 2.168 *IT-System-Analyse vor Einführung eines Systemmanagementsystems*), Festlegung der Managementstrategie (siehe M 2.169 *Entwickeln einer Systemmanagementstrategie*) und Auswahl eines geeigneten Managementsystems (siehe M 2.171 *Geeignete Auswahl eines Systemmanagement-Produktes*) muss die Installation des Produktes detailliert geplant und entsprechend umgesetzt werden. In Abhängigkeit von der dem Management-Produkt zugrunde liegenden Architektur ist für das lokale Netz die konkrete Managementsystemkonfiguration zu erstellen, die insbesondere der formulierten Managementstrategie Rechnung trägt.

Zur Installation der meisten Managementsysteme muss auf den beteiligten Rechnern Managementsoftware installiert werden, die die Kommunikation zwischen Managementkonsole oder -servern und dem lokalen Rechner übernimmt. Oft müssen auf den zentralen Rechnern (Server oder Gateways) auch Datenbanksysteme installiert werden, in denen die Managementinformationen von der Managementsoftware persistent abgelegt werden. Je nach Produkt ist hier auch die Einbindung eines schon vorhandenen Datenbanksystems möglich. Generell stellt die zusätzlich zu installierende Software Anforderungen an die lokalen Ressourcen des Rechners. Daher ist bei der Planung zu beachten, welche Systemressourcen lokal vorhanden sind. Unter Umständen müssen einzelne Systeme aufgerüstet werden. Diese Kosten sollten bei der Auswahl des Management-Produktes berücksichtigt werden.

Neben diesen Kriterien, die im wesentlichen den geregelten technischen Ablauf des Systems garantieren sollen, ist aus Sicherheitsgesichtspunkten die dem Managementsystem zugehörige Software und die entsprechenden Daten in die Schutzbedarfsfeststellung gemäß IT-Grundschutz (siehe BSI-Standard 100-2 *IT-Grundschutz-Vorgehensweise*) aufzunehmen und der Schutzbedarf als "hoch" bis "sehr hoch" einzustufen. Die Kompromittierung des Managementsystems kann nicht nur den Ausfall des gesamten Netzes nach sich ziehen; durch unbemerkte Veränderungen am System kann vielmehr beträchtlicher Schaden entstehen, der sehr schnell existenzbedrohende Formen annehmen kann.

Insbesondere ist bei der Installation auf folgende Punkte zu achten:

- Alle Rechner, auf denen Managementinformationen gelagert werden, sind besonders zu sichern:
  - Es sind die Maßnahmen der Bausteine aus Schicht 3, je nach vorliegendem System, durchzuführen.
  - Insbesondere sind die Betriebssystemmechanismen so zu konfigurieren, dass auf die lokal gespeicherten Managementinformationen nicht unberechtigt zugegriffen werden kann.

  - Der Zugang zur Managementsoftware ist nur den berechtigten Administratoren und Revisoren zu gestatten.
  - Der Zutritt zu den Rechnern sollte beschränkt werden.
- Die Kommunikation zwischen den Managementkomponenten sollte verschlüsselt erfolgen - sofern dies vom Produkt unterstützt wird - um zu verhindern, dass Managementinformationen mitgehört und gesammelt werden können. Unterstützt das Produkt keine Verschlüsselung, so sind gesonderte Maßnahmen zu ergreifen, um die Kommunikation abzusichern (siehe M 5.68 *Einsatz von Verschlüsselungsverfahren zur Netzkommunikation*).

Ergänzende Kontrollfrage:

- Sind die Systemmanagementsysteme sicher installiert worden?

M 4.92 Sicherer Betrieb eines Systemmanagementsystems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Für den sicheren Betrieb eines Systemmanagementsystems, welches auch aus verschiedenen Management-Tools (siehe M 2.171 *Geeignete Auswahl eines Systemmanagement-Produktes*) bestehen kann, ist die sichere Konfiguration aller beteiligten Komponenten zu prüfen und sicherzustellen (siehe auch M 4.91 *Sichere Installation eines Systemmanagementsystems*). Hierzu ist es nötig, die jeweiligen Betriebssysteme der Komponenten, die durch das Systemmanagementsystem verwaltet werden und damit Teile des Systems in Form von Software und/oder Daten installiert haben, entsprechend zu sichern. Zur Absicherung gehört dabei auch die sichere Aufstellung der Rechner, die zentrale Aufgaben für das Managementsystem erfüllen (Managementserver, Rechner mit Managementdatenbanken). Daneben muss für die sichere Datenübertragung Sorge getragen werden (siehe M 5.68 *Einsatz von Verschlüsselungsverfahren zur Netzkommunikation*).

Auf die folgenden Punkte ist insbesondere während des laufenden Betriebs eines Managementsystems zu achten:

- Im Rahmen der Fortschreibung der Systemdokumentation müssen die durch das Managementsystem neu hinzugekommenen Hard- und Softwarekomponenten dokumentiert werden.
- Auch Änderungen am Managementsystem selbst müssen dokumentiert und/oder protokolliert werden.
- Die Fortschreibung gilt in gleicher Weise für das Notfallhandbuch. Insbesondere sind einerseits die Anlauf- und Recovery-Pläne zu modifizieren, da viele Standardfunktionen der verwalteten Betriebssysteme nach Einführung eines Managementsystems nun nur noch mit Hilfe der Funktionen des Managementsystems erfolgen können. Andererseits muss das Notfallhandbuch aber auch Anweisungen dafür enthalten, wie das System ohne Managementsystem (etwa bei Totalausfall zentraler Komponenten) innerhalb kurzer Zeit in hinreichendem Maße (Notbetriebsregelung) verfügbar gemacht werden kann (siehe auch Baustein B 1.3 *Notfallvorsorge-Konzept*).
- Ein Zugriff auf die Komponenten oder Daten des Managementsystems erfolgt in der Regel ausschließlich durch das Managementsystem selbst oder berechtigte andere Systemmechanismen (z. B. Datensicherungssystem). Daher ist der Zugriff für normale Benutzer zu unterbinden. Dies gilt im Normalfall auch für die Rolle des lokalen Administrators eines einzelnen Rechners. Muss in Ausnahmefällen tatsächlich direkt auf einem Rechner auf die lokalen Komponenten des Managementsystems zugegriffen werden (z. B. bei Crashrecovery oder Neuinstallation von Komponenten, sofern das Managementsystem dies nicht im Rahmen des Managements unterstützt), so sollte diese Berechtigung explizit und nur für die Durchführung dieser Aufgabe erteilt werden.

- Im Rahmen der Sicherheitspolitik müssen die Befugnisse festlegt sein. Auch für den Bereich Management ergibt sich eine Rollentrennung Administrator und Revisor - je nach Produkt auch zwischen Administratoren mit unterschiedlichen Rechten (z. B. Arbeitsgruppenadministrator, Bereichsadministrator). Es empfiehlt sich, bestimmte Rollen zu definieren und gemäß diesen verschiedenen Rollen Benutzer mit entsprechenden Berechtigungen einzurichten. Dadurch werden dem Zugreifenden lediglich die Rechte auf Komponenten oder Daten des Managementsystems erlaubt, die für seine momentane Aufgabe nötig sind. Je nach Managementsystem geschieht die Einrichtung der Benutzer im Managementsystem oder in der Benutzerverwaltung der Rechner. Da die existierenden Systeme nicht direkt die Definition unterschiedlicher Rollen (etwa Administrator und Revisor) vorsehen, müssen die Rollen bestmöglich durch das Einrichten unterschiedlicher Benutzerkonten (z. B. "Administrator", "Revisor", "RechnerAdmin", "Datenschutzbeauftragter") mit entsprechenden Berechtigungen nachgebildet werden. Je nach System ist diese Nachbildung der Rollen nur unvollständig und mit einigem Aufwand möglich, da u. U. für jede Systemkomponente (Dateien, Programme) die Berechtigungen für die einzelnen Rollen explizit vergeben und gewartet werden müssen.
- Der Zugang zur Managementsoftware ist durch sichere Passwörter zu schützen. Die Passwörter sollten gemäß Sicherheitspolitik regelmäßig geändert werden.
- Funktionen der Managementsoftware, die gemäß Managementstrategie nicht zum Einsatz kommen sollen, sind - wenn möglich - zu sperren.
- Die Protokollierungsdateien sind in regelmäßigen Abständen auf Anomalien (z. B. Ausführung von Funktionen, die nicht zum Einsatz kommen sollen) zu untersuchen. Hier empfiehlt sich der Einsatz von Protokoll-Analysatoren, die entweder in das Managementprodukt integriert oder auch als Zusatzsoftware erhältlich sein können und die (meist) regelgesteuert im Bedarfsfall Alarmmeldungen (z. B. Mail, Pager) erzeugen können.
- Das Managementsystem ist in Abständen Integritätstests zu unterziehen, so dass unberechtigte Änderungen so früh wie möglich entdeckt werden können. Dies gilt insbesondere für sämtliche Konfigurationsdaten des Managementsystems.
- Wird über das Systemmanagementsystem auch Software verteilt, so sind auch die zu verteilenden Programmdaten regelmäßig auf Veränderungen zu überprüfen, um das Verteilen modifizierter Software über das gesamte Netz zu verhindern.
- Das Managementsystem sollte auf sein Verhalten bei einem Systemabsturz getestet werden. Je nach Management- und Sicherheitspolitik muss ein automatischer Neustart des Managementsystems oder lokaler Teilkomponenten des Systems sichergestellt werden. Damit wird verhindert, dass Rechner, die dem Managementsystem angeschlossen sind, längere Zeit nicht für das Management zugreifbar sind (siehe auch M 6.57 *Erstellen eines Notfallplans für den Ausfall des Managementsystems*).

- Beim Systemabsturz dürfen die Managementdatenbanken nicht zerstört werden oder in einen inkonsistenten Zustand gelangen, damit vermieden wird, dass ein möglicher Angreifer provozierte Inkonsistenzen zum Angriff nutzen kann. Dazu muss das Managementsystem entweder auf ein Datenbanksystem zurückgreifen, das entsprechende Recovery-Mechanismen unterstützt, oder diese Mechanismen selbst implementieren (siehe M 2.170 *Anforderungen an ein Systemmanagementsystem*). Werden diese Mechanismen von dem gewählten System nicht zur Verfügung gestellt (z. B. beim Einsatz von mehreren Management-Tools), sollten die Rechner, die Managementinformationen speichern, maximal möglich (auch physikalisch) gesichert werden (siehe die Bausteine der Schicht 3).
- Das Managementsystem sollte einen geeigneten Backup-Mechanismus zur Sicherung der Managementdaten enthalten oder mit einem Backup-System zusammenarbeiten. Beim Einspielen alter Datenbestände aus einer Datensicherung ist darauf zu achten, dass diese in der Regel manuell nachbearbeitet werden müssen, um der aktuellen Systemkonfiguration zu entsprechen.
- Auch mittels Backup-Verfahren gesicherte Managementdatenbestände sind so zu lagern, dass kein unberechtigter Dritter Zugriff darauf erlangen kann. In der Regel sind die Daten nicht in sicherer Form auf dem Backupdatenträger gespeichert, so dass sie von jedem, der über das Backup-Programme und ein entsprechendes Laufwerk verfügt, eingesehen werden können.
- Die Aufteilung in Managementdomänen und deren Zuständigkeiten sollte in regelmäßigen Abständen auf Gültigkeit hin untersucht werden. Dies gilt insbesondere für den Fall innerbetrieblicher Umstrukturierungen.

M 4.93 Regelmäßige Integritätsprüfung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Eine regelmäßige Kontrolle des Dateisystems auf unerwartete Veränderungen hilft dabei, Inkonsistenzen zu erkennen. Dadurch können auch Angriffe zeitnah entdeckt werden. Sollte tatsächlich ein Angriff vorliegen, ist es wichtig, das Vorgehen des Angreifers zu rekonstruieren. Dies dient einerseits dazu, sicherzustellen, dass die Benutzer nicht auf verfälschte Daten zurückgreifen, andererseits dazu, verborgene Hintertüren zu erkennen, die ein Angreifer für einen späteren Zugriff auf den Rechner installiert haben könnte.

Dazu können Programme genutzt werden, die kryptographische Prüfsummen über einen Großteil der Dateien des Dateisystems berechnen. Unter Unix bieten z. B. Programme wie *tripwire* oder *aide* diese Funktionalität. Vergleichbare Programme sind auch für alle anderen verbreiteten Betriebssysteme verfügbar, z.B. für Windows 2000 / Windows XP das Tool "File Checksum Integrity Verifier" (FCIV.EXE), das von Microsoft im Internet kostenlos zur Verfügung gestellt wird.

Tripwire und ähnliche Programme können jede Veränderung am Dateisystem feststellen, da die Prüfsummen bei einer Veränderung nicht mehr übereinstimmen. Dabei testen sie meist nicht nur, ob die Datei selbst modifiziert wurde, sondern auch eine Veränderung der Zugriffsrechte oder ein Löschen mit anschließendem Zurückspielen wird festgestellt. Mit einer speziellen Einstellung kann in vielen Fällen auch ein nur lesender Zugriff auf die Datei bemerkt werden.

Neben dem Dateisystem sollte es auch möglich sein, weitere wichtige Elemente der Systemkonfiguration (beispielsweise unter Windows die Registry) einer Integritätsprüfung zu unterziehen.

Um zu verhindern, dass das Programm oder die Prüfsummendatei von einem Angreifer verfälscht werden können, sollten sich diese auf einem Datenträger befinden, der wahlweise nur einen lesenden Zugriff gestattet. Allerdings muss die Prüfsummendatei bei Veränderungen am Dateisystem ebenfalls geändert werden, so dass sich bei kleinen Dateisystemen Disketten, bei größeren Wechselplatten empfehlen.

Eine Integritätsprüfung sollte regelmäßig, beispielsweise jede Nacht, durchgeführt werden. Eine Benachrichtigung über das Ergebnis sollte, auch wenn keine Veränderungen festgestellt wurden, automatisch per E-Mail an den Administrator erfolgen.

Ergänzende Kontrollfragen:

- Welche Integritätschecker werden eingesetzt?
- Wie häufig werden die Ergebnisse der Integritätschecker geprüft?
- Wie sind die Prüfsummendatei und das Programm selbst vor Manipulationen gesichert?

M 4.94 Schutz der WWW-Dateien

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Dateien und Verzeichnisse auf einem Webserver müssen gegen unbefugte Veränderungen, aber auch - je nach Sicherheitsanforderungen - gegen unbefugten lesenden Zugriff geschützt werden. Werden Inhalte auf dem Webserver dynamisch erzeugt, so gilt dies zusätzlich und ganz besonders für die Programme (Skripte oder Server-Erweiterungen), die dafür verwendet werden.

Generelle Aspekte

Generell muss zwischen zwei verschiedenen Aspekten unterschieden werden, nämlich dem Schutz vor unbefugtem Zugriff lokaler Benutzer und dem Schutz vor unbefugtem Zugriff von außen über das WWW.

Schutz vor unbefugten Veränderungen

Auf vielen Webservern ändern sich nur die Protokolldateien ständig, alle anderen Dateien sind statisch. Dies trifft insbesondere auf Systemprogramme und die WWW-Seiten zu. WWW-Seiten werden zwar regelmäßig aktualisiert, sollten aber nicht auf dem Webserver selber bearbeitet werden.

Die Schreib- und Leserechte der WWW-Dateien sollten als lokale Dateien nur berechtigten Benutzern Zugriff erlauben. Daher sollte bereits bei der Planung des Webangebots ein Benutzer- und Rollenkonzept erstellt werden (siehe auch M 2.173 *Festlegung einer WWW-Sicherheitsstrategie*).

Um sicherzustellen, dass keine Dateien auf dem Webserver unbemerkt abgeändert werden können, können über alle statischen Dateien und Verzeichnisse Prüfsummen gebildet werden, z. B. mit einem Programm wie *tripwire*, siehe auch M 4.93 *Regelmäßige Integritätsprüfung*. Diese sollten dann regelmäßig überprüft werden.

Um zu verhindern, dass WWW-Dateien überhaupt von Unbefugten geändert werden können, können statische Daten auf einem schreibgeschützten Speichermedium (z. B. CD-ROM oder Festplatte mit Schreibschutz) gespeichert werden.

Sichere Programmierung eigener serverseitiger Programme

Falls das Webangebot nicht nur aus statischen HTML-Dateien besteht, sondern bestimmte Inhalte dynamisch erzeugt werden, so müssen die dazu benutzten Programme (beispielsweise CGI-Skripte, Java Server Pages) besonders sorgfältig programmiert werden, um zu verhindern, dass auf diesem Weg ein unbefugter Zugriff oder gar eine Kompromittierung des Servers erfolgen kann.

Schutz von CGI-Skripten, Programmen und Konfigurationsdateien

Auf dem Server müssen solche Programme vor unbefugtem Zugriff geschützt werden. Nur die Benutzer oder Benutzergruppen, die unbedingt Zugriff auf diese Programme oder Skripte brauchen (etwa Entwickler oder Administratoren), dürfen eine Schreibberechtigung haben. Normalerweise dürfen die Programme nicht für den Benutzer schreibbar sein, unter dessen Kennung der Webserver-Prozess ausgeführt wird. Für normale Benutzer sollten insbesondere Skripte nicht lesbar sein, da diese eventuell sensitive Informationen wie Authentisierungsdaten für den Zugriff auf Datenbanken enthalten können. Gleiches gilt für eventuell vorhandene Konfigurationsdateien.

Schutz vor unbefugtem Zugriff über das Internet

Der Zugriff über das WWW auf Dateien oder Verzeichnisse eines Webservers kann auf verschiedene Arten gesteuert werden.

Welche Arten der Zugriffssteuerung unterstützt werden und wie diese implementiert sind hängt vom verwendeten Serverprodukt ab. Die folgenden Möglichkeiten sind verbreitet und werden von den meisten Webservern und Clients unterstützt.

Authentisierung von Clients über IP-Adressen

Der Zugriff auf WWW-Dateien kann bei vielen Servern auf frei wählbare IP-Adressen, Teilnetze oder Domänen beschränkt werden. Die Authentisierung über numerische IP-Adressen bietet nicht den Schutz kryptographischer Verfahren, da sie über einen auf IP-Spoofing basierenden Angriff unwirksam gemacht werden kann. Bei IP-Spoofing fälscht ein Angreifer IP-Pakete, um vorzugeben, von einem vertrauenswürdigen IT-System zu kommen (siehe G 5.48 *IP-Spoofing*). Über eine Firewall kann jedoch verhindert werden, dass Externe vortäuschen können, Interne zu sein. Wird der Zugriff nicht auf numerische IP-Adressen oder Teilnetze sondern auf bestimmte Rechnernamen oder Domainnamen beschränkt, ist außerdem die Gefährdung durch DNS-Spoofing (siehe G 5.78 *DNS-Spoofing*) zu betrachten.

Problem mit Proxy-Servern

Wenn der WWW-Browser über einen Proxy-Server auf den Webserver zugreift, ist zu bedenken, dass der Webserver nur die IP-Adresse des Proxy erfährt. Ein Proxy kann aber nur dann als vertrauenswürdig angesehen werden, wenn alle IT-Systeme und Benutzer, die hinter ihm verborgen sind, ebenfalls vertrauenswürdig sind.

Wenn der Zugriff auf WWW-Dateien auf vorgegebene IP-Adressen, Teilnetze oder Domänen beschränkt wird, kann es daher sinnvoll sein, diese zusätzlich mit einem Passwort zu schützen.

Passwortschutz

Eine weitere Möglichkeit der Zugriffssteuerung, die in praktisch allen Webservern implementiert ist, stellt der Schutz über Benutzernamen und Passwörter dar. Der Benutzer gibt beim erstmaligen Zugriff auf ein entsprechend geschütztes Verzeichnis in seinem Browser einen Benutzernamen und ein Passwort an, das zum Zugriff auf die entsprechende Ressource berechtigt. Über das Protokoll HTTP lässt sich ein Passwortschutz (Benutzer-Authentisierung) auf verschiedene Arten realisieren, die sich im Bezug auf Implementierungsaufwand und Sicherheit unterscheiden.

In Abhängigkeit von den Sicherheitsanforderungen muss eine geeignete Methode zur Benutzer-Authentisierung ausgewählt werden. Bei höheren Sicherheitsanforderungen sollte SSL zur Verschlüsselung der Datenübertragung und gegebenenfalls auch zur Benutzer-Authentisierung über Client-Zertifikate eingesetzt werden. Näheres ist in M 4.176 *Auswahl einer Authentisierungsmethode für Webangebote* beschrieben, Informationen zu SSL finden sich in M 5.66 *Verwendung von SSL*.

Dateiverschlüsselung

Eine weitere Möglichkeit zum Schutz von WWW-Dateien ist es, Dateien verschlüsselt auf einem Webserver abzulegen, so dass nur diejenigen die Daten lesen können, die im Besitz des richtigen kryptographischen Schlüssels sind. Dieses Vorgehen bietet zusätzlich den Schutz vor unbefugtem lokalem Zugriff, verlangt allerdings ein entsprechendes, unter Umständen aufwendiges, Schlüsselmanagement.

Ergänzende Kontrollfragen:

- Wie werden die WWW-Dateien gegen unbefugten lokalen Zugriff geschützt?
- Sind CGI-Skripte und Konfigurationsdateien besonders geschützt?

M 4.95 Minimales Betriebssystem

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Rechner in einem sicherheitskritischen Umfeld sollten so konzipiert sein, dass sie möglichst wenig Angriffspunkte bieten. Da heutige Betriebssysteme standardmäßig viele Netzdienste bereitstellen, reicht für den Betrieb eines sicheren Servers ein gut konzipierter Serverdienst (z. B. ein SSL-basierter Webserver) nicht aus. Vielmehr muss auch das Betriebssystem abgesichert werden, da ansonsten über eine Schwachstelle im Betriebssystem die Sicherheitsfunktionen des Serverdienstes umgangen werden könnten. Ein sogenanntes minimales Betriebssystem zeichnet sich dadurch aus, dass es im Idealfall keinen einzigen Netzdienst zur Verfügung stellt. Ein potentieller Angreifer kann also eine Schwachstelle in einem Netzdienst dieses Betriebssystems nicht ausnutzen. Und sollte ein Angreifer doch durch eine Schwachstelle Zugriff auf den Rechner bekommen haben, so wird er durch das Minimalsystem weiter behindert. Je weniger Programme ein Angreifer auf einem Zielrechner vorfindet, desto schwieriger wird es für ihn, weitere Schwachstellen in dem Zielrechner zu finden bzw. auszunutzen. Außerdem erleichtert dies die Pflege eines Servers sehr stark, da die Patches bzw. Service Packs für Diensteprogramme nicht mehr eingespielt werden müssen, wenn diese nicht vorhanden sind.

Im folgenden wird die Konfiguration eines Betriebssystems anhand eines Internet-Servers beschrieben, da hier im allgemeinen sehr hohe Sicherheitsanforderungen an das Betriebssystem gestellt werden müssen.

Ein Internet-Server hat meist nur eine einzige Aufgabe: stabil eine bestimmte Anzahl von Diensten (z. B. die Bereitschaft, E-Mail entgegenzunehmen) anderen Rechnern zur Verfügung zu stellen. Das zugrunde liegende Betriebssystem sollte keine weiteren Dienste anbieten. Deshalb sollte bei der Installation eines Internet-Servers folgendes Vorgehen eingehalten werden:

1. Grundinstallation des Betriebssystems

   Kann man bei der Installation den Umfang der zu installierenden Pakete beeinflussen, so sollten schon hier nur die notwendigen Pakete eingespielt werden. Die Notwendigkeit bestimmter Pakete ist allerdings nicht immer zu erkennen, so dass zumindest die offensichtlich überflüssigen Pakete nicht eingespielt werden sollten.

2. Abschalten nicht benötigter Programme

   Beim Start eines Rechners werden eine Vielzahl von Programmen automatisch gestartet. Einige dieser Programme sind für einen Internet-Server völlig überflüssig und sollten deaktiviert werden. Die Deaktivierung kann durch das Verhindern des automatischen Starts erfolgen (Startskripte unter Unix, Autostart und Dienstemanager unter Windows NT) und durch zusätzliches Löschen der entsprechenden Programme. Aus Gründen der Sicherheit wird das Löschen empfohlen, da dann ein Angreifer die Dienste nicht wieder reaktivieren kann. Allerdings

ist es manchmal sehr schwierig, alle zu einem bestimmten Dienst gehörigen Dateien zu finden und zu löschen, so dass im Zweifel das Löschen unterbleiben sollte.

3. Konfiguration der Netzparameter

   Falls dies nicht schon bei der Installation geschehen ist, müssen die Netzparameter des Internet-Servers eingestellt werden. Relevant für die Sicherheit des Internet-Servers sind unter anderem die Wahl eines *Default Gateways* und eines *Domain Name Servers*. Findet beispielsweise die Kommunikation des Internet-Servers mit dem Internet über einen Proxy (siehe M 2.73 *Auswahl geeigneter Grundstrukturen für Sicherheits-gateways*) statt, so ist ein *Default Gateway* überflüssig. Ohne ein *Default Gateway* ist eine direkte Antwort vom Internet-Server ins Internet nicht möglich, so dass bei Umgehung des Proxies keine Kommunikation, d. h. auch kein Angriff, stattfinden kann. Auch DNS ist für einen Internet-Server häufig überflüssig und sollte möglichst vermieden werden, da dies einen direkten Kommunikationskanal zum Betriebssystem ermöglicht (siehe M 4.96 *Abschaltung von DNS*). Zusätzlich gibt es noch eine Vielzahl von Parametern, die den sogenannten TCP/IP-Stack direkt beeinflussen, z. B. die maximale Größe von IP-Paketen. Diese Parameter sind extrem stark vom jeweiligen Betriebssystem abhängig, so dass hier nur das Abschalten von IP-Forwarding erwähnt werden kann. Weitere Änderungen könnten beispielsweise die Stabilität gegenüber fehlerhaften IP-Paketen oder aber auch den Netzdurchsatz erhöhen.

4. Abschalten nicht benötigter Netzdienste

   Einige benötigte Diensteprogramme stellen eine Vielzahl weiterer Dienste bereit (insbesondere ist hier der *inetd* unter Unix gemeint). Die entsprechenden Konfigurationsdateien sind auf die notwendigen Netzdienste einzuschränken (siehe auch M 5.16 *Übersicht über Netzdienste*).

5. Installation von Sicherheitsprogrammen

   Das Betriebssystem sollte um zusätzliche Sicherheitsprogramme erweitert werden, falls diese nicht schon Teil des Betriebssystems sind. Insbesondere sinnvoll sind ein Integritätsprüfprogramm (siehe M 4.93 *Regelmäßige Integritätsprüfung*) und ein Softwarepaketfilter (bei Windows NT schon enthalten). Empfehlenswert sind zusätzlich Programme zur Virensuche und zur Auswertung der Protokolleinträge. Ist eine Fernadministration des Internet-Servers gewünscht, so muss ein entsprechendes Sicherheits-produkt installiert werden, z. B. der Secure Shell Daemon (siehe M 5.64 *Secure Shell*), und regelmäßig die Sicherheit des Systems überprüft werden (siehe auch M 4.26 *Regelmäßiger Sicherheitscheck des Unix-Systems*).

6. Konfiguration und Überprüfung der Netzdienste

   Idealerweise stellt ein minimales Betriebssystem keinen einzigen Netzdienst zur Verfügung und ist somit von außen nicht angreifbar. Gerade in größeren Netzen ist dieses Vorgehen aufgrund der

Administration nicht mehr praktikabel, so dass ein Fernzugang notwendig ist. Ob der Internet-Server Dienste bereitstellt, kann sowohl unter Unix als auch Windows NT mit dem Befehl *netstat -a* überprüft werden. Jeder der aufgelisteten Dienste sollte in seiner Konfiguration so eingeschränkt werden, dass nur berechtigte Rechner auf ihn zugreifen können (z. B. ist der Fernzugang zum Internet-Server auf die Rechner des Netzmanagements einzuschränken).

7. Löschen nicht mehr benötigter Programme

   Sobald die Installation eines minimalen Betriebssystems abgeschlossen ist, sollten verschiedene Programme gelöscht werden, die einem potentiellen Angreifer hilfreich sein könnten. Insbesondere sind eventuell vorhandene Compiler zu entfernen, da diese einem Angreifer ein wertvolles Hilfsmittel sein könnten. Außerdem sind Compiler auf Internet-Servern auch deshalb nicht sinnvoll, da diese Rechner Produktionsmaschinen sind und Programmentwicklung und Tests auf anderen Rechnern durchgeführt werden sollten. Ebenfalls denkbar ist das Löschen aller Editoren, was einem Angreifer die Manipulation von Konfigurationsdateien sehr stark erschweren würde. Allerdings ist dann auch die Administration komplizierter. Bei Änderungen an Konfigurationsdateien muss dann jeweils wieder ein Editor installiert werden oder aber, und dies ist empfehlenswert, die Konfigurationsdateien müssen auf einem anderen Rechner editiert und dann überspielt werden.

Ein minimales Betriebssystem sollte natürlich kein Selbstzweck sein. Für einen Internet-Server muss selbstverständlich noch der eigentliche Serverdienst installiert werden. Ob dies am Ende der obigen Liste geschieht oder beispielsweise zwischen den Punkten 6 und 7 oder auch direkt nach Punkt 1, hängt von der jeweiligen Installation ab. Problematisch wird es, wenn die Installation wegen fehlender Betriebssystempakete fehlschlägt, da man dann die fehlenden Pakete suchen und selber nachinstallieren muss. Besser wäre es, der Hersteller des Serverdienstes gäbe die Betriebssystemabhängigkeiten an, so dass das Minimalsystem von Anfang an darauf ausgerichtet werden könnte.

Auch ein mit einem Minimalsystem konfigurierter Rechner ist nicht gänzlich vor Angriffen geschützt. Die wahrscheinlichste Ursache für einen erfolgreichen Angriff ist sicherlich der Serverdienst, aber auch das Minimalsystem selber ist noch angreifbar, insbesondere nämlich der TCP/IP-Stack, der die Netzpakete zur Applikation weiterleiten muss. Nahezu alle bisher bekannt gewordenen Angriffe gegen den TCP/IP-Stack betrafen allerdings nur die Verfügbarkeit, indem die betroffenen Rechner abstürzten, d. h. ein Eindringen in Rechner ist noch nicht beobachtet worden. Um auch diese Gefahr weiter zu verkleinern, sollte auch M 4.98 *Kommunikation durch Paketfilter auf Minimum beschränken* umgesetzt werden.

Ergänzende Kontrollfragen:

- Sind nicht benötigte Programme bei den Servern deaktiviert worden?
- Sind alle nicht benötigten Netzdienste abgeschaltet?
- Werden die Server auf ihre Netzdienste regelmäßig überprüft?

M 4.96 Abschaltung von DNS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Ein Internet-Server braucht normalerweise kein DNS (Domain Name System), um Informationen zur Verfügung zu stellen, es sei denn, über ihn wird die E-Mail versandt, wovon aber abzuraten ist (siehe dazu auch M 4.97 *Ein Dienst pro Server*). So wird bei den meisten WWW-Servern DNS nur dazu verwendet, in den jeweiligen Protokolldateien Rechnernamen statt IP-Adressen einzutragen. Diese Umwandlung von IP-Adressen zu Rechnernamen könnte auch später bei der Analyse der Protokolldateien durchgeführt werden. Zwar ist dann der Umgang mit den Protokolldateien etwas umständlicher, aber die Vertrauenswürdigkeit der Protokolldaten steigt. Die Zuordnung zwischen einer IP-Adresse und einem Rechnernamen ist nämlich weder eindeutig noch statisch. Ein Verzicht auf DNS gibt zusätzlich Schutz vor DNS-Spoofing (siehe M 5.59 *Schutz vor DNS-Spoofing*) und erhöht häufig die Performance des Internet-Servers.

Folgendes Szenario zeigt mögliche negative Auswirkungen:

Ein Angreifer verfüge über eine eigene Domain mit einem Test-PC. Dieser Test-PC ist gleichzeitig auch DNS-Server für diese Domain. Mit dem Test-PC baut er eine Verbindung zu einem Internet-Server auf. Der Internet-Server kennt am Anfang der Verbindungsanfrage nur die IP-Adresse des Test-PCs und versucht, sich über DNS den Rechnernamen des Test-PCs zu verschaffen. Zu diesem Zweck muss das Betriebssystem eine Verbindung mit einem DNS-Server aufnehmen, der sich wiederum die Daten von dem Test-PC holen muss, da dieser der DNS-Server der Angreifer-Domain ist. Anstatt nun dem DNS-Server des Internet-Servers zu antworten, kann der Angreifer nun auch direkt eine beliebige Antwort zum Internet-Server selber schicken (unter Verwendung von IP-Spoofing, siehe G 5.78). Auf diese Weise kann der Angreifer nicht nur Daten zu dem eigentlichen DNS-Server schicken, sondern auch direkt zum Internet-Server. Eventuelle Fehler in dessen Betriebssystem könnten so ausgenutzt werden.

Hinweis: Soll beispielsweise der Zugriff auf einen WWW-Server nur einer bestimmten Domain erlaubt sein, z. B. nur *.de, so kann allerdings nicht auf DNS verzichtet werden. Jedoch ist ein solcher Zugriffsschutz sehr schwach und daher nicht empfehlenswert.

Ergänzende Kontrollfrage:

- Ist DNS bei den Internet Server abgeschaltet?

M 4.97 Ein Dienst pro Server

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Viele Schwachstellen in IT-Systemen sind einzeln nicht für einen potentiellen Angreifer ausnutzbar. Häufig wird erst durch die Kombination von Schwachstellen ein erfolgreiches Eindringen in einen Rechner möglich. Eine Empfehlung für den Betrieb von sicheren Servern ist deshalb: Verschiedene Dienste gehören auf verschiedene Rechner!

Auf einem Minimalsystem (siehe auch M 4.95 *Minimales Betriebssystem*) sollte deshalb nur ein einziger Dienst aufgesetzt werden, also beispielsweise entweder ein WWW-Server oder ein E-Mailserver. Außerdem sind einzelne Dienste auch unterschiedlich in ihrer Sicherheitseinstufung. So ist ein erfolgreiches Eindringen in einen WWW-Server unter Umständen sehr ärgerlich, insbesondere wenn der Angreifer die extern verfügbaren WWW-Seiten abändert. Zugriff auf interne Informationen ist dem Angreifer hierdurch aber nicht möglich. Ist der WWW-Server aber gleichzeitig der E-Mailserver, so kann der Angreifer unter Umständen den gesamten E-Mail-Verkehr mitlesen, was möglicherweise viel schlimmere Auswirkungen hat.

Die Aufteilung kann sogar noch verstärkt werden, indem für einen einzelnen Dienst verschiedene Aufgaben auf unterschiedliche Rechner verteilt werden. So könnte es beispielsweise einen E-Mailserver A geben, der E-Mails aus dem Internet annimmt und in das interne Netz weiterleitet, und einen anderen E-Mailserver B, der E-Mails aus dem internen Netz an das Internet weiterleitet. Da die Kommunikationsaufnahme aus dem Internet nur mit dem E-Mail-server A möglich ist, kann ein Angreifer auch nur diesen attackieren. Der E-Mailserver A darf selber keine E-Mails in das Internet verschicken, deshalb kann dieser Rechner auch nicht für E-Mail-Spamming missbraucht werden.

Eine Aufteilung verschiedener Dienste auf unterschiedliche Rechner hat unter anderem folgende Vorteile:

- Leichtere Konfiguration der einzelnen Rechner
- Einfachere und sicherere Konfiguration eines vorgeschalteten Paketfilters
- Erhöhte Widerstandsfähigkeit gegenüber Angriffen
- Erhöhte Ausfallsicherheit

Eine eventuelle negative Auswirkung wie erhöhte Hardware-Kosten für die Anschaffung mehrerer Rechner sollte dadurch ausgeglichen werden können, dass die einzelnen Rechner weniger Leistung erbringen müssen und dadurch in der Summe bei gleicher Performance nicht teurer als ein besonders leistungsfähiger Rechner sein müssen. Auch muss der Administrations-aufwand nicht zwangsläufig mit der Anzahl der Rechner steigen, da eine einfachere Konfiguration der einzelnen Rechner für Zeitersparnis sorgt.

Ergänzende Kontrollfrage:

- Wird darauf geachtet, nur einen Dienst pro Server anzubieten?

M 4.98 Kommunikation durch Paketfilter auf Minimum beschränken

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Paketfilter sind IT-Systeme mit spezieller Software, die die Informationen der unteren Schichten des OSI-Modells filtern und entsprechend spezieller Regeln Pakete weiterleiten oder abfangen (siehe M 2.74 *Geeignete Auswahl eines Paketfilters*).

Die Konfiguration eines Paketfilters, der zum Schutz von Internet-Servern eingesetzt wird, sollte sehr restriktiv sein, um die Widerstandsfähigkeit gegen Angriffe zu maximieren. Zwar sollte ein gut konfigurierter Internet-Server (siehe M 4.95 *Minimales Betriebssystem*) sich selbst vor Angriffen schützen können, jedoch ist die Software eines Internet-Servers viel komplexer und fehleranfälliger als die eines auf Sicherheit konzipierten Paketfilters. Der Paketfilter sollte nur diejenigen Kommunikationskanäle durchlassen, die für die Funktion der Internet-Server notwendig sind. Insbesondere ist nicht nur die Kommunikation zu kontrollieren, die vom Internet zum Internet-Server initiiert wird, sondern auch die Kommunikation, die der Internet-Server zum Internet hin aufbauen darf. Für viele Angriffe ist es eine notwendige Voraussetzung, dass der angegriffene Rechner neue Verbindungen zum Internet hin aufbauen kann. Ist dies nicht möglich, so sind auch viele Angriffe nicht erfolgreich. So war 1997 ein Angriff auf News-Server sehr "beliebt", bei dem sich der Angreifer über einen Fehler in einem News-Daemon per E-Mail wichtige Systeminformationen zuschicken lassen konnte. Hätten die angegriffenen Rechner nicht die Berechtigung zum Verschicken von E-Mails gehabt, so hätte der Angreifer auch keine Rückmeldung bekommen. Der Angriff wäre nicht erfolgreich gewesen.

Im folgenden werden einige Beispiele für die Konfiguration von Paketfiltern für verschiedene Internet-Server dargestellt.

1. WWW-Server:
   Internet darf auf Port 80 des WWW-Servers TCP
   WWW-Server darf ins Internet von Port 80 TCP/ack, sonst nichts!

2. News-Server:
   Newsfeed-Server dürfen auf Port 119 des News-Servers TCP
   News-Server darf von Port 119 auf Newsfeed-Server TCP/ack
   News-Server darf auf Port 119 der Newsfeed-Server TCP
   Newsfeed-Server dürfen von Port 119 auf den News-Server TCP/ack

3. E-Mailserver (Provider stellt E-Mail-Gateway zur Verfügung):
   E-Mailserver des Providers darf auf Port 25 des E-Mailservers TCP
   E-Mailserver darf von Port 25 auf E-Mailserver des Providers TCP/ack
   E-Mailserver darf auf Port 25 des E-Mailservers des Providers TCP
   E-Mailserver des Providers darf von Port 25 auf E-Mailserver TCP/ack

4. E-Mailserver (eigenes Verschicken ins Internet):
   Internet darf auf Port 25 des E-Mailservers TCP
   E-Mailserver darf von Port 25 ins Internet TCP/ack
   E-Mailserver darf auf Port 25 im Internet TCP
   Internet darf von Port 25 auf den E-Mailserver TCP/ack

Werden nur diese Regeln implementiert, ist eine Kommunikationsaufnahme aus dem Internet nur auf die freigegebenen Dienste beschränkt. Können zusätzlich die Kommunikationspartner noch weiter eingeschränkt werden (siehe obige Beispiele 2 und 3), so kann ein Angreifer gar keine direkte Verbindung zu dem Internet-Server aufbauen.

Hinweis: Obige Regeln können bewirken, dass der Internet-Server nicht von jedem Rechner aus erreicht werden kann, da ICMP nicht durchgelassen wird. Deshalb empfiehlt es sich, den ICMP Subtype *icmp unreachable* vom Internet hin zum Internet-Server durchzulassen.

Ergänzende Kontrollfrage:

- Wird regelmäßig überprüft, ob die Kommuniktaion durch Paketfilter auf ein Minimum reduziert wurde?

M 4.99 Schutz gegen nachträgliche Veränderungen von Informationen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Dateien, die an Dritte weitergegeben werden, können von diesen im allgemeinen auch weiterbearbeitet werden. Dies ist nicht immer im Sinne des Erstellers. Daher wäre ein Schutz gegen nachträgliche Veränderungen, auszugsweise Weitergabe oder Verarbeitung wünschenswert.

Häufig steht man vor dem Problem, dass Informationen über das Internet oder andere Netze Dritten zwar zur Verfügung gestellt, aber nicht hundertfach ausgedruckt oder nahtlos in andere Werke integriert werden sollen.

Hierzu gibt es verschiedene Lösungen, die teilweise auch miteinander kombiniert werden können. Beispiele hierfür sind:

- Die Verwendung von digitalen Signaturen, um unbemerkte Änderungen an Dateien zu verhindern (siehe auch M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen* oder M 3.23 *Einführung in kryptographische Grundbegriffe*).
- Das Hinzufügen von Copyright-Vermerken zu WWW-Informationen oder Dateien. Diese können wie folgt lauten: "Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen des Urheberrechtsgesetzes ohne Zustimmung des Autors ist unzulässig und strafbar." sowie "Copyright (©) 7/1999 by BSI".
- Die Verwendung von Dateiformaten, die nachträgliche Änderungen bzw. auszugsweise Weiterverarbeitung erschweren. Hierfür kann z. B. Postscript genutzt werden oder die Sicherheitseigenschaften von Anwendungsprogrammen, z. B. bei PDF-Dateien.

  PDF-Dokumente können bei der Erstellung mit Zugriffsbeschränkungen versehen werden. So kann z. B. das Öffnen, Drucken oder Kopieren von PDF-Dateien eingeschränkt werden.

  Mit Acrobat Exchange, also der Anwendung, mit der PDF-Dateien erstellt und nachbearbeitet werden können, ist die Vergabe von zwei Arten von Passwörtern möglich. Die einen werden zum Öffnen des Dokuments, die anderen zum Ändern der Sicherheitsattribute benötigt. Gegen unbefugtes Öffnen geschützte PDF-Dokumente werden dabei mit RC4 verschlüsselt. Über die Sicherheitsattribute können folgende Funktionen eingeschränkt werden:

  - Drucken
  - Ändern des Dokuments
  - Text oder Graphik auswählen
  - Notizen und Formularfelder hinzufügen oder ändern

  So können sehr einfach die Rechte beschränkt werden, so dass niemand mit Cut and Paste die Inhalte einer Veröffentlichung übernehmen kann. Wenn

im Extremfall sogar das Ausdrucken verhindert wird, kann die Datei nur online gelesen werden.

Leider bietet dies nur einen rudimentären Schutz, da PDF-Dateien nämlich auch mit Programmen geöffnet werden können, die diese Sicherheitsattribute ignorieren. Solange z. B. Drucken erlaubt wird, kann das Dokument sogar jederzeit wieder in eine PDF-Datei ohne jegliche Einschränkungen verwandelt werden.

Ergänzende Kontrollfragen:

- Welche Sicherheitsmaßnahmen werden ergriffen, damit Dateien nicht unerwünscht verändert werden?

M 4.100 Sicherheitsgateways und aktive Inhalte

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Eines der größten Probleme bei der Konzeption eines Sicherheitsgateways ist die Behandlung der Probleme, die durch die Übertragung aktiver Inhalte zu den Rechnern im zu schützenden Netz entstehen. Derzeit existieren noch keine brauchbaren Programme, die eine ähnlich wirksame Erkennung von Schadfunktionen in ActiveX-Controls, Java-Applets oder Scripting-Programmen ermöglichen, wie sie im Bereich der Computer-Viren möglich ist.

Die Größe der Gefährdung, die von aktiven Inhalten für die Rechner im zu schützenden Netz ausgeht, lässt sich anhand des folgenden Beispiels darstellen: Ein Java-Applet bzw. der Browser darf gemäß der Java-Spezifikationen eine Netzverbindung zu dem Server aufbauen, von dem es geladen worden ist. Diese zur Zeit noch recht wenig benutzte Möglichkeit ist eine zentrale Voraussetzung, wenn Netz-Computer (NC) oder ähnliches eingesetzt werden sollen, die auch ohne spezielle Initiierung durch den Anwender Programme vom Server laden müssen. Um diese Eigenschaft trotz der Verwendung eines Paketfilters vollständig unterstützen zu können, müssen sehr viel mehr Ports freigeschaltet werden oder es muss ein dynamischer Paketfilter eingesetzt werden. Ist das der Fall, können Java-Applets verwendet werden, um kaum zu kontrollierende IP-Verbindungen aufbauen zu können.

Die Kontrolle aktiver Inhalte kann auf verschiedene Weise geschehen:

1. Zentrale Filterung der aktiven Inhalte auf dem Sicherheitsgateway

Sämtliche als schädlich eingestuften Inhalte werden von einer Komponente des Sicherheitsgateways (in der Regel vom ALG) gefiltert, so dass keine potenziell schädlichen Programme mehr auf den Client-Rechnern eintreffen.

Aktive Inhalte werden über spezielle Tags innerhalb einer HTML-Seite eingebunden. In der Regel werden aktive Inhalte anhand der entsprechenden Tags aus einer HTML-Seite erkannt und gelöscht, oder sie werden durch einen Textbaustein ersetzt, der dem Anwender einen Hinweis über die Tatsache der Filterung gibt. Das Problem besteht dabei darin, dass wegen der komplexen Möglichkeiten der aktuellen HTML-Spezifikation oft nicht alle zu löschenden Tags von den Sicherheitsproxies erkannt werden.

Weiterhin ist problematisch, dass beispielsweise Java-Applets nicht notwendigerweise als Datei mit der Endung .class verschickt werden müssen. Stattdessen können auch komprimierte Dateien eingesetzt werden, die z. B. die Endung .jar (Java-Archive) haben. Das bedeutet, dass ein Java-Filter auch alle von den verwendeten Browsern unterstützten Dateiendungen für Java-Dateien kennen muss. Zusätzliches Schadenspotential resultiert auch aus der Möglichkeit, JavaScript aus Java heraus auszuführen. Ähnliche Probleme existieren im Zusammenhang mit Flash-Objekten, .NET Assemblies und anderen aktiven Inhalten.

Es sollte unbedingt beachtet werden, dass auch aktive Inhalte außerhalb von Webseiten gefiltert werden müssen, beispielsweise in HTML-E-Mails.

2. Dezentrale Abwehr auf den angeschlossenen Clients

Die Ausführung aktiver Inhalte sollte normalerweise durch entsprechende Einstellungen im Browser unterbunden werden. Die Umsetzung einer Whitelist-Strategie für aktive Inhalte wird von verschiedenen Browsern in unterschiedlicher Weise und mehr oder weniger gut unterstützt (Beispiele: Zonenmodell des Microsoft Internet Explorers, Browser-Profile bei Mozilla). Idealerweise sollte ein Browser die Möglichkeit bieten, die Ausführung bestimmter Typen aktiver Inhalte getrennt für einzelne Server oder Domains freigeben oder verbieten zu können.

Dabei ist allerdings zu beachten, dass es auf Grund von Schwachstellen in den Browsern Angreifern möglich sein kann, entsprechende Einschränkungen zu umgehen.

Signierte aktive Inhalte

Java-Applets, Acitve-X Objekte und mit Einschränkungen auch Javascript können mit einer digitalen Signatur versehen werden. Die Signatur dient dazu, die Integrität und Authentizität des jeweiligen aktiven Inhalts zu schützen. Werden ausschließlich signierte aktive Inhalte zugelassen, so bietet dies eine erhöhte Sicherheit vor Schadfunktionen. Diese Sicherheit ist jedoch nur indirekt, da der Nutzer auf die Vertrauenswürdigkeit der Signaturstelle, die in Zusammenarbeit mit dem Anbieter der aktiven Inhalte die Signatur erstellt, angewiesen ist.

Selbst die vollständige Deaktivierung der Ausführung aktiver Inhalte bietet aber nur einen begrenzten Schutz vor bösartigen aktiven Inhalten. Aufgrund der Vielzahl von Software-Schwachstellen in den Browsern können die Sicherheitseinstellungen umgangen werden, so dass der intendierte Schutz tatsächlich nicht oder nicht in vollem Umfang existiert.

3. Installation von Anti-Viren-Software und Personal Firewalls auf den Clients

Anti-Viren-Produkte können vor Viren, Makroviren und Trojanischen Pferden schützen, die durch aktive Inhalte automatisch heruntergeladen wurden. Sie bieten einen guten Schutz vor bereits bekannten Schadprogrammen. Mehr zu Anti-Viren-Produkten findet sich in Baustein B 1.6 *Computer-Viren-Schutzkonzept*.

Personal Firewalls

Personal Firewalls sind Programme, die auf dem Client-Rechner installiert werden und dort meist mehrere Funktionen wahrnehmen. Sie bieten meist neben der Funktion eines lokalen Paketfilters weitere Funktionen an. Beispielsweise bieten einige Personal Firewalls die Möglichkeit einer Überwachung anderer Programme, die versuchen eine Netz-Verbindung aufzubauen. Solche Verbindungsaufnahmen können dann meist entweder automatisch anhand festgelegter Regeln oder im Einzelfall vom Benutzer selbst erlaubt oder verboten werden. In einigen Fällen bieten sie auch sogenannte "Sandboxen", die die Ausführung aktiver Inhalte kontrollieren und auf unbedenkliche Operationen beschränken können.

Personal Firewalls bieten zusammen mit Anti-Viren-Programmen einen recht guten Schutz vor bösartigen aktiven Inhalten. Allerdings muss berücksichtigt werden, dass die richtige Konfiguration dieser Programme zusätzlichen

Administrationsaufwand erfordert, und dass Personal Firewalls selbst Sicherheitslücken aufweisen können, die das System gefährden.

Sensibilisierung der Benutzer

Bei allen drei Optionen ist eine Sensibilisierung der Benutzer zusätzlich notwendig. Zudem muss sichergestellt werden, dass die Einstellungen auf den Clients bei allen unter Punkt 2 und 3 genannten Schutzvorkehrungen nicht versehentlich oder absichtlich vom Benutzer deaktiviert oder umgangen werden können.

Vorteile der zentralen Filterung	Vorteile der dezentralen Filterung
- Einfache Installation und Administration, da die Filtersoftware nur einmal installiert werden muss.	- Im Vergleich zur zentralen Filterung höhere Ausfallsicherheit, da die Filterung dezentral erfolgt.
- Einfache Protokollierung und Auswertung, da im Gegensatz zur dezentralen Filterung keine Protokolldaten von mehreren Rechnern zusammengeführt werden müssen.	- Schutz vor verschlüsselten aktiven Inhalten. Bei Filterung auf dem Endgerät können aktiven Inhalte erkannt werden, da sie auf dem Endgerät entschlüsselt werden.
- Im Gegensatz zur dezentralen Filterung ist keine triviale Manipulation der Filtersoftware durch den Benutzer möglich.	- Die Ausführung von aktiven Inhalten kann unabhängig vom Sicherheitsgateway abgeschaltet werden.
- Filterprogramme für aktive Inhalte auf dem ALG sind dedizierte Sicherheitsprodukte. Der Schutz vor aktiven Inhalten auf den Clients (z. B. im Browser) ist hingegen oft fehlerhaft implementiert.	- Es entstehen keine Kompatibilitätsprobleme, die sich durch den Einsatz einer zentralen Filtersoftware auf dem ALG ergeben könnten.
- Die Verwendung der Filtersoftware ist unabhängig von der Software auf den Clients möglich. Es entstehen keine Kompatibilitätsprobleme mit der auf den Clients eingesetzten Software	

Tabelle: Vorteile der zentralen beziehungsweise dezentralen Filterung

Empfehlung

Die Entscheidung, wie mit aktiven Inhalten in Webseiten umgegangen wird, hängt in erster Linie vom Schutzbedarf der betreffenden Clients ab. Die folgende Tabelle kann bei der Festlegung der individuellen Strategie als Grundlage dienen:

Schutzbedarf der Clients	Empfehlung
Normal	Allgemein: Deaktivierung aktiver Inhalte im Browser und Freischaltung nur für vertrauenswürdige Websites. Virenscanner auf dem Client (siehe auch Baustein B 1.6 *Computer-Virenschutzkonzept*). Eine Filterung aktiver Inhalte auf dem Sicherheitsgateway mit Freischaltung für vertrauenswürdige Websites (Whitelist) ist empfehlenswert.
Hoch	Deaktivierung aktiver Inhalte im Browser und Freischaltung nur für vertrauenswürdige Websites. Virenscanner auf dem Client (siehe auch Baustein B 1.6 *Computer-Virenschutzkonzept*). Filterung aktiver Inhalte auf dem Sicherheitsgateway mit Freischaltung für vertrauenswürdige Websites (Whitelist). Zusätzlich Filterung von Cookies (Whitelist). Die Kriterien, für welche Websites aktive Inhalte freigeschaltet werden, sollten deutlich restriktiver sein als bei normalem Schutzbedarf. Eine ergänzende Sicherheitsanalyse wird empfohlen, um sicher zu stellen, dass ein angemessenes Sicherheitsniveau erreicht wurde.
Bei zusätzlichen oder speziellen Anforderungen	Einsatz einer Personal Firewall auf dem Client.

Tabelle: Empfehlungen für den Umgang mit aktiven Inhalten in Webseiten

Die Entscheidung für eine bestimmte Vorgehensweise und die Gründe, die dafür ausschlaggebend waren, sollten nachvollziehbar dokumentiert werden.

Vorsicht ist besser als Nachsicht

Eine zu "liberale" Einstellung oder gar eine generelle Freigabe aktiver Inhalte ist auch bei normalem Schutzbedarf nicht zu empfehlen. Die möglichen Schäden, die durch bösartige aktive Inhalte in Verbindung mit Schwachstellen in Webbrowsern oder im unterliegenden Betriebssystem entstehen können, sind dafür zu gravierend. Falls für bestimmte, Anwendungen aktive Inhalte zwingend nötig sind, sollten sie nur für die betreffenden Server freigegeben werden.

Notwendigkeit aktiver Inhalte hinterfragen

Bei Neuentwicklungen browserbasierter Anwendungen oder bei einer Weiterentwicklung einer bestehenden Anwendung, die aktive Inhalte im Browser benötigt, sollte kritisch hinterfragt werden, ob die Verwendung der aktiven Inhalte wirklich notwendig ist. Oft lassen sich aktive Inhalte bei gleichwertiger Funktionalität durch serverseitig dynamisch erzeugte Webseiten ersetzen.

Ergänzende Kontrollfragen

- Wie werden aktive Inhalte behandelt?

M 4.101 Sicherheitsgateways und Verschlüsselung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Da im Internet die Daten über nicht vorhersagbare Wege und Knotenpunkte verschickt werden, sollten die versandten Daten möglichst nur verschlüsselt übertragen werden. Eine Verschlüsselung des Datenverkehrs über das Internet kann auf zwei verschiedene Arten realisiert werden:

- Verschlüsselung auf dem Sicherheitsgateway bzw. auf Netzkoppelelementen, die zum Aufbau sicherer Teilnetze eingesetzt werden kann
- Verschlüsselung auf den Endgeräten, die z. B. von Benutzern bedarfsabhängig eingesetzt wird

Beide Verfahren haben spezifische Vor- und Nachteile, die je nach Anwendungszusammenhang für die eine oder die andere Variante sprechen.

Verschlüsselung durch das Sicherheitsgateway

Um mit externen Kommunikationspartnern Daten über ein offenes Netz auszutauschen und / oder diesen Zugriff auf das eigene Netz zu geben, kann der Aufbau von virtuellen privaten Netzen (VPNs) sinnvoll sein. Dafür sollten alle Verbindungen von und zu diesen Partnern verschlüsselt werden, damit Unbefugte keinen Zugriff darauf nehmen können. Zum Aufbau von verschlüsselten Verbindungen können eine Vielzahl von Hard- und Softwarelösungen eingesetzt werden. Sollen hierbei nur wenige Liegenschaften miteinander verbunden werden, sind insbesondere Hardware-Lösungen basierend auf symmetrischen kryptographischen Verfahren eine einfache und sichere Lösung.

Möglichkeiten zur Einbindung von VPN-Komponenten in Sicherheitsgateways finden sich in M 4.224 *Integration von Virtual Private Networks in ein Sicherheitsgateway*.

Die Ver- und Entschlüsselung kann gegebenenfalls auf verschiedenen Geräten erfolgen. So könnte eine Hardware-Lösung im Paketfilter als Schlüsselgerät arbeiten. Dies ist insbesondere dann sinnvoll, wenn keine unverschlüsselte Kommunikation über dieses Gerät gehen soll.

Die Integration der Verschlüsselung auf dem ALG hat den Vorteil einer leichteren (zentralen) Benutzerverwaltung. Zudem kann ein Angreifer, der einen externen Informationsserver unter seine Kontrolle gebracht hat, die verschlüsselte Kommunikation nicht belauschen.

Verschlüsselung auf den Endgeräten

Zum Schutz der Vertraulichkeit bestimmter Daten, insbesondere bei der Versendung von E-Mails, bietet sich auch der Gebrauch von Mechanismen an, die eine Ende-zu-Ende-Verschlüsselung ermöglichen. Hierfür wird beim Dienst E-Mail zum Beispiel das frei verfügbare Programmpaket PGP (Pretty Good Privacy) sehr häufig eingesetzt (siehe M 5.63 *Einsatz von GnuPG oder PGP*), für den Zugriff auf andere Rechner das Secure-Shell Protokoll (SSH). Für eine vertrauenswürdige Datenübertragung mit ausgewählten Partnern im

Internet sollten nur Übertragungsprogramme und -protokolle verwendet werden, die eine Verschlüsselung der übertragenen Daten unterstützen. Unsichere Klartextprotokolle wie Telnet und FTP sollten ohne zusätzliche Maßnahmen (etwa Tunneln über eine verschlüsselte Verbindung oder ein echtes VPN) nicht mehr in öffentlichen Netzen eingesetzt werden.

Problem der Ende-zu-Ende-Verschlüsselung

Die Ende-zu-Ende-Verschlüsselung der Daten stellt andererseits aber auch ein großes Problem für den wirksamen Einsatz von Filtermechanismen eines Sicherheitsgateways dar. Wenn die Übertragung verschlüsselter Daten über das Sicherheitsgateway zugelassen wird (z. B. SSL), sind Filter auf der Anwendungsschicht nicht mehr in der Lage, die Nutzdaten beispielsweise auf Viren oder andere Schadprogramme zu kontrollieren. Auch die Protokollierungsmöglichkeiten werden durch eine Verschlüsselung stark eingeschränkt.

Eventuell temporäre Entschlüsselung auf dem Sicherheitsgateway

Eine Lösung dieses Problems kann darin bestehen, den Datenverkehr temporär vom Sicherheitsgateway entschlüsseln zu lassen. Beispielsweise existieren für SSL entsprechende Proxies, die die SSL-Verbindung am Sicherheitsgateway terminieren und den entschlüsselten Datenstrom für eine Filterung zugänglich machen. Gegebenenfalls können die Daten dann wieder für die Übertragung zum Endgerät verschlüsselt werden.

Eine generelle Empfehlung für oder gegen den Einsatz von Verschlüsselung über das Sicherheitsgateway kann nicht gegeben werden. Dies hängt von den Anforderungen im Einzelfall ab, daher sollte eine Bewertung im Anwendungszusammenhang erfolgen.

Auf dem Sicherheitsgateway:	Auf den Endgeräten:
+ Zentrale Datenprüfung	+ Ende-zu-Ende Sicherheit
+ Zentrale Schlüsselverteilung	+ Keine Protokollprobleme
+ Detailliertes Accounting	+/- benutzerabhängig
- Zugriff vom Sicherheitsgateway auf internes Netz	- Keine Kontrollmöglichkeiten auf dem Sicherheitsgateway
- Keine Ende-zu-Ende-Sicherheit	- Oft werden Public-Key-Infrastrukturen benötigt

Tabelle: Vor- und Nachteile der verschiedenen Realisierungsmöglichkeiten

Wird für bestimmte Dienste oder Protokolle festgelegt, dass eine Ende-zu-Ende-Verschlüsselung eingesetzt (bzw. zugelassen) werden soll, so kann es erforderlich werden, für die Endgeräte zusätzliche Maßnahmen zu ergreifen. Dies sollte im Rahmen einer ergänzenden Sicherheitsbetrachtung geprüft werden.

Ergänzende Kontrollfragen:

- Wird für einen Dienst eine Ende-zu-Ende-Verschlüsselung eingesetzt? Falls ja: Wurde im Rahmen einer ergänzenden Sicherheitsbetrachtung geprüft, ob auf den Endgeräten zusätzliche Sicherungsmaßnahmen erforderlich sind?

M 4.102 C2-Sicherheit unter Novell 4.11

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Zur Bewertung von IT-Produkten bzw. IT-Systemen haben sich als einheitlicher Beurteilungsmaßstab international die US-amerikanischen Kriterien TCSEC (Trusted Computer System Evaluation Criteria) bzw. die europäischen ITSEC (Information Technology Security Evaluation Criteria) und mittlerweile deren Weiterentwicklung CC (The Common Criteria for Information Technology Security Evaluation) durchgesetzt. Novell Netware 4.11 hat im Herbst 1997 eine Zertifizierung gemäß Funktionalitätsklasse C2 der TCSEC durch das *National Computer Security Center* (NCSC) erhalten, dies entspricht ITSEC Klasse F-C2/E2.

Der Einsatz eines zertifizierten Produktes bietet die Gewähr, dass die Sicherheitsfunktionalität dieses Produktes unabhängig geprüft wurde und den im Evaluationslevel spezifizierten Standard nicht unterschreitet (siehe auch M 2.66 *Beachtung des Beitrags der Zertifizierung für die Beschaffung*).

Vielfach anzutreffende Standardfälle sind in den genannten Sicherheitskriterien zu Funktionalitätsklassen zusammengefasst. Die Anforderungen der Funktionalitätsklassen F-C2 sind im wesentlichen für Betriebssysteme gedacht. Darin sind z. B. folgende Merkmale definiert:

- Übernahme der C1 Spezifikationen
  - Existenz von Mechanismen zur Zugriffsbeschränkung von Benutzern auf bestimmte Dokumente
  - Identifizierung von Benutzern
- Verfeinerung der Zugriffsberechtigungen
- Auditing aller sicherheitsrelevanten Ereignisse mit Zeitstempel, Benutzername, Objekt und Meldung über Erfolg bzw. Misserfolg
- Verwaltung der Audit Dateien (Zugriffsschutz, Steuerung des Umfangs, etc.)
- Abgrenzung der Ressourcen (Zugriffsschutz)
- Abgrenzung von Daten aus verschiedenen Prozessen gegenüber anderen Prozessen selbst nach Freigabe

Die Einhaltung dieser Vorgaben wird in speziellen Testverfahren überprüft.

Um C2-Sicherheit zu erreichen, reicht es allerdings nicht aus, ein C2-zertifiziertes Produkt zu erwerben. Wesentlich für die tatsächliche Realisierung eines C2-Systems ist die genaue Umsetzung der Vorgaben des Zertifizierungsreports.

Die zur Erreichung der C2-Sicherheit bei Netware 4.11 notwendigen Sicherheitsoptionen wurden in der Datei SECURE.NCF zusammengefasst. In den nachfolgenden Abschnitten wird die Datei SECURE.NCF dargestellt und die einzelnen Optionen näher erläutert.

Die Datei SECURE.NCF und ihre Optionen

Damit ein Novell Netware 4.11 Server die erweiterten Sicherheitsmechanismen nutzen kann, sind folgende Punkte zu beachten:

- Die Datei SECURE.NCF muss auf dem Server in SYS:SYSTEM gespeichert sein.
- Die Datei SECURE.NCF ist eine Ablaufdatei ähnlich einer Batch-Datei unter DOS und sollte daher nur mit einem ASCII-Editor (z. B. EDIT.NLM) bearbeitet werden.
- Für den Aufruf der Datei SECURE.NCF muss in der AUTOEXEC.NCF die Zeile "SET ENABLE SECURE.NCF=ON" eingefügt werden. Alternativ hierzu kann auch der Befehl "SECURE" in die AUTOEXEC.NCF eingefügt oder dieser Befehl auf der Server-Konsole abgesetzt werden.

Der nachfolgende Auszug aus der Datei SECURE.NCF zeigt nur die darin enthaltenen Befehle. In der Originaldatei ist zu jedem Befehl eine kurze Erläuterung enthalten.

```
SET ALLOW UNENCRYPTED PASSWORDS = OFF

SET ALLOW AUDIT PASSWORDS = OFF

SET AUTOMATICALLY REPAIR BAD VOLUMES = ON

SET REJECT NCP PACKETS WITH BAD LENGTHS = ON

SET REJECT NCP PACKETS WITH BAD COMPONENTS = ON

SET IPX NETBIOS REPLICATION OPTION = 0

SET ADDITIONAL SECURITY CHECKS = ON

# SET CHECK EQUIVALENT TO ME = ON

# SET NCP PACKET SIGNATURE = 3

# SECURE CONSOLE

## DISPLAY NCP BAD COMPONENT WARNINGS

## DISPLAY NCP BAD LENGTH WARNINGS
```

Alle Befehlszeilen, die mit einem "#" auskommentiert wurden, sind zusätzliche Sicherheitsparameter und für die Einhaltung der C2 bzw. F-C2/E2 Bestimmungen nicht notwendig. Befehlszeilen, die mit "##" gekennzeichnet sind, gehören nicht zum Standardumfang der Datei SECURE.NCF, stellen aber im alltäglichen Gebrauch eine sinnvolle Bereicherung dar.

Die Befehle im Einzelnen

Alle Befehle bzw. SET-Anweisungen können auch an der Konsole abgesetzt oder mittels des Programms SERVMAN.NLM bzw. MONITOR.NLM gesetzt werden.

Nachfolgend werden alle SET-Parameter der Datei SECURE.NCF beschrieben und die Standardwerte (Default) angegeben.

SET ALLOW UNENCRYPTED PASSWORDS = OFF (Default = OFF)

Dieser Parameter dient dazu, die Kompatibilität von Netware 2.x Clients und Print-Servern zu gewährleisten. Ein Setzen des Parameters auf den Wert ON hat zur Folge, dass ein Passwort, das zur Authentisierung notwendig ist, unverschlüsselt zum Server übertragen werden kann. Dies begünstigt ein unberechtigtes Eindringen in das betreffende System. Der Standardwert OFF stellt sicher, dass beim Anmeldevorgang jedes Passwort verschlüsselt werden muss. Unverschlüsselte Passwörter werden nicht akzeptiert.

SET ALLOW AUDIT PASSWORDS = OFF (Default = OFF)

Dieser Parameter steht in Verbindung mit den Auditing Mechanismen des Netware-Betriebssystems. Beim Auditing werden gemäß der Vorgaben der Konfigurationen mittels des Programms AUDITCON.NLM Veränderungen (Manipulationen) an Objekten aufgezeichnet. Durch entsprechende Berechtigungen, die z. B. in der allgemeinen Berechtigungsvergabe des Betriebssystems für jeden Auditor individuell eingestellt werden können, ist ein Auditor in der Lage, die Auditing-Datei zu lesen. Die jeweilige Berechtigung schränkt dabei den Leseumfang ein. Der Standardwert OFF bewirkt, dass sich der Auditor nicht durch ein zusätzliches Passwort identifizieren muss.

SET AUTOMATICALLY REPAIR BAD VOLUMES = ON (Default = ON)

Mit diesem Parameter wird das Betriebssystem angewiesen, ein Volume, das beim Systemstart nicht gemountet werden kann, durch den Aufruf des Programms VREPAIR.NLM zu reparieren. Dies stellt sicher, dass nach einem unkontrollierten Systemabsturz und dem darauf folgenden Neustart mögliche Fehler auf Volumes (Datenbereichen der Plattenstapel) ohne zusätzlichen Eingriff des Systemadministrators behoben werden.

SET REJECT NCP PACKETS WITH BAD LENGTHS = ON (Default =OFF)

Dieser Parameter bewirkt in der Einstellung ON, dass NCP Pakete mit inkorrekter Länge abgewiesen werden. Dabei kann es zu Fehlern mit älteren Anwendungen (Utilities) kommen.

SET REJECT NCP PACKETS WITH BAD COMPONENTS = ON (Default = OFF)

Dieser Parameter bewirkt in der Einstellung ON, dass NCP Pakete mit inkorrekten Komponenten abgewiesen werden. Auch hier kann es zu Fehlern mit älteren Anwendungen (Utilities) kommen.

SET IPX NETBIOS REPLICATION OPTION = 0 (Default = 2)

Dieser Parameter legt die Vorgehensweise des IPX Routers fest, wie mit NetBIOS Broadcast Meldungen umzugehen ist. Für die Werteauswahl stehen zur Verfügung:

- 0 = keine Replizierung von Typ 20 IPX Paketen
- 1 = Replizierung von Typ 20 IPX Paketen an alle verfügbaren Netzadapter
- 2 = Replizierung von Typ 20 IPX Paketen mit zwei speziellen Filterfunktionen

a) Reverse Path Forwarding: Typ 20 IPX Pakete von derselben Quelle werden nur einmal an alle verfügbaren Netzkarten weitergeleitet, selbst wenn die Pakete über unterschiedliche Netzadapter empfangen wurden.

b) Split Horizon: Typ 20 IPX Pakete werden nicht in das Netz zurückgeleitet, aus dem sie empfangen wurden.

3 = Replizierung wie bei Option 2, aber nicht über Weitverkehrsstrecken

SET ADDITIONAL SECURITY CHECKS = ON

Dieser Parameter aktiviert zusätzliche Sicherheitsüberprüfungen, die mit früheren NDS Versionen inkompatibel sind.

Die zuvor aufgeführten Parameter sind für die Einhaltung der Sicherheitszertifizierung gemäß Klasse C2 und Klasse F-C2/E2 zwingend erforderlich. Die nachfolgenden Parameter können zur Erweiterung der Sicherheitsfunktionen eingesetzt werden.

SET CHECK EQUIVALENT TO ME = ON (Default = OFF)

Dieser Parameter erzwingt am Server die Überprüfung des NDS Attributes "Equivalent To Me". Wenn der Wert für die erweiterte Sicherheit auf ON gesetzt wird, müssen mit der Anwendung DSREPAIR die Attribute "Equivalence" und "Equivalent To Me" synchronisiert werden. Das Aktivieren der Option hat möglicherweise nachteilige Effekte auf die Authentisierungsgeschwindigkeit des Systems.

SET NCP PACKET SIGNATURE = 3 (Default = 1)

Die Kommunikation eines Novell Netware Clients mit einem Novell Netware Server wird durch das Netware Core Protokoll (NCP) gesteuert. Client und Server tauschen hierbei einzelne Pakete aus, in denen die Daten enthalten sind. Ein potentieller Angreifer kann diese Pakete mittels spezieller Programme (siehe G 5.58 *"Hacking Novell Netware"*) überwachen und die Datenpakete höher privilegierter Benutzer manipulieren.

Um dieser Bedrohung entgegenzuwirken, wurde die Paket-Signatur entwickelt. Bei der Anmeldung eines Benutzers am Netz wird ein geheimer Schlüssel ermittelt. Wann immer die Workstation daraufhin eine Anfrage über NCP an das Netz sendet, wird diese mit einer Signatur versehen, die aus dem geheimen Schlüssel und der Signatur des vorherigen Pakets gebildet wird. Diese Signatur wird an das betreffende Paket angehängt und zum Server gesandt. Bevor die eigentliche Anfrage bearbeitet wird, verifiziert der Server die Paket-Signatur.

Durch den Parameter kann die Paket-Signatur am Server aktiviert werden. Hierbei sind folgende NCP-Paket-Signatur Level möglich:

0 = Es findet keine NCP-Paket-Signatur statt.

1 = Der Novell Netware Server arbeitet auf Anforderung des Clients mit der NCP-Paket-Signatur.

2 = Der Novell Netware Server fordert vom Client NCP-Paket-Signatur an. Sollte der Client dieses nicht realisieren können, so wird die Kommunikation zwischen Client und Novell Netware Server trotzdem zugelassen.

3 = Die NCP-Paket-Signatur ist zwingend vorgeschrieben.

Zur Gewährleistung der IT-Sicherheit sollte die NCP-Paket-Signatur mit dem Wert "3" gewählt werden und der Novell Netware Server sowie die Client-Software der Arbeitsstationen entsprechend konfiguriert werden. Da sich jedoch die Netzlast beim Einsatz der NCP-Paket-Signatur erhöht, sollte im Vorfeld des Einsatzes geklärt werden, ob die Performance hierdurch nicht unzumutbar eingeschränkt wird.

SECURE CONSOLE

Mit diesem Befehl werden mehrere Funktionen ausgelöst. Daher sollte dieser Befehl nur an sicherheitssensitiven Systemen ausgeführt werden. Die Funktionen sind:

1. Alle Suchpfaderweiterungen werden rückgängig gemacht. Für den Aufruf von NLMs steht nur noch der Suchpfad auf das Laufwerk SYS:SYSTEM zur Verfügung.
2. Eine Suchpfaderweiterung mit dem Befehl SEARCH ADD ist nicht mehr möglich.
3. Das Verändern von verschiedenen Server-Parametern mit dem Befehl SET ist nicht mehr möglich.
4. Das Verändern von Systemzeit und Systemdatum ist nicht mehr möglich.
5. Der System Debugger kann nicht mehr durch die spezielle Tastenkombination aufgerufen werden.

Hinweis: Da SECURE CONSOLE die Suchpfade auf das Systemminimum reduziert, kann es zu erheblichen Problemen mit Serverapplikationen kommen, die eine spezielle Suchpfaderweiterung benötigen.

DISPLAY NCP BAD COMPONENT WARNINGS

Mit diesem Parameter wird der Server angewiesen, eine Warnmeldung auf der Konsole auszugeben, wenn NCP Pakete mit ungültigem Inhalt bzw. Anteilen empfangen werden. Dies könnte auf Angriffe hindeuten.

DISPLAY NCP BAD LENGTH WARNINGS

Mit diesem Parameter wird der Server angewiesen, eine Warnmeldung auf der Konsole auszugeben, wenn NCP Pakete mit ungültiger Länge empfangen werden. Dies könnte auf Angriffe hindeuten.

M 4.103 DHCP-Server unter Novell Netware 4.x

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Beim Einrichten von TCP/IP-Protokollen entsteht ein hoher Aufwand, wenn für jede Workstation manuell die IP-Adresse, die Subnetz-Maske, das Default Gateway, etc. vergeben werden müssen. Soll z. B. in einem Segment nur der Default Gateway Eintrag geändert werden, erfordert dies einen hohen Arbeitsaufwand und erhöht zudem die Gefahr von Falscheingaben. Durch den Einsatz eines DHCP-Servers (Dynamic Host Configuration Protocol) können diese Aufgaben zentralisiert und automatisiert werden.

Um einen sicheren Umgang mit dem DHCP-Server von Novell Netware 4.x zu gewährleisten, ist es erforderlich, dass die Struktur des TCP/IP-Netzes, dessen Adressen mit Hilfe des DHCP-Servers verwaltet werden sollen, bekannt ist. Wichtig sind hierbei neben der Adressklasse (TCP/IP-Netz Klasse A - C) auch die eingesetzten Subnetz-Masken und die Adressen der Default Gateways, um segmentübergreifenden Datenverkehr auf TCP/IP Basis zu ermöglichen.

Im folgenden wird auf einige Aspekte bei der Konfiguration des DHCP-Dienstes unter Novell Netware 4.x eingegangen, die für die Sicherheit des Gesamtsystems von besonderer Relevanz sind.

Konfiguration der TCP/IP-Segmente

Über die Option SUBNETWORK PROFILE werden die TCP/IP-Segmente definiert, die vom Server versorgt werden sollen. Dabei werden Werte wie Subnetzname, Adressbereich und Zuweisungsart vom Konfigurationsmenü des DHCP-Servers bei dessen Start automatisch ausgelesen. Soll der DHCP-Server mehrere IP-Segmente versorgen, so ist es empfehlenswert, die automatisch eingelesenen Werte zu löschen und durch "sprechende", manuell konfigurierte Werte zu ersetzen. Wurde z. B. als Subnetzname "3CX9_1_EII" ausgelesen, so ist es für die Fehlersuche und für spätere Konfigurationsarbeiten für dieses Segment einfacher, wenn dieser Eintrag manuell durch einen Eintrag ersetzt wird, der das Segment besser beschreibt, z. B. der Name "EthernetII". Andere sprechende Namensgebungen, die das Segment etwa nach seiner topologischen Anordnung bezeichnen (Gebäude A, 2. OG oder Geschäftsführung), sind ebenfalls einsetzbar.

Automatische Zuordnung von IP-Adressen

Ein wesentlicher Dienst des DHCP-Servers ist die automatische Zuordnung von IP-Adressen. Der Parameter AUTOMATIC IP ADDRESS ASSIGNMENT kennzeichnet den Adressbereich, aus dem heraus der DHCP-Server dynamisch die Adressen an die Netzknoten verteilt, die eine Adresse anfordern. Dieser Bereich sollte so ausgewählt werden, dass die Adressen für Server, Drucker und Router nicht in den Bereich der dynamischen Zuteilung fallen. Generell sollten Servern, Druckern, Routern und den Netzknoten mit dynamischer Adresszuordnung klar unterscheidbare IP-Adressbereiche zugewiesen werden. Dadurch ist gewährleistet, dass bereits am Adressbereich

erkennbar ist, zu welchem Typ ein Netzknoten gehört, wenn Probleme im IP-Bereich auftreten.

Statische Zuordnung von IP-Adressen

Für bestimmte Komponenten im Netz ist es empfehlenswert, mittels einer statischen Adresszuordnung die erforderliche IP-Adresse permanent auf die MAC-Adresse (Medium Access Control) des Netzknotens zu binden. Hierzu gehören z. B. Netzdrucker und Router. Der Vorteil einer statischen Zuordnung durch einen DHCP-Server im Vergleich zu einer manuellen Konfiguration vor Ort am Netzknoten ist die zentrale Verwaltung der Zuordnungen über das Konfigurationstool des DHCP-Servers. Obwohl Server ebenfalls zwingend ihre IP-Adresse statisch zugeordnet bekommen müssen, werden diese nicht über den DHCP-Server vergeben. Bei Netware Servern erfolgt die Zuteilung ihrer IP-Adresse immer manuell.

Die Konfiguration der statischen Adresszuordnung geschieht über die Option IP ADDRESS ASSIGNMENT. Der Knoten wird über einen beliebigen Namen dem Menü hinzugefügt und die IP-Adresse direkt auf die Netzkarte (MAC-Adresse) des Knotens gebunden. Für die Auswahl des Namens empfiehlt Novell, den Login-Namen des Benutzers zu verwenden, der an diesem Arbeitsplatzrechner arbeitet.

Lease Time

Anhand der Lease Time wird festgelegt, wie lange ein Netzknoten, der seine TCP/IP-Adresse vom DHCP-Server dynamisch erhält, diese behalten kann. Die Zuteilung der IP-Adressen wird dabei beim Booten des Netzknotens realisiert. Für die Lease Time sollte ein Zeitraum von mindestens 24 Stunden gewählt werden, da sonst folgende Probleme auftreten können:

- Programme, deren Zugriffsberechtigungen anhand von TCP/IP-Adressen erteilt werden, können nach einem Reboot des Rechners unter Umständen nicht mehr ausgeführt werden, da sich die IP-Adresse des darauf zugreifenden Rechners geändert hat. Die neue Adresse ist evtl. nicht berechtigt, das Programm auszuführen.
- Wenn Arbeitsplatzrechner instabil laufen und pro Tag mehrfach erneut gestartet werden, entsteht nach jedem Neustart eine unnötige Netzlast durch die Zuweisung einer neuen IP-Adresse.
- Beim Zugriff auf das Internet protokollieren zwischengeschaltete Proxy Server die Internet-Seiten, die von den Arbeitsplatzrechnern aus aufgerufen wurden. In den entsprechenden Protokolldateien werden meist die DNS Namen der aufgerufenen Internet-Seiten den IP-Adressen der Rechner zugeordnet, von denen aus diese Seiten angefordert wurden. Wenn sich diese IP-Adressen ständig ändern, dann ist im Problemfall nur sehr schwer nachvollziehbar, welcher Arbeitsplatzrechner zu welchem Zeitpunkt die entsprechende IP-Adresse zugewiesen bekommen hat.

Die Vergabe einer Lease Time wird beim Einsatz von DHCP-Servern benötigt, wenn sich in einem Netz mehr Knoten befinden, als IP-Adressen zur Verfügung stehen. Mittels einer geeignet gewählten Lease Time kann so eine IP-Adresse, die frei geworden ist, weil der Knoten sie nicht mehr braucht (PC

wurde ausgeschaltet), einem anderen Knoten, der eine Adresse vom DHCP-Server anfordert, zugewiesen werden. In Netzen, die über mindestens genauso viele IP-Adressen verfügen wie Knoten installiert sind, kann auf die Konfiguration der Lease Time verzichtet werden. Seit geraumer Zeit kann in LANs mit sogenannten privaten IP-Adressen (siehe RFC 1597) gearbeitet werden. Das Problem, mehr Knoten als IP-Adressen zu haben, kann somit umgangen werden. Die Vergabe von privaten IP-Adressen nach diesen Vorgaben ist z. B. aus Revisionsgründen für Netze, die einen Internet-Zugang realisieren, empfehlenswert. Datenschutzrechtliche und mitbestimmungsrechtliche Aspekte sind zu beachten.

Im DHCP-Server von Netware 4.x kann die Lease Time derzeit noch nicht abgeschaltet werden. Es ist daher empfehlenswert, diese auf den maximalen Wert von 10000 Tagen und 23 Stunden einzustellen.

Ausschluss bestimmter Netzknoten von der Adresszuordnung

Für bestimmte Netzknoten kann die Zuweisung einer IP-Adresse unterbunden werden. Unter dem Menüpunkt EXCLUDED NODES sind hierzu dieselben Schritte auszuführen, wie bei der statischen Zuordnung von IP-Adressen. Hiermit wird erreicht, dass bestimmte Programme, die auf TCP/IP aufsetzen, von diesen Arbeitsplätzen aus nicht aufgerufen werden können. Diese "Sperre" ist allerdings leicht zu unterwandern, indem dem "gesperrten" Netzknoten manuell eine IP-Adresse zugeordnet wird (sofern auf diesem Knoten der TCP/IP-Protokollstack geladen wurde). Sobald bei der manuellen Zuordnung eine freie IP-Adresse gefunden wird, kann mit diesem Rechner genauso über TCP/IP kommuniziert werden, wie mit Knoten, die ihre IP-Adresse vom DHCP-Server erhalten haben. Der Weg, Netzknoten über EXCLUDED NODES von der Vergabe einer IP-Adresse auszuschließen, bietet daher nur eine relative Sicherheit.

Das Sperren von MAC-Adressen für die Vergabe durch den DHCP-Server kann zudem dazu dienen, in Netzen mit mehreren DHCP-Servern die Lastverteilung zu steuern. Außerdem kann verhindert werden, dass Knoten, in deren Segment sich ein eigener DHCP-Server befindet, die IP-Adresse von einem DHCP-Server anfordern, der sich in einem anderen Segment befindet. Hierbei sollte beachtet werden, dass in diesem Fall bei Ausfall des lokalen DHCP-Servers lokalen Clients keine IP-Adresse zugeordnet werden kann. Der Einsatz der Option EXCLUDED NODES bedarf daher sorgfältiger Planung.

DHCP-Dienst in gerouteten Netzen

Ein zwischengeschalteter Router, der sich zwischen dem Segment des DHCP-Clients und dem Segment des DHCP-Servers befindet, unterbindet u. U. die DHCP-Anfrage. Router, die RFC 1542 kompatibel sind, besitzen einen sogenannten DHCP/BOOTP Relay Agenten. Dieser Agent sorgt dafür, dass DHCP Relay Pakete weitergeroutet werden. Bei Routern, die nicht RFC 1542 kompatibel sind, müssen in jedem Netzsegment jeweils eigene DHCP-Server definiert sein. Die Zuteilung einer IP-Adresse durch den DHCP-Server geschieht dann auf dieselbe Art und Weise wie in nicht gerouteten Netzen. Durch die Weiterleitung der DHCP Relay Pakete werden aber nicht automa-

tisch die gesamten Broadcast Pakete weitergeleitet. "Normale" Broadcast Datenpakete werden weiterhin vom Router herausgefiltert.

Einsatz von mehreren DHCP-Servern in Netzen

In Netzen, die über eine entsprechende Größe verfügen, sollte unter Umständen mit mehreren DHCP-Servern gearbeitet werden. Als Lastobergrenze gilt in manchen Betriebssystemen die Verwaltung von 10000 IP-Adressen pro DHCP-Server. Dieser Wert kann vom Netware DHCP-Server um ein Vielfaches überschritten werden. Zudem sollte bei der Überlegung, wie viele DHCP-Server im Netz erforderlich sind, die Position der Router berücksichtigt werden.

Unabhängig von der Struktur des IP-Netzes ist bei Verwendung von mehreren DHCP-Servern unbedingt zu verhindern, dass zwei (oder mehr) Netzknoten, die von verschiedenen DHCP-Servern "versorgt" werden, dieselbe IP-Adresse zugewiesen bekommen. Diese Gefahr besteht, wenn jeder DHCP-Server im Netz (bzw. im Segment) jeweils den gesamten IP-Bereich verwaltet, der für die dynamische Vergabe eingerichtet wurde, da sich die DHCP-Server unter Netware 4.x untereinander nicht synchronisieren. Jeder einzelne DHCP-Server speichert seine Konfigurationsdaten in einer separaten DHCPTAB-Datei. Da diese Datei unter Netware 4.x aber nicht Bestandteil der NDS ist, wird sie auch nicht über deren Replizierungsmechanismen auf andere Server verteilt, bzw. mit anderen DHCPTAB-Dateien abgeglichen. Daher sollte bei Verwendung mehrerer DHCP-Server jedem Server ein eigener IP-Adressbereich zugewiesen werden, den er exklusiv verwaltet.

M 4.104 LDAP Services for NDS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Das Lightweight Directory Access Protocol (LDAP) hat sich zum De-facto-Standard für den Zugriff auf X.500-Standard basierende Verzeichnis-informationen über das Internet/Intranet entwickelt. Die Novell Directory Services (NDS) gehören zu den LDAP Directories, deren Hauptaufgabe darin liegt, eine Vielzahl von Suchoperationen gleichzeitig bearbeiten zu können. Über die NDS ist es dem Administrator möglich, alle Firmenmitarbeiter und alle im Netz verfügbaren Ressourcen als Objekte in einem hierarchischen Verzeichnisbaum anzulegen und zu verwalten. So können z. B. den Benutzern Zugriffsrechte auf Unix-, Microsoft Windows NT-, Novell Netware Server oder anderen Ressourcen wie der Zugriff auf das Mailing-System und Druckern zugewiesen werden. Bisher musste die Information in applikationsspezifischen Listen gepflegt und über die unterschiedlichen Systemgrenzen hinaus konsolidiert werden. Werden verzeichnisfähige Applikationen eingesetzt, so entsteht ein "Single Point of Administration", d. h. die Pflege der Gesamtinformation geschieht von einer Stelle aus.

Alle auf X.500 basierenden Verzeichnisdienste verwenden ein Directory Access Protocol (DAP), um die Verzeichnisinformationen zu synchronisieren und eine Kommunikationsschnittstelle zwischen den unterschiedlichen Netzkomponenten bereitzustellen.

Bei LDAP handelt es sich um ein Directory Access Protocol, dessen Hauptaufgabe die schnelle Informationsextraktion, gestützt auf einen geringeren Protokolloverhead, ist. Es wird nicht der gesamte OSI-Protokollstack implementiert, sondern LDAP setzt direkt auf dem TCP/IP Protokoll auf. Als Folge daraus sind die LDAP Clients weit weniger komplex als die DAP Clients. Da sich die Implementierung von LDAP auf den Internet-Standard RFC 1777 abstützt, sind die Entwickler in der Lage, plattformunabhängige Application Program Interfaces (APIs) zu verwenden. Es muss daher keine Rücksicht auf die herstellerspezifische Notation genommen werden, da der LDAP Server das Umsetzen einer LDAP Anfrage in das erforderliche Format vornimmt.

In den LDAP Services for NDS für Netware 4.11 ist LDAP Version 2 implementiert worden, die sich mit der Client-to-Directory Kommunikation beschäftigt. Die Version 3 von LDAP beinhaltet Spezifikationen zur Directory-to-Directory Kommunikation, wie z. B. die Replikation und die Synchronisation von Verzeichnisinformationen im Netz. Der Standard (RFC 2551) ist aber bisher noch nicht endgültig verabschiedet worden. Eine Implementierung von LDAP Version 3 kommt unter Netware 5 zum Einsatz.

Die LDAP Services for NDS übernehmen eine Mittlerfunktion zwischen der NDS, die natürlich installiert sein muss, und dem LDAP Client. Der Client stellt eine LDAP Anfrage an den Server, auf dem die LDAP Services laufen. Diese Anfrage wird entgegengenommen und von den LDAP Services for

NDS in eine NDS Anfrage umgewandelt. Die NDS wertet die Anfrage aus und liefert die angeforderten Informationen an die LDAP Services for NDS zurück. Diese wiederum generieren aus der NDS Antwort eine LDAP Antwort und leiten diese an den Client weiter.

Novell selbst bietet keinen LDAP Client an. Die gebräuchlichsten Clients sind derzeit Browser, wie z. B. der Netscape Communicator, die eine entsprechende LDAP Schnittstelle haben. Es gibt aber auch andere, frei verfügbare LDAP Clients im Internet. Dabei sind jedoch vor dem Einsatz dieser Clients einige Dinge zu beachten. So ist zum Beispiel der Netscape Communicator nicht in der Lage, Zugriffe auf LDAP Server zu gewähren, die einen Benutzernamen und ein Passwort erfordern. Daher erkennen die LDAP Services for NDS einen Benutzer, der diesen Browser als Client verwendet, als Anonymous User und machen ihn standardmäßig zum Trustee von [Public], was typischerweise nur ein Browse-Recht auf die NDS beinhaltet. Wenn zusätzliche Rechte benötigt werden, so ist ein Proxy User einzurichten, der über die entsprechenden NDS Rechte verfügt. Zusätzlich muss im LDAP Group Objekt noch das Proxy User Feature freigegeben werden.

Da die LDAP Services for NDS vollständig in die NDS integriert sind, muss bei der Installation eine Erweiterung des NDS Schemas vorgenommen werden. Dies kann nur über einen Account mit Supervisor Berechtigung auf das [Root] Objekt erfolgen. Bei der Installation des ersten LDAP Servers in einem NDS Baum wird das Datenbankschema der NDS erweitert, sodass die zwei neuen NDS Objekte *LDAP Server* und *LDAP Group* zur Verfügung stehen. Über diese beiden Objekte werden die LDAP Services for NDS konfiguriert. Werden weitere LDAP Server in diesem NDS Baum installiert, so ist es nicht notwendig, die Schemaerweiterung noch einmal zu installieren, da die NDS bereits das aktuelle Datenbankschema besitzt.

Die Konfiguration der LDAP Services for NDS wird über die Eigenschaften ("Properties") der beiden Objekte *LDAP Server* und *LDAP Group* festgelegt. Die Einstellung ist anhand der erarbeiteten Sicherheitsstrategie vorzunehmen. Im folgenden wird auf einige Properties eingegangen, die im Hinblick auf die Sicherheit des Systems besonders relevant sind.

Log file size limit (*LDAP Server* Objekt)

Mit dieser Property kann die maximale Größe der in der Property *Log filename* angegebenen Log-Datei eingerichtet werden. Erreicht die Log-Datei die festgelegte Dateigröße, so werden die Informationen der *Log filename* Datei in die unter *Backup log file* angegebene Datei kopiert. Alle neuen Log-Daten werden in die *Log filename* Datei geschrieben.

Default: 1.000.000

Minimum: 0 (unbegrenzte Dateigröße)

Maximum: 4.294.967.295

Wird der Wert auf Null gesetzt, so besteht keine Größenlimitation für die Log-Datei. In diesem Fall sollte man die Datei nicht auf dem Volume SYS ablegen, da die Datei so stark anwachsen kann, dass der verfügbare Speicherplatz auf dem Volume komplett belegt wird. Als Folge können

Inkonsistenzen innerhalb der NDS auftreten, und die Verfügbarkeit des Servers wird reduziert.

Im *LDAP Group* Objekt sind die folgenden Properties besonders sicherheitsrelevant:

Suffix

Über das Feld *Suffix* wird der Unterbaum definiert, der den LDAP Clients zur Verfügung gestellt wird. Ist dieses Feld leer, so wird den Clients Zugriff auf den gesamten NDS Baum gewährt, also vom [Root] Objekt aus. Stellt ein Client eine Anfrage an den Server, die sich auf ein Objekt außerhalb des definierten Unterbaums bezieht, so wird ein Fehler zurückgegeben, außer das Feld *Referral* ist mit einem Wert belegt worden.

Referral

In dieses Textfeld kann ein Uniform Resource Locator (URL) eines alternativen LDAP Servers eingetragen werden. Stellt z. B. ein Client eine Anfrage an den Server, die dieser nicht beantworten kann, da das *Suffix* gesetzt wurde, so wird diese URL an den LDAP Client zurückgeliefert. Der Client ist nun in der Lage, seine Anfrage an diesen Server weiterzuleiten.

Enable NDS User Bind

Ist diese Checkbox aktiviert, so muss sich ein Benutzer bei einem Bind Request mit seinem NDS Passwort authentisieren. Die Passwörter werden jedoch zwischen dem LDAP Client und dem LDAP Server nicht verschlüsselt, d. h. sie werden im Klartext über das Netz übertragen. Durch einen geeigneten Netzmonitor (Lanalyzer) ist deshalb ein Angreifer in der Lage, auf diese Weise Passwörter auszuspionieren. Aus Sicherheitsgründen sollte dieser Wert nicht gesetzt werden, außer man verwendet Accounts, die speziell für LDAP Zugriffe eingerichtet worden sind und ansonsten keine weiteren Rechte in der NDS und auf das Netware Dateisystem haben.

Proxy Username

Beim Proxy User handelt es sich um einen NDS Account, der kein Passwort und auch keine Passwortänderung benötigt. Wird ein Anonymous Bind (Verbindungsaufbau ohne Benutzername und Passwort) angefordert, so authentisiert der LDAP Server diese Anforderung mit dem *Proxy Username* in der NDS. Typischerweise sind diese Proxy User in ihren Rechten stark eingeschränkt. Ist aber kein *Proxy Username* definiert worden, so werden diese Anonymous Binds als Benutzer [Public] validiert und erhalten daher auch die entsprechenden Rechte.

Über die Access Control Page erhalten die LDAP Services for NDS ein zusätzliches Sicherheitsfeature, die **Access Control List** (ACL). Die LDAP ACL definiert die Zugriffsrechte auf die LDAP Objekt Properties für Benutzer und Gruppen. Der LDAP Server benutzt die ACL um festzustellen, ob eine Benutzeranfrage an die NDS weitergereicht oder zurückgewiesen wird. Hat ein Benutzer die entsprechenden Rechte, so wird die Anfrage an die NDS weitergereicht. Die NDS ihrerseits prüft, basierend auf den NDS Rechten, ob die Anfrage bearbeitet oder zurückgewiesen wird.

Über das LDAP ACL Dialogfenster können den Benutzern Rechte zugewiesen werden. Dabei sind folgende Abstufungen möglich:

None

Ist diese Option aktiviert, erhält der Benutzer keinerlei Rechte auf den NDS Baum.

Search

Dieses Recht erlaubt dem Benutzer, nach LDAP Objekt Properties zu suchen. Diese müssen aber in der *Access To* Liste definiert sein. Über den Add Button können Properties explizit freigegeben werden.

Compare

Über dieses Recht wird es dem Benutzer erlaubt, LDAP Objekt Property Werte mit den korrespondierenden NDS Objekt Property Werten zu vergleichen.

Read

Besitzt ein Benutzer das *Read* Recht, so ist es ihm erlaubt, die in der *Access To* Liste definierten LDAP Property Werte zu sehen. Das *Read* Recht umfasst das *Search* und das *Compare* Recht.

Write

Besitzt ein Benutzer das *Write* Recht, so kann er die in der *Access To* Liste definierten LDAP Property Werte schreiben. Das *Write* Recht umfasst das *Search*, *Compare* und *Read* Recht.

Neben diesen fünf Sicherheitsstufen im Zugriff (Access Level) lässt sich der Zugriff noch weiter einschränken. Z. B. kann durch das Feld *IP Address* erzwungen werden, dass eine Anfrage nur von einer oder einer Gruppe von IP-Adressen akzeptiert wird.

M 4.105 Erste Maßnahmen nach einer Unix-Standardinstallation

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die meisten Unix-Systeme entsprechen nach einer Standardinstallation nicht den Anforderungen an einen sicheren Systembetrieb. Hier werden von den Herstellern häufig zu viele sicherheitskritische Dienste und Konfigurationen aktiviert bzw. mit zu weitreichenden Rechten versehen.

Die folgende Übersicht soll exemplarisch das erste Absichern einer Standardinstallation aufzeigen:

- Vor der Installation ist der Administrator entsprechend zu schulen, insbesondere hinsichtlich der Sicherheitsaspekte. In diesem Rahmen sollte er sich über alle potentiellen Sicherheitslücken des IT-Systems kundig machen (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*). Dazu gehört auch die Subskription entsprechender Mailinglisten.
- Nach der Installation sollte das Account des Systemadministrators ein gutes Passwort erhalten (siehe M 2.11 *Regelung des Passwortgebrauchs*).
- Es sollte überprüft werden, welche Dienste auf dem IT-System laufen. Dies kann z. B. mit dem Befehl *netstat -a | grep LISTEN* überprüft werden. Nicht benötigte Dienste sollten deaktiviert oder entfernt werden (siehe M 5.72 *Deaktivieren nicht benötigter Netzdienste*).
- Wenn das System nicht als Mailserver fungiert, sollte der Maildaemon als Netzdienst deaktiviert werden. Wenn Mail **lokal** auf dem System zugestellt werden soll, kann sendmail mit der Option *-q15* oder als Cron-Prozess gestartet werden:

  ```
  1 * * * * /usr/sbin/sendmail -q 2>&1 >/dev/null
  ```

  Die Mail-Queue wird in regelmäßigen Abständen geleert und die Mail lokal zugestellt.
- Die aktuellste *sendmail*-Version des Herstellers sollte installiert werden (siehe auch M 4.107 *Nutzung von Hersteller-Ressourcen* und M 5.19 *Einsatz der Sicherheitsmechanismen von sendmail*). Alternativ kann auch auf Public-Domain-Mailprogramme wie z. B. *qmail* zurückgegriffen werden. Die laufende *sendmail*-Version kann mit dem Befehl *telnet localhost 25* herausgefunden werden.
- Nach der Standardinstallation sollten die verfügbaren Security-Patches des Herstellers installiert werden (siehe auch M 4.107 *Nutzung von Hersteller-Ressourcen*). Danach ist unbedingt zu überprüfen, dass durch die Patch-Installation keine nichtbenötigten Dienste aktiviert wurden.
- Die Filesysteme sollten restriktiv im- bzw. exportiert werden. Es ist darauf zu achten, dass Filesysteme nicht für alle schreibbar exportiert werden.
- Wenn zum Einsatz von *NIS* keine Alternativen existieren, sollte *NIS+* eingesetzt werden, das über erweiterte Sicherheitsmechanismen verfügt.

- Wenn *tftp* verfügbar sein muss, dann sollte es mit der Option *-s* gestartet werden, damit nicht jede Datei vom System kopiert werden kann (siehe auch M 5.21 *Sicherer Einsatz von telnet, ftp, tftp und rexec* und M 5.72 *Deaktivieren nicht benötigter Netzdienste*).
- Die Protokollierungsfunktion des *inetd* sollte mit *-t* aktiviert werden, damit jeder Verbindungsaufbauversuch protokolliert wird (siehe M 5.72 *Deaktivieren nicht benötigter Netzdienste*). Hilfreich ist die Installation der Public-Domain-Tools *xinetd* oder TCP-Wrapper. Mit diesen Tools können u. a. alle Verbindungsversuche frühzeitig protokolliert werden, noch bevor der angesprochene Daemon via *inetd* gestartet wird.
- Protokolldateien sollten täglich bzw. wöchentlich untersucht werden. Zur halb-automatischen Auswertung sollten Analyseprogramme wie *swatch*, *logdaemon* oder *logsurfer* installiert werden (siehe M 2.64 *Kontrolle der Protokolldateien*).
- Regelmäßig sollten Sicherheitschecks mit *COPS*, *Tripwire* oder *Tiger* durchgeführt werden.
- Neben allen anderen nicht benötigten Diensten sollten *rshd*, *rlogind*, *rexecd* unbedingt deaktiviert werden (siehe M 5.72 *Deaktivieren nicht benötigter Netzdienste*). Zur Konvertierung von RPC-Programmnummern in Portadressen wird von den meisten Herstellern das Programm *rpcbind* mit ausgeliefert. Als Ergänzung bzw. als Ersatz sollte der Daemon *portmapper* eingesetzt werden, wenn er für die vorliegende Plattform verfügbar ist.

  Alle Clients, die diese Dienste benutzen, sollten für normale Anwender nicht ausführbar gemacht werden. Weitere Authentisierungsverfahren, die auf Hostnamen beruhen, sollten vollkommen abgelöst werden.
- *Telnet* sollte durch *ssh* ersetzt werden. *ssh* ermöglicht eine stark verschlüsselte und authentisierte interaktive Verbindung zwischen zwei Systemen. *ssh* ist als Ersatz für *telnet*, *rsh*, *rlogin* und *rcp* zu verstehen. X-Windows kann dadurch auch abgesichert übertragen werden (siehe auch M 5.64 *Secure Shell*).
- *Xauth* ist *xhost* vorzuziehen - es sollte niemals "xhost +" verwendet werden (siehe auch M 4.9 *Einsatz der Sicherheitsmechanismen von X-Windows*).
- Aus der Konfigurationsdatei */etc/inetd.conf* sollten alle nicht benötigten Einträge entfernt werden (siehe M 5.72 *Deaktivieren nicht benötigter Netzdienste*,).
- Die Konfigurationsdatei */etc/syslog.conf* ist für die Aktivierung der Protokollfunktionen zu modifizieren (siehe M 4.106 *Aktivieren der Systemprotokollierung*).
- Eine Liste aller world-writable Dateien und Verzeichnisse kann mit folgenden Befehlen erstellt werden:

  ```
  find / -type f -perm -22 -exec ls -l {} \;

  find / -type d -perm -22 -exec ls -ld {} \;
  ```

Die Ergebnisse sollten regelmäßig mit dem Installationszustand verglichen werden.

- Das Programm *Tripwire* sollte vor der Inbetriebnahme installiert werden, um eine Checksummenübersicht des installierten Systems bei der Aufnahme in den Wirkbetrieb zu bekommen. Die erstellte Übersicht sollte auf einem nichtbeschreibbaren Datenträger gespeichert werden.
- */var* sollte eine große Partition sein, damit ein vorsätzliches Produzieren von Protokolldaten das Unix-System nicht zum Stillstand bringt.

Alle durchgeführten Veränderungen sollten sorgfältig dokumentiert werden und unter allen Systemadministratoren abgestimmt werden. Diese Dokumentation kann in Papierform erfolgen oder in einer Datei auf dem jeweiligen System geführt werden. Sie sollte aber jederzeit eingesehen und aktualisiert werden können (siehe auch M 2.34 *Dokumentation der Veränderungen an einem bestehenden System*).

Ergänzende Kontrollfragen:

- Welche Dienste laufen auf dem IT-System?
- Sind alle verfügbaren Security-Patches ordnungsgemäß installiert?
- Werden alle Änderungen zeitnah dokumentiert und unter allen Systemadministratoren abgestimmt?
- Sind alle vorgenommenen Änderungen an der Betriebssystemkonfiguration dokumentiert und nach einer Neuinstallation nachvollziehbar?

M 4.106 Aktivieren der Systemprotokollierung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die systemeigene Unix-Protokollierung *syslog* dient dem Festhalten von Informationen, die vom Betriebssystem oder von Anwendungsprozessen generiert werden. Sicherheitsrelevante Ereignisse, wie versuchte Anmeldung bzw. Ausführung des Befehls *su* sollten unbedingt protokolliert werden und einer späteren Auswertung zur Verfügung stehen.

Der erforderliche Daemon *syslogd* wird in der Regel automatisch gestartet und über die Datei */etc/syslog.conf* konfiguriert. Durch geeignete Rechtevergabe muss sichergestellt werden, dass nur Systemadministratoren diese Datei ändern können und dass die Protokolldateien in */var/log* und */var/adm* nur von Systemadministratoren gelesen werden können. Alle Änderungen an */etc/syslog.conf* sind zu dokumentieren. Bei der Anpassung an das vorliegende IT-System sollte zunächst alles protokolliert werden, danach können bei Bedarf stufenweise einzelne Bereiche deaktiviert werden. Durch eine ausreichende Dimensionierung der */var*-Partition ist sicherzustellen, dass ausreichend Platz für die Protokolldateien zur Verfügung steht. Das folgende Beispiel für eine Konfigurationsdatei ist in Anlehnung an eine SunOS-Konfiguration erstellt worden und definiert eine ausführliche Protokollierung in verschiedenen Dateien.

```
#ident  "@(#)syslog.conf        1.3     93/12/09 SMI"   /* SunOS 5.0 */
#
# Alle Meldungen werden zu einem Loghost geschickt, der in der Datei
# /etc/hosts definiert werden muss.
#
# Es muss TAB als Separator verwendet werden!
#
# Test: . syslogd mit der Option "-d" starten
#       . syslogd mit kill -HUP nach jeder Änderung dieser Datei starten
#       . die Logdatei muss vor dem Start/Neustart bereits existieren
#       . mit/usr/ucb/logger können Testmeldungen für jede facility
#         und priority generiert werden
#
*.err;kern.warning;auth.err;daemon.err          /dev/console
*.alert;kern.err;daemon.err                     operator
*.alert                                 root
# zeigt emerg-Meldungen auf Terminals an (verwendet WALL)
*.emerg                 *
```

```
#
kern.info           ifdef(`LOGHOST', /var/log/kernlog, @loghost)
user.info           ifdef(`LOGHOST', /var/log/userlog, @loghost)
mail.info           ifdef(`LOGHOST', /var/log/maillog, @loghost)
daemon.info         ifdef(`LOGHOST', /var/log/daemonlog, @loghost)
auth.info           ifdef(`LOGHOST', /var/log/authlog, @loghost)
lpr.info            ifdef(`LOGHOST', /var/log/lprlog, @loghost)
news,uucp.info      ifdef(`LOGHOST', /var/log/newslog, @loghost)
cron.info           ifdef(`LOGHOST', /var/log/cronlog, @loghost)
#

## alle anderen "local" Nachrichten, für eigene Programme
local0,local1.info          ifdef(`LOGHOST', /var/log/locallog, @loghost)
local2,local3,local4.info   ifdef(`LOGHOST', /var/log/locallog, @loghost)
local5,local6,local7.info   ifdef(`LOGHOST', /var/log/locallog, @loghost)

#
# alle Alarme und höher werden in eine separate Datei geschrieben:
*.err           ifdef(`LOGHOST', /var/log/alertlog, @loghost)

#
# Beispiel Log levels:
# ------------------------------------
# 'su root' failed for ..       auth.err
# ROOT LOGIN REFUSED ON ...     auth.err
# 'su root' succeeded for..     auth.notice
```

Ergänzende Kontrollfragen:

- Sind die Änderungen in */etc/syslog.conf* dokumentiert worden?
- Ist sichergestellt, dass nur der Systemadministrator die Konfiguration ändern darf?
- Ist sichergestellt, dass die Protokolldateien in */var/log* bzw. */var/adm* nur für den Systemadministrator lesbar sind?

M 4.107 Nutzung von Hersteller-Ressourcen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Alle Hersteller von IT-Systemen oder IT-Komponenten bieten diverse Unterstützungs- und Informationsangebote für die Anwender ihrer Produkte. Dazu gehören beispielsweise Hilfestellungen zur Problembehebung (Support, Hotline, Updates, Patches, etc.) und Informationsmöglichkeiten über Sicherheitslösungen (WWW-Seiten, Newsgroups, Mailinglisten, etc.). Einige dieser Angebote sind kostenfrei, andere nicht.

Bereits bei der Beschaffung von IT-Systemen oder -Produkten sollte überlegt werden, welche Unterstützungsangebote der Hersteller in Anspruch genommen werden sollen, insbesondere wenn dies laufende Kosten verursacht.

Es sollte sichergestellt sein, dass für **alle** eingesetzten IT-Systeme und -Produkte regelmäßig überprüft wird, ob neue Informationen über Sicherheitsprobleme und Lösungsmöglichkeiten seitens der Hersteller vorhanden sind. Dies ist besonders bei allen Server-Betriebssystemen wichtig, da eine Sicherheitslücke auf einem Server wesentlich mehr Schäden verursachen kann als eine, die nur ein einzelnes IT-System betrifft.

Sicherheitsspezifische Updates sollten, wenn sie nicht direkt vom Hersteller auf CD-ROM geliefert werden, nur von vertrauenswürdigen Stellen bezogen werden, z. B. von CERTs (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*). Die Updates sind auf Unversehrtheit mittels kryptographischer Methoden (beispielsweise SHA-1, RIPEMD-160, GnuPG) zu überprüfen, soweit die Dateien entsprechend verschlüsselt bzw. signiert angeboten werden.

Damit jederzeit auf sicherheitsrelevante Hinweise der Hersteller zugegriffen werden kann, sollte für alle eingesetzten Betriebssysteme und alle wichtigen IT-Produkte eine Übersicht geführt werden. Aus dieser sollte hervorgehen, unter welchen WWW-Adressen sicherheitsspezifische Updates und Patches bzw. Informationen der Hersteller gefunden werden können. Die Adressen sind in der Produktdokumentation zu finden. Sehr oft wird auf der WWW-Seite des Herstellers direkt auf diese Informationen verwiesen. Leider verändern sich Links erfahrungsgemäß häufig, so dass es wichtig ist, diese regelmäßig auf ihre Korrektheit zu überprüfen und, wenn es erforderlich ist, zu aktualisieren.

Ergänzende Kontrollfragen:

- Woher werden Hersteller-Patches bezogen?
- Wie ist sichergestellt, dass immer die Informationen über die aktuellsten Patches vorliegen?
- Wie wird der Patch-Level-Stand der Systeme verifiziert?
- Wird die Integrität der Patches kryptographisch verifiziert?

M 4.108 Vereinfachtes und sicheres Netzmanagement mit DNS Services unter Novell NetWare 4.11

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Verknüpfung zwischen IP-Adressen und Hostnamen

Jedem IT-System in einem TCP/IP-Netz muss eine eindeutige Adresse zugewiesen werden. Das Internet Protocol (IP) beschreibt diese Adresse als vier Dezimalzahlen getrennt durch einen Punkt, mit jeweils einem Wertebereich von 0-255. Da sich numerische Adressen schwer merken lassen, können den IT-Systemen zusätzlich erklärende Hostnamen, z. B. *www.bsi.bund.de*, zugewiesen werden. Die Auflösung von Hostnamen in IP-Adressen kann über zwei Mechanismen durchgeführt werden. Zum einen kann eine ASCII-Textdatei namens HOSTS, die im SYS:ETC Verzeichnis abgelegt wird, manuell erstellt werden. Diese Methode sollte unter sicherheitstechnischen und administrativen Gesichtspunkten nur in kleinen Netzen angewandt werden, da diese Datei individuell auf jedem Server und jeder Workstation abgelegt werden muss, um eine lokale Auflösung zu ermöglichen. Durch spezielle Routinen (z. B. Login Scripts) kann die Verteilung der HOSTS Datei automatisiert werden.

Der zweite Mechanismus ist die Nutzung eines DNS-Servers. Im folgenden werden einige Aspekte der Einrichtung und Konfiguration eines DNS-Servers unter Novell NetWare 4.11 betrachtet, die im Hinblick auf die Sicherheit des Systems besonders zu beachten sind.

Funktion der DNS-Komponenten

Die zwei Hauptbestandteile von DNS sind zum einen der *Nameserver*, zum anderen der *Resolver*, der auf dem Client geladen wird und die Anfragen an den Nameserver stellt.

- **Primärer Nameserver**

  ein primärer Nameserver pro Zone

  Er erhält die DNS-Einträge für die Zonen, für die er autorisiert ist, aus einer Datei auf seiner Festplatte. Autorisiert bedeutet, dass der primäre Nameserver die DNS-Information nicht mit einem weiteren Nameserver der Zone gegenprüfen muss. Der primäre Nameserver ist gleichzeitig auch der *Single Point of Administration* für die Domäne. Es existiert nur ein primärer Nameserver für jede Zone.

- **Sekundärer Nameserver**

  Lastverteilung, Reduzierung des Netzverkehrs und Redundanz

  Dieser Server besitzt eine schreibgeschützte Kopie der DNS-Datenbank des primären Nameservers. Aktualisiert wird diese Kopie in einem definierten Zeitraum, der in dem Record Typ SOA (Start of Authority) festgelegt wird. Record Typen definieren die *Resource Records*, die die Einträge in der DNS-Datenbank bilden. Der Kopiervorgang wird Zonentransfer genannt und bildet die Grundlage für die Aktualisierung der verteilten DNS-Datenbank einer Domäne. Sekundäre Nameserver übernehmen Aufgaben der Lastenverteilung, bieten die Möglichkeit, die DNS-Datenbank in der Nähe der Resolver zur Verfügung zu stellen, und schaffen die Redundanz der DNS-Domäneninformation. Mindestens ein sekundärer

Nameserver sollte aus Gründen der Ausfallsicherheit für jede Zone eingerichtet werden.

- **Resolver**

  Der Resolver ist die Software, die DNS-Anfragen an einen der definierten Nameserver sendet. Dabei kann ein Nameserver, der die Namensauflösung nicht durchführen kann, ebenfalls zum Resolver werden und die Anfrage an einen Nameserver außerhalb der Domäne senden. Der Resolver übernimmt ebenfalls die Interpretation der Antworten des Nameservers und gibt Informationen an die Programme zurück, die diese angefordert haben.

Anfragen an den DNS-Server und Interpretation der Antworten

Einrichten des DNS-Servers

DNS wird bei einem NetWare 4.11 Server über UNICON.NLM eingerichtet. Zunächst wird über *Manage Global Objects* unter *Configure Server Profile* der *DNS Client Access* aktiviert. Es muss zumindest ein Nameserver aufgeführt werden, der die Adressauflösung durchführt. Maximal können drei Nameserver eingetragen werden. Damit ein großer Adressbereich schneller erfasst werden kann und es sichergestellt ist, dass die Namensauflösung durchgeführt werden kann, sollten die Angaben für die drei Nameserver ausgeschöpft werden. Die Reihenfolge der Nameserver bestimmt die Abfragereihenfolge und sollte im Hinblick auf die Geschwindigkeit der Namensauflösung festgelegt werden.

drei Nameserver eintragen

Der erste Nameserver kann der Haupt-DNS-Server der Behörde bzw. des Unternehmens sein. Auch wenn dieser Server nicht jeden Host außerhalb der eigenen Domäne adressieren kann, bietet er die Möglichkeit, die Auflösung von Hostnamen innerhalb der Organisation schnell durchführen zu können.

Der zweite Nameserver kann der des Internet Service Providers (ISP) sein, um Zugang zu einem umfangreicheren Datenbestand an Hostnamen zu bekommen. Die Auflösungsgeschwindigkeit wird dabei durch die höhere Auslastung, die Entfernung sowie die zur Verfügung stehende Bandbreite meist etwas geringer sein als beim lokalen Nameserver. Hat die Redundanz der eigenen Domäne Priorität, so sollte der Server mit der schreibgeschützten Kopie der DNS-Datenbank (sekundärer Nameserver) als zweiter Nameserver eingetragen werden.

Der dritte definierte Nameserver kann ein sogenannter *Root Server* sein. Auf diesen Servern sind die Daten aller registrierten Domänen abgelegt. Eine Liste der Root Server kann unter *ftp://rs.internic.net/netinfo/root-servers.txt* abgerufen werden.

Konfiguration der DNS-Server

Im Hauptmenü von UNICON.NLM gelangt man über *Manage Services* und *DNS* zu den Konfigurations- und Administrationsfunktionen für das Domain Name System. Der Menüpunkt *Administer DNS* erlaubt sowohl das Einrichten einer Master Database als auch einer schreibgeschützten Replica Database.

Die Domänen bzw. Zonen, für die der primäre Nameserver autorisiert ist, werden im Hauptmenü von UNICON.NLM über *Manage Services - DNS - Administer DNS - Manage Master Database - Delegate Subzone Authority* eingegeben.

alle sekundären Nameserver in die Datenbank eintragen

Über *Manage Services - DNS - Administer DNS - Manage Master Database* werden die DNS-Datenbankeinträge eingegeben. Bei einer Standard Implementation von DNS müssen der *Start of Authority* (SOA), der den Beginn für die Autorität einer Zone innerhalb der DNS-Hierarchie kennzeichnet, und der Record Typ *Name Server* (NS) eingetragen werden. Der primäre Nameserver muss Einträge für alle sekundären Nameserver der Zone enthalten. Die Verbindung dieser Zone zur DNS-Hierarchie wird durch Nameserver Einträge für primäre Nameserver, die Autorität für übergeordnete oder untergeordnete Zonen besitzen, sichergestellt. Damit die Namensauflösung für die Hosts in der Zone gewährleistet ist, muss für jedes zu adressierende Endgerät der Record Typ *Address* (A) eingetragen werden.

Innerhalb des Record Typ SOA werden unter anderem der Name und die Adresse des Zonen-Verantwortlichen (*Zone Supervisor)* eingetragen. Standardmäßig ist diese Adresse auf root.<domain_name> gesetzt. Weiterhin werden im Record Typ SOA die Einstellungen für das Synchronisationsverhalten der sekundären Nameserver getroffen.

Refresh Validity Period bestimmt die Zeit, innerhalb der ein sekundärer Nameserver noch Anfragen von Hosts beantwortet, nachdem er vergeblich versucht hat, den primären Nameserver zu kontaktieren. Je kürzer diese Zeit eingestellt ist, desto geringer ist die Wahrscheinlichkeit, dass der sekundäre Nameserver ungültige DNS-Einträge verschickt und so keine Namensauflösung möglich ist. Aus Gründen der Ausfallsicherheit sollte diese Zeit nicht zu kurz eingestellt werden, da bei einem Ausfall des primären Nameservers das Domain Name System für diese Zone dann nicht mehr funktioniert. Für diesen Parameter muss ein Kompromiss gefunden werden zwischen der Wahrscheinlichkeit, einzelne Hostnamen nicht auflösen zu können, oder - bei zu kurzer Periode - keine Endgeräte über individuelle Hostnamen ansprechen zu können.

Das *Minimum Caching Interval* bestimmt die Zeit, in der Informationen aus Anfragen im Cache des primären Nameserver gehalten werden. Wird diese Einstellung zu kurz gewählt, kann dies die Netzlast bei häufigen Anfragen nach denselben Hosts erhöhen und die Auflösung der Hostnamen in IP-Adressen verzögern. Auf der anderen Seite kann ein zu großer Wert für das *Minimum Caching Interval* dazu führen, dass veraltete Informationen weitergegeben werden.

Verbindung zur externen DNS-Hierarchie

Querverbindungen zur Beschleunigung der Namensauflösung

Anfragen über Hostadressen außerhalb der eigenen Domäne werden automatisch durchgeführt, sobald der DNS-Server läuft. Informationen über die DNS-Hierarchie erhält der DNS-Server aus der Datei SYS:ETC\DNS\ROOT.DB, die eine Liste über Nameserver der US Top Level Domänen enthält. Unter dem Menüpunkt *Manage Services - DNS - Administer DNS - Link to existing DNS Hierarchy* kann über zwei verschiedene Methoden, nämlich *Link Direct* und *Link Indirect via Forwarder*, eine Querverbindung zu anderen Domänen aufgebaut werden. Wird häufig auf bestimmte Domänen zugegriffen, kann über diese Verfahren die Auflösung der Hostnamen beschleunigt werden.

Prüfen von Nameservern

Mit *Manage Services - DNS - Administer DNS - Query Remote Name Server* kann zum einen überprüft werden, welche Informationen auf anderen Nameservern abgelegt sind, und zum anderen ist es möglich festzustellen, ob ein bestimmter Nameserver auf Anfragen antwortet. Dabei muss der Name bzw. die IP-Adresse des Servers angegeben werden. Ebenso ist der Resource Record Type, der abgefragt wird, und die Domäne, aus der die Information benötigt wird, anzugeben.

Backup der DNS-Datenbank

Regelmäßig sollte ein Backup der DNS-Datenbank angelegt werden. Dieses Backup kann beispielsweise verwendet werden, um

- eine unbrauchbar gewordene DNS-Datenbank wiederherzustellen,
- die Datenbank auf einen anderen Server zu verschieben.

Über *Manage Services - DNS - Save DNS Master to Text Files* wird die Datenbank in *SYS:ETC/DBSOURCE/DNS/HOSTS* abgelegt.

Verwendung von UNICON.NLM

Zugriffsbeschränkungen vornehmen

Mit UNICON werden u. a. die Einstellungen für das Domain Name System getroffen. Aus administrativen und sicherheitstechnischen Gesichtspunkten ist es unter Umständen erforderlich, eine Aufgabenverteilung und Zugriffsbeschränkung vorzunehmen. Bei der Installation eines NetWare Produktes, das über UNICON gesteuert wird, werden im NDS-Verzeichnisbaum Gruppenobjekte angelegt, die bestimmte Aufgabenbereiche innerhalb von UNICON regeln. Benutzer, die bestimmte Aufgaben mit UNICON durchführen sollen, werden der jeweiligen Gruppe als Mitglied zugefügt.

Gruppenname	Verantwortungsbereich	Zugängliche UNICON Menü Optionen
UNICON MANAGER	Voller Umfang von UNICON	Zugang zu allen Menü Optionen
UNICON SERVICES MANAGER	Starten, Anhalten und Verwalten der Services	Start/Stop Services und Manage Services
UNICON HOST MANAGER	Verändern von Host Einträgen	Manage Global Objects - Manage Hosts

Tabelle: Kompatibilität mit *bind* (Berkeley Internet Name Domain)

TCP/IP-Netze entwickelten sich aus der Unix-Umgebung heraus. Das am weitesten verbreitete DNS-Programm für Unix ist *bind*. Deshalb ist es wichtig, dass andere DNS-Produkte auf *bind* abgestimmt sind. Der DNS-Service von Novell ist mit der *bind*-Version 4.8.3 voll kompatibel.

M 4.109 Software-Reinstallation bei Arbeitsplatzrechnern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Bei Arbeitsplatzrechnern kann es häufiger zu Problemen mit dem Betriebssystem oder den Anwendungen kommen, die nur durch den Benutzersupport wieder behoben werden können. Dies kann z. B. durch Softwarefehler, Konfigurationsänderungen, Aufspielen neuer Software oder Computer-Viren verursacht werden.

Standardkonfiguration wiederherstellen

Damit die Administratoren bei den oben beschriebenen Problemen auf den Benutzerrechnern nicht zeitaufwendig nach Fehlern suchen müssen, sollte eine Software-Reinstallation der Standardkonfiguration vorgenommen werden.

Identifikation des IT-Systems

Dafür muss zunächst der Rechner eindeutig identifiziert werden und dann über eine entsprechende Dokumentation oder ein Programm anhand dieser Identifikation genau ermittelt werden, welche Software in welcher Konfiguration auf genau diesem Rechner installiert werden muss. Dabei ist es hilfreich, wenn sich die Systeme weitestgehend gleichen, zumindest in Bereichen mit ähnlicher Aufgabenstellung.

Es empfiehlt sich, die Festplatte des Arbeitsplatzrechners neu zu formatieren und anschließend die erforderliche Software und Daten neu aufzuspielen.

zeitkritische Reinstallation

Eine Software-Reinstallation kann auf verschiedene Weise durchgeführt werden, so gibt es z. B. spezielle Programme, die eine vorgegebene Konfiguration von einem Server auf den neu zu installierenden Arbeitsplatzrechnern überspielen. Hierbei ist zu beachten, dass solche Arbeiten meist in zweierlei Hinsicht zeitkritisch sind: Die Neueinrichtung sollte möglichst schnell erfolgen können, damit das IT-System wieder verfügbar ist, und das Netz sollte möglichst wenig belastet werden. Dies ist insbesondere bei Schulungsrechnern oder PC-Pools wichtig.

Natürlich kann eine Reinstallation auch "von Hand" vorgenommen werden. Zu diesem Zweck sollte als erstes eine Standardinstallation vorgenommen werden. Im Anschluss daran werden die Besonderheiten der einzelnen Rechner kopiert, wie spezielle Gerätetreiber, andere Konfigurationsdateien oder spezielle Software. Dafür müssen diese allerdings vorkonfiguriert verfügbar sein, z. B. auf dem Netz oder auf mobilen Datenträgern. Ein aktuelles Viren-Suchprogramm muss anschließend zum Einsatz kommen.

Ergänzende Kontrollfrage:

- Wie werden Software-Reinstallationen bei Arbeitsplatzrechnern durchgeführt?

M 4.110 Sichere Installation des RAS-Systems

Verantwortlich für Initiierung: IT-Sicherheitsmanagement-Team, Leiter IT

Verantwortlich für Umsetzung: Administrator

Nachdem im Rahmen organisatorischer Vorarbeiten die zur Realisierung notwendige Hard- und Software beschafft worden ist, müssen die einzelnen Komponenten installiert und betrieben werden. In der Regel kann das RAS-System in Folge nur dann sicher betrieben werden, wenn schon bei der Installation sorgfältig verfahren wird. Voraussetzung für eine sichere Installation ist die Auswahl geeigneter Hard- und Software für den RAS-Zugang (Qualität, Interoperabilität, Konformität zu bestehenden Standards) durch den vorangegangenen Entscheidungsprozess (siehe M 2.186 *Geeignete Auswahl eines RAS-Produktes*). Dies unterstreicht nochmals die Wichtigkeit eines geregelten Entscheidungsprozesses.

Die physikalischen Komponenten eines RAS-Systems bestehen aus herkömmlichen IT-Systemen: meist aus mindestens einem Server und mehreren Clients, Netzkoppelelementen, Modems oder anderen technischen Geräten. Für diese muss die physikalische Sicherheit, wie für alle anderen Komponenten eines Rechnernetzes, gewährleistet werden. Daher sind zunächst die generellen Sicherheitsmaßnahmen für jede dieser Komponenten durchzuführen, wie sie in den jeweiligen Bausteinen beschrieben sind.

Im Rahmen der Installation sollten folgende zusätzliche Punkte Beachtung finden:

- Weder das RAS-System noch Teile davon sollten während der Installationsphase für Benutzer oder fremde Dritte zugreifbar sein. Es sollten also keine Verbindungen zum produktiven LAN und kein Anschluss an TK-Systeme aktiv sein.
- Die Installation ist durch qualifiziertes Personal durchzuführen.
- Die Installation sollte gemäß der RAS-Systemplanung erfolgen.
- Die Installation und Konfiguration ist zu dokumentieren. Dies kann entweder durch eine separate Installationsdokumentation erfolgen, oder aber durch eine Bestätigung, dass die Installation mit den Planungsvorgaben übereinstimmt.

Sorgfältige Dokumentation der Installation

- Ergibt sich im Rahmen der Installation eine Abweichung von den Planungsvorgaben (z. B. geänderte Leitungsführung, zusätzliche Geräte), so sind diese zu dokumentieren und ein begründeter Änderungsvermerk in die Planungsunterlagen zu übernehmen. Diese Dokumentation ist auch im Hinblick auf die Verbesserung zukünftiger Planungen besonders wichtig.
- Das korrekte Funktionieren jeder einzelnen Komponente muss festgestellt werden (z. B. durch Funktionsprüfung bzw. Selbsttest).
- Für jede sicherheitsrelevante Einstellung muss ein Funktionstest der Sicherheitsmechanismen durchgeführt werden. Beispielsweise sollte die Kommunikationsverschlüsselung mittels eines Netzanalysators überprüft werden.

- Das korrekte Funktionieren des Gesamtsystems ist nach Abschluss der Installationsarbeiten zu überprüfen (Abnahme und Freigabe der Installation). In der Regel muss dies durch vorgegebene Abnahmekonfigurationen und nachgestellte Nutzungsszenarien erfolgen. Bei den Tests ist darauf zu achten, dass nur die zum Test befugten Personen Zugriff zum RAS-System erhalten.

Systemtest vor Freigabe

Die Installation eines RAS-Systems sollte mit einer sicheren Anfangskonfiguration abgeschlossen werden, die zunächst nur den berechtigten Administratoren Zugriffe erlaubt (siehe auch M 4.111 *Sichere Konfiguration des RAS-Systems*). Diese überführen das RAS-System dann in einen sicheren Betriebszustand. Ist dieser erreicht, kann der laufende Betrieb aufgenommen werden.

Beispiel:

Unter Windows NT gestaltet sich die Installation von RAS-Server und RAS-Client sehr einfach und weist kaum Unterschiede auf, da der RAS-Dienst von Windows NT sowohl Client- als auch Server-Funktionen enthält.

Für einen RAS-Client unter Windows NT gilt:

- Die Server-Funktionen des RAS-Dienstes müssen deaktiviert werden. Dies erfolgt dadurch, dass auf allen Geräten, die für Remote Access verwendet werden können (z. B. Modem, ISDN-Karte, VPN-Adapter), nur ausgehende Anrufe erlaubt werden. Zu den entsprechenden Dialogfeldern gelangt man über die Optionen *Systemsteuerung, Netzwerk, Dienste, RAS-Dienst, Gerät, Konfigurieren*.
- Für den RAS-Client sind nur die über Remote Access zugelassenen Protokolle freizugeben. Dies geschieht über *Systemsteuerung, Netzwerk, Dienste, RAS-Dienst, Gerät, Netzwerk*.
- Die Eigenschaften einer RAS-Verbindung werden über das DFÜ-Netzwerk von Windows NT festgelegt. Hier sind die gemäß RAS-Sicherheitskonzept notwendigen Parameter einzustellen (z. B. Datenverschlüsselung erforderlich).

Für einen RAS-Server unter Windows NT gilt:

- Die Client-Funktionen des RAS-Dienstes müssen deaktiviert werden. Dies erfolgt dadurch, dass auf allen Geräten, die für Remote Access verwendet werden können, nur eingehende Anrufe erlaubt werden.
- Für den RAS-Server sind nur die über Remote Access zugelassenen Protokolle freizugeben.
- Die gemäß RAS-Sicherheitskonzept notwendigen Parameter für eingehende RAS-Verbindungen sind einzustellen. Dies geschieht über *Systemsteuerung, Netzwerk, Dienste, RAS-Dienst, Gerät, Netzwerk.*
- Die Einwahl sollte nur berechtigten Benutzern gestattet werden. Dies kann mit dem RAS-Manager oder dem Benutzermanager von Windows NT erfolgen.

Ergänzende Kontrollfragen:

- Sind alle Abweichungen von den Planungsvorgaben für das RAS-System in den Planungsunterlagen vermerkt?
- Wurde ein Funktionstest der Sicherheitsmechanismen durchgeführt (z. B. Überprüfen der Kommunikationsverschlüsselung mittels eines Netzanalysators)?

M 4.111 Sichere Konfiguration des RAS-Systems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement-Team

Verantwortlich für Umsetzung: Administrator

Die Funktion und die Sicherheit eines RAS-Systems wird wesentlich durch die eingestellten Konfigurationsparameter bestimmt. Da jedoch ein RAS-System nicht aus nur einer Komponente und deren Konfiguration besteht, ergibt sich naturgemäß eine erhöhte Komplexität für die Gesamtkonfiguration. Aufgrund dieser Komplexität können leicht Konfigurationsfehler entstehen, die die Sicherheit des Gesamtsystems verringern können. Das nicht abgestimmte Ändern eines Konfigurationsparameters bei einer Komponente kann daher im Zusammenspiel mit den anderen Komponenten zu Fehlfunktionen führen. Im Extremfall kann dadurch auch die Sicherheit des LANs beeinträchtigt werden.

Da die Konfiguration eines RAS-Systems in der Regel Veränderungen unterworfen ist (z. B. durch Personaländerungen, neue Nutzungsszenarien, Systemerweiterungen), kann nicht davon ausgegangen werden, dass es genau eine sichere (und statische) Konfiguration gibt, die einmal eingestellt und nie wieder verändert wird. Vielmehr unterliegt die Konfiguration fortschreitenden Versionsänderungen. Es ist Aufgabe der für das RAS-System zuständigen Administratoren, dass jeweils nur sichere Versionen der Systemkonfiguration definiert werden und das System von einer sicheren Konfiguration in die nachfolgende sichere Konfiguration überführt wird.

Generell kann zwischen den folgenden Konfigurationskategorien unterschieden werden:

- Die *Default-Konfiguration* ergibt sich durch die vom Hersteller voreingestellten Werte für die Konfigurationsparameter. Diese ist in der Regel nicht ausreichend sicher und sollte daher nicht verwendet werden.
- Nach der Installation und vor der Inbetriebnahme muss - ausgehend von der Default-Konfiguration - eine sichere *Anfangskonfiguration* durch die Administratoren eingestellt werden. Hier sollten möglichst restriktive Einstellungen gelten, sodass nur die berechtigten Administratoren Veränderungen vornehmen können, um z. B. eine erste Betriebskonfiguration einzustellen, die das geplante Sicherheitskonzept umsetzt.

Voreinstellung muss angepasst werden

- Die sicheren *Betriebskonfigurationen* ergeben sich aus den jeweiligen Konfigurationen im laufenden Betrieb. Hier muss auch regelmäßig überprüft werden, ob neu bekannt gewordene Sicherheitslücken Anpassungen erfordern (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*).
- Schließlich sollten sichere *Notfallkonfigurationen* im Rahmen der Notfallplanung definiert und dokumentiert werden. Sie dienen dazu, auch bei eingeschränkter Betriebsfähigkeit die Sicherheit aufrechtzuerhalten. In der Regel werden durch die Notfallplanung mehrere Notfallsituationen definiert. Es empfiehlt sich, für jede der definierten Situationen eine

adäquate Notfallkonfiguration festzulegen. Im einfachsten Fall besteht die Notfallkonfiguration darin, den Zugang zum RAS-System zu sperren.

Allgemein sollten folgende Punkte bei den gewählten Einstellungen für eine sichere Konfiguration beachtet werden:

- Neben der Konfiguration des RAS-Systems kann auch die Aufteilung des Netzes in Teilnetze zur Zugriffssteuerung dienen. Aus Gründen der IT-Sicherheit kann es daher zweckmäßig sein, so genannte Zugangsnetze (Access-Networks) einzurichten (siehe auch M 5.77 *Bildung von Teilnetzen*).

Einrichtung von Zugangsnetzen

- Die Routing-Einstellungen der für das RAS-System verwendeten Netzkoppelelemente sollte zur restriktiven Steuerung des Netz-Verkehrsflusses eingesetzt werden. Netzpakete dürfen nur auf den erlaubten Verbindungen weitergeleitet werden. Zusätzlich erlauben moderne Netzkoppelelemente das selektive Weiterleiten von Paketen innerhalb erlaubter Netzverbindungen (Paketfilter-Funktion). Auf diese Weise kann z. B. erreicht werden, dass ausschließlich Verbindungsanfragen an den HTTP-Dienst eines Servers weitergeleitet werden.

Routing-Einstellungen

- Das Einschränken des Zugangs zu RAS-Clients ist insbesondere für mobile Rechner schwierig zu realisieren. Bei mobilen RAS-Clients ist es daher besonders wichtig, dass sich die Benutzer strikt an die festgelegten Regelungen halten (z. B. Diebstahlschutz, siehe auch Baustein B 3.203 *Laptop*).

- Die sichere Konfiguration der RAS-Server-Software erfordert, dass die durch die Software angebotenen und im vorliegenden Einsatzszenario sinnvollen Sicherheitseinstellungen auch aktiviert sind und genutzt werden können. Die Nutzung von bestimmten Sicherheitseinstellungen setzt u. U. voraus, dass auch andere Komponenten des RAS-Systems entsprechende Funktionen besitzen bzw. entsprechend konfiguriert werden können. So ist z. B. bei der Nutzung der Rufnummernübertragung (Calling Line Identification Protocol - CLIP) sicherzustellen, dass diese für den gewählten Anschluss auch aktiviert ist. Damit die Benutzer-Identifikation beispielsweise beim Zugriff über das Internet über X.509-Zertifikate erfolgen kann, muss dem RAS-System der Speicherort der Benutzerzertifikate bekannt sein. Dazu muss die RAS-Software entweder externe Authentisierungsserver unterstützen oder eine eigene Zertifikatsverwaltung anbieten.

  Daher sollte vorab überprüft werden, ob alle angebotenen Sicherheitsmechanismen auch genutzt werden können oder ob hierzu andere bzw. zusätzliche Hard- oder Software benötigt wird. Im laufenden Betrieb muss dann regelmäßig die Korrektheit der Einstellungen überprüft werden.

Nutzung vorhandener Sicherheitsmechanismen

- Für die sichere Konfiguration der RAS-Client-Software gelten ähnliche Anforderungen wie für die Server-Software. Zusätzlich ist darauf zu achten, dass zum RAS-Zugang benötigte Passwörter nicht durch die Software gespeichert werden, auch wenn dies vielfach angeboten wird. Wenn dies nicht technisch verhindert werden kann, muss es allen

Client-Konfiguration

Benutzern untersagt werden. Außerdem sollten alle Benutzer über die Problematik aufgeklärt werden.

- Damit Client und Server in sicherer Art und Weise kommunizieren können, ist auf eine konsistente Konfiguration der beteiligten Komponenten zu achten (z. B. beim benutzten Verfahren zur Kommunikationsabsicherung).
- Die sichere und konsistente Konfiguration von Client und Server kann dadurch unterstützt werden, dass eine Standardkonfiguration für RAS-Clients (Hard- und Software) durch das RAS-Konzept festgelegt und durch organisatorische Maßnahmen durchgesetzt wird. Dadurch wird erreicht, dass nur eine feste Anzahl unterschiedlicher Client-Konfigurationen im Einsatz ist. Dies erleichtert die gesamte Konfiguration, insbesondere hilft es aber auch, eine sichere und konsistente Konfiguration aufrechtzuerhalten.

Einrichten von standardisierten IT-Systemen

- Änderungen an der RAS-Systemkonfiguration sollten einem organisatorischen Prozess unterliegen, der sicherstellt, dass das RAS-System nur mit geprüften Konfigurationen aktiviert wird. Alle Änderungen sollten dokumentiert und genehmigt sein. Hinweis: Das Hinzufügen oder Löschen von RAS-Benutzern macht in der Regel keine Änderung der RAS-Systemkonfiguration nötig, da diese Änderungen oft durch die Benutzerverwaltung des Betriebssystems (z. B. RAS unter Windows NT) oder eines Authentisierungsservers (siehe RADIUS, TACACS+) erfolgen.

Änderungsmanagement

- Die RAS-Konfiguration sollte regelmäßig überprüft werden. Dabei ist sicherzustellen, dass alle Vorgaben der RAS-Sicherheitsrichtlinie umgesetzt sind und die Einstellungen keine Schwachstellen aufweisen.

Regelmäßige Prüfung der RAS-Konfiguration

Obwohl RAS-Systeme eine recht einfache Aufgabe übernehmen, gestaltet sich der Aufbau und der Betrieb ähnlich komplex wie z. B. der eines Firewall-Systems. Die hier angeführten Themenbereiche sind daher immer im Rahmen der RAS-Systemplanung und des RAS-Betriebes zu konkretisieren, zu erweitern und anzupassen.

Beispiele:

- Unter Windows NT sollte die Berechtigung zum RAS-Zugriff nach der Installation des RAS-Dienstes beschränkt werden. Dies kann bei Windows NT nur auf Benutzer-Ebene erfolgen, was bei vielen Benutzern nicht mehr effizient über den Benutzermanager zu administrieren ist. Das Werkzeug zur RAS-Administration unter Windows NT erlaubt es hingegen, auch allen Benutzern auf einmal die Einwahlberechtigung zu entziehen.
- Für einen RAS-Server sollte nur das Einwählen erlaubt sein, abgehende Verbindungen vom RAS-Server selbst sind in der Regel nicht notwendig und sollten daher unterbunden werden. Unter Windows NT kann dies über den Eigenschaftsdialog des RAS-Dienstes für jedes Gerät, das für Remote Access geeignet ist (z. B. Modem, ISDN-Karte, VPN-Adapter), konfiguriert werden. Zu den entsprechenden Dialogfeldern gelangt man über *Systemsteuerung, Netzwerk, Dienste, RAS-Dienst, Gerät, Konfigurieren*.

- Bei Verwendung von RAS-Diensten sollten nur die Protokolle über den RAS-Zugang erlaubt werden, die auch tatsächlich notwendig sind. Nicht benötigte Protokolle sind entsprechend zu deaktivieren. Dies geschieht unter Windows NT über *Systemsteuerung, Netzwerk, Dienste, RAS-Dienst, Netzwerk, Servereinstellungen*. Die Konfiguration der benötigten Protokolle muss den Sicherheitsrichtlinien entsprechen, beispielsweise in Bezug auf Authentisierung, Verschlüsselung, IP-Adressbereich, lokaler oder netzweiter Zugriff.

Ergänzende Kontrollfragen:

- Ist die RAS-Client-Software so konfiguriert, dass zum Zugang benutzte Passwörter nicht gespeichert werden?
- Ist eine konsistente Konfiguration aller RAS-Komponenten sichergestellt?
- Wird die RAS-Konfiguration regelmäßig überprüft?

M 4.112 Sicherer Betrieb des RAS-Systems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Voraussetzung für den sicheren Betrieb eines RAS-Systems ist die sichere Installation und Konfiguration der beteiligten Hard- und Software-Komponenten. Die Maßnahmen M 4.110 *Sichere Installation des RAS-Systems* und M 4.111 *Sichere Konfiguration des RAS-Systems* müssen daher vor Inbetriebnahme durchgeführt worden sein. Zusätzlich müssen alle organisatorischen Abläufe definiert und umgesetzt worden sein (z. B. Meldewege und Zuständigkeiten). Weiterhin ist zu beachten, dass die angestrebte Systemsicherheit nur gewährleistet werden kann, wenn auch die physikalische Sicherheit der beteiligten Hardware-Komponenten sichergestellt ist (siehe auch M 4.110 *Sichere Installation des RAS-Systems*).

Die Sicherheit eines RAS-Systems lässt sich grob in drei Bereiche aufteilen:

1. die Sicherheit des RAS-Servers,
2. die Sicherheit der RAS-Clients und
3. die Sicherheit der Datenübertragung.

Kann die gewünschte Sicherheit des RAS-Servers noch durch die Durchsetzung einer lokalen Sicherheitsrichtlinie gesteuert werden, so unterliegt der RAS-Client typischerweise nicht mehr der vollen Kontrolle des für das LAN verantwortlichen IT-Personals. Die Sicherheit der Datenübertragungsmedien entzieht sich in der Regel vollständig der Kontrolle. Aus diesem Grund muss die Absicherung der Kommunikation zwischen Client und Server mit zusätzlichen Mitteln erfolgen.

Im Umfeld des **RAS-Servers** sind folgende Empfehlungen für den sicheren Betrieb zu berücksichtigen:

Überwachung des RAS-Zugangs

- Der RAS-Zugang sollte durch den Einsatz von Protokollierungs- und Management-Werkzeugen einer ständigen Überwachung unterliegen.

regelmäßige Auswertung der Protokolldateien

- Die im Rahmen der Überwachung gesammelten Informationen sollten regelmäßig durch einen geschulten Administrator kontrolliert werden. Er sollte dabei nach Möglichkeit durch eine Software zur Auswertung von Protokollierungsdaten unterstützt werden. Die Bestimmungen des Datenschutzes sind zu beachten (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*).
- Werden Sicherheitsvorfälle festgestellt, so sind sofort die vorher festgelegten Maßnahmen zu ergreifen. Die festgestellten Sicherheitsvorfälle sollten in einem Vorfall-Report dokumentiert werden (siehe dazu auch Baustein B 1.8 *Behandlung von Sicherheitsvorfällen*).
- Damit eine geregelte Benutzer-Authentisierung (z. B. RAS unter Windows NT, RADIUS, TACACS, TACACS+, SECURE-ID) beim RAS-Zugriff möglich ist, muss die Konsistenz der Authentisierungsdaten sichergestellt sein. Dies kann durch zentrale Verwaltung der Daten (Authentisierungsserver) oder durch periodischen Abgleich geschehen.

- Für **jede** Verbindungsaufnahme ist immer die Benutzer-Authentisierung über den gewählten Mechanismus durchzuführen. Insbesondere ist die alleinige Nutzung des CLIP-Mechanismus (Rufnummernübertragung) zur Authentisierung nicht ausreichend.
- Für **jede** Verbindung sollte die Absicherung der Kommunikation durch eines der im RAS-Sicherheitskonzept erlaubten Verfahren erzwungen werden, damit die übertragenen Daten geschützt sind.
- Die durch die Zugangstechnik zur Verfügung gestellten *zusätzlichen* Sicherheitsmechanismen (Nutzung der Rufnummernübertragung, Rückruf einer voreingestellten Telefonnummer für nicht mobile oder über Mobiltelefon angebundene RAS-Clients) sollten genutzt werden.
- Das RAS-System sollte in regelmäßigen Abständen einer Revision unterzogen werden. Die Rollen Administrator und Revisor dürfen nicht der gleichen Person zugeordnet werden.

Revision

- Die Anbindung eines tragbaren IT-Systems an ein LAN kann über GSM realisiert werden (siehe auch M 5.81 *Sichere Datenübertragung über Mobiltelefone*). Bei der Nutzung von RAS über Mobiltelefon-Netze ist zu beachten, dass sich der CLIP-Mechanismus (Rufnummernübertragung) in der Regel nur als *zusätzliches* Authentisierungsmerkmal eignet, da das über die Rufnummer identifizierte Mobiltelefon sehr leicht entwendet werden kann.

Anbindung über Mobiltelefon

Da RAS-Clients in der Regel in nicht vollständig kontrollierten Umgebungen betrieben werden, müssen für diesen Fall spezielle Mechanismen, Verfahren und Maßnahmen zum Einsatz kommen, die den Schutz des Clients gewährleisten können. Insbesondere mobile RAS-Clients sind hier einer besonderen Gefahr ausgesetzt, da diese physikalisch besonders leicht anzugreifen sind (Diebstahl, Vandalismus). Ist ein RAS-Client kompromittiert, so besteht die Gefahr, dass dadurch auch die Sicherheit des LANs beeinträchtigt wird.

Für den sicheren Betrieb von **RAS-Clients** sind daher folgende Aspekte zu berücksichtigen:

- Die Grundsicherheit des IT-Systems muss gewährleistet werden (siehe auch Bausteine B 3.203 *Laptop*, B 4.3 *Modem*, B 3.404 *Mobiltelefon* und B 5.8 *Telearbeit*).
- Da mobile RAS-Clients größeren Risiken ausgesetzt sind als stationäre, sollten diese durch zusätzliche Maßnahmen gesichert werden. Hierzu bietet sich eine Festplattenverschlüsselung an, um sicherzustellen, dass von abhanden gekommenen Geräten weder Daten ausgelesen noch unbefugt eine RAS-Verbindung aufgebaut werden kann.

Festplattenverschlüsselung

- Insbesondere beim RAS-Zugriff über Internetverbindungen ist die Installation von Computer-Viren-Schutzprogrammen auf allen RAS-Clients notwendig (siehe auch Baustein B 1.6 *Computer-Viren-Schutzkonzept*).

aktuelle Computer-Viren-Schutzprogramme

- Es sollte überlegt werden, auf den RAS-Clients so genannte PC-Firewalls einzusetzen und so vor unberechtigten Zugriffen aus dem Internet durch Dritte zu schützen. Ähnlich wie herkömmliche Firewalls

PC-Firewalls

(siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)*) filtern PC-Firewalls die Pakete der Netzkommunikationsprotokolle. Die Filterregeln können jedoch meist dynamisch durch den Benutzer erzeugt werden. Hierzu wird bei jedem Zugriff, für den noch keine Regel vorliegt, eine Auswahl an möglichen Reaktionen (z. B. erlauben, ablehnen, bedingte Verarbeitung) angeboten, um eine neue Regel zu definieren. Da es für den Benutzer jedoch in vielen Fällen schwierig ist, zwischen erlaubten und unberechtigten Zugriffen zu unterscheiden, sollte der Regelsatz durch einen Administrator vorinstalliert werden.

RAS-Clients in Systemmanagement einbeziehen

- Auch RAS-Clients sollten in das Systemmanagement einbezogen werden, soweit dies möglich ist. Dies erlaubt einerseits die Überwachung der Clients im Rahmen der Aufrechterhaltung des laufenden Betriebes. Andererseits können so einfach Software-Updates (Viren-Datenbanken, Anwendungsprogramme) auf geregeltem Weg eingespielt werden. Entfernte Rechner stellen jedoch erhöhte Anforderungen an das Systemmanagement, da diese nicht permanent mit dem Netz verbunden sind, so dass die Rechner regelmäßig auf (unzulässige) Konfigurationsveränderungen untersucht werden müssen. Hier kann - je nach Managementprodukt - die "Discovery"-Funktion genutzt werden, um den aktuellen Zustand des Rechners zu erfassen. Es ist dabei zu beachten, dass diese Erfassung der Informationen den RAS-Client belastet und die Daten über die RAS-Verbindung übertragen werden müssen. Bei RAS-Verbindungen mit geringer Bandbreite (z. B. über Mobiltelefon) kann dies zu nicht akzeptablen Antwortzeiten für den Benutzer führen.

eindeutige Zuordnung von IP-Adresse und Rechner

- Falls TCP/IP als Protokoll verwendet wird, sollte überlegt werden, für RAS-Clients feste IP-Adressen zu benutzen und diese nicht dynamisch zu vergeben. Dieses Vorgehen bedeutet zwar einen höheren administrativen Aufwand (Wartung der Zuordnungstabellen), erlaubt jedoch eine eindeutige Zuordnung von Netzadresse und Rechner. Der Nachteil bei einer dynamischen Vergabe der Netzadressen besteht darin, dass protokolliert werden muss, welchem RAS-Client zu welchem Zeitpunkte eine bestimmte Netzadresse zugewiesen wurde. Anderenfalls ist es meist nicht möglich festzustellen, welcher RAS-Client eine bestimmte Aktion ausgeführt hat.

Die **Kommunikationsverbindung** zwischen RAS-Client und RAS-Server wird in der Regel über Netze von Dritten aufgebaut. Die dabei benutzten Netzkomponenten unterliegen meist nicht der Kontrolle durch den Betreiber des LANs, mit dem die Verbindung aufgebaut werden soll. Es muss weiter davon ausgegangen werden, dass die Daten nicht nur über das Telekommunikationsnetz eines Anbieters übertragen werden, sondern dass auch die Netze von Kooperationspartnern des Telekommunikationsanbieters benutzt werden. Dies gilt insbesondere beim Zugriff auf ein LAN aus dem Ausland. Um dem Schutzbedarf der so übertragenen Daten gerecht zu werden, müssen Sicherheitsmaßnahmen getroffen werden, die z. B. die Vertraulichkeit der Daten sicherstellen. Daher gilt für die Datenübertragung:

- Die Nutzung der Datenverschlüsselung für alle übertragenen Daten ist für den sicheren Betrieb zwingend erforderlich.

- Es sollten Signaturmechanismen eingesetzt werden, um die Authentizität und Integrität der Daten sicherzustellen.

Um diesen Anforderungen an den Schutz der Daten gerecht zu werden, können verschiedene Sicherungsmechanismen für RAS-Verbindungen benutzt werden. Relevant sind hier unter anderem:

Tunneling

- Die Kommunikation kann auf niedriger Protokollebene verschlüsselt werden (so genanntes Tunneling, siehe M 5.76 *Einsatz geeigneter Tunnel-Protokolle für die RAS-Kommunikation*). Dazu muss ein geeignetes Verfahren ausgewählt werden. Die herkömmlichen RAS-Systeme stellen solche Verfahren standardmäßig, jedoch in unterschiedlicher Zahl und Ausprägung zur Verfügung.

SSL-Verschlüsselung

- Zur Verschlüsselung kann auch SSL eingesetzt werden, wenn von der Verschlüsselung auf niedriger Protokollebene aus bestimmten Gründen kein Gebrauch gemacht werden kann. Dies gilt besonders für Zugriffe auf WWW-Server oder E-Mail-Server über WWW-Browser, die standardmäßig SSL-gesicherte Kommunikation unterstützen. Dazu sollte auch M 5.66 *Verwendung von SSL* beachtet werden.

Verschlüsselung durch Netzkoppelelemente

- Neben der Absicherung der Kommunikation durch Software kann auch der Einsatz von verschlüsselnden Netzkoppelelementen (Router, Modems) erwogen werden. Diese sind besonders für den stationären Einsatz und zur Anbindung mehrerer Rechner sinnvoll, da die Verschlüsselung transparent erfolgt und die Clients und Server nicht belastet werden. Zu beachten ist jedoch, dass die Geräte sorgfältig konfiguriert und gewartet werden müssen.

E-Mail-Verschlüsselung

- Für den Austausch von E-Mails über unsichere Kanäle kann die Nutzung von E-Mail-Verschlüsselung sinnvoll sein (siehe auch M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*).

Die Sicherheit beim entfernten Zugriff über eine RAS-Verbindung kann nur dann gewährleistet werden, wenn alle Komponenten des RAS-Systems korrekt und konsistent konfiguriert sind. Zu beachten ist jedoch, dass je nach Zugriffsverfahren ein Grossteil der benutzten Komponenten nicht der direkten Kontrolle der lokalen RAS-Administration untersteht. Daher ist der RAS-Zugang zu einem LAN mit besonderer Sorgfalt und Aufmerksamkeit zu überwachen.

Beispiel:

Da Windows NT standardmäßig mit RAS-Unterstützung ausgeliefert wird, soll der RAS-Dienst von Windows NT als Beispiel dienen. Die angebotene Funktionalität sowie die verfügbaren Sicherheitsmechanismen sind jedoch in der Regel nur für eine geringe Anzahl an RAS-Benutzern und Daten mit geringem Schutzbedarf geeignet. Bei großen Benutzermengen und erhöhtem Schutzbedarf sollten auch zusätzliche RAS-Produkte in Betracht gezogen werden.

Für **RAS-Clients unter Windows NT** gilt:

- Für RAS-Clients sollte das Speichern von Benutzernamen und Passwort zum automatischen Verbindungsaufbau abgeschaltet sein. Dazu muss die

Option "Kennwort speichern" im Verbindungsdialog des DFÜ-Netzwerks deaktiviert werden. Wurde das Passwort aus Versehen gespeichert, so kann es wieder gelöscht werden, indem in den Verbindungseigenschaften auf der Karte "Sicherheit" der Knopf "Unsicheres Kennwort" gedrückt wird.

- Der automatische Aufbau einer DFÜ-Verbindung sollte nur nach Bestätigung durch den Benutzer erfolgen. Dies geschieht über die Option "Automatisches Wählen immer bestätigen" auf der Karte "Einstellungen" in den "Benutzereigenschaften" einer DFÜ-Verbindung. Vorzugsweise ist das automatische Wählen jedoch komplett abzuschalten. Hierzu ist die Option "Auto-Wahl nach Standorten aktivieren" für alle Standorte auf der Karte "Wählen" in den "Benutzereigenschaften" einer DFÜ-Verbindung zu deaktivieren.
- Es ist darauf zu achten, dass keine eingehenden Verbindungen erlaubt werden. Für die Einstellung "Anschlussverwendung" unter *Systemsteuerung, Netzwerk, Dienste, RAS-Dienst, Gerät, Konfigurieren* ist hierzu die Option "Nur ausgehende Anrufe" zu aktivieren.
- Damit die Kommunikationsabsicherung (MPPE-Verschlüsselung) benutzt wird, muss für die DFÜ-Verbindung unter der Karte "Sicherheit" die Option "Nur Microsoft-verschlüsselte Echtheitsbestätigungen annehmen" und "Datenverschlüsselung erforderlich" aktiviert werden. Zu beachten ist, dass dazu auch der RAS-Server entsprechend konfiguriert sein muss.
- Es sollte überlegt werden, jedem RAS-Client eine feste IP-Adresse zuzuordnen. Dadurch wird die Nachvollziehbarkeit von Aktivitäten, die über die RAS-Verbindung getätigt werden, erhöht. Die IP-Adresse kann in den TCP/IP-Eigenschaften der DFÜ-Verbindung unter *Telefonbuch, Server, TCP/IP-Einstellungen*, im Feld "IP-Adresse angeben" eingetragen werden.

Für **RAS-Server unter Windows NT** gilt:

- Die RAS-Einwahl sollte nur den berechtigten Benutzern gestattet werden. Für alle anderen Benutzer ist die Option "Dem Benutzer Einwählrechte erteilen" zu deaktivieren. Dies kann entweder über den Benutzermanager oder über den RAS-Manager erfolgen.
- Die Möglichkeit des Rückrufes durch den RAS-Server ist nur für diejenigen Benutzer zu aktivieren, für die dies explizit vorgesehen ist. Wenn möglich, sollte eine feste Rückrufnummer Verwendung finden.
- Damit RAS-Clients eine feste IP-Adresse anfordern können, ist die Option "Remote Clients erlauben, eine vorbestimmte IP-Adresse anzufordern" unter *Systemsteuerung, Netzwerk, Dienste, RAS-Dienst, Gerät, Netzwerk, TCP/IP-Konfigurieren* zu aktivieren.
- Soll von der MPPE-Verschlüsselung Gebrauch gemacht werden, so ist dies entsprechend zu aktivieren. Dies erfolgt über das Dialogfeld *Systemsteuerung, Netzwerk, Dienste, RAS-Dienst, Gerät, Netzwerk, Verschlüsselung*.
- Für einen RAS-Server unter Windows NT kann eingestellt werden, ob RAS-Clients nur auf die Ressourcen des RAS-Servers oder auch auf das Netz zugreifen können, an das der RAS-Server angeschlossen ist. Je nach

Verwendungszweck (z. B. Export lokaler Ressourcen, RAS-Zugangsserver für ein Netz) sollte die entsprechende Zugriffsbeschränkung eingestellt werden. Dies geschieht über die Option "TCP/IP-Clients dürfen zugreifen auf" unter Systemsteuerung, Netzwerk, Dienste, RAS-Dienst, Gerät, Netzwerk, TCP/IP-Konfigurieren.

Ergänzende Kontrollfragen:

- Werden alle festgestellten Sicherheitsverletzungen dokumentiert?
- Wird für jede Verbindungsaufnahme immer die Benutzer-Authentisierung über den festgelegten Mechanismus durchgeführt?
- Wird für jede Verbindung die Absicherung der Kommunikation durch eines der im RAS-Sicherheitskonzept erlaubten Verfahren erzwungen?
- Können mobile RAS-Clients durch zusätzliche Maßnahmen gesichert werden (z. B. Festplattenverschlüsselung)?

M 4.113 Nutzung eines Authentisierungsservers beim RAS-Einsatz

Verantwortlich für Initiierung: IT-Sicherheitsmanagement-Team

Verantwortlich für Umsetzung: Administrator

Für RAS-Systeme mit vielen Benutzern muss darüber nachgedacht werden, wie die Benutzerverwaltung für den RAS-Zugang effizient durchgeführt werden kann. In der Regel muss jeder RAS-Benutzer auch eine Systemidentität (Benutzerkonto des Betriebssystems) erhalten bzw. über ein solches Benutzerkonto identifiziert werden. Einige Betriebssysteme bieten hier die direkte Integration der RAS-Funktionalität (z. B. Windows NT) und eine gemeinsame Benutzerverwaltung. Für mittlere und große Netze, die organisatorisch meist in mehrere Teilnetze (Domänen, Verwaltungsbereiche) aufgeteilt sind, besteht in vielen Fällen das Problem, dass in jedem Verwaltungsbereich eine getrennte Verwaltung der Benutzerdaten durchgeführt wird. Sollen sich Benutzer auch an fremden Teilnetzen anmelden können, müssen hier Querberechtigungen (Cross-Zertifikate, Vertrauensstellungen) oder ein zentraler Verzeichnisdienst eingerichtet und gepflegt werden. Eine weitere Alternative ist, dass die Benutzer zusätzlich ein Benutzerkonto in dem anderen Teilnetz erhalten, dies erschwert aber die Verwaltung der Benutzerdaten. Insbesondere im RAS-Kontext haben sich hier spezielle Authentisierungssysteme herausgebildet, die auch für den "normalen" Authentisierungsprozess bei der Systemanmeldung genutzt werden können. Typische Vertreter sind beispielsweise RADIUS, TACACS, TACACS+, SecureID, SafeWord, etc.

Prinzipiell besitzen diese Systeme folgenden Aufbau:

- Die Authentisierungsdaten der Benutzer werden durch einen zentralen Server verwaltet.
- Das Programm zur Systemanmeldung wendet sich zur Überprüfung der vom Benutzer eingegebenen Authentisierungsdaten an den Authentisierungsserver.
- Zur Kommunikation zwischen Anmeldeprozess und Authentisierungsserver wird in der Regel ein abgesichertes Protokoll eingesetzt.

Der Anmeldeprozess muss dazu die Nutzung externer Authentisierungsserver unterstützen und die Netzadresse des zu benutzenden Authentisierungsservers muss in den Konfigurationsdaten des Anmeldeprozesses korrekt eingetragen sein. Will sich ein Benutzer nun am System anmelden - gleichgültig ob er dazu eine RAS-Verbindung benutzt oder sich direkt im LAN befindet - laufen grob vereinfacht folgende Schritte ab:

- Findet ein Verbindungsaufbau mit dem System- oder RAS-Anmeldeprozess statt, kontaktiert dieser den Authentisierungsserver und informiert ihn über den eingegangenen Verbindungswunsch eines Benutzers. Der Authentisierungsserver sendet - sofern ein "Challenge-Response" Verfahren zum Einsatz kommt - eine so genannte "Challenge" an den Prozess zurück, der diese an den Benutzer weiterleitet.

- Der Benutzer gibt sein Authentisierungsgeheimnis ein. Dies kann je nach verwendetem System ein Passwort oder ein Einmalpasswort in den unterschiedlichsten Ausprägungen (Nummern, Text) sein.
- Der Anmeldeprozess leitet die Daten (meist transparent für den Benutzer) an den Authentisierungsserver weiter.
- Der Authentisierungsserver verifiziert die Benutzerdaten und signalisiert dem Anmeldeprozess das Ergebnis der Überprüfung.
- Der Zugang zum (Access-)Netz wird nach erfolgreicher Überprüfung gewährt.

Durch die Verwendung von zentralen Authentisierungsservern kann erreicht werden, dass einerseits die Authentisierungsdaten konsistent verwaltet werden und andererseits bessere Authentisierungsmechanismen genutzt werden können, als sie von den Betriebssystemen standardmäßig unterstützt werden. Hier sind insbesondere Chipkarten- und Token-basierte Mechanismen zu nennen. Je nach System erzeugen diese z. B. Einmalpasswörter, die auf einem Display angezeigt werden und die der Benutzer als Passwort angeben muss.

Für mittlere und große Netze wird die Verwendung von Authentisierungsservern insbesondere im RAS-Bereich empfohlen, da diese eine wesentlich höhere Sicherheit bei der Benutzer-Authentisierung bieten. Berücksichtigt werden muss jedoch, dass auch diese Server administriert und gewartet werden müssen. Ein Authentisierungsserver muss so im Netz platziert werden, dass er einerseits performant erreicht werden kann, aber andererseits auch vor unberechtigten Zugriffen geschützt ist.

Ergänzende Kontrollfragen:

- Wird das externe Authentisierungssystem durch das Betriebssystem und das RAS-System unterstützt?
- Erlaubt die RAS-Client-Software die Nutzung eines Chipkartenlesers für chipkartenbasierte Authentisierungssysteme?
- Welche Sicherheitsmechanismen werden durch das externe Authentisierungssystem angeboten?

M 4.114 Nutzung der Sicherheitsmechanismen von Mobiltelefonen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Mobiltelefone und dazu angebotene Dienstleistungen können an verschiedenen Stellen durch PINs oder Passwörter abgesichert werden. Hierzu gehören:

Zugriff auf die SIM-Karte

Die SIM-Karte kann durch eine vier- bis achtstellige PIN gegen unberechtigten Zugriff geschützt werden. Mit dieser PIN identifiziert sich der Teilnehmer gegenüber der Karte. Gelangt ein Unbefugter in den Besitz einer SIM-Karte, kann er ohne Kenntnis der PIN diese Karte nicht aktivieren. Um eine missbräuchliche Nutzung der SIM-Karte zu verhindern, sollte daher unbedingt diese PIN-Abfrage aktiviert werden,sodasss die PIN nach dem Einschalten des Mobiltelefons eingegeben werden muss. Die PIN sollte nicht zusammen mit dem Mobiltelefon bzw. der SIM-Karte aufbewahrt werden.

Bei der Auslieferung ist meist die PIN-Abfrage deaktiviert und eine PIN voreingestellt. Bei der ersten Benutzung sollte unbedingt die PIN geändert und aktiviert werden. Hierbei sollte keine triviale oder leicht vorhersagbare PIN gewählt werden (1111, Geburtsdatum, etc.).

Hinweis: Auf der Tastatur der meisten Mobiltelefone sind unter den Ziffern Buchstaben unterlegt. Dies kann dazu benutzt werden, sich statt PINs Passwörter auszuwählen, die leichter zu merken sind, aber natürlich auch wieder nicht zu einfach sein sollten. Beispiel: "4AUGEN" entspricht der PIN "428436".

Nach dreimaliger falscher PIN-Eingabe wird die SIM-Karte gesperrt. Um diese Sperre aufheben zu können, muss ein achtstelliger Entsperrcode eingegeben werden. Dieser wird häufig auch als PUK (PIN Unblocking Key) oder Super-PIN bezeichnet. Nach zehnmaliger Falscheingabe der PUK wird die Karte unbrauchbar. Dieser Entsperrcode wird normalerweise in einem PIN-Brief zusammen mit der SIM-Karte ausgeliefert. Er sollte äußerst sorgfältig und vor unbefugtem Zugriff geschützt aufbewahrt werden. Die PUK darf auf keinen Fall zusammen mit dem Mobiltelefon aufbewahrt werden.

Neben der PIN gibt es mit der PIN2 noch eine weitere Geheimzahl, mit der der Zugriff auf bestimmte Funktionen der SIM-Karte abgesichert werden kann. Sie wird häufig benutzt für Konfigurationsänderungen der SIM-Karte, die nicht vom Benutzer selbst durchgeführt werden können, z. B. Nutzungsrestriktionen. Dies kann aber beispielsweise auch ein Firmentelefonbuch sein, das nur nach der Eingabe der PIN2 geändert werden kann. Die PIN2 hat einen eigenen Entsperrcode (PUK2).

Zugriff auf das Mobiltelefon

Darüber hinaus gibt es im Allgemeinen noch einen Sicherheitscode für das Mobiltelefon (Geräte-PIN), um den Zugriff auf bestimmte Funktionen zu schützen. Auch dieser sollte schnellstmöglich auf einen individuell gewählten

Wert gesetzt werden. Er sollte notiert und vor unbefugtem Zugriff geschützt aufbewahrt werden. Die Geräte-PIN muss nicht bei jedem Einschalten des Mobiltelefons eingegeben werden. Mit ihr kann z. B. verhindert werden, dass das Mobiltelefon mit einer anderen SIM-Karte benutzt wird (Diebstahlschutz).

Zugriff auf Mailbox

Beim Netzbetreiber kann für jeden Teilnehmer eine Mailbox eingerichtet werden, die unter anderem als Anrufbeantworter dient. Da die Mailbox von überall und auch von beliebigen Endgeräten aus abgefragt werden kann, muss sie mit einer PIN vor unbefugtem Zugriff geschützt werden. Bei der Neueinrichtung vergibt der Netzbetreiber hierzu eine voreingestellte PIN. Diese sollte unbedingt sofort geändert werden.

Weitere Kennwörter

Neben den diversen oben aufgeführten Geheimnummern kann es für verschiedene Nutzungsarten noch weitere Kennwörter geben. Dies ist z. B. der Fall beim Zugriff auf Benutzerdaten beim Netzbetreiber. So muss bei Fragen an die Hotline wegen der Abrechnung u. U. ein Kennwort genannt werden. Auch kostenpflichtige Dienstleistungen wie z. B. der Abruf von Informationen oder die Durchführung bestimmter Konfigurationen seitens des Netzbetreibers werden häufig durch zusätzliche Kennwörter geschützt. Diese sollten, wie alle anderen Passwörter auch, sorgfältig ausgewählt und sicher aufbewahrt werden.

Generell sollte mit allen PINs und Passwörtern sorgfältig umgegangen werden (siehe auch M 2.11 *Regelung des Passwortgebrauchs*).

Hinweis: Angreifer haben in jüngster Zeit wiederholt versucht, telefonisch die PIN oder PUK von Mobilfunknutzern zu erfragen, indem sie sich als Mitarbeiter eines Netzbetreibers ausgegeben und einen technischen Defekt vorgetäuscht haben. Über Geheimnummern sollte **nie** telefonisch Auskunft gegeben werden!

Es gibt viele verschiedene Sicherheitsmechanismen bei Mobiltelefonen. Welche hiervon vorhanden sind bzw. wie diese aktiviert werden können, ist abhängig vom eingesetzten Mobiltelefon, von der SIM-Karte und vom gewählten Netzbetreiber. Daher sollten die Bedienungsanleitung und die Sicherheitshinweise vom Netzbetreiber sorgfältig daraufhin ausgewertet werden. Beim Einsatz von Firmentelefonen empfiehlt es sich, die wichtigsten Sicherheitsmechanismen sowohl vorzukonfigurieren als auch auf einem übersichtlichen Handzettel zu dokumentieren.

Ergänzende Kontrollfragen:

- Welche Sicherheitsmechanismen sind für die Nutzung von Mobiltelefonen vorgeschrieben?

M 4.115 Sicherstellung der Energieversorgung von Mobiltelefonen

Verantwortlich für Initiierung: Administrator, Benutzer

Verantwortlich für Umsetzung: Administrator, Benutzer

Um die Energieversorgung von Mobiltelefonen jederzeit aufrechterhalten zu können, werden üblicherweise Akkus eingesetzt. Je nach Kapazität der Akkus und Bauweise eines Mobiltelefons reicht dies für einen beschränkten Zeitraum, üblicherweise einige Stunden, aus. Damit ein Mobiltelefon im Bedarfsfall jederzeit verfügbar ist bzw. keine Daten in flüchtigen Speichern verloren gehen, sollten einige Randbedingungen eingehalten werden:

- Die Warnanzeigen des Mobiltelefons, die den Spannungsabfall anzeigen, dürfen nicht ignoriert werden.
- Falls es absehbar ist, dass der mobile Einsatz längerfristig ist, sollte das Ladegerät mitgeführt werden.
- Beim Laden sollten die Hinweise im Handbuch zum Mobiltelefon beachtet werden, insbesondere sollte die Lebensdauer des Akkus nicht beeinträchtigt werden.
- Bei der Übergabe eines Mobiltelefons ist der ausreichende Ladezustand der Akkus sicherzustellen. Der Ladezustand der Akkus sollte regelmäßig überprüft werden, da sich ein Akku im Laufe der Zeit entlädt, auch wenn er nicht verwendet wird.

Ladezustand regelmäßig überprüfen

Es empfiehlt sich darüber hinaus, auf dem Mobiltelefon gespeicherte Daten (Telefonbuch, SMS, etc.) in regelmäßigen Abständen auf einem anderen Medium zu speichern.

Kurzschlüsse am Akku vermeiden

Wenn eine längere Nutzung des Mobiltelefons absehbar ist, z. B. bei Dienstreisen, sollte ein geladener Ersatzakku mitgeführt werden. Der Ersatzakku sollte in einer Schutzhülle verwahrt werden, da Schäden durch Überhitzung oder Brand entstehen können, wenn die Kontakte des Akkus mit leitenden Materialien in Berührung kommen. Dies kann durch viele Gegenstände des täglichen Gebrauchs wie Schlüssel oder Ketten verursacht werden.

Ein Mobiltelefon sollte ausgeschaltet werden, bevor der Akku gewechselt wird, damit der Speicher nicht beschädigt wird.

Vorsicht vor extremen Temperaturen

Ein Mobiltelefon sollte keinen extremen Temperaturen ausgesetzt werden. Insbesondere der Akku, aber auch das Display können anderenfalls ihre Funktionsfähigkeit einbüßen. Daher sollten weder Mobiltelefone noch Akkus in geparkten Autos zurückgelassen werden.

Ergänzende Kontrollfrage:

- Welche Sicherheitsmaßnahmen werden für die Sicherstellung der Energieversorgung von Mobiltelefonen getroffen?

M 4.116 Sichere Installation von Lotus Notes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Schon im Rahmen des Installationsprozesses eines Lotus Domino Systems sind sicherheitsrelevante Aspekte zu berücksichtigen. In der Regel genügt eine Standardinstallation nicht den geltenden Sicherheitsanforderungen, sodass der Installationsprozess erst dann als abgeschlossen betrachtet werden kann, wenn direkt nach der Softwareinstallation eine sichere Konfiguration der Software erfolgt. Folgende Schritte sind während oder direkt nach der Installation durchzuführen:

Während der Installation:

Passwörter für Notes-IDs festlegen

- Es werden drei wichtige Notes-IDs erzeugt: die so genannte Certifier-ID (Datei "cert.id"), die Server-ID (Datei "server.id") und die des Administrators (Datei "user.id"). Für alle Notes-IDs sind geeignete Passwörter festzulegen. Die Notes-IDs sollten nicht im Names- und Adressbuch gespeichert werden, sondern in Dateien, die geschützt vorgehalten werden.

ACL-Eintrag für anonymen Zugriff einrichten

- Lotus Notes bietet die Option, für Datenbanken einen zusätzlichen ACL-Eintrag (Access Control List, Zugriffsliste) für die Gruppe "Anonymous" mit dem Zugriffslevel "No Access" einzurichten. Gibt es keinen "Anonymous"-Eintrag, so kommen in der Regel die Rechte des "-Default-"-Eintrages zur Anwendung. Diese Option sollte daher genutzt werden, um für alle Datenbanken explizite Zugriffsrechte für anonyme Anwender eintragen zu können.

Nach der Installation:

- Die Certifier-ID sollte mit einem Mehrfachpasswort versehen werden, sodass die ID nur im Vier-Augen-Prinzip genutzt werden kann. Die Passwörter sollten eine hohe Qualität besitzen. Mindestens eine Kopie der Certifier-ID mit zugehörigen Passwörtern sollte an einem gesicherten Ort aufbewahrt werden.
- Die mit einem Passwort versehene Kopie der Server-ID sollte mit zugehörigem Passwort an einem gesicherten Ort aufbewahrt werden. Soll der Domino Server automatisch gestartet werden, ist das Passwort der Server-ID zu entfernen (Passwortlänge auf "0" setzen). Die Datei "server.id", die in der Regel im "data"-Verzeichnis des Servers abgelegt ist, muss mit entsprechenden Dateizugriffrechten vor unberechtigtem Zugriff geschützt werden. Die Datei darf nicht auf einem Netz-Share abgelegt werden.
- Für alle Verzeichnisse und Dateien des Domino Systems sollten Zugriffsbeschränkungen eingerichtet werden, sodass der direkte Dateizugriff auf Betriebssystemebene nur autorisierten Administratoren erlaubt ist.
- Der Zugriff auf den Server sollte beschränkt werden, so dass nur die mit der Konfiguration betrauten Administratoren auf den Server zugreifen

können (siehe M 4.119 *Einrichten von Zugangsbeschränkungen auf Lotus Notes Server*).

- Für **alle** Datenbanken müssen die ACL-Einstellungen kontrolliert werden. Dabei sollten **alle** Einträge der ACL-Liste überprüft werden, insbesondere die "-Default-"-Berechtigung (siehe M 4.120 *Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken*).

ACLs prüfen

Für jedes Domino-Server-Modul, das zum Einsatz kommt, muss sichergestellt werden, dass während und nach der Installation keine unerlaubten Zugriffe erfolgen, bis die Konfiguration abgeschlossen ist und ein sicherer Betrieb gewährleistet werden kann (siehe hierzu auch M 4.117 *Sichere Konfiguration eines Lotus Notes Servers*).

Die Installation aller Domino-Server-Module muss dokumentiert werden, insbesondere die Konfiguration der Datenbanken und Systemdateien.

Dokumentation der Installation

Ergänzende Kontrollfragen:

- Sind vor der Installation alle erforderlichen Parameter bekannt, die während der Installation benötigt werden?
- Sind alle Nacharbeiten bekannt, die nach der Installation durchgeführt werden müssen?
- Wurde der Installationsvorgang, die Erstellung und Konfiguration der Datenbanken und Systemdateien dokumentiert?

M 4.117 Sichere Konfiguration eines Lotus Notes Servers

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der Lotus Domino Application Server besteht aus einer Vielzahl von Funktionsmodulen und kann daher nicht nur als reiner Datenbankserver genutzt werden, obwohl sich daraus immer noch die meisten Anwendungsszenarien ableiten. Durch die erfolgte Integration von Internet-Technologien stehen u. a. auch folgende Module zur Verfügung:

Datenbankzugriff
- Das Datenbankservermodul erlaubt den Datenbankzugriff für Notes-Clients.

HTML
- Das HTTP-Servermodul erlaubt den Datenbankzugriff via Browser und kann auch als normaler WWW-Server zum Bereitstellen von HTML-Seiten genutzt werden.

LDAP
- Das LDAP-Servermodul (Lightweight Directory Access Protocol) erlaubt einen Zugriff auf die Benutzerinformationen für LDAP-Clients.

E-Mail
- Die E-Mail-Servermodule (z. B. SMTP- und POP3-Server) erlauben die Nutzung von E-Mail mittels Internet-Protokollen.

News
- Das NNTP-Servermodul erlaubt den Zugriff auf sogenannte News-Nachrichten.

Je nach Einsatzszenario und dem vom Domino-Server angebotenen Funktionsumfang muss überprüft werden, welche Module durch die Standardinstallation aktiviert wurden und welche "Tasks" (als eigene Betriebssystemprozesse oder als Threads) daher durch den Server ausgeführt werden,

nur benötigte Module aktivieren

Ebenso muss festgelegt werden, welche Module genutzt werden sollen. Nicht genutzte Module dürfen nicht installiert werden bzw. sind zu deaktivieren. Jedes installierte Modul ist bei Fehlkonfiguration als potentielle Sicherheitslücke anzusehen. Dies gilt insbesondere für die Module (z. B. HTTP, POP, SMTP, LDAP), die Zugriffe auf Server-Daten auch mit Fremdprogrammen ermöglichen (z. B. Browser, E-Mail-Programme).

Für jedes aktivierte Modul muss eine entsprechende Sicherheitsplanung durchgeführt werden und diese ist durch geeignete Konfigurationsparameter umzusetzen (siehe auch M 2.207 *Festlegen einer Sicherheitsrichtlinie für Lotus Notes*).

Da die meisten Funktionsmodule des Domino Application Servers in der Regel auf Datenbanken aufsetzen und deren Informationen über entsprechende Kommunikationsprotokolle für Clients bereitstellen, muss in jedem Fall eine sichere, datenbankbezogene Grundkonfiguration erstellt werden. Danach sind weitere Konfigurationen der modulbezogenen Parameter notwendig.

Es gibt zwei Hauptzugriffsarten auf ein Notes-Systems: über einen Notes-Client und über einen Browser. Die damit zusammenhängenden Empfehlungen sind gesondert

- in M 4.118 *Konfiguration als Lotus Notes Server*, die die sicherheitsrelevanten Basiskonfigurationen beschreibt, und
- in M 4.122 *Konfiguration für den Browser-Zugriff auf Lotus Notes*, die die zusätzlichen Konfigurationsmaßnahmen für den Zugriff via Browser beschreibt,

zusammengefasst.

Replikationskonzept erstellen

Ein Notes-System besteht in der Regel nicht nur aus einem Notes-Server, sondern aus einem ganzen Serververbund (siehe auch M 3.24 *Schulung zur Lotus Notes Systemarchitektur für Administratoren*). Die einzelnen Server können dabei Datenbanken untereinander replizieren. Dadurch kann Datenverlusten entgegengewirkt, aber auch eine Lastverteilung durch die Bereitstellung von Datenbank-Kopien auf mehreren Servern erreicht werden. Damit die Aktualität der Datenbankkopien in gewissen Grenzen gewahrt bleibt, müssen Veränderungen an den Daten zwischen den Servern ausgetauscht werden. Aus Sicherheitsgründen muss daher ein Replikationskonzept erstellt werden. Unter anderem sind dabei folgende Aspekte zu berücksichtigen:

- Welcher Server hält das Original einer Datenbank?
- Auf welche Server soll eine Datenbank repliziert werden?
- Wie oft muss repliziert werden? Wann soll repliziert werden?
- Welche Informationen einer Datenbank sollen repliziert werden?
- Sollen Änderungen an Replikaten einer Datenbank erlaubt sein und sollen diese auf das Original übertragen werden?
- Dürfen Benutzer server- oder clientseitige Replikate einer Datenbank erzeugen?
- Ist das Verändern der Zugriffslisten oder Eigenschaften von Datenbanken auf Replikaten erlaubt?

Die Zugriffberechtigungen einer Datenbank sind so zu setzen, dass die zur Replikation notwendigen Operationen durchgeführt werden können. Das Replikationslog muss regelmäßig überprüft werden.

Client-Sicherheit

Die Sicherheit eines Notes-Systems hängt außerdem auch von der Sicherheit der zum Zugriff benutzten Clients ab. Daher müssen in die Umsetzung einer sicheren Konfiguration eines Notes-Systems auch die Client-Rechner und Client-Programme einbezogen werden. Die dabei zu beachtenden IT-Sicherheitsaspekte sind in den Maßnahmen

- M 4.126 *Sichere Konfiguration eines Lotus Notes Clients* und
- M 4.127 *Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes*

zusammengefasst.

kontinuierliche Anpassung

Da ein System in der Regel permanenten Veränderungen durch den laufenden Betrieb unterworfen ist, muss auch die Sicherheit ständig überprüft und ggf. neu konfiguriert werden. Hinweise dazu finden sich in M 4.128 *Sicherer Betrieb von Lotus Notes*.

Managementsysteme in die Überlegungen einbeziehen

Falls ein Netz- und Systemmanagementsystem im Einsatz ist oder zukünftig eingesetzt werden soll, ist dies in die Überlegungen zur Konfiguration einzubeziehen. Beispielsweise ist zu klären, ob über dieses System auch Notes-spezifische Einstellungen auf den beteiligten IT-Systemen vornehmen soll und ob das verwendete bzw. vorgesehene Produkt dies unterstützt. Gegebenenfalls sind hier zusätzliche Anpassungen oder Erweiterungen erforderlich.

Ergänzende Kontrollfragen:

- Besteht eine Sicherheitskonzeption für den Einsatz der verschiedenen Funktionsmodule von Lotus Notes?
- Ist dokumentiert, welche Module in welcher Konfiguration eingesetzt werden sollen?
- Existiert ein Replikationskonzept?

M 4.118 Konfiguration als Lotus Notes Server

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Konfiguration eines Notes-Servers als Datenbankserver kann nur unter Beachtung seiner Umgebung und des vorgesehenen Anwendungsprofils erfolgen (siehe dazu M 2.206 *Planung des Einsatzes von Lotus Notes* und M 4.117 *Sichere Konfiguration eines Lotus Notes Servers*). Generell ist auch die physikalische Sicherheit und die sichere Konfiguration des Betriebssystems des Rechners, auf dem die Notes-Software eingesetzt wird, für die Sicherheit einer Notes-Installation erforderlich. Die Maßnahmen der relevanten Bausteine (z. B. Serverraum, Schutzschränke, Windows NT Netz, Unix Server) sind daher jeweils anzuwenden.

Allgemein müssen folgende Aspekte für die sichere Konfiguration eines Notes Servers berücksichtigt werden:

- Die Zugangskontrolle für den Server muss eingestellt werden. Diese regelt, wer sich mit dem Server verbinden darf, und greift, bevor die Zugriffskontrollen auf Datenbanken zum Einsatz kommen. Die Zugangsbeschränkungen für den Server müssen gemäß der Zugangsplanung konfiguriert werden (siehe M 4.119 *Einrichten von Zugangsbeschränkungen auf Lotus Notes Server*).

Zugang zum Server

- Die Zugriffskontrolle für Datenbanken muss gemäß der Zugriffsplanung eingestellt werden. Dazu müssen die Zugriffslisten (Access Control Lists, ACLs) für alle Datenbanken gemäß der durchzusetzenden Zugriffsbeschränkungen geändert werden (siehe M 4.120 *Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken* und M 4.121 *Konfiguration der Zugriffsrechte auf das Namens- und Adressbuch von Lotus Notes*).

Zugriff auf Datenbanken

- Der Administrationsprozess muss korrekt eingerichtet werden, damit die durch den Prozess periodisch ausgeführten administrativen Tätigkeiten angestoßen werden können. Hinweise hierzu finden sich in der Notes-Hilfe.

Administrationsprozess

- Alle Datenbanken sollten mit einer dafür vorgesehenen speziellen Notes-ID signiert werden. Dabei sollten insbesondere Agenten und Skripte signiert werden. Dadurch kann die Ausführung von Agenten und Skripten auf Notes-Clients an die benutzte Signatur geknüpft werden, sodass unsignierte, fremde Agenten und Skripte nicht automatisch ausgeführt werden.

Notes-ID

- Die notwendigen Logging- und Funktionsdatenbanken müssen erzeugt werden. Nicht alle für den Betrieb eines Domino-Servers notwendigen Datenbanken werden während des Installationsprozesses angelegt. So muss z. B. die Protokolldatenbank, die alle Zertifizierungsprozesse eines Servers protokolliert (unter anderem das Ausstellen von Benutzer-IDs) von Hand erzeugt werden. Dies betrifft z. B. die Datei "certlog.nsf" und das Template "certlog.ntf" (siehe auch M 5.86 *Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes*).

Protokollierung

- Der Server sollte in einem Serverraum (siehe Baustein B 2.4 *Serverraum*) bzw. in einem Serverschrank (siehe Baustein B 2.7 *Schutzschränke*) untergebracht werden. Die Serverkonsole muss außerdem gegen unbefugtes Benutzen gesichert sein. Dazu ist vorzugsweise der Sperrmechanismus des Betriebssystems (z. B. *Arbeitsstation sperren* unter Windows NT) oder ein passwortgeschützter Bildschirmschoner (z. B. unter Unix) einzusetzen. Das Konsolenpasswort von Lotus Notes zu aktivieren, bietet hier wenig Schutz, da es bei der Eingabe im Klartext angezeigt wird und die Eingabezeile in der Regel über die Bildlaufleiste des Konsolenfensters wieder sichtbar gemacht werden kann.

sichere Aufstellung

Datenaustausch zwischen Servern und Datenbankreplikation

Befindet sich ein Server im Verbund mit weiteren Servern, so müssen zusätzlich die Berechtigungen der Server untereinander konfiguriert werden. Dies betrifft auch den Datenaustausch zwischen Servern durch die Datenbankreplikation. Die für die Kommunikation erforderlichen Verbindungswege müssen dabei durch Anlegen so genannter Connection-Dokumente konfiguriert werden. Hinweise zur unter Umständen notwendigen Verschlüsselung von Kommunikationsverbindungen sind in M 5.84 *Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation* beschrieben.

Qualität der Notes-ID-Passwörter

Die Sicherheit des Servers hängt auch von der Sicherheit der Benutzerauthentisierung ab. Diese wird wesentlich auch von der Sicherheit des Notes-ID-Passwortes eines jeden Benutzers bestimmt. Für die Passwörter können Qualitätsanforderungen eingestellt werden, die beim Erzeugen einer neuen Benutzer-ID festgelegt und dann auch bei jedem Passwortwechsel beachtet werden. Es steht eine numerische Qualitätsskala von 0 (kein Passwort) bis 16 zur Verfügung. Die minimale Passwortqualität für Benutzer sollte auf den Wert "8" oder höher eingestellt sein (siehe auch M 4.129 *Sicherer Umgang mit Notes-ID-Dateien*).

Ergänzende Kontrollfragen:

- Ist die Konfiguration der Lotus Notes Server dokumentiert?
- Sind alle Kommunikationspartner eines Servers bekannt?
- Ist die physikalische Sicherheit der Server-Rechner gewährleistet?
- Ist der Schutz der Notes-Server-Konsole gewährleistet?
- Sind Zugriffsbeschränkungen auf der Ebene der Betriebssysteme umgesetzt?

M 4.119 Einrichten von Zugangsbeschränkungen auf Lotus Notes Server

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Bevor der Zugriff auf eine Datenbank eines Notes-Servers erlaubt wird, führt der Server schon beim Verbindungsaufbau eines Clients eine erste Zugriffskontrolle durch. Dadurch kann erreicht werden, dass die vom Server angebotenen Datenbanken nur einem bestimmten Benutzerkreis zugänglich sind oder dass der Zugang an weitere Eigenschaften geknüpft ist. Folgende Mechanismen zur Zugriffsbeschränkung können verwendet werden:

Prüfung der Notes-ID

- Bei der Benutzerauthentisierung wird der in der Benutzer-ID enthaltene öffentliche Schlüssel mit der Kopie des öffentlichen Schlüssels des Benutzers im Namens- und Adressbuch verglichen. Dies verhindert, dass gefälschte IDs benutzt werden können.

anonymer Zugriff

- Der anonyme Zugriff auf den Server kann verweigert werden. Anonym ist ein Zugriff auch dann, wenn ein Benutzer mit einer Notes-ID zugreift, die von einer Zertifizierungsinstanz ausgestellt wurde, die der Server nicht kennt, d. h. es existiert kein gemeinsames Root-CA-Zertifikat (CA = Certificate Authority) oder kein Cross-Zertifikat.

zusätzliche Passwortprüfung

- Das Notes-ID-Passwort kann zusätzlich überprüft werden. Dabei wird jeweils ein Hash-Wert des aktuellen Passwortes genau einer Benutzer-ID gespeichert und bei Passwortänderungen nachgezogen. Dadurch wird erreicht, dass nur mit einer bestimmten Benutzer-ID auf den Server zugegriffen werden kann. Mit Kopien der Benutzer-ID (z. B. mit kompromittiertem Passwort), die nicht das aktuelle Passwort tragen, ist das Anmelden dann nicht mehr möglich. **Achtung**: Ist diese Option aktiviert, wird die Benutzer-ID-Kopie, auf der zuerst das Passwort geändert wird, zu der ID, mit der ab dann nur noch die Anmeldung möglich ist (dies kann auch die des Angreifers sein).

- Der Zugriff kann auf die Benutzer eingeschränkt werden, die im Namens- und Adressbuch des Servers enthalten sind.

Ja-/Nein-Listen

- Es können explizite Erlaubnis- und Ausschlusslisten angegeben werden (Access/Deny Listen). Ausschlusslisten haben dabei Vorrang vor Erlaubnislisten. Dies kann z. B. dazu genutzt werden, einzelnen Benutzern den Zugriff zu verweigern. Zur einfacheren Administration der Listen empfiehlt sich die Verwendung von Gruppen.

- Auch Server besitzen eine Identität und können in Access/Deny Listen bzw. den darin enthaltenen Gruppen angegeben werden.

Funktionalitäten einschränken

- Bestimmte Server-Operationen können auf eine Liste von Benutzern oder Gruppen eingeschränkt werden. Beispiele für solche Operationen sind das Anlegen von Datenbanken, das Erzeugen von Replikaten, die Nutzung von Monitoren, die Administration über die Web-Schnittstelle und das Ausführen von Agenten und Skripten. Je nach Option kommen verschiedene Vor-

gaben zum Einsatz, wenn keine explizite Liste angegeben wird. Beispielsweise dürfen standardmäßig alle Benutzer neue Datenbanken anlegen.

Einsatz von Vermittlungs-Servern planen

- Notes erlaubt es, Server als Vermittlungs-Server, z. B. bei der Einwahl, einzusetzen oder Server über Vermittlungs-Server anzusprechen. Im Rahmen des Notes-Sicherheitskonzeptes ist zu planen, ob dies notwendig ist und welchen Benutzergruppen die Berechtigung zum so genannten "Pass-through"-Zugriff erteilt werden soll.

Es ist für jede Server-Installation im Rahmen der vorhergehenden Planung zu entscheiden, welche dieser Mechanismen genutzt werden sollen.

Ergänzende Kontrollfragen:

- Sind adäquate Zugriffskontroll-Mechanismen auf den Notes Servern eingerichtet?

M 4.120 Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Eine der wichtigsten Sicherheitsmechanismen eines Notes-Servers ist die Zugriffskontrolle auf Datenbanken. Hiermit kann gesteuert werden, welcher Benutzer mit welchen Rechten auf eine Notes Datenbank zugreifen kann. Nachdem ein Client (Notes-Client oder Browser) die allgemeine Zugangskontrolle auf einen Server passiert hat (siehe M 4.119 *Einrichten von Zugangsbeschränkungen auf Lotus Notes Server*), kommt die Zugriffskontrolle auf Datenbanken zur Anwendung. Damit der Schutz für die in den einzelnen Datenbanken enthaltenen Daten gewährleistet werden kann, müssen die Zugriffslisten (Access Control Lists, ACLs) für jede Datenbank korrekt eingestellt werden. Dabei sind folgende Aspekte zu beachten:

- Für jede Datenbank ist ein Zugriffskonzept zu entwerfen.
- Datenbanken können unter Notes grob in zwei Gruppen eingeteilt werden:

  1. Systemdatenbanken, die für den Ablauf des Notes-Systems notwendig sind (z. B. Protokolldatenbanken, Datenbank zur Zertifikatsverwaltung), und
  2. Datenbanken, die produktive Daten enthalten (z. B. Projektdatenbanken).

  Die unterschiedlichen Verwendungszwecke müssen in den Zugriffskonzepten berücksichtigt werden.
- Alle Systemdatenbanken müssen mit restriktiven Zugriffsberechtigungen geschützt werden, beispielsweise names.nsf, admin4.nsf, catalog.nsf, log.nsf, event4.nsf, domcfg.nsf, domlog.nsf, setup.nsf, homepage.nsf, certlog.nsf. **Hinweis:** Je nach Serverkonfiguration existieren einige der genannten Datenbanken nicht oder es sind zusätzliche vorhanden.
- Wenn eine gruppenbasierte Zugriffskontrolle eingesetzt wird, sollten alle Benutzer aus der Zugriffsliste entfernt werden. Mindestens einer Gruppe müssen "Manager"-Rechte zugeordnet werden. In der Regel wird beim Erzeugen einer Datenbank der Benutzer, der die Datenbank erzeugt (in der Regel ein Administrator), automatisch mit "Manager"-Rechten in die ACL eingetragen. Auch dieser Eintrag sollte entfernt werden, damit nur noch gruppenbasierte Rechte übrigbleiben, aber erst dann, wenn alle administrativen Einstellungen an der Datenbank erfolgt sind.
- Bei der Konfiguration der Datenbank-Zugriffsrechte sollte nicht davon ausgegangen werden, dass für den Server Zugangsbeschränkungen gelten. Dies vermeidet Sicherheitslücken, wenn sich Zugangsbeschränkungen auf Server ändern oder Fehler enthalten.
- Auf produktiven Datenbanken sollten keine "Designer"-Rechte vergeben werden. Für Veränderungen am Datenbankdesign sollte ein Change-Management existieren, das einen geregelten Update-Zyklus erlaubt und

beispielsweise die Phasen Antrag mit Begründung, Entscheidung, Umsetzung, Test, Einführung umfasst.

- ACL-Listen haben bei Client-lokalem Zugriff **keine** Wirkung. Ein Benutzer hat in der Regel volle Kontrolle über eine Datenbank oder Datenbankreplik, die auf dem Client-Rechner gespeichert ist. Insbesondere kann er Veränderungen an der Datenbank-ACL vornehmen und sich damit "Manager"-Rechte zuweisen.
- Die Option "Konsistente ACL über alle Repliken erzwingen" kann nicht dazu benutzt werden, das Durchsetzen der ACL im lokalen Zugriff zu erzwingen, da das entsprechende "Flag" durch existierende Administrationswerkzeuge zurückgesetzt werden kann.
- Die Replikation einer Datenbank-ACL über Domänengrenzen hinweg ist nicht ohne weiteres möglich, da sich die Namensräume in der Regel unterscheiden.
- Der ACL-Eintrag "-Default-" legt die Berechtigungen für Benutzer fest, die durch keinen anderen ACL-Eintrag erfasst werden. In der Regel soll solchen Benutzern kein Zugriff erlaubt werden ("No Access"). Die voreingestellten Rechte dieses Eintrags sind immer zu überprüfen und gegebenenfalls zu verändern.
- Der ACL-Eintrag "-Anonymous-" legt die Berechtigungen für Benutzer fest, die sich nicht authentisiert haben (falls der Server das anonyme Verbinden erlaubt). Zur Zugriffsteuerung für anonyme Benutzer sollte dieser Eintrag in jeder ACL enthalten sein. Fehlt der Eintrag, so kommen in der Regel die Rechte des "-Default-"-Eintrages zur Anwendung.
- Es müssen nicht nur Benutzern, sondern auch Servern Zugriffsrechte auf eine Datenbank eingeräumt werden. Dies gilt insbesondere für Datenbanken, die repliziert werden sollen.
- Neben Zugriffsrechten können auch so genannte Rollen zur Zugriffssteuerung in Skripten und Agenten einer Datenbank zum Einsatz kommen. Auch die Zuteilung der Rollen muss im Rahmen der Zugriffsplanung berücksichtigt werden.

Ergänzende Kontrollfragen:

- Existiert für jede Datenbank ein Zugriffskonzept?
- Werden die ACL-Veränderungen auf wichtigen Datenbanken regelmäßig überprüft (ACL-Log)?

M 4.121 Konfiguration der Zugriffsrechte auf das Namens- und Adressbuch von Lotus Notes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Das Namens- und Adressbuch (NAB) eines Notes-Servers ist die zentrale Verwaltungsdatenbank, in der nicht nur die Benutzerverwaltung enthalten ist, sondern auch die wesentlichen Konfigurationsdaten eines Servers. Hierzu sind im NAB entsprechende Benutzerdokumente und Serverdokumente enthalten.

Die korrekte Zugriffskontrolle über die ACL-Einstellungen des NAB ist daher besonders wichtig. Bei der Konfiguration ist folgendes zu beachten:

- Das NAB enthält personenbezogene Daten, die entsprechend geschützt werden müssen.
- Im NAB sind auch wichtige Daten abgelegt, die für bestimmte Systemfunktionen zugreifbar sein müssen, z. B. E-Mail-Adresse und Zertifikate für die E-Mail-Verschlüsselung.
- Ein vollständiger Schutz persönlicher Daten ohne gleichzeitige Funktionseinbußen lässt sich in der Regel nur schwer realisieren.

Folgende Zugriffskonfigurationen auf das NAB für Benutzer können unterschieden werden:

- Die Gruppe "Alle Benutzer (All Users)" erhält "Autoren (Author)"-Rechte ohne optionale Attribute und ohne zusätzliche Rollen. Benutzer dürfen dann im NAB auf die Informationen anderer Benutzer lesend zugreifen. Insbesondere können jedoch folgende Felder der jeweiligen Registerkarten (Tabs) ihres eigenen Personendokuments verändert werden: **erweiterte Rechte**
  - Basic: Personal Title, Generation Qualifier, **Internet-Passwort**
  - Mail: Format preference incoming mail (z. B. MIME oder Richtext), Encryption incoming mail
  - Work/Home: alle Felder
  - Misc: alle Felder

  Diese Berechtigungskonfiguration (Author-Recht für alle Benutzer) erlaubt es insbesondere, dass Benutzer ihr eigenes Internet-Passwort verändern können, das z. B. an der Web-Schnittstelle und beim E-Mail-Zugriff via POP3 zur Authentisierung genutzt wird. Da zur Zeit keine integrierte Qualitätssicherung für das Internet-Passwort angeboten wird, können Benutzer so auch schwache Passwörter eintragen. Abhilfe kann hier nur durch entsprechende Benutzerschulung geschaffen werden oder indem das eigenständige Ändern des Internetpasswortes unterbunden wird (siehe nachfolgend).
- Die Gruppe "Alle Benutzer (All Users)" erhält "Leser (Reader)"-Rechte ohne optionale Attribute und ohne zusätzliche Rollen. Mit dieser Berechtigungskonfiguration können Benutzer nur lesend auf das NAB **nur Lese-Recht**

zugreifen. Alle Veränderungen an ihrem eigenen Personendokument (z. B. Verändern des Internet-Passwortes) müssen durch einen Administrator erfolgen.

- Die Gruppe "Alle Benutzer (All Users)" erhält keine Zugriffsrechte "Kein Zugriff (No Access)" auf das NAB. Diese Berechtigungskonfiguration stellt zwar den Schutz der im NAB enthaltenen persönlichen Daten sicher, hat jedoch Funktionseinbußen zur Folge, die für den Betrieb eines Notes-Systems nicht tolerierbar sind.

keine Zugriffsrechte

Für administrative Tätigkeiten kann eine Rollenaufteilung erfolgen. Es können jeweils Rollen vergeben werden für das Erzeugen oder Verändern von

- Gruppendokumenten (Rollen "[GroupCreator]" und "[GroupModifier]"),
- Serverdokumenten (Rollen "[ServerCreator]" und "[ServerModifier]"),
- Benutzerdokumenten (Rollen "[UserCreator]" und "[UserModifier]") sowie
- allen restlichen Dokumente des NAB (Rollen "[NetCreator]" und "[NetModifier]").

Trennung der administrativen Rollen

Die Aufteilung der Administrationstätigkeiten in verschiedene Rollen ist generell zu empfehlen. Es sollte geprüft werden, ob dies im vorliegenden Einsatzumfeld zweckmäßig ist.

Ergänzende Kontrollfragen:

- Soll das NAB über die Web-Schnittstelle sichtbar und zugreifbar sein?
- Soll das NAB in den Notes-Katalog aufgenommen werden?
- Sind Administrator-Rollen getrennt worden?

M 4.122 Konfiguration für den Browser-Zugriff auf Lotus Notes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Soll auf einen Lotus Domino Server mittels Browser zugegriffen werden, so muss auch bei dieser Zugriffsart angemessene Sicherheit gewährleistet werden.

Zur Absicherung des Browser-basierten Zugriffs sollten folgende Empfehlungen umgesetzt werden, die Server, Client und deren Kommunikationsmechanismen betreffen:

Einsatz von SSL

1. Jeder Zugriff, der eine Authentisierung benötigt, sollte mit SSL geschützt werden (siehe M 4.124 *Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes*).

starke Verschlüsselung

2. Es müssen Browser eingesetzt werden, die das SSL-Protokoll beherrschen (siehe M 4.127 *Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes*). Der Browser sollte starke Verschlüsselung unterstützen, also Verfahren mit mindestens 80 Bit Schlüssellänge.

geeignete Programmversion einsetzen

3. Der Domino Server muss für den SSL-geschützten Web-Zugriff konfiguriert werden (siehe M 4.123 *Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes*). Um starke Verschlüsselung zu gewährleisten, sollte mindestens die Version 5.0.4 des Domino Servers zum Einsatz kommen.

Zugriffsbeschränkungen auf Datenbankebene

4. Auch auf Datenbankebene sollten Zugriffsbeschränkungen eingerichtet werden (siehe M 4.125 *Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken*).

Wird der Web-Zugriff auf ein Notes-System geplant, so sind außerdem noch folgenden sicherheitsrelevanten Aspekte zu berücksichtigen:

- Das Notes-ID-Passwort darf nicht mit dem Internet-Passwort übereinstimmen.

  Für die Authentisierung an der Web-Schnittstelle kann u. a. der Mechanismus "Benutzername und Passwort" eingesetzt werden. Dabei kann das so genannte Internet-Passwort für jeden Benutzer frei festgelegt werden. Dies geschieht meist schon beim Anlegen neuer Benutzer. Es muss dabei jedoch darauf geachtet werden, dass hier nicht von der Option Gebrauch gemacht wird, das Internet-Passwort auf den Wert des Notes-ID-Passwortes zu setzen. Dies hat im wesentlichen zwei Gründe: einmal besteht die Möglichkeit, dass das Internet-Passwort auch im Klartext zwischen Client und Server übertragen wird, sodass es leicht kompromittiert werden kann. Weiterhin wird der Passwort-Hash im Personendokument eines Benutzers im Namens- und Adressbuch gespeichert. Je nach Konfiguration kann dieser Wert auch von anderen Personen eingesehen werden, sodass eine Wörterbuchattacke auf den Hash-Wert durchgeführt werden könnte. In beiden Fällen kann nach Kenntnis des Internet-Passwortes auch auf eine

Notes-ID-Datei zugegriffen werden, wenn hier das gleiche Passwort gewählt wurde (siehe auch M 4.124 *Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes*).

- Die gewünschte "Zugriffsart" für Benutzer auf das Namens- und Adressbuch muss eingerichtet werden.

  Der Zugriff für Benutzer auf das Namens- und Adressbuch kann "lesend" und "schreibend" eingerichtet werden. Bei schreibendem Zugriff können Benutzer nur ihr eigenes Personendokument verändern. Dadurch ist insbesondere das Verändern des Internet-Passwortes durch den Benutzer möglich, was u. U. die Administration vereinfacht. Nachteilig ist jedoch, dass damit keine Kontrolle über das Internet-Passwort, z. B. in Bezug auf Qualität und Länge, besteht und der Benutzer auch andere Einträge seines Personendokumentes editieren kann. Die "lesende" Konfiguration verhindert dies, erfordert jedoch das Eingreifen eines Administrators, wenn ein Benutzer sein Internet-Passwort verändern will. Der Benutzerzugriff auf das Namens- und Adressbuch kann auch ganz unterbunden werden. Dies hat den Vorteil, dass der Hash-Wert des Internet-Passwortes vor Kenntnisnahme durch Dritte geschützt ist. Dies verhindert jedoch auch, dass das Namens- und Adressbuch für die Adressierung, z. B. von E-Mails, zur Verfügung steht (siehe auch M 4.120 *Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken* und M 4.121 *Konfiguration der Zugriffsrechte auf das Namens- und Adressbuch von Lotus Notes*).

Ergänzende Kontrollfragen:

- Sind alle Browser-Zugriffe auf Lotus Notes SSL-gesichert?
- Wurde festgelegt, welche Zugriffsart für den Browser-Zugriff auf Lotus Notes eingerichtet wird?

M 4.123 Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der Web-Zugriff auf einen Domino Server kann ungeschützt über das Protokoll HTTP (HyperText Transfer Protocol) oder mit SSL (Secure Socket Layer) abgesichert über das Protokoll HTTPS erfolgen. Generell kann ein Server beide Varianten gleichzeitig unterstützen. Ist die Nutzung des ungeschützten Zugriffs möglich, so kann die SSL-Absicherung auch bei Bedarf angefordert werden, wenn auf eine Datenbank zugegriffen wird, deren Daten während der Übertragung geschützt werden müssen, oder wenn eine abgesicherte Authentisierung notwendig ist. Dazu kann in den Eigenschaften einer Datenbank angegeben werden, dass für den Zugriff eine SSL-Verbindung erforderlich ist (siehe M 4.125 *Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken*).

SSL-Port aktivieren

Damit der SSL-Zugriff überhaupt ermöglicht werden kann, muss der so genannte SSL-Port des Servers aktiviert werden. Dazu muss im Serverdokument der Status des SSL-Ports auf den Wert "Enabled" (Aktiviert) gesetzt werden. Durch diese Einstellung wird jedoch nur der SSL-Port zur Nutzung freigegeben. Damit eine SSL-Verbindung zustande kommen kann, muss der Server auf den SSL-Einsatz vorbereitet werden, indem für ihn ein SSL-Zertifikat ausgestellt wird (siehe M 5.86 *Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes*).

Sollen Web-Clients auf einen Server ausschließlich über SSL-geschützte Verbindungen zugreifen, so kann dies auf zwei Arten erreicht werden:

1. **HTTP-Port deaktivieren**

   Der ungeschützte HTTP-Port wird deaktiviert, indem im Serverdokument der Status des HTTP-TCP/IP-Ports auf "Disabled" (Deaktiviert) gesetzt wird. Durch diese Einstellung werden Client-Anfragen an den ungeschützten Port abgewiesen und es kommen keine unverschlüsselten Verbindungen mehr zustande.

2. **HTTP-Port umleiten**

   Der ungeschützte HTTP-Port wird auf den geschützten SSL-Port umgeleitet. Dazu wird im Serverdokument der Status des HTTP-TCP/IP-Ports auf "Redirect to SSL" gesetzt. Diese Einstellung hat den Vorteil, dass Client-Anfragen über ungeschützte Verbindungen nicht abgelehnt werden, sondern - sofern der Client SSL unterstützt - über eine geschützte Verbindung beantwortet werden.

Welche Konfiguration verwendet werden soll, hängt von den beabsichtigten Einsatzszenarien ab (siehe M 2.210 *Planung des Einsatzes von Lotus Notes im Intranet mit Browser-Zugriff*) und muss im Einzelfall entschieden werden.

Beispiele:

1. Folgende Tabelle zeigt die Einstellungen im Serverdokument, die ungeschützte anonyme Zugriffe sowie geschützte authentisierte und anonyme Zugriffe erlauben.

Das Anfordern der geschützten Authentisierung muss dabei durch das Aktivieren der Datenbank-Eigenschaft "Web access: Require SSL connection" erfolgen (siehe M 4.125 *Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken*).

Darf der Zugriff auf eine solche Datenbank nicht anonym erfolgen, so ist zusätzlich ein ACL-Eintrag für "Anonymous" mit dem Zugriffslevel "No access" einzurichten (siehe M 4.120 *Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken*).

HTTP-Einstellungen	TCP/IP port status:	Enabled
	Name & Password:	No
	Anonymous:	Yes
HTTPS(SSL)-Einstellungen	SSL port status:	Enabled
	Client certificate:	Enabled
	Name & Password:	Enabled
	Anonymous:	Yes

Tabelle: Serverdokument/Ports/Internet Ports

2. Folgende Tabelle zeigt die Einstellungen im Serverdokument, die die SSL-Absicherung für den Web-Zugriff erzwingen, indem entweder alle Anfragen an den ungeschützten Port auf den mit SSL geschützten Port umgeleitet werden ("Redirect to SSL") oder indem Anfragen auf dem ungeschützten Port nicht beantwortet werden ("Disable").

HTTP-Einstellungen	TCP/IP port status:	Redirect to SSL oder Disabled
	Name & Password:	No
	Anonymous:	No
HTTPS(SSL)-Einstellungen	SSL port status:	Enabled
	Client certificate:	Enabled* oder Disabled*
	Name & Password:	Enabled* oder Disabled*
	Anonymous:	Yes* oder No*

Tabelle: Serverdokument/Ports/Internet Ports

*: Mindestens einer der Authentisierungsmechanismen muss aktiviert sein, damit Anfragen vom Server angenommen werden. Sind alle Mechanismen aktiviert und ist eine Authentisierung für die angeforderte Web-Seite notwendig, wird zunächst nach einem Client-Zertifikat verlangt. Wenn der Client nicht im Besitz eines Zertifikats ist, werden danach Benutzername und Passwort angefordert.

Ergänzende Kontrollfragen:

- Welches Protokoll wird für den Zugriff auf den Domino Server genutzt?

- Wie wird die Vertraulichkeit der übertragenen Daten sichergestellt?

M 4.124 Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Bei der Nutzung von Browsern zum Zugriff auf einen Lotus Domino Server muss entschieden werden, welches Authentisierungsverfahren an der Web-Schnittstelle zum Einsatz kommen soll. An der Web-Schnittstelle stehen verschiedene Authentisierungsmechanismen zur Verfügung:

1. Keine Authentisierung: Anonymer Zugriff
2. Authentisierung über Benutzername und Passwort
3. Authentisierung mittels Client-Zertifikaten

anonyme Zugriffe

Zunächst ist daher zu ermitteln, ob anonyme Zugriffe auf den Server erlaubt werden müssen. Dies ist dann der Fall, wenn öffentliche Daten auch Benutzern zugänglich gemacht werden sollen, die keine Notes-Benutzer sind. Es empfiehlt sich jedoch, öffentliche Daten auf einem speziellen Server zu halten, der ausschließlich öffentliche Daten enthält. Für einen solchen Server kann der anonyme Zugriff erlaubt werden. Auf einem Produktionsserver sollten anonyme Zugriffe generell nicht erlaubt sein, sodass an der Web-Schnittstelle immer authentisiert wird.

Die Art der zu nutzenden Authentisierungsverfahren hängt von verschiedenen Faktoren ab. Folgendes muss dabei (auch im Rahmen einer Risikoabschätzung) berücksichtigt werden:

1. Authentisierung über Benutzername und Passwort

   Im Rahmen des HTTP-Protokolls kann ein Benutzer durch das Eingeben von Benutzername und Passwort authentisiert werden. Die Daten werden durch den Browser eingelesen und von diesem bei jeder Anfrage an den Server (hier das Domino Web-Server-Modul) gesendet.

   Folgende sicherheitsrelevanten Aspekte sind bei der Nutzung dieses Authentisierungsverfahrens zu berücksichtigen:

   a. **Web-Zugriff nur mit SSL**

      Ohne SSL-Absicherung werden die Authentisierungsdaten bei jeder Anfrage nur in 7-Bit-Code umgewandelt aber offen (im base64-Format) übertragen und können daher leicht abgehört und durch Dritte in Erfahrung gebracht werden. Der Web-Zugriff sollte daher immer mit SSL erfolgen (siehe M 4.123 *Einrichten des SSL-geschützten Browser-Zugriffs auf Lotus Notes*).

   b. **unterschiedliche Passwörter wählen**

      Das Internet-Passwort muss verschieden vom Passwort der Notes-ID gewählt werden. Gelingt es einem Angreifer, das Internet-Passwort in Erfahrung zu bringen, und wird dieses Passwort auch für die Notes-ID verwendet, so kann der Angreifer auch die Notes-ID verwenden (sofern er darauf Zugriff erlangen kann). Mit der Notes-ID kann der Angreifer dann über einen Notes-Client auf das Lotus Domino System zugreifen, und die erweiterten Funktionen von

Notes-Clients nutzen, beispielsweise Zertifikate exportieren und das Passwort der Notes-ID ändern).

c. In älteren Notes-Versionen (vor 4.6) wird das Internet-Passwort im Personendokument so gespeichert, dass gleiche Passwörter zum gleichen Wert führen (es wird ein so genannter "unsalted hash" genutzt). Dadurch ist es sehr einfach, gleiche Passwörter zu suchen bzw. zu entdecken. Ältere Notes-Versionen sollten daher möglichst nicht eingesetzt werden.

aktuelle Notes-Version einsetzen

d. An der Web-Schnittstelle existiert keine Beschränkung für Fehlversuche bei der Authentisierung. Eine solche Beschränkung kann mit Hilfe von Zusatzprodukten von Drittherstellern nachgerüstet werden. Es wird empfohlen zu prüfen, ob der Einsatz eines solchen Zusatzprodukts im vorliegenden Anwendungsfall erforderlich ist.

zusätzliche Sicherheitsprodukte

Dieser Authentisierungsmechanismus weist bei seiner Nutzung über ungeschützte Verbindungen inhärente Schwächen auf. Daher sollte der Zugriff auf einzelnen Datenbanken für Benutzer eingeschränkt werden (siehe Maßnahme M 4.125 *Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken*), wenn sie über diesen Mechanismus authentisiert werden.

2. Authentisierung mittels Client-Zertifikaten

Folgende sicherheitsrelevanten Aspekte sind bei der Nutzung dieses Authentisierungsverfahrens zu berücksichtigen:

a. Damit Client-Zertifikate verwendet werden können, muss SSL (Version 3) mit Client-Authentisierung benutzt werden. Da alle Browser-Verbindungen generell mit SSL gesichert werden sollten, stellt dies keine Einschränkung dar.

Client-Zertifikate erfordern SSL

b. Jeder Benutzer (genauer: dessen Browser) muss mit einem Client-Zertifikat versorgt werden. Dies bedeutet entweder den Betrieb eines eigenen Zertifizierungsservers oder das Einrichten einer Vertrauensstellung für eine externe Zertifizierungsstelle. Zusätzlich muss die Verwaltung der Zertifikate erfolgen. Dies bedeutet erhöhten Aufwand und setzt entsprechendes Wissen bei den Administratoren und auch Benutzern voraus. Insbesondere die Benutzer müssen mit den Managementfunktionen für Zertifikate im Browser vertraut sein.

Zertifikats-Management

c. Die Sicherheit der Authentisierung hängt wesentlich von der lokalen Sicherheit des Web-Clients ab (siehe M 4.127 *Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes*).

Sicherheit der Clients

Ein generelles Votum für genau einen der beiden Mechanismen kann an dieser Stelle nicht gegeben werden. Es ist jedoch möglich, beide Mechanismen parallel zu aktivieren. In diesem Fall wird vom Server zunächst vom Client eine Authentisierung mittels SSL-Client-Zertifikat angefordert. Besitzt der Client kein Zertifikat oder verweigert der Benutzer die Nutzung des Zertifikats, so kommt der Mechanismus "Benutzername und Passwort" zum Einsatz.

Beispiel:

Folgende Tabelle zeigt die Einstellungen im Serverdokument, die eine SSL-Authentisierung mittels Client-Zertifikat ("Client Certificate" = Enabled) und/oder die SSL-gesicherte Authentisierung über Benutzername und Passwort ("Name & Password" = Enabled) erzwingen. Damit keine ungesichertenVerbindungen angenommen werden, werden alle Verbindungswünsche entweder an den SSL-Port weitergeleitet ("TCP/IP port status" = Redirect to SSL) oder verweigert ("TCP/IP port status" = Disable). Der SSL-Port wird so konfiguriert, dass auch keine anonymen Verbindungen über eine SSL-Verbindung angenommen werden ("Anonymous" = No).

HTTP-Einstellungen	TCP/IP port status:	Redirect to SSL oder Disable
	Name & Password:	No
	Anonymous:	No
HTTPS(SSL)-Einstellungen	SSL port status:	Enabled
	Client certificate:	Enabled oder Disabled*
	Name & Password:	Enabled oder Disabled*
	Anonymous:	No

Tabelle: Serverdokument/Ports/Internet Ports

Ergänzende Kontrollfrage:

- Welche Authentisierungsmechanismen werden bei dem Browser-Zugriff auf dem Lotus Domino Server genutzt?

M 4.125 Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Wird auf einen Lotus Domino Server auch mittels Browser zugegriffen, so müssen neben den übrigen Server-bezogenen Sicherheitsmechanismen (siehe M 4.122 *Konfiguration für den Browser-Zugriff auf Lotus Notes*) auch Datenbank-bezogene Mechanismen zum Einsatz kommen. Damit wird einerseits erreicht, dass der Zugriff auf eine Datenbank nur erfolgen kann, wenn eine gesicherte Verbindung zwischen Client und Server besteht (oder aufgebaut werden kann), und andererseits kann der Zugriff für Web-Clients generell eingeschränkt werden.

Folgende Datenbank-bezogenen Sicherheitsmechanismen sollten eingesetzt werden:

1. Für alle Datenbanken sollte die Nutzung von SSL (Zugriff mittels HTTPS) als Zugriffsvoraussetzung in den Eigenschaften der jeweiligen Datenbank aktiviert werden. Dies ist insbesondere dann wichtig, wenn der Server auch für den ungesicherten Zugriff mittels HTTP konfiguriert ist.

Zugriff nur über SSL

2. Wird als Authentisierungsverfahren "Benutzername und Passwort" genutzt (siehe M 4.124 *Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes*), so ist für jede Datenbank der maximale Zugriffslevel in den Datenbankberechtigungen einzustellen. Insbesondere kann durch die Nutzung des Zugriffslevels "No Access" der Web-Zugriff auf einzelne Datenbanken unterbunden werden. Falls der Web-Zugriff als alleiniger Zugriffsmechanismus genutzt wird, muss bei der Wahl des Zugriffslevels bedacht werden, dass für die Benutzer an der Web-Schnittstelle keine zusätzlichen Funktionseinbußen entstehen sollten. In diesem Fall müssen Benutzer in der Regel auch mindestens schreibenden Zugriff erhalten, sodass dieser zugriffeinschränkende Mechanismus nicht als solcher verwendet werden kann.

   möglichst restriktiver Zugriffslevel

   Hinweis: Der in der Abbildung angegebene Zugriffslevel "Reader" stellt keine Empfehlung für den hier einzustellen Parameter dar. Vielmehr muss dieser Wert für jede Datenbank separat bestimmt werden.

Weiterhin ist folgender sicherheitsrelevanter Aspekt beim Web-Zugriff auf Lotus Notes Datenbanken zu berücksichtigen: Kann auf einen Domino Server über die Web-Schnittstelle zugegriffen werden und wird die Authentisierung mittels SSL-Client-Zertifikaten genutzt (siehe M 4.124 *Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes*), so können einzelne Datenbanken nicht vom Web-Zugriff ausgenommen werden. Vielmehr werden den authentisierten Benutzern die für sie eingetragenen ACL-Berechtigungen zugestanden (siehe auch M 4.120 *Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken*).

M 4.126 Sichere Konfiguration eines Lotus Notes Clients

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Zum Zugriff auf einen Notes-Server wird in der Regel der Lotus Notes Client benutzt. Für den Zugriff auf den Server erfolgt eine Authentisierung durch die Notes-ID. Die Notes-ID ist daher vor fremden Zugriffen geschützt aufzubewahren. Naturgemäß muss auch die Client-Konfiguration so verändert werden, dass ein möglichst sicheres Arbeiten mit dem Notes-Client erfolgen kann.

Neben der physikalischen Sicherheit und der sicheren Betriebssystemkonfiguration der Clients (siehe auch die jeweils relevanten Bausteine), sind insbesondere die folgenden Notes-spezifischen Sicherheitsaspekte zu berücksichtigen:

Bildschirmschoner aktivieren bei kurzfristiger Abwesenheit

- Damit der Client auf die Notes-ID-Datei zugreifen kann, muss der Benutzer das Notes-ID-Passwort eingeben. Nachdem die Notes-ID in dieser Form freigeschaltet wurde, kann im Prinzip jeder, der Zugriff auf die Konsole des Clients besitzt, auf den oder die Server authentisiert zugreifen. Um dies zu verhindern, kann der Notes-Client durch Drücken der Funktionstaste "F5" veranlasst werden, vor der nächsten Aktion das Notes-ID-Passwort erneut abzufragen. Dieser Mechanismus kann zum Sperren des Notes-Clients bei kurzzeitiger Abwesenheit vom Arbeitsplatz benutzt werden (siehe auch M 4.129 *Sicherer Umgang mit Notes-ID-Dateien*). Die Benutzer müssen darauf hingewiesen werden, dass bei Verlassen des Arbeitsplatzes dieser oder ein anderer Passwort-geschützter Bildschirmschoner zu aktivieren ist.

unsignierte aktive Datenbankinhalte nicht ausführen

- Beim Zugriff auf Datenbanken werden - je nach Datenbank - auch aktive Datenbankinhalte (Skripten oder Agenten) durch den Client ausgeführt. Je nach Ursprungsort birgt dies Gefahren, z. B. könnte jemand durch ein trojanisches Pferd unerlaubten Zugriff auf lokale Datenbanken nehmen. Alle Datenbanken und alle aktiven Inhalte sollten daher durch eine spezielle Notes-ID signiert werden (siehe M 4.130 *Sicherheitsmaßnahmen nach dem Anlegen neuer Lotus Notes Datenbanken*). Danach kann über die so genannte ECL (Execution Control List) eingestellt werden, ob aktive Inhalte, die durch eine bestimmte Notes-ID signiert wurden, auf einem Client ausgeführt werden dürfen und welche nicht: Generell kann hier empfohlen werden, dass unsignierte aktive Datenbankinhalte nicht ausgeführt werden dürfen. Die ECL wird Server-gesteuert an alle Clients beim Client-Setup verteilt. Problematisch ist, dass die ECL auf einem Client unter Windows NT in der Datei "DESKTOP.DSK" gespeichert wird, die der Benutzer löschen kann, so dass die ECL-Einstellungen umgangen werden können. Daher sollten die Benutzer auf die Bedeutung dieser Einstellung für die Systemsicherheit hingewiesen werden. Das automatische Update der Client-ECL kann jedoch auch periodisch geschehen, sodasss die Client-ECL immer wieder "aktiviert" werden kann. Dazu stehen zwei Mechanismen zur Verfügung:

- Der Parameter "ECLSetup" wird in der Datei "Notes.ini" des Clients auf einen Wert kleiner 3 gesetzt. Dadurch wird beim nächsten Start des Clients die ECL vom Server geladen. Dies bedeutet jedoch einen zusätzlichen organisatorischen Aufwand, da der Parameter auf dem Client verändert werden muss.
- Das Update erfolgt skriptgesteuert (Funktion "@RefreshECL") durch Verändern der Schablone einer Datenbank, auf die Benutzer regelmäßig zugreifen (z. B. die E-Mail-Datenbank). Dies erfordert jedoch Eigenprogrammierung und das Verändern einer Datenbank-Schablone.

Für die eigentliche ECL gilt, dass die Berechtigungen für alle ECL-Einträge überprüft und entsprechend der IT-Sicherheitsrichtlinie gesetzt werden müssen. Insbesondere sollten die Einträge "-Default-" und "Keine Unterschrift (No Signature)" einer genauen Prüfung unterzogen werden.

Um die sichere Kommunikation zwischen Server und Client zu erzwingen, kann die Port-Verschlüsselung genutzt werden (siehe M 5.84 *Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation*).

Beispiel:

Folgende ECL-Einstellungen können als Ausgangspunkt für eigene ECLs dienen. Je nach Anwendungsszenario müssen die ECLs um Berechtigungen für aktive Inhalte, die entsprechende Signaturen tragen, erweitert werden. <admin> ist ein Platzhalter für einen Administrator und <QS> ist ein Platzhalter für eine organisationsinterne Prüfinstanz, die aktive Inhalte prüft und zur Benutzung freigibt.

Flag	-Default-	-keine Unterschrift-	<admin>	Lotus Notes Template development/ Lotus Notes	<QS>
Allow user to modify ECL	--	--	--	--	--
Access to the file system			X	X	X
Access to the current database			X	X	X
Access to environment variables			X	X	X
Access to non-Notes databases			X	X	X

Tabelle: ECL-Einstellungen

Flag	-Default-	-keine Unterschrift-	<admin>	Lotus Notes Template development/ Lotus Notes	<QS>
Access to external code			X	X	X
Access to external programs			X	X	X
Ability to send mail			X	X	X
Ability to read other databases			X	X	X
Ability to modify other databases			X	X	X
Ability to export data			X	X	X
Access to the Workstation Security ECL			X		

Tabelle: ECL-Einstellungen (Fortsetzung)

Ergänzende Kontrollfragen:

- Wird eine aktuelle Notes-Client Version eingesetzt?
- Wurden die Benutzer über die Sicherheitsmechanismen des Notes-Clients informiert?
- Wird die Notes-ID gesichert aufbewahrt, sodass das unbefugte Kopieren nicht möglich ist?
- Wird ein Passwort-geschützter Bildschirmschoner eingesetzt?

M 4.127 Sichere Browser-Konfiguration für den Zugriff auf Lotus Notes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Browser-Zugriff über HTTP

Um über die Web-Schnittstelle auf einen Lotus Domino Server zuzugreifen, benötigt der Benutzer einen "Web-Client" in Form eines Browsers. Der Zugriff auf die Serverdaten erfolgt durch Anfragen an das HTTP-Modul des Domino Servers. Dieses extrahiert seinerseits die Daten aus den entsprechenden Datenbanken und wandelt sie in WWW-Seiten um, sodasss diese vom Browser des Benutzers dargestellt werden können. Durch die Nutzung von aktiven Inhalten (JavaScript, Java-Applets) können Modifikationen der Datenbankinhalte über eine dem normalen Notes-Client nachempfundene graphische Oberfläche erfolgen.

Server, Client und Kommunikation müssen sicher sein

Die Sicherheit beim Web-Zugriff hängt von der Sicherheit der beteiligten Komponenten ab. Neben der sicheren Konfiguration der Server (siehe M 4.122 *Konfiguration für den Browser-Zugriff auf Lotus Notes*) und der Nutzung der Kommunikationsabsicherung (siehe M 5.86 *Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes*), ist die Sicherheit des Web-Clients ein wesentlicher Faktor.

Schutz der Authentisierungsdaten

Bei Web-Zugriffen erfolgt die Speicherung der Authentisierungsgeheimnisse auf dem Client. Erlangt ein unberechtigter Dritter Zugriff auf diese Daten, so kann er unter den Berechtigungen des kompromittierten Benutzers auf die Datenbanken eines Server zugreifen. Die in diesem Zusammenhang zu schützenden Authentisierungsdaten sind:

- Benutzername und Passwort für den Web-Zugriff. Diese Daten sollten nicht lokal gespeichert werden, da die Sicherheit der Authentisierung darauf beruht, dass diese Daten ausschließlich dem jeweiligen Benutzer bekannt sind und dieser sie bei jeder Authentisierung erneut eingibt. Leider bieten moderne Browser vielfach die Möglichkeit, diese Daten lokal zu speichern, so dass sie bei späteren Zugriffen auf die ebenfalls gespeicherte Adresse des Servers automatisch an den Server übertragen werden. Daher müssen die Benutzer darauf hingewiesen werden, dass das Passwort für den Web-Zugriff nicht lokal gespeichert werden darf.
- Kryptographische Schlüssel und Zertifikate, die im Rahmen der SSL-Client-Authentisierung benutzt werden. Da diese Authentisierungsdaten nur in maschinenlesbarer Form vorliegen, ist die Speicherung der Daten notwendig. In der Regel werden die Daten lokal auf dem Client abgelegt.

Sicherheit des Rechners und des Browsers

Generell kann unterschieden werden zwischen der physikalischen Sicherheit des als Client verwendeten Rechners und der Sicherheit des als Web-Client benutzten Browsers. Dadurch ergeben sich die im folgenden beschriebenen Sicherheitsaspekte.

Durch das lokale Speichern der Authentisierungsdaten kommt der physikalischen Sicherheit besondere Bedeutung zu. Daher sollten für die Client-

Sicherheit die jeweiligen Bausteine sorgfältig umgesetzt werden.

Insbesondere sollten folgende Maßnahmen, sofern sie anwendbar sind, für die genutzten Rechner umgesetzt werden:

- M 4.1 *Passwortschutz für IT-Systeme*
- M 1.33 *Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz*
- M 1.34 *Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz*
- M 1.44 *Geeignete Einrichtung eines häuslichen Arbeitsplatzes*
- M 1.46 *Einsatz von Diebstahl-Sicherungen*

Zusätzlich muss auch die Sicherheit des Browsers in Betracht gezogen werden. Dies gilt insbesondere, wenn Authentisierungsdaten durch den Browser lokal abgespeichert werden. Es müssen unter anderem folgende Fragestellungen berücksichtigt werden:

- Wo werden die Authentisierungsdaten gespeichert?

  Mögliche Speicherorte sind z. B. eine Datei, eine Datenbank, die Registry, eine Chipkarte oder der Systemzertifikatsspeicher (bei Windows 2000).

- Werden die Authentisierungsdaten geschützt gespeichert?

  Mögliche Schutzmechanismen sind beispielsweise Verschlüsselung, Passwort-Schutz oder ein PIN-geschütztes Hardware-Token (etwa eine Chipkarte).

- Wie stark ist der Schutz der eingesetzten Sicherheitsmechanismen?

  Bei Verschlüsselung wird die Stärke des Schutzes wesentlich durch die eingesetzten Verfahren und die verwendeten Schlüssellängen bestimmt.

Werden Authentisierungsdaten lokal auf dem Client gespeichert, so sollten diese Daten so geschützt sein, dass sie auch nach einer erfolgten physikalischen Kompromittierung des Rechners oder der Schutzmechanismen des Betriebssystems nicht erlangt werden können. Dies erfordert in der Regel den Einsatz von Verschlüsselungsmechanismen durch den Browser. Werden diese Anforderungen durch den Browser nicht erfüllt, so muss im Rahmen einer Risikoabschätzung entschieden werden, ob der Web-Zugriff dennoch erlaubt werden soll. Dies hängt letztendlich auch davon ab, auf welche Daten zugegriffen werden soll.

aktive Inhalte

Ein weiteres Problemfeld stellen die beim Web-Zugriff verwendeten aktiven Inhalte dar. Damit die Funktionalität der Web-Schnittstelle maximal genutzt werden kann, muss im verwendeten Browser die Verarbeitung und die Ausführung aktiver Inhalte aktiviert werden, da die vom Domino Server generierten HTML-Seiten JavaScript und Java-Applets enthalten. Wird die entsprechende Unterstützung im Browser deaktiviert, so ist mit fast vollständigem Funktionsverlust zu rechnen.

gemischte Nutzung des Browsers vermeiden

Wird der Browser auch zum Zugriff auf das Internet genutzt, so ist hier jedoch in der Regel die Ausführung aktiver Inhalte zu deaktivieren (siehe M 5.69 *Schutz vor aktiven Inhalten*). Erfolgt die Umstellung durch den

Benutzer selbst, so kann durch die gemischte Nutzung leicht das Abschalten aktiver Inhalte für den Internetzugriff vergessen werden. Dies bedeutet dann eine erhöhte Gefahr für das lokale Rechnernetz, da nun unter Umständen schädliche aktive Inhalte durch den Browser ausgeführt werden. Eine gemischte Nutzung des Browsers sollte daher nach Möglichkeit vermieden werden.

Benutzer einweisen

Bei der Nutzung von Browsern können durch falsche Handhabung durch die Benutzer verschiedene Sicherheitsprobleme auftreten. Daher müssen die Benutzer in deren sichere Bedienung eingewiesen und verpflichtet werden, die aufgeführten Sicherheitsrichtlinien zu beachten.

Ergänzende Kontrollfrage:

- Wie wird der Browser-Zugriff auf den Domino Server abgesichert?

M 4.128 Sicherer Betrieb von Lotus Notes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Sicherheit eines komplexen Systems muss im Betrieb permanent aufrechterhalten werden, insbesondere da sich im laufenden Betrieb notwendige Systemveränderungen ergeben. Es genügt daher nicht, eine sichere Anfangskonfiguration zu erzeugen (siehe M 4.116 *Sichere Installation von Lotus Notes* und M 4.117 *Sichere Konfiguration eines Lotus Notes Servers*). Folgende Sicherheitsaspekte sind im laufenden Betrieb für ein Lotus Notes System zu berücksichtigen.

Sicherheit der Notes-ID ist wesentlich für die Gesamtsicherheit von Lotus Notes

- Die Sicherheit, die die Zugriffsmechanismen auf Lotus Notes Server und Datenbanken bieten, basiert auf der Authentisierung der Benutzer durch ihre Notes-ID, die in einer Datei gespeichert wird. Die Systemsicherheit hängt damit direkt von der Sicherheit im Umgang mit der Notes-ID-Datei ab. Im Rahmen des Sicherheitskonzepts (siehe M 2.207 *Festlegen einer Sicherheitsrichtlinie für Lotus Notes*), sind daher u. a. auch Richtlinien für den Umgang mit Notes-ID-Dateien festzulegen. Die dabei zu berücksichtigenden Aspekte sind in der Maßnahme M 4.129 *Sicherer Umgang mit Notes-ID-Dateien* zusammengefasst.

sorgfältige Installation von Datenbanken

- Veränderungen in einem Notes-System ergeben sich insbesondere dann, wenn neue Datenbanken auf einem Server erzeugt werden. Neu angelegte Datenbanken sind jedoch in der Regel noch nicht in die bestehenden Sicherheitsstrukturen eingebunden. Die Installation einer Datenbank sollte daher erst als abgeschlossen betrachtet werden, wenn mindestens die in der Maßnahme M 4.130 *Sicherheitsmaßnahmen nach dem Anlegen neuer Lotus Notes Datenbanken* zusammenfassten Schritte durchgeführt worden sind. Die Berechtigung zum Erstellen neuer Datenbanken oder zum Erzeugen von Datenbank-Repliken kann explizit durch entsprechende Zugriffslisten gesteuert werden (siehe M 4.119 *Einrichten von Zugangsbeschränkungen auf Lotus Notes Server*).

Verschlüsselung von Datenbanken

- Die in verschiedenen Datenbanken enthaltenen Daten besitzen in der Regel unterschiedlichen Schutzbedarf (siehe auch die Schutzbedarfsfeststellung aus der IT-Grundschutz-Vorgehensweise). Lotus Notes bietet neben der reinen Zugriffskontrolle auch die Möglichkeit, Datenbanken zu verschlüsseln. Ergibt die Schutzbedarfsfeststellung für eine Datenbank die Notwendigkeit, die Daten mittels Verschlüsselung zu schützen, so sind die Empfehlungen aus M 4.131 *Verschlüsselung von Lotus Notes Datenbanken* zu berücksichtigen.

Überwachung der Systeme

- Um Aussagen über die Sicherheit eines Lotus Notes Systems zu erhalten, ist es notwendig, das System zu überwachen. Ziel einer solchen Überwachung ist es, Verstöße gegen die geltenden Sicherheitsvorschriften zu entdecken, bestehende Sicherheitslücken aufzudecken oder Fehlkonfigurationen, die potentiell zu Sicherheitslücken führen können, zu erkennen. Ein entsprechendes Überwachungskonzept sollte Teil des IT-Sicherheitskonzepts sein. Komplexe Systeme wie Lotus Notes können dabei in

der Regel nicht mehr manuell durch einzelne Administratoren überwacht werden, sondern die Überwachung muss automatisch durch entsprechende Systemkomponenten oder Produkte von Drittherstellern erfolgen. Dabei muss auch die Konfiguration der Überwachung regelmäßig an das sich verändernde System angepasst werden. Die Empfehlungen zur Überwachung sind in M 4.132 *Überwachen eines Lotus Notes-Systems* zusammengefasst.

gruppenbasiertes Zugriffskonzept

- Ein wichtiger Aspekt der Sicherheit eines Lotus Notes Systems ist die konsistente Verwaltung von Benutzern und Berechtigungen. Das administrative Konzept hat dabei Auswirkungen auf die Komplexität der durchzuführenden administrativen Aufgaben. Komplexe Abläufe können jedoch dazu führen, dass Fehlkonfigurationen entstehen. Um einen sicheren Systemzustand zu erhalten, sollten die administrativen Aufgaben daher möglichst einfach sein. Das Zugriffskonzept sollte deshalb auf Gruppen basieren. Dadurch wird die Verwaltung von Zugriffsrechten auf Datenbanken wesentlich vereinfacht und weniger fehleranfällig. Beispielsweise sollte im Rahmen des Gruppenkonzeptes eine so genannte "Termination Group" vorgesehen werden, in die alle "gelöschten" Benutzer übernommen werden und der alle Rechte explizit verweigert sind.

  Hinweis: Unter der Version 4.x können Gruppen nur eine bestimmte Anzahl von Benutzern aufnehmen, da diese in einem entsprechenden Feld im Serverdokument gespeichert werden. Wird die maximale Feldgröße erreicht, so funktioniert die jeweilige Gruppe nicht mehr korrekt. Bei Gruppen mit vielen Mitgliedern (z. B. alle Serverbenutzer, Termination Group) empfiehlt sich daher die Schachtelung von Gruppen.

- Die Sicherheitseinstellungen eines Servers sollten regelmäßig überprüft werden.

- Die Protokolldateien eines Servers sollten regelmäßig überprüft werden. Dies kann manuell oder mit Hilfe von Tools geschehen.

Beispiele:

- **Gruppenbasiertes Zugriffskonzept:**

  Ein Mitarbeiter wechselt die Abteilung, wodurch die Anpassung der Zugriffsrechte erforderlich ist.

  Werden benutzerbezogene ACL-Listen genutzt, so muss jede Datenbank "angefasst" werden, um den Benutzer entweder aus der ACL-Liste auszutragen oder neu einzutragen.

  Werden gruppenbezogene ACL-Listen genutzt, so muss der Benutzer lediglich in der Benutzerverwaltung aus den relevanten Gruppen entfernt bzw. eingetragen werden. Die Änderung kann zentral auf dem Benutzerobjekt erfolgen.

- **Termination Group:**

  Ein Mitarbeiter verlässt das Unternehmen. Das Konto wird versehentlich nicht aus einer Notes-Gruppe gelöscht. Über diese Gruppenmitgliedschaft besitzt der ehemalige Mitarbeiter weiterhin das Recht, auf den Notes-

Server zuzugreifen. Da sein Notes-Konto jedoch auch in die Termination Group eingefügt wird, erhält er keinen Zugriff auf den Server. Der Grund ist, dass der Termination Group explizit der Zugriff auf den Server (und dessen Datenbanken) verweigert ist und Verweigerungen vorrangig gegenüber Zugeständnissen von Zugriffsrechten sind.

Ergänzende Kontrollfragen:

- Werden die Sicherheitseinstellungen der Notes Server regelmäßig überprüft?
- Werden die Protokolldateien der Notes Server regelmäßig überprüft?

M 4.129 Sicherer Umgang mit Notes-ID-Dateien

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Notes-ID ist sicherheitskritisch

Lotus Notes-Benutzer authentisieren sich einem Domino Server gegenüber durch die Notes-ID. Die Notes-ID liegt in Form einer Datei vor und wird in der Regel mit dieser identifiziert. In der Notes-ID können - neben dem Notes-Zertifikat (zertifizierter öffentlicher Schlüssel) und dem zugehörigen privaten Schlüssel eines Benutzers - auch weitere Informationen gespeichert werden. So sind darin u. a. auch Internet-Zertifikate, symmetrische Verschlüsselungsschlüssel und Informationen, die zum Wiederherstellen von Notes-ID-Dateien (Recovery-Informationen) benötigt werden, enthalten. Alle diese Informationen werden durch das so genannte Notes-ID-Passwort geschützt. Bevor die Notes-ID genutzt werden kann, muss der Benutzer das entsprechende Passwort eingeben. Da eine Notes-ID sicherheitskritische Informationen enthält, kommt ihr ein erhöhter Schutzbedarf zu. Folgende Aspekte sind daher für den Umgang mit Notes-IDs zu berücksichtigen:

vier verschiedene Kategorien von Notes-IDs

Notes-IDs können in vier Kategorien unterteilt werden:

1. Certifier-IDs: Diese stellen die Identitäten dar, die Notes-IDs für Server und Benutzer ausstellen. In der Regel repräsentieren Certifier-IDs organisatorische Einheiten innerhalb einer Behörde bzw. eines Unternehmens und bilden eine Hierarchie. Certifier-IDs sind aufgrund ihres Verwendungszwecks besonders sicherheitskritisch und müssen daher besonders geschützt werden. Dies gilt insbesondere für die erste erzeugte Certifier-ID - die so genannte Root-Certifier-ID - mit der alle weiteren Certifier-IDs signiert werden.
2. Server-IDs: Diese weisen Server gegenüber Benutzern (genauer: deren Notes-Clients) und anderen Servern aus. Damit ein Server lauffähig ist, benötigt er eine eigene Identität in Form der Server-ID. Die Server-ID wird während der Serverinstallation automatisch erzeugt und durch eine Certifier-ID zertifiziert. Da Server-IDs für ausgezeichnete Systemkomponenten zur Identifikation benutzt werden, müssen sie entsprechend gut geschützt werden.
3. Administrator-IDs: Diese weisen Administratoren gegenüber Servern aus. Administrator-IDs unterscheiden sich von Benutzer-IDs durch erweiterte Privilegien, die die Administration von Servern ermöglicht. Da Administratoren unter den Benutzern eine privilegierte Stellung einnehmen, müssen Administrator-IDs besonders geschützt werden.
4. Benutzer-IDs: Diese weisen normale Benutzer gegenüber Servern aus.

Entsprechend den unterschiedlichen Sicherheitsanforderungen müssen unterschiedliche Schutzmaßnahmen für Notes-IDs getroffen werden. Zu betrachten sind dabei die Aspekte

- Erzeugung,
- Gültigkeitsdauer,

- Passwortqualität,
- Verteilung und Aufbewahrungsort sowie
- Wiederherstellung.

Qualitätsskala für Passwörter

Für die Passwörter können Qualitätsanforderungen beim Erzeugen einer neuen Benutzer-ID festgelegt werden. Dafür steht eine numerische Qualitätsskala von 0 (kein Passwort) bis 16 zur Verfügung. Generell stimmt zwar die akzeptierte Passwortlänge mit dem numerischen Qualitätswert überein, ist jedoch nicht das einzige Bewertungskriterium. Leider ist aber zur Zeit keine Liste von Lotus verfügbar, in der beschrieben wird, welche genauen Voraussetzungen ein Passwort zum Erreichen eines speziellen Qualitätsniveaus erfüllen muss.

Für die verschiedenen Kategorien von Notes-IDs enthält die folgende Liste entsprechende Empfehlungen, die je nach Anforderungen adaptiert und erweitert werden können.

- **Certifier/Root-Certifier-ID:**
  - **Erzeugung**: Die ID wird automatisch beim Einrichten des ersten Notes-Servers erzeugt. Erzeugung in sicherer Umgebung, unter Vier-Augen-Prinzip.
  - **Gültigkeit**: Lange Gültigkeit (mehrere Jahrzehnte, Default = 100 Jahre), wird nie gewechselt (Ausnahme: Kompromittierung der Certifier-ID).
  - **Passwort**: Mehrfachpasswort notwendig (mindestens zwei Personen, Vier-Augen-Prinzip). Erfordert sichere Passwörter (Notes-Qualität mindestens 10). Zur Realisierung des Vier-Augen-Prinzips bietet Notes die Möglichkeit an, eine Notes-ID-Datei mit mehreren Passwörtern zu schützen. Die Notes-ID-Datei kann nur nach Eingabe *aller* Passwörter verwendet werden. Es sind Intervalle für den erzwungenen Passwortwechsel anzugeben (empfohlen werden höchstens 30 bis 40 Tage).
  - **Speicherung**: Wird beim Anlegen neuer Benutzer oder Server benötigt. Eine Speicherung im Namens- und Adressbuch (NAB) ist nicht zulässig. Speicherung nur auf mobile Datenträger, z. B. Diskette oder CD-ROM, zwei Sicherheitskopien mit hinterlegten Passwörtern, an verschiedenen Orten vor fremden Zugriffen geschützt aufzubewahren.
  - **Wiederherstellung**: Muss Wiederherstellungsinformationen enthalten, damit damit zertifizierte Benutzer-IDs wiederhergestellt werden können. Für die Wiederherstellung sind weitere Schritte notwendig (z. B. das Anlegen einer Datenbank), die in der Notes-Hilfe beschrieben sind.

- **Server-ID:**
  - **Erzeugung**: Die ID wird automatisch bei der Serverinstallation erzeugt. Erzeugung in sicherer Umgebung. Nutzung des Vier-Augen-Prinzips.
  - **Gültigkeit**: Lange Gültigkeit (mehrere Jahrzehnte, Default = 100 Jahre), wird nie gewechselt (Ausnahme: Kompromittierung).
  - **Passwort**: Die Verwendung eines Passwortes erfordert die Passworteingabe bei jedem Serverstart. Falls keine organisatorischen Gründe dagegen sprechen (z. B. wenn der Remote-boot von Servern an verschiedenen Standorten regelmäßig und ohne Vor-Ort-Unterstützung erfolgen muss), wird die Nutzung von Server-ID-Passwörtern empfohlen. Sicherheitskopien müssen immer mit einem Passwort versehen sein. Es sind Intervalle für den erzwungenen Passwortwechsel anzugeben (empfohlen werden höchstens 60 Tage).
  - **Speicherung**: Wird bei jedem Serverstart benötigt. Speicherung im "Data"-Verzeichnis des Notes-Servers. Darf nicht auf einem Netz-Share liegen. Eine Speicherung im Namens- und Adressbuch (NAB) ist nicht zulässig. Wird kein Passwort verwendet (automatischer Server-Restart), müssen restriktive Dateiberechtigungen eingerichtet werden. **Achtung**: Kann eine nicht passwortgeschützte Server-ID von einem Unbefugten zugegriffen werden, so kann dieser (unter den meist privilegierten Berechtigungen) auf andere Server zugreifen. Sicherheitskopien analog zur Certifier-ID.
  - **Wiederherstellung**: Enthält die Wiederherstellungsinformationen der Certifier-ID, mit der die Server-ID zertifiziert wurde.
- **Administrator-ID:**
  - **Erzeugung**: Wird automatisch bei der Serverinstallation erzeugt (Datei: "User.id"). Erzeugung in sicherer Umgebung. Nutzung des Vier-Augen-Prinzips.
  - **Gültigkeit**: Die Gültigkeit muss den lokalen Gegebenheiten angepasst werden. Hier müssen Sicherheit und administrativer Aufwand beim Wechsel der Adminstrator-ID gegeneinander abgewogen werden.
  - **Passwort**: Die Administrator-ID muss mit einem Passwort versehen sein. Aufgrund der privilegierten Stellung ist ein sehr sicheres Passwort zu wählen (mindestens Notes-Qualität 9-10). Es sind Intervalle für den erzwungenen Passwortwechsel anzugeben (empfohlen werden höchstens 90 Tage).
  - **Speicherung**: Die Administrator-ID ist dem Administrator auf sicherem Weg zuzustellen. Eine Speicherung im Namens- und Adressbuch (NAB) ist nicht zulässig. Die Notes-ID-Datei ist vor fremdem Zugriff geschützt aufzubewahren. Das Anlegen einer Sicherheitskopie empfiehlt sich.

  - **Wiederherstellung**: Enthält die Wiederherstellungsinformationen der Certifier-ID, mit der die Administrator-ID zertifiziert wurde.

- **Benutzer-ID:**
  - **Erzeugung**: Wird durch die Benutzerverwalter eines Servers erzeugt. Erzeugung in sicherer Umgebung. Nutzung des Vier-Augen-Prinzips, da die Certifier-ID benötigt wird.
  - **Gültigkeit**: Die Gültigkeit muss den lokalen Gegebenheiten angepasst werden. Eine Gültigkeit von 2 Jahren hat sich jedoch in der Praxis bewährt.
  - **Passwort**: Benutzer-IDs müssen mit einem Passwort versehen werden. Ein sicheres Passwort ist zu wählen (Notes-Qualität mindestens 8). Es sind Intervalle für den erzwungenen Passwortwechsel anzugeben (empfohlen werden 90 Tage).
  - **Speicherung**: Die Benutzer-ID ist dem Benutzer auf sicherem Weg zuzustellen. Eine Speicherung im Namens- und Adressbuch (NAB) ist nicht zulässig. Die Notes-ID ist vor fremden Zugriffen geschützt aufzubewahren. Das Anlegen einer Sicherheitskopie empfiehlt sich.
  - **Wiederherstellung**: Enthält die Wiederherstellungsinformationen der Certifier-ID, mit der die Benutzer-ID zertifiziert wurde. Alte Notes-ID-Dateien (Version 4.x) müssen auf den neuen Recovery-Mechanismus der Version 5 umgestellt werden (siehe Notes-Hilfe).

Notes-ID-Passwort sicher wählen und nicht weitergeben

Generell ist für den Umgang mit Notes-IDs zu berücksichtigen, dass diese zur eindeutigen Benutzerauthentisierung (Ausweis) genutzt werden. Zwar sind die Notes-ID-Dateien durch ein Passwort geschützt, dies muss jedoch von entsprechender Qualität sein und darf nur dem Besitzer der Notes-ID bekannt sein. Wird das Passwort kompromittiert, so können sich u. U. unberechtigte Dritte mit der Notes-ID einem Server gegenüber ausweisen.

Ein Benutzer (oder Administrator) kann auch mehrere Kopien einer Notes-ID besitzen. Jede Notes-ID-Kopie eines Benutzers kann mit einem eigenen Passwort versehen sein. Ist eine Notes-ID-Datei unbefugt kopiert und deren Passwort kompromittiert worden, so kann die unbefugte Nutzung ohne zusätzliche Maßnahmen **nicht** durch den Passwortwechsel auf dem Original unterbunden werden.

Ergänzende Kontrollfragen:

- Werden alle Notes-ID gesichert aufbewahrt, sodass das unbefugte Kopieren nicht möglich ist?

M 4.130 Sicherheitsmaßnahmen nach dem Anlegen neuer Lotus Notes Datenbanken

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Werden auf einem Server neue Datenbanken angelegt, so geschieht dies durch die Nutzung von Datenbankvorlagen (Templates), die das Datenbankdesign bestimmen. Einige Datenbankvorlagen werden mit der Domino Software ausgeliefert, sie können jedoch auch von Drittherstellern stammen oder selbst erstellt werden.

Die Datenbankvorlagen enthalten das Datenbankdesign, zu dem u. a. auch Skripten und Agenten gehören. Insbesondere sind in der Datenbankvorlage auch Voreinstellungen für die Zugriffskontrollliste (Access Control List, ACL) enthalten. Generell empfehlen sich folgende Schritte nach dem Anlegen einer neuen Datenbank:

neue ACLs prüfen

- Alle von der Datenbankvorlage erzeugten ACL-Einträge sind zu überprüfen.
- Insbesondere sind die Berechtigungen für den "-Default-"-Eintrag zu überprüfen. In der Regel sollte der Zugriffslevel auf "No Access" gesetzt sein bzw. dahingehend verändert werden. Einige Vorlagen gewähren hier zu weitgehende Rechte (z. B. "Manager"-Recht) oder enthalten u. U. eine fehlerhafte Bezeichnung für dieses Standardrecht. In der Vorlage ist hier die Bezeichnung "-Default-" enthalten, statt "Default". Dies führt in der neu erzeugten Datenbank zum fehlerhaften Eintrag "--Default--". Als Folge wird der so generierte Eintrag von Lotus Notes nicht mehr als "Default"-ACL-Eintrag erkannt. Hier muss die Vorlage korrigiert werden. Der Fehler resultiert daraus, dass beim Erstellen einer Datenbank aus einer Vorlage einem Eintrag, der die Zeichenkette "Default" enthält, das Zeichen "-" als Begrenzer vor- und nachgestellt wird.
- Zur Steuerung des anonymen Zugriffs sollte der Benutzer "Anonymous" eingetragen und zunächst der Zugriffslevel "No Access" zugewiesen werden.
- Die ACL muss entsprechend der für die Datenbank geplanten Zugriffskontrolle eingerichtet werden (siehe auch M 4.120 *Konfiguration von Zugriffslisten auf Lotus Notes Datenbanken*).
- Für jede Datenbank muss ein administrativer Server bestimmt werden, der den für die Datenbank verantwortlichen "adminp"-Prozess ausführt und die Verwaltung der Datenbank übernimmt.
- Ist der Zugriff auf die Datenbank über die Web-Schnittstelle notwendig, so sind die damit verbundenen Einstellungen vorzunehmen (siehe M 4.125 *Einrichten von Zugriffsbeschränkungen beim Browser-Zugriff auf Lotus Notes Datenbanken*).

SSL aktivieren

- Sollen die Daten der Datenbank beim Web-Zugriff geschützt werden, so muss das Erzwingen der SSL-Absicherung aktiviert werden.

Datenbank signieren

- Als abschließende Maßnahme ist die Datenbank und deren Inhalte (Skripte, Agenten, Ansichten usw.) zu signieren. Dazu sollte eine spezielle Notes-ID verwendet werden. Dies dokumentiert, dass die Datenbank geprüft und für die unbedenkliche (bestimmungsgemäße) Verwendung freigegeben ist.

Enthalten Datenbanken Skripte oder Agenten, die zur Ausführung bestimmter Aktionen Notes-Rollen benutzen, so muss eine Planung der Rollenverteilung durchgeführt werden. Dies setzt eine detaillierte Dokumentation des Designs (bei Drittherstellern) oder eine enge Kooperation mit den Datenbankentwicklern (bei Eigenentwicklung) voraus. In der Regel muss das Datenbankdesign von Eigenentwicklungen die lokalen Sicherheitsvorschriften und das benutzte administrative Konzept berücksichtigen und darauf aufbauen.

Ergänzende Kontrollfragen:

- Wurden nach dem Anlegen einer neuen Datenbank alle Einstellungen überprüft?
- Ist jede Datenbank und deren Inhalte signiert worden?

M 4.131 Verschlüsselung von Lotus Notes Datenbanken

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Die abstrakte Struktur von Lotus Notes Datenbanken kann wie folgt dargestellt werden. Eine Datenbank enthält mehrere Dokumente und ein Dokument besteht aus mehreren Dokumentfeldern. Die Felder enthalten nun die eigentlichen Daten. Wenn Datenbanken Daten mit erhöhtem Schutzbedarf enthalten, so können diese zusätzlich durch Verschlüsselung geschützt werden. Die Verschlüsselung kann dabei entweder auf Datenbankebene angewandt werden - hier wird der gesamte Inhalt der Datenbank verschlüsselt - oder es kann die Verschlüsselung einzelner Dokumentfelder erfolgen, wenn die Datenbank Daten mit unterschiedlichem Schutzbedarf enthält. Beispielsweise können in einer Produktdatenbank die Felder mit bestimmten Einkaufspreisen verschlüsselt vorgehalten werden. Eine Verschlüsselung auf Dokumentebene ist nicht vorgesehen. Der Speicherort einer Datenbank - auf dem Server oder lokal beim Client - hat einen entscheidenden Einfluss auf die Verschlüsselungsmöglichkeiten.

Folgende Aspekte sind für die beiden Verschlüsselungsarten zu berücksichtigen:

Datenbankverschlüsselung

- Die Datenbankverschlüsselung schützt Datenbanken vor Angriffen auf Dateiebene.
- Eine Datenbank kann nur **für genau eine** Notes-ID verschlüsselt werden. Die Datenbank kann dann nur noch unter dieser Notes-ID zugegriffen werden. Dies hat folgende Konsequenzen:
  - Datenbanken, die auf dem Server abgelegt sind, können ausschließlich mit der Server-ID verschlüsselt werden (da in letzter Konsequenz der Server unter der Server-ID im Auftrag eines Clients auf die Datenbank zugreift). In diesem Fall kann die Verschlüsselung nicht dazu eingesetzt werden, die Datenbankinhalte für genau einen Benutzer zugreifbar zu machen.
  - Datenbanken, die vom Server auf einen Client repliziert oder lokal angelegt wurden, können mit einer (beliebigen) Benutzer-ID verschlüsselt werden. Dies erfordert Zugriff auf die jeweilige ID sowie das jeweilige Passwort. Nun kann nur noch unter dieser Benutzer-ID auf die Datenbank (lokal) zugegriffen werden. Wird die Datenbank auf den Server zurückrepliziert, so liegt die Datenbank dort **nicht** mehr mit der Benutzer-ID verschlüsselt vor. Ist die auf dem Server gespeicherte Datenbank mit der Server-ID verschlüsselt, so bleibt diese weiterhin verschlüsselt. Ist die Datenbank nicht verschlüsselt, bleiben die Daten unverschlüsselt.

- Der Verschlüsselungsgrad kann in drei Stufen eingestellt werden:
  - "einfach (simple)": Hierbei wird eine einfache, Notes-eigene Kodierung benutzt.
  - "mittel (medium)": Es wird ein Notes-eigenes Stream-Cipher Verfahren angewandt.
  - "stark (strong)": Hierbei wird ein auf RC2/RC4 basierendes Verfahren eingesetzt, das aber auch Notes-spezifisch ist.
- Die Nutzung der Verschlüsselungsstufe "einfach (simple)" kann für vertrauliche Daten nicht empfohlen werden.
- Datenbanken, die mit dem Verschlüsselungsgrad "mittel (medium)" oder "stark (strong)" verschlüsselt wurden, können nicht komprimiert vorgehalten werden.
- Die Daten zwischen Server und Client werden bei der Datenbankverschlüsselung unverschlüsselt über das Notes-Protokoll übertragen. Gegen Abhören müssen sie also zusätzlich geschützt werden (siehe dazu auch M 5.84 *Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation*).

Feldverschlüsselung

- Die Feldverschlüsselung erlaubt den Schutz vor Angriffen auf Dateisystemebene und bietet auch Schutz vor unerlaubter Einsichtnahme durch den Administrator.
- Felder müssen durch das Datenbankdesign für die Verschlüsselung vorgesehen sein.
- Es können nur alle verschlüsselbaren Felder eines Dokumentes gleichzeitig verschlüsselt/entschlüsselt werden.
- Die Entschlüsselung/Verschlüsselung findet durch den Client statt. Die verschlüsselten Daten werden daher verschlüsselt vom Server zum Client übertragen.
- Zur Feldverschlüsselung können sowohl symmetrische als auch asymmetrische Schlüssel eingesetzt werden.
- Es können gleichzeitig mehrere Schlüssel (symmetrische und asymmetrische) eingesetzt werden, sodasss eine Verschlüsselung für mehrere Benutzer erreicht werden kann.
- Symmetrische Schlüssel können von jedem Benutzer mit dem Notes-Client erzeugt werden. Für den Schlüsselaustausch sollten folgende Empfehlungen berücksichtigt werden:
  - Für Gruppen muss der gemeinsame, geheime Schlüssel auf sicherem Weg verteilt werden. Der Notes-Client stellt hier eine E-Mail-basierte Möglichkeit zur Verfügung, die den Schlüssel geschützt überträgt.
  - Alternativ besteht die Möglichkeit, den Schlüssel in eine (zunächst ungeschützte) Datei zu exportieren. Diese lässt sich mit einem

Passwort verschlüsseln und damit vor unberechtigtem Zugriff sichern. Das Passwort muss den Empfängern der Datei jedoch auf sicherem Weg mitgeteilt werden.

  - Die Weitergabe eines solchen Schlüssels durch die Empfänger an Dritte kann durch eine entsprechende Option verhindert werden, sodass die Nutzung des Schlüssels auf die Empfänger begrenzt werden kann.

- Beim Einsatz asymmetrischer Schlüssel werden die öffentlichen Schlüssel der Benutzer verwendet, die auf die Feldinhalte zugreifen sollen. Dabei werden die öffentlichen Notes-Schlüssel benutzt, auf die über das Namens- und Adressbuch zugegriffen werden kann.
- Es muss sichergestellt sein, das die Verschlüsselung mit jeweils mindestens einem Schlüssel der Benutzer erfolgt, die auf die verschlüsselten Feldinhalte zugreifen müssen.

Verstecken schützt nicht

Hinweis: Die Nutzung von so genannten "hidden paragraphs" - Textfeldern, die jedoch nicht angezeigt werden - ist nicht dafür geeignet, sensitive Daten zu schützen. Auch deren Inhalte können angezeigt werden, beispielsweise im Eigenschaftsdialog einer Datenbank oder mit dem Notes-Designer.

In Abhängigkeit von der Art der in einer Datenbank gespeicherten Informationen und den sich daraus ergebenden Anforderungen an deren Vertraulichkeit und Integrität kann es notwendig werden, diese Daten zu verschlüsseln. Die Randbedingungen hierbei sollten geregelt werden, z. B. in der Sicherheitsrichtlinie für Lotus Notes (siehe M 2.207 *Festlegen einer Sicherheitsrichtlinie für Lotus Notes*). Die Benutzer müssen über die Funktionsweise und Schutzmechanismen bei der Verschlüsselung von Lotus Notes Datenbanken informiert sein.

Ergänzende Kontrollfragen:

- Existiert ein Konzept für die Verschlüsselung von Lotus Notes Datenbanken?
- Sind die Verantwortlichen über ein ordnungsgemäßes Schlüsselmanagement informiert?

M 4.132 Überwachen eines Lotus Notes-Systems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Damit die Sicherheit eines Notes-Systems im laufenden Betrieb aufrecht erhalten werden kann, ist eine Überwachung des Systems unumgänglich. Nur so lassen sich mögliche Konfigurationsfehler, eventuelle Sicherheitslücken, Sicherheitsverstöße durch Benutzer oder Angriffe auf das System in Erfahrung bringen.

benutzerbezogene Daten

Bei der Überwachung des Systems müssen in der Regel auch benutzerbezogene Daten gesammelt werden. Anderenfalls ist es nicht möglich, Benutzer im Fall von Sicherheitsverstößen zur Verantwortung zu ziehen. Daher muss möglichst frühzeitig der Datenschutzbeauftragte sowie der Personal- bzw. Betriebsrat in die Planung des Überwachungskonzepts einbezogen werden.

Lotus Notes bietet insbesondere unter IT-Sicherheitsaspekten bisher keinen systematischen Auditing-Mechanismus, vielmehr werden Systemaktivitäten in verschiedenen Protokolldateien erfasst. Allerdings ist es möglich, automatisch auf das Auftreten verschiedener Systemereignisse zu reagieren.

Generelle Empfehlungen zu Logging-Einstellungen können an dieser Stelle nicht gemacht werden, da die Art und der Umfang der zu protokollierenden Informationen stark vom jeweiligen Einsatzszenario und dem verwendeten Überwachungskonzept abhängt.

Folgendes ist für die Überwachung eines Notes-Systems zu berücksichtigen:

Datenbank "certlog.nsf" anlegen

- Einige Protokoll-Datenbanken müssen explizit durch den Administrator oder Auditor angelegt werden (z. B. "certlog.nsf") oder das Erzeugen von Protokolleinträgen muss konfiguriert werden (z. B. "domlog.nsf"). Das Anlegen der Datenbank "certlog.nsf" wird dringend empfohlen, damit die durch den jeweiligen Server zertifizierten Benutzer dokumentiert werden können.
- Die Granularität der Protokolleinträge ist vielfach nicht ausreichend, um eine detaillierte Überwachung zu gewährleisten. Je nach Anforderungen müssen hier u. U. weitere Maßnahmen außerhalb des Notes-Systems ergriffen werden (z. B. durch den Einsatz von Drittprodukten, organisatorische Maßnahmen oder Eigenentwicklungen).

Protokollierung auf Servern und Clients

- Aktivitäten auf den Clients werden nicht in den Server-Protokolldateien erfasst. Es existieren jedoch auch lokale Protokolldateien auf den Clients.
- Die Protokolldateien können in mittleren und großen Systemen nur noch werkzeuggestützt überwacht und ausgewertet werden. Dritthersteller bieten hierfür entsprechende Zusatzwerkzeuge an.

restriktive Zugriffsrechte auf Protokolldaten

- Für die Protokolldateien müssen restriktive Zugriffsrechte vergeben werden. Die Zugriffrechte für Administratoren müssen je nach Auditing-Sicherheitsrichtlinie entzogen werden. Statt dessen erhalten Revisoren entsprechende Zugriffsrechte (in der Regel "Reader"-Zugriff).

Überwachungsregeln einrichten

- Die Event-Datenbank ("events4.nsf") erlaubt die Definition von Überwachungsregeln, die beim Auftreten von bestimmten Ereignissen vordefinierte Aktionen auslösen (z. B. Benachrichtigungen von Administratoren oder Einträge in das Betriebssystemprotokoll). Insbesondere für die Ereignisse der Kategorie "Sicherheit (Security)" müssen entsprechende Aktionen gemäß Überwachungskonzept eingerichtet werden.
- Der Protokollierungsgrad kann über die Konfigurationsdatei von Lotus Notes, z. B. "notes.ini" unter Windows NT, gesteuert werden. Die vorgegebenen Werte sollen überprüft und gegebenenfalls angepasst werden.
- Die Größe der Protokolldateien muss der Serverbelastung angepasst werden. So kann die Protokolldatei "log.nsf" von Lotus Notes über Einträge in der Konfigurationsdatei (z. B. den Parameter "log=log.nsf,1,0,7,40000" in "notes.ini" unter Windows NT) konfiguriert werden. Bei der Planung des Auditing-Konzeptes ist darauf zu achten, dass keine Protokolleinträge unbeabsichtigt verloren gehen können.

Ergänzende Kontrollfragen:

- Wie können Protokolldateien gesichert und aufbewahrt werden?

M 4.133 Geeignete Auswahl von Authentikationsmechanismen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Identifikations- und Authentikationsmechanismen von IT-Systemen bzw. IT-Anwendungen müssen so gestaltet sein, dass Benutzer eindeutig identifiziert und authentisiert werden. Die Identifikation und Authentisierung muss vor jeder anderen Interaktion zwischen IT-System und Benutzer erfolgen. Weitere Interaktionen dürfen nur nach der erfolgreichen Identifikation und Authentisierung möglich sein. Die Authentisierungsinformationen müssen so gespeichert sein, dass nur autorisierte Benutzer darauf Zugriff haben (sie prüfen oder ändern können). Bei jeder Interaktion muss das IT-System die Identität des Benutzers feststellen können.

Systemnutzung immer erst nach Identifikation und Authentikation

Vor der Übertragung von Nutzerdaten muss der Kommunikationspartner (Rechner, Prozess oder Benutzer) eindeutig identifiziert und authentisiert sein. Erst nach der erfolgreichen Identifikation und Authentisierung darf eine Übertragung von Nutzdaten erfolgen. Beim Empfang von Daten muss deren Absender eindeutig identifiziert und authentisiert werden können. Alle Authentisierungsdaten müssen vor unbefugtem Zugriff und vor Fälschung geschützt sein.

Es gibt verschiedene Techniken, über die die Authentizität eines Benutzers nachgewiesen werden kann. Die bekanntesten sind:

- PINs (Persönliche Identifikationsnummern)
- Passwörter
- Token wie z. B. Zugangskarten
- Biometrie

Für sicherheitskritische Anwendungsbereiche sollte starke Authentisierung verwendet werden, hierbei werden zwei Authentisierungstechniken kombiniert, wie Passwort plus Transaktionsnummern (Einmalpasswörter) oder plus Chipkarte. Daher wird dies auch häufig als Zwei-Faktor-Authentisierung bezeichnet. Beide eingesetzten Authentisierungstechniken müssen sich auf dem Stand der Technik befinden.

Auswahlkriterien

Im Folgenden werden verschiedene Kriterien aufgezeigt, die bei der Auswahl von Identifikations- und Authentikationsmechanismen beachtet werden sollten. Nicht alle marktgängigen Systeme erfüllen alle Kriterien, diese sollten aber bei der Auswahl entsprechend berücksichtigt werden. Viele IT-Produkte beinhalten bereits neben ihrer eigentlichen Funktionalität Authentikations-mechanismen, beispielsweise Betriebssysteme. Hier ist zu überprüfen, ob diese den Ansprüchen genügen oder ob sie um zusätzliche Funktionalitäten erweitert werden müssen. Auch dazu eignen sich die folgenden Kriterien.

Administration der Authentikationsdaten

Es müssen Sicherheitsfunktionen bereitstehen, um Authentikationsdaten für Benutzer anlegen und verändern zu können. Diese Funktionen sollten nur von

autorisierten Administratoren ausgeführt werden können. Bei der Verwendung von Passwörtern sollten autorisierte Benutzer ihre eigenen Authentikationsdaten innerhalb festgesetzter Grenzen verändern können. Das IT-System sollte einen geschützten Mechanismus zur Verfügung stellen, damit Benutzer ihre Passwörter selbstständig verändern können. Dabei sollte es möglich sein, eine Mindestlebensdauer für Passwörter vorzugeben.

Nach einer erfolgreichen Anmeldung sollte den Benutzern Zeit und Ort seines letzten erfolgreichen Zugriffs angezeigt werden.

Schutz der Authentikationsdaten gegen Veränderung

Das IT-System muss die Authentikationsdaten bei der Verarbeitung jederzeit gegen Ausspähung, Veränderung und Zerstörung schützen. Dies kann beispielsweise durch Verschlüsselung der Passwortdateien und durch Nicht-Anzeigen der eingegebenen Passwörter geschehen. Die Authentikationsdaten sind getrennt von Applikationsdaten zu speichern.

Systemunterstützung

Beim Einsatz von organisationsweiten Authentikationsverfahren sollten diese nur auf Servern betrieben werden, deren Betriebssystem einen adäquaten Schutz gegen Manipulationen bietet. Bei der Auswahl von Authentikationsverfahren sollte darauf geachtet werden, dass diese möglichst plattformübergreifend eingesetzt werden können.

Fehlerbehandlung bei der Authentikation

Das IT-System sollte Anmeldevorgänge nach einer vorgegeben Anzahl erfolgloser Authentikationsversuche beenden können. Nach Ende eines erfolglosen Anmeldevorgangs muss das IT-System den Benutzer-Account bzw. das Terminal sperren können bzw. die Verbindung unterbrechen. Nach erfolglosen Authentikationsversuchen sollte das IT-System jeden weiteren Anmeldeversuch zunehmend verzögern (Time-delay). Die Gesamtdauer eines Anmeldeversuchs sollte begrenzt werden können.

Administration der Benutzerdaten

Das IT-System sollte die Möglichkeit bieten, den Benutzern verschiedene Voreinstellungen zuweisen zu können. Diese sollten angezeigt und verändert werden können. Die Möglichkeit, Benutzerdaten zu verändern, muss auf den autorisierten Administrator beschränkt sein. Wenn die Administration der Benutzerdaten über eine Kommunikationsverbindung erfolgen soll, muss diese ausreichend kryptographisch gesichert sein.

Definition der Benutzereinträge

Das IT-System muss die Umsetzung der Sicherheitsrichtlinie ermöglichen, indem für jeden Benutzer die entsprechenden Sicherheitseinstellungen gewählt werden können.

Ein Authentikationsverfahren sollte auch erweiterbar sein, z. B. um die Unterstützung starker Authentikationstechniken wie dem Einsatz von Token oder Chipkarten (siehe auch M 5.34 *Einsatz von Einmalpasswörtern*).

Umfang der Benutzerdaten

Neben Benutzernamen und Rechteprofil sollten noch weitere Informationen über jeden Benutzer hinterlegt werden (siehe auch M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*):

- Es sollte mindestens Vorname und Nachname eines Benutzers in der Benutzerverwaltung aufgenommen werden. Zusätzlich ist auch Telefon- und Raumnummer hilfreich.
- Um mit dem Benutzer in Kontakt zu treten, sollten zusätzlich auch Informationen wie E-Mail-Adresse, Telefonnummer und geographischer Standort (Adresse, Raumnummer) erfasst werden.
- Zusätzlich sollte erfasst werden, wie lange die Benutzerkennung gültig sein soll. Ist die Benutzerkennung abgelaufen, sollte sie gesperrt werden.

Passwortgüte

Wenn Passwörter zur Authentikation eingesetzt werden, sollte das IT-System Mechanismen bieten, die folgende Bedingungen erfüllen (siehe M 2.11 *Regelung des Passwortgebrauchs*):

- Es wird gewährleistet, dass jeder Benutzer individuelle Passwörter benutzt (und diese auch selbst auswählen kann).
- Es wird überprüft, dass alle Passwörter den definierten Vorgaben genügen (z. B. Mindestlänge, keine Trivialpasswörter). Die Prüfung der Passwortgüte sollte individuell regelbar sein. Beispielsweise sollten vorgegeben werden können, dass die Passwörter mindestens ein Sonderzeichen enthalten müssen oder bestimmte Zeichenkombinationen verboten werden.
- Das IT-System generiert Passwörter, die den definierten Vorgaben genügen. Das IT-System muss die so erzeugten Passwörter dem Benutzer anbieten.
- Der Passwortwechsel sollte vom System regelmäßig initiiert werden. Die Lebensdauer eines Passwortes sollte einstellbar sein.
- Die Wiederholung alter Passwörter beim Passwortwechsel sollte vom IT-System verhindert werden (Passwort-Historie).
- Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.
- Nach der Installation bzw. der Neueinrichtung von Benutzern sollte das Passwort-System einen Passwort-Wechsel nach der Erst-Anmeldung erzwingen.

Biometrie

Unter Biometrie im hier verwendeten Sinn ist die automatisierte Erkennung von Personen anhand ihrer körperlichen Merkmale zu verstehen. Um biometrische Verfahren für die Authentisierung einsetzen zu können, werden zusätzliche Peripherie-Geräte benötigt, die die Benutzer auf Grundlage besonderer Merkmale eindeutig authentisieren können. Eine oder mehrere der folgenden biometrischen Merkmale können beispielsweise für eine Authentisierung verwendet werden:

- Iris
- Fingerabdruck
- Gesichtsproportionen
- Stimme und Sprachverhalten
- Handschrift
- Tippverhalten am Rechner

Neben einer Vielzahl von biometrischen Merkmalen und darauf basierenden biometrischen Verfahren bestehen darüber hinaus auch große Unterschiede zwischen den verfügbaren konkreten biometrischen Systemen und Produkten. Die Leistungsfähigkeit von biometrischen Verifikationssystemen ist sehr unterschiedlich. Bei einem Einsatz in sicherheitskritischen Bereichen muss darauf geachtet werden, dass das biometrische System eine akzeptable Erkennungsleistung und eine hohe Sicherheit bietet. Es darf nicht möglich sein, dass dieses mit Hilfe von Nachbildungen (z. B. einer Gesichtsmaske, Wachsnachbildung des Fingers, Kontaktlinsen mit Irismuster...) überlistet werden kann.

Authentisierung mit Token

Eine weitere Alternative bieten Authentikationstoken, also handliche Datenträger, die als sicherer Speicherplatz für die für die Authentikation benötigten Informationen wie z. B. kryptographischer Schlüssel dienen. Typische Beispiele für Authentikationstoken sind Chipkarten, USB-Sticks oder taschenrechnerähnliche Geräte zur Erzeugung von Einmal-Passwörtern.

Anforderungen an Authentikationsmechanismen für Benutzer

Das IT-System muss vor jeder anderen Benutzertransaktion die Benutzeridentität überprüfen. Das IT-System sollte darüber hinaus das Wiedereinspielen von Authentikationsdaten für Benutzer oder das Einspielen gefälschter oder kopierter Benutzerauthentikationsdaten erkennen und verhindern können. Das IT-System darf die Authentikationsdaten erst dann überprüfen, wenn sie vollständig eingegeben wurden.

Es sollte für jeden Benutzer individuell einstellbar sein, wann und von wo er auf das IT-System zugreifen darf.

Protokollierung der Authentisierungsmechanismen

Authentisierungsvorgänge sind in einem sinnvollen Umfang zu protokollieren. Die Protokolldateien sollten in regelmäßigen Abständen von den Administratoren überprüft werden. Das IT-System muss die folgenden Ereignisse protokollieren können:

- Ein- und Ausschalten der Protokollierung.
- Jeden Versuch, auf Mechanismen zum Management von Authentikationsdaten zuzugreifen.
- Erfolgreiche Versuche, auf Authentikationsdaten zuzugreifen.
- Jeden Versuch, unautorisiert auf Benutzer-Authentikationsdaten zuzugreifen.
- Jeden Versuch, auf Funktionen zur Administration von Benutzer-Einträgen zuzugreifen.
- Änderungen an Benutzereinträgen.
- Jeden durchgeführten Test auf Passwort-Güte.

- Jede Benutzung von Authentisierungsmechanismen.
- Jede Konfiguration der Abbildung von Authentisierungsmechanismen zu spezifischen Authentikationsereignissen.
- Die Installation von Authentisierungsmechanismen.

Jeder Protokollierungseintrag sollte Datum, Uhrzeit, Art des Ereignisses, Bezeichnung des Subjektes sowie Erfolg bzw. Misserfolg der Aktion enthalten.

Ergänzende Kontrollfragen:

- Welche Authentisierungsmechanismen werden verwendet?
- Nach welchen Kriterien wurden diese gewählt?

M 4.134 Wahl geeigneter Datenformate

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Benutzer

Es gibt eine Vielzahl von unterschiedlichen Datenformaten, die von den verschiedenen IT-Anwendungen unterstützt werden. Diese sind allerdings im Allgemeinen nicht kompatibel, also untereinander austauschbar. Leider können häufig nicht einmal IT-Anwendungen mit demselben Aufgabenfeld (z. B. Textverarbeitungssysteme) mit den Datenformaten ähnlicher Produkte umgehen. Dieses Problem wird noch dadurch gesteigert, dass oft Anwendungsprogramme nach einem Versionswechsel die Datenformate ihrer Vorgänger nicht mehr verarbeiten können.

Kompatibilität neuer Programme hinterfragen

Daher muss bei der Beschaffung neuer Anwendungsprogramme untersucht werden, welche Datenformate unterstützt werden und wie verbreitet die unterstützten Datenformate sind. Da viele wichtige Vorgänge dauerhaft elektronisch gespeichert werden sollen, ist es ebenso wichtig zu hinterfragen, welche "Lebensdauer" von einem Datenformat erwartet wird. Generell sollte bei jedem Systemwechsel überprüft werden, ob alle gespeicherten Daten mit den neuen IT-Systemen oder IT-Anwendungen noch verarbeitet werden können.

Kann der Empfänger die Daten lesen?

Ebenso muss aber auch bei jeder Nutzung eines Anwendungsprogramms überlegt werden, in welchem Format die bearbeiteten Daten gespeichert werden sollen. Dabei sollte immer berücksichtigt werden, wer und zu welchem Zeitpunkt diese Daten lesen können soll.

Zusatzinformationen verursachen Zusatzprobleme

Bei der Wahl von Datenformaten für den Dateiaustausch sollte auch berücksichtigt werden, ob diese unerwünschte Zusatzinformationen enthalten können (siehe auch M 4.64 *Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen*). Dateien, die in bestimmten Datenformaten erstellt wurden, können auch andere sicherheitsrelevante Probleme wie Makros und damit die Gefahr von Makro-Viren mit sich bringen (siehe M 4.3 *Regelmäßiger Einsatz eines Anti-Viren-Programms*).

Beispiel:

Bei der Textverarbeitung hat es sich als sinnvoll erwiesen, mit Microsoft Winword erstellte Dateien im Rich Text Format (RTF) zu speichern. Dies kann von einer größeren Zahl von Textverarbeitungsprogrammen gelesen werden und stellt darüber hinaus sicher, dass die Datei keine Makro-Viren enthält.

Ergänzende Kontrollfragen:

- Gibt es Empfehlungen, welche Datenformate für den Datenaustausch, die Archivierung oder andere Anwendungsbereiche zu verwenden sind?
- Wird bei der Beschaffung neuer Programme hinterfragt, ob diese mit den bisher unterstützten Datenformaten kompatibel sind?

M 4.135 Restriktive Vergabe von Zugriffsrechten auf Systemdateien

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator

Systemdateien bzw. -verzeichnisse sind Dateien und Verzeichnisse, für die der Administrator zuständig ist. Diese sind entweder für alle Benutzer von Bedeutung oder sie dienen Administrationszwecken.

Auf Systemdateien sollten möglichst nur die Systemadministratoren Zugriff haben. Der Kreis der zugriffsberechtigten Administratoren sollte möglichst klein gehalten werden. Auch Verzeichnisse dürfen nur die notwendigen Privilegien für die Benutzer zur Verfügung stellen. Die Vergabe von Zugriffsrechten auf Systemdateien sollte grundsätzlich restriktiv und nur in Übereinstimmung mit den hausinternen Sicherheitsrichtlinien erfolgen (siehe auch M 2.220 *Richtlinien für die Zugriffs- bzw. Zugangskontrolle*).

Trennen von anderen Dateien

Systemdateien sollten getrennt von Applikationsdaten und Benutzerdateien gespeichert werden (siehe auch M 2.138 *Strukturierte Datenhaltung*). Dies sorgt für eine bessere Übersicht und erleichtert auch die Durchführung von Datensicherungen und die Sicherstellung des korrekten Zugriffsschutzes.

Der Zugriff auf Systemdateien sollte immer protokolliert werden. Überflüssige, also nicht benötigte Systemdateien sollten vom System entfernt werden, damit sie nicht für Angriffe missbraucht werden können und auch nicht ständig auf Integrität kontrolliert werden müssen.

Bei der restriktiven Vergabe von Zugriffsrechten reicht es nicht aus, nur die Rechte eines Programms zu überprüfen. Zusätzlich muss auch die Rechtevergabe aller Programme überprüft werden, die von diesem Programm aus aufgerufen werden.

regelmäßige Kontrolle der Zugriffsrechte

Die Integrität aller Systemdateien und -verzeichnisse, sowie die Korrektheit der Zugriffsrechte sollte nach Möglichkeit regelmäßig verifiziert werden. Für viele Betriebssysteme gibt es dafür Tools, mit denen solche Prüfungen schnell und zuverlässig durchgeführt werden können.

Ergänzende Kontrollfragen:

- Wird die Rechtevergabe auf Systemdateien regelmäßig überprüft?
- Gibt es Tools oder Listen, anhand derer diese Überprüfungen durchgeführt werden?

M 4.136 Sichere Installation von Windows 2000

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Nach erfolgter Planung eines Windows 2000 Systems (siehe M 2.227 *Planung des Windows 2000 Einsatzes*) muss das Windows 2000 Betriebssystem auf den relevanten Rechnern installiert werden. Während der Installationsphase ist ein Windows 2000 Rechner nicht vollständig konfiguriert, sodass auch die gewünschten Sicherheitseinstellungen noch nicht aktiviert sind. Es empfiehlt sich daher, die initiale Konfiguration entweder in einer geschützten Umgebung durchzuführen oder alternativ eine vorbereitete Standardkonfiguration aufzuspielen.

Während der Installation erfolgt unter anderem auch die Konfiguration der lokalen Sicherheitseinstellungen. Die wichtigsten Grundeinstellungen beziehen sich auf die

- Dateisystemsicherheit,
- Sicherheit der Registrierdatenbank (Registry),
- Sicherheit für den Netzzugriff,

Zugriffsrechte, Basisdienste und Serverdienste konfigurieren

die während der Standardinstallation zunächst mit Standardwerten initialisiert werden. Generell erfolgt die Installation eines Rechners in mehreren Schritten: in einem ersten Schritt erfolgt nach dem Aufspielen der Systemdateien die Konfiguration der Dateisystem- und Registrierdatenbanksicherheit durch das Festlegen von Zugriffsrechten. Danach werden die Basisdienste eines Systems konfiguriert, z. B. die Netzkonfiguration. In einem letzten Schritt erfolgt insbesondere für Server die Konfiguration von Serverdiensten. Für Server, die als Domänen-Controller betrieben werden sollen, erfolgt ein weiterer Schritt, in dem die für Domänen-Controller spezifischen Dienste (z. B. Active Directory, Kerberos) installiert und konfiguriert werden.

Mitgliedschaft in einer Domäne

Das Hinzufügen eines Rechners zu einer Domäne ist ein weiterer wichtiger Konfigurationsschritt für Clients und Server. Als Spezialfall ist hier die Konfiguration des ersten Domänen-Controllers einer neuen Domäne zu sehen. Dabei sind besondere Sorgfalt und besondere Rechte notwendig, da nur ein Mitglied der Gruppe *Domänen-Admins* eine neue Domäne in einen existierenden Domänenverbund aufnehmen kann.

Neuinstallation oder Upgrade?

Generell ist bei der Installation aus Sicherheitssicht Folgendes zu beachten:

- Die geltenden Zugriffseinstellungen für das Dateisystem und die Registrierdatenbank eines Rechner nach einer Windows 2000 Installation hängen davon ab, ob der Rechner neu installiert wurde oder ob ein Upgrade (z. B. von Windows NT) auf Windows 2000 erfolgt ist. Bei einem Upgrade kommen die Windows 2000 Standardeinstellungen nicht zum tragen. Vielmehr werden die vorgefundenen Einstellungen übernommen. Es ist dabei zu beachten, dass mit Windows 2000 die Trennung zwischen Benutzer (*User*) und Hauptbenutzer (*Poweruser*) wesentlich strenger erfolgt, sodass ein System nach einem Upgrade in der Regel mit weniger strengen Sicherheitseinstellungen konfiguriert ist.

- Nach Aufspielen der reinen Betriebssystemsoftware müssen auf Servern weitere Dienste konfiguriert werden. Dabei ist zu beachten, dass auf Server in der Regel sofort nach Einstellen der Netzparameter vom Netz aus zugegriffen werden kann. Daher muss der Netzzugriff entsprechend eingeschränkt werden.

Dienste konfigurieren

- Soll ein neuer Rechner in eine existierende Windows 2000 Domäne aufgenommen werden, so erlaubt es der Mechanismus der Gruppenrichtlinien, die initiale Konfiguration deutlich abzukürzen. Beim Beitritt zu einer Domäne werden die für den Rechner relevanten Gruppenrichtlinienobjekte ausgewertet und der Rechner wird entsprechend konfiguriert. Dazu muss entweder ein entsprechendes Computerkonto in der Domäne vorbereitet werden, oder das Computerkonto wird beim Beitritt erzeugt. Dazu sind dann entsprechende administrative Berechtigungen notwendig. Wird das Computerkonto erst beim Beitritt erzeugt, so muss das Computerkonto anschließend in die gewünschte Organisationseinheit (OU) im Active Directory verschoben werden, da solche Computerkonten standardmäßig im AD-Container *Computer* erzeugt werden. Damit solche Computer eine Standardsicherheitseinstellung erhalten, bis sie in die gewünschte OU verschoben sind, sollten diese Einstellungen über die Gruppenrichtlinieneinstellungen der Domäne erfolgen, da an AD-Container keine Gruppenrichtlinienobjekte angehängt werden können.

Konfiguration durch Gruppenrichtlinien

- Wird ein Rechner als Stand-alone Rechner betrieben, ist also dieser in keine Domäne aufgenommen worden, muss die Konfiguration der Gruppenrichtlinien, die auch die Sicherheitseinstellungen enthalten, lokal erfolgen.

Stand-alone-Rechner

Für die Installation von Domänen-Controllern gilt außerdem:

- Bei der Installation von Domänen-Controllern ist besondere Sorgfalt gefordert, da diese im späteren Betrieb sensitive Daten speichern, beispielsweise Passwörter oder Kerberos-Schlüssel in nicht gehashter Form.
- Domänen-Controller dürfen nur auf Rechnern installiert werden, die sich in einer physikalisch sicheren Umgebung befinden (siehe auch M 1.29 *Geeignete Aufstellung eines IT-Systems*).
- Wird ein Windows 2000 Server zu einem Domänen-Controller heraufgestuft, so muss ein Passwort angegeben werden, welches im so genannten *Active Directory Recovery Modus* abgefragt wird. In diesem Modus, der für Notfallreparaturen am Active Directory gedacht ist, können u. a. aktuelle Active Directory Daten mit Backup-Daten überschrieben werden. Da dies eine sehr sicherheitskritische Operation darstellt, darf dieser Zugang nicht ungeschützt sein. Im Rahmen der Heraufstufung wird ein Domänen-Administratorkonto erzeugt und das rechnerlokale Administratorkonto als Anmeldekonto für den Active *Directory Recovery Modus* genutzt. Dieses muss mit einem starken Passwort gesichert sein.

starkes Passwort für Recovery Modus

- Die Installationsreihenfolge der jeweils ersten Domänen-Controller einer Domäne muss eingehalten werden. Die erste in einem Netz durch die Installation eines zugehörigen Windows 2000 Domänen-Controllers erzeugte Domäne übernimmt die Rolle der Forest-Root-Domäne (FRD),

Installationsreihenfolge einhalten

die wichtige Verwaltungsaufgaben im zukünftigen Domänenverbund übernimmt. Die Rolle der FRD kann nachträglich nicht anderen Domänen zugewiesen werden.

Hinweise zu Einstellungen der Gruppenrichtlinienparameter finden sich in Maßnahme M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000*.

Ergänzende Kontrollfragen:

- Wurden die installierten Zugriffsrechte für Dateien und die Registrierdatenbank bedarfsgerecht geplant?
- Wurden die Zugriffsrechte für Dateien und die Registrierdatenbank bei Systemen, die von Windows NT auf Windows 2000 aktualisiert wurden, ebenfalls aktualisiert?
- Sind alle Gruppenrichtlinienobjekte installiert, damit neue Rechner mit den neuen Sicherheitseinstellungen versorgt werden?
- Wurde die FRD als erste Domäne installiert?
- Ist der AD Recovery Modus für jeden Domänen-Controller mit einem starken Passwort gesichert?

M 4.137 Sichere Konfiguration von Windows 2000

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Nach der Installation von Windows 2000 Rechnern erfolgt deren Konfiguration. Die jeweils vorzunehmenden Einstellungen hängen dabei wesentlich vom Verwendungszweck ab. Grob kann bei Windows 2000 unterschieden werden zwischen der Verwendung als

- Workstation oder Arbeitsplatzrechner,
- Server (Dateiserver, Applikationsserver, Dienstserver) oder
- Domänen-Controller.

Dabei kommen jeweils die entsprechenden Windows 2000 Versionen (Professional, Server, Advanced Server, Datacenter Server) zum Einsatz.

System und Dienste sicher konfigurieren

Für die sichere Konfiguration ist jeweils zu beachten, dass neben der reinen Betriebssystemkonfiguration, die im Wesentlichen über Gruppenrichtlinien erfolgen kann, auch die sichere Konfiguration einzelner Dienste notwendig ist. Dies trifft insbesondere auf die Server-Versionen von Windows 2000 zu.

Folgende Punkte sind für die sichere Grundkonfiguration eines Windows 2000 Systems zu beachten:

- Die Sicherheitseinstellungen sind gemäß der festgelegten Windows 2000 Sicherheitsrichtlinie und der Planung der Windows 2000 Gruppenrichtlinien umzusetzen (siehe M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000*).
- Die Anmeldeprotokollierung sollte aktiviert sein (siehe auch M 4.148 *Überwachung eines Windows 2000/XP Systems*).
- Für Windows 2000 Professional (Arbeitsplatzrechner) darf der Autologon-Mechanismus nicht genutzt werden.
- Eine ausreichende Passwortqualität muss sichergestellt sein. Dies gilt insbesondere dann, wenn die Dateiverschlüsselung mit EFS (siehe M 4.147 *Sichere Nutzung von EFS unter Windows 2000/XP*) genutzt wird. Die Benutzer sollten dementsprechend geschult werden.
- Für jeden Benutzer muss ein eigenes Benutzerkonto eingerichtet werden. Gemeinsam genutzte Konten sind abzulehnen, da in diesem Fall die Verantwortlichkeit nicht eindeutig zuweisbar ist.

Benutzer- und Administratorkonten trennen

- Das Verwaltungskonzept (siehe auch M 2.227 *Planung des Windows 2000 Einsatzes*) sollte eine strikte Trennung von Benutzer- und Administratorkonten vorsehen. Administrative Tätigkeiten sollten nur unter Administratorkonten ausgeführt werden. Umgekehrt sollten unter Administratorkonten keine normalen Benutzertätigkeiten durchgeführt werden. Windows 2000 bietet hier zur Unterstützung den *run-as*-Mechanismus an. Damit können Personen mit administrativen Befugnissen unter normalen Benutzerkonten angemeldet sein und für administrative Tätigkeiten Prozesse unter einem Administratorkonto starten, ohne sich vom System abmelden zu müssen.

- Das Gast-Konto sollte nicht genutzt und daher möglichst auch nicht aktiviert werden. Das Umbenennen des Gast-Kontos ist möglich, bietet jedoch keinen wirklichen Schutz, da das Gast-Konto beispielsweise über die Security-ID (SID) des Kontos identifiziert werden kann.
- Konten sollten nach einer vorgegebenen Anzahl von Passwortfehleingaben automatisch gesperrt werden. Die dann notwendige Freischaltung sollte nur durch einen befugten Administrator erfolgen (siehe auch M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000*).
- Sämtliche Verwaltungsaktivitäten an Benutzerkonten sollten protokolliert werden (siehe auch M 4.148 *Überwachung eines Windows 2000 Systems*).
- Die im Rahmen der Windows 2000 Planung festgelegten Gruppen, die sich an einem Rechner lokal oder über das Netz anmelden dürfen, müssen konfiguriert werden.
- Für alle Rechner muss ein passwortgeschützter Bildschirmschoner aktiviert sein, der nach einem vorgegebenen Zeitintervall automatisch startet.
- Ist die abgesicherte Kommunikation zwischen Windows 2000 Rechnern gewünscht oder notwendig, so kann die Verschlüsselung mittels IPSec erfolgen (siehe M 5.90 *Einsatz von IPSec unter Windows 2000/XP*).

In Abhängigkeit vom Verwendungszweck sind außerdem folgende Aspekte jeweils zu berücksichtigen:

- **Arbeitsplatzrechner**: Die Sicherheit eines Arbeitsplatzrechners hängt im Wesentlichen davon ab, ob ein Benutzer administrativ auf den Rechner einwirken kann, welche Funktionen dem Benutzer verfügbar gemacht werden und ob der Benutzer die ihm zur Verfügung gestellten Sicherheitsmechanismen korrekt nutzt. Detaillierte Maßnahmen sind im Baustein B 3.209 *Client unter Windows XP* sowie in M 4.150 *Konfiguration von Windows 2000 als Workstation* und M 3.28 *Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer* beschrieben. Für die Verwendung als Laptop ist außerdem die Maßnahme M 4.147 *Sichere Nutzung von EFS unter Windows 2000/XP* relevant.
- **Server**: Die Sicherheit eines Servers hängt im Wesentlichen davon ab, ob die von ihm angebotenen Dienste sicher konfiguriert wurden. Dies muss durch eine sichere Grundkonfiguration des Betriebssystems unterstützt werden. Detaillierte Empfehlungen dazu finden sich in M 4.139 *Konfiguration von Windows 2000 als Server*, sowie in der Maßnahme M 4.140 *Sichere Konfiguration wichtiger Windows 2000 Dienste* und den dort referenzierten Maßnahmen.
- **Domänen-Controller**: Auf Domänen-Controllern werden im Active Directory wichtige Systemdaten gehalten. Diese müssen besonders geschützt werden. Die für Domänen-Controller spezifischen Maßnahmen sind in M 4.138 *Konfiguration von Windows 2000 als Domänen-Controller* zusammengefasst. Da einige wichtige Windows Dienste auch auf Domänen-Controllern ablaufen können oder müssen, findet auch die Maßnahme M 4.140 *Sichere Konfiguration wichtiger Windows 2000 Dienste* Anwendung.

Freigaben auf Arbeitsplatzrechnern und Domänencontrollern vermeiden

Windows 2000 erlaubt es, Netzfreigaben für jeden Rechner, d. h. für Arbeitsplatzrechner, Server oder Domänen Controller, zu konfigurieren. Netzfreigaben können unter Sicherheitsgesichtspunkten problematisch sein. Freigaben auf Arbeitsplatzrechnern sollten möglichst vermieden werden, da ein Netzzugriff auf diese in der Regel nicht sinnvoll ist (siehe auch M 5.37 *Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz*). Ausnahmen sollten daher begründet und dokumentiert werden. Für Netzfreigaben auf Servern (z. B. Dateiserver, Druckserver) gilt, dass die Freigaben durch Zugriffsrechte zu schützen sind, so dass diese nur den autorisierten Benutzergruppen zur Verfügung stehen. Die Zugriffsrechte auf die durch die Freigaben zur Verfügung gestellten Ressourcen (z. B. Dateien und Verzeichnisse) sind durch restriktive Zugriffsrechte zu schützen. Netzfreigaben auf Domänen-Controller stellen u. U. eine besondere Gefahr dar, da die Daten auf Domänen-Controllern besonders geschützt werden müssen. Auch hier sind Freigaben zu begründen und zu dokumentieren.

restriktive Zugriffsrechte vergeben

Generell sollte für jede Freigabe eine Risikoabschätzung erfolgen. Die Sicherheit der durch eine Netzfreigabe angebotenen Ressourcen hängt vor allem von den eingestellten Zugriffsrechten ab. Diese können unter Windows 2000 feingranular vergeben werden. Welche Zugriffsrechte zu verwenden sind, kann nur im Einzelfall bestimmt werden. Generell gilt jedoch, dass die Zugriffsrechte so restriktiv wie möglich vergeben werden sollten. Spezielle Hinweise zum Umgang mit Dateizugriffsrechten finden sich auch in M 4.149 *Datei- und Freigabeberechtigungen unter Windows 2000/XP*.

Unter Windows 2000 wird standardmäßig Kerberos als Authentisierungsmechanismus eingesetzt. Da die Systemsicherheit auch von der korrekten und zuverlässigen Authentisierung abhängt, kommt den Komponenten von Kerberos eine wichtige Rolle zu. Die Windows 2000 Komponenten von Kerberos benötigen keine umfangreiche Konfiguration und stellen nur wenige Konfigurationsparameter bereit. Diese können über Gruppenrichtlinien angepasst werden. Es existieren folgende Konfigurationsmöglichkeiten:

Computer Richtlinien / Kontorichtlinien / Kerberos Richtlinien	
Zugriffsbeschränkungen durchsetzen	Ist diese Einstellung aktiviert, überprüft der Kerberos KDC-Server (Key Distribution Center), ob der Benutzer die notwendigen Benutzerrechte (z. B. Recht zum Anmelden über das Netz) zum Zugriff auf den angeforderten Dienst besitzt, bevor das Ticket ausgestellt wird.
Max. Gültigkeitsdauer des Benutzertickets	Diese Einstellung bestimmt die maximale Gültigkeit eines Benutzertickets. Ist ein Ticket abgelaufen, so muss es erneuert werden (s. u.).
Max. Gültigkeitsdauer des Diensttickets	Nach Ablauf dieser Zeitspanne kann das Ticket nicht mehr zur Authentisierung beim Dienst genutzt werden. Einmal aufgebaute Dienstverbindungen werden jedoch nicht abgebrochen, da die Authentisierung innerhalb der Gültigkeitsdauer erfolgte.

Max. Toleranz für die Synchronisation des Computertakts	Kerberos Tickets enthalten Zeitstempel (Ausstellungszeit, Gültigkeitsdauer). Damit die Authentisierung mittels "alter" Tickets ausgeschlossen ist, müssen alle Rechneruhren möglichst synchron laufen, was in einem Windows 2000 Netz automatisch durch den integrierten Zeitdienst gewährleistet wird. Die hier angegebene Zeitspanne gibt an, innerhalb welcher Toleranz Zeiten auf verschiedenen Rechnern als "gleich" angesehen werden.
Max. Zeitraum, in dem ein Benutzerticket erneuert werden kann	Gibt den Zeitraum an, nach der die Verlängerung eines Benutzertickets nicht mehr möglich ist. Ist diese Zeitspanne für ein Benutzerticket abgelaufen, so muss sich der Benutzer erneut gegenüber dem Kerberos-Server authentisieren, damit ein neues Benutzerticket ausgestellt werden kann. Die Komponenten von Windows führen diesen Vorgang transparent für den Benutzer durch, sodass keine neue Passworteingabe notwendig ist.

Tabelle: Computer Richtlinien / Kontorichtlinien / Kerberos Richtlinien

Bei der Konfiguration der Parameter über eine Gruppenrichtlinie (GPO) ist Folgendes zusätzlich zu beachten:

- Die Parameter sollten im Probebetrieb an die lokalen Gegebenheiten angepasst werden.
- Die GPO-Einstellungen werden nur wirksam, wenn sie zu einem GPO-Objekt gehören, das mit einem Domänen-Objekt verbunden ist.
- Für Stand-alone-Rechner wird Kerberos als Authentisierungsverfahren zur Anmeldung an lokale Benutzerkonten nicht genutzt.

Neben den hier angesprochenen Windows 2000 spezifischen Maßnahmen muss generell für jeden Rechner bzw. für jede Gruppe von Rechnern eine Schutzbedarfsfeststellung erfolgen (siehe IT-Grundschutz-Vorgehensweise), die die speziellen Risiken, z. B. durch installierte Software oder Einsatzszenarien, berücksichtigt. Zusätzlich sollten auch die generellen Maßnahmen Anwendung finden, wie sie in den übrigen relevanten Bausteinen der IT-Grundschutz-Kataloge beschrieben sind.

Ergänzende Kontrollfragen:

- Sind alle Rechner gemäß der ihnen zugedachten Rolle konfiguriert?
- Werden die geplanten Protokolleinstellungen umgesetzt?
- Sind eventuell notwendige Änderungen in den Kerberos-Parametern umgesetzt und getestet?

M 4.138 Konfiguration von Windows 2000 als Domänen-Controller

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Domänen-Controller (DC) stellen in einem Windows 2000 Netz die zur Verwaltung einer Windows 2000 Domäne nötigen Dienste zur Verfügung, unter denen der Active Directory Dienst (Active Directory Service, ADS) die wichtigste Rolle einnimmt. In der Regel wird von einem DC auch der Namensdienst DNS (Domain Name Service) angeboten, ohne den das Active Directory nicht betrieben werden kann. Im DNS werden von Windows Referenzen auf wichtige Windows 2000 Ressourcen gehalten, deren Integrität für das korrekte Funktionieren einer Windows 2000 Domäne essentiell sind. Da ein DC als Anmeldeserver fungiert, führt er den dazu notwendigen Kerberos-Dienst aus. Die Kerberos-Komponenten auf dem DC bewahren zudem die im Rahmen des Authentisierungs-Protokolls genutzten geheimen Schlüssel auf.

Da jedem DC daher eine wichtige Rolle zukommt und durch ihn schützenswerte Daten gespeichert werden, sind für die Konfiguration folgende Punkte zu beachten. Daneben gelten auch für einen Domänen-Controller die in der Maßnahme M 4.137 *Sichere Konfiguration von Windows 2000* und M 4.139 *Konfiguration von Windows 2000 als Server* beschriebenen Aspekte entsprechend.

Sicherheit des Betriebssystems und des ADS

- Die Sicherheit eines Domänen-Controllers leitet sich hauptsächlich aus zwei wesentlichen Bereichen ab: der Sicherheit der Betriebssystemkonfiguration und der Sicherheit des Active Directories, welches auf eigene Sicherheitsmechanismen zurückgreift (siehe auch M 3.27 *Schulung zur Active Directory-Verwaltung*). Die Sicherheitseinstellungen des Betriebssystems erfolgen im Wesentlichen durch Gruppenrichtlinien, die Sicherheitseinstellungen des Active Directories erfordern entsprechende Planung und Umsetzung (siehe M 2.229 *Planung des Active Directory*, M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000*).
- An einem Domänen-Controller dürfen sich nur berechtigte Administratoren lokal anmelden. Ein Benutzerbetrieb auf einem Domänen-Controller darf nicht erlaubt werden. Nach einer Standardinstallation ist es normalen Benutzern daher nicht gestattet, sich lokal an einem DC anzumelden.

keine zusätzlichen Dienste aktivieren

- Ein Domänen-Controller sollte neben den zwingend notwendigen Standard DC Diensten, wie z. B. ADS, Kerberos und DNS, keine weiteren Infrastrukturdienste (z. B. DFS, DHCP) anbieten. Insbesondere vom Betrieb eines DHCP-Servers auf einem DC muss aus Sicherheitsgründen abgeraten werden (siehe auch Microsoft Dokumentation zu DNS und DHCP). Beide Dienste laufen unter den gleichen Berechtigungen ab. Dadurch können - stark vereinfacht dargestellt - die Zugriffsrechte auf DNS-Daten nicht mehr durchgesetzt werden, wenn der DHCP-Dienst Veränderungen an DNS-Daten durchführt.
- Ein Domänen-Controller sollte keine (Applikations-) Serverdienste anbieten, da bei Fehlern in den Serverprogrammen eine Kompromittierung des DC und damit der gesamten Windows 2000 Domäne möglich ist.

Domänen-Controller sollten so sicher wie möglich konfiguriert werden. Nach der Standardinstallation sollte die Vorlagendatei *secdc.inf* oder *hisecdc.inf* angewandt werden. Die Vorlagendateien finden sich im Windows 2000 Systemverzeichnis unter *C:\WINNT\security\templates* und können entweder von der Kommandozeile mittels des Kommandos *secedit* konfiguriert werden, oder über die MMC-Plug-ins *Sicherheitsvorlagen* und *Sicherheitskonfiguration und -analyse* angesehen oder angewandt werden. Wurde der Rechner von NT nach Windows 2000 migriert und nicht neu installiert, so ist zunächst das Template *basicdc.inf* anzuwenden, um eine Standard Windows 2000 Konfiguration zu erreichen. Je nach Umfeld müssen die durch die Vorlagen *secdc.inf* bzw. *hisecdc.inf* vorgenommen Einstellungen angepasst werden. Dies kann beispielsweise erforderlich sein, wenn im Netz noch Altsysteme, z. B. OS/2, vorhanden sind, die weniger sichere Einstellungen bieten. Weitere Hinweise zur Planung der Sicherheitseinstellungen finden sich in M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000*.

- Die Konfiguration des Kanals, der zur Kommunikation von Verwaltungsdaten zwischen Rechnern einer Windows 2000 Domäne genutzt wird, sollte so sicher wie möglich sein (siehe dazu M 5.89 *Konfiguration des sicheren Kanals unter Windows 2000/XP*).

DC im native mode betreiben

- Wenn möglich, sollte ein Domänen-Controller im *native mode* betrieben werden, damit alle Windows 2000 Mechanismen voll ausgenutzt werden können. Dies sind beispielsweise universelle Gruppen, Gruppenschachtelung und die Vergabe der RAS-Zugangsberechtigung über eine Gruppenzugehörigkeit. Ein Umschalten in den *native mode* ist dann möglich, wenn in der Domäne kein Windows NT BDC (Backup-Domänen-Controller) betrieben wird. Der Betrieb von Windows NT Servern und Workstations ist auch im *native mode* möglich. Zu beachten ist, dass eine Rückkehr in den *mixed mode* und damit zu einer NT-Domäne danach nicht mehr möglich ist.

Restore Modus durch Passwort schützen

- Kann ein Domänen-Controller in den so genannten AD-Restore-Modus gebootet werden, so ist es möglich, Veränderungen am AD durchzuführen, indem z. B. alte Zustände (teilweise oder vollständig) von Backup-Medien geladen werden. Diese Veränderungen lassen sich so einspielen, dass sie nach dem regulären Booten durch die AD-Replikation an alle anderen DCs einer Domäne propagiert werden. Es ist daher sicherzustellen, dass der AD-Restore-Modus durch ein geeignetes Passwort geschützt ist und Arbeiten in diesem Modus nur unter Einhaltung des Vier-Augen-Prinzips erfolgen. Der AD-Restore-Modus ist kommandozeilenbasiert und Tippfehler können gravierende Folgen haben, z. B. Löschen oder Überschreiben des falschen AD-Zweiges. Daher bietet das Vier-Augen-Prinzip hier neben der Tätigkeitskontrolle auch eine Sicherheit durch die Kontrolle aller Eingaben durch zwei Personen.
- Die Domänen-Controller der Forest-Root-Domäne (FRD) sind aufgrund der Sonderstellung der FRD besonders schutzbedürftig.

Generell ist für jeden Domänen-Controller immer die physikalische Sicherheit zu gewährleisten, z. B durch Aufstellung in einem Serverraum.

Ergänzende Kontrollfragen:

- Sind für alle Domänen-Controller restriktive Zugriffsrechte auf Betriebssystemebene vergeben?
- Wurden die AD-Berechtigungen restriktiv vergeben?
- Ist die physikalische Sicherheit aller Domänen-Controller gewährleistet?
- Sind nur die gemäß Planung benötigten Dienste für jeden Domänen-Controller installiert?

M 4.139 Konfiguration von Windows 2000 als Server

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Nutzung von Windows 2000 als Serverbetriebssystem stellt eine der drei Hauptnutzungsvarianten dar. Generell können Server als Rechner angesehen werden, die Dienste zur Nutzung durch Clients, d. h. durch Arbeitsplatzrechner, aber auch durch andere Server, anbieten. Die angebotenen Dienste können sehr vielfältig sein, wenn zusätzliche Produkte von Drittherstellern zum Einsatz kommen.

Schon in einer Standarddistribution von Windows 2000 Server sind verschiedene Dienste enthalten, die meist Systemdienst-Charakter besitzen und damit als Infrastrukturdienste angesehen werden können (siehe auch M 4.140 *Sichere Konfiguration wichtiger Windows 2000 Dienste*).

Aus Sicherheitssicht ist für einen Server Folgendes zu beachten:

Dienste sicher konfigurieren

- Die Sicherheit eines Servers hängt wesentlich von den eingesetzten Diensten ab. Ist ein Dienst fehlerhaft konfiguriert oder programmiert, so können diese Fehler unter Umständen dazu genutzt werden, auf den Server in unberechtigter Weise zuzugreifen. Aus diesem Grund kommt der sicheren Konfiguration aller von einem Server angebotenen Dienste eine besondere Bedeutung zu. Hinweise zur sicheren Konfiguration von wichtigen Windows 2000 Diensten finden sich in M 4.140 *Sichere Konfiguration wichtiger Windows 2000 Dienste*. Für die Konfiguration von Diensten von Drittherstellern können an dieser Stelle keine allgemeinen Empfehlungen geben werden.

nicht benötigte Dienste abschalten

- Auf einem Server sollten alle nicht benötigten Systemdienste abgeschaltet werden. Dies verhindert, dass diese Dienste durch Dritte unberechtigt oder für Angriffe genutzt werden können.

Verträglichkeit der Dienste prüfen

- Die auf einem Server eingesetzten Dienste sollten auf ihre wechselseitige Verträglichkeit geprüft werden. Oft entstehen Sicherheitslücken erst durch die Kombination von Diensten. Die Verträglichkeitsprüfung ist jedoch schwierig und erfordert in der Regel eine genaue Analyse. Allgemeine Hinweise dazu lassen sich leider nicht geben. Es empfiehlt sich jedoch auch aus Gründen der Fehlertoleranz, Dienste nicht auf einem Server zu kumulieren, sondern auf verschiedene, unter Umständen dedizierte Server zu verteilen.
- Auf einem Server sollte kein Benutzerbetrieb stattfinden. Ausnahmen sind naturgemäß Terminalserver. Die Konfiguration der zulässigen Benutzer kann unter Windows 2000 über Gruppenrichtlinien gesteuert werden. Die dazu wichtigen Einstellungen sind die Benutzerrechte *Logon Locally* und *Access this computer from the network*.
- Dienste können unter den Berechtigungen eines bestimmten Benutzerkontos ablaufen. Nach der Standardinstallation eines Dienstes wird jedoch meist das Konto des lokalen Rechners (*Local System*) benutzt, welches dem Dienst Betriebssystemprivilegien gibt. Für Dienste, die diese privilegierten Berechtigungen nicht zwingend zum Ablauf benötigen, empfiehlt sich daher die Nutzung eines eigenen, dedizierten Dienstkontos. Das ge-

wünschte Konto ist nach dem Anlegen unter dem Punkt *Dieses Konto* auf der Registerkarte *Anmelden* im *Eigenschaftsdialog* des Dienstes in der Diensteverwaltung (*Systemsteuerung/Computerverwaltung/Dienste*) einzutragen. Hier muss auch das Passwort des jeweiligen Kontos angegeben werden. Auf diese Weise lässt sich auch die Zugriffskontrolle auf lokale oder entfernte Ressourcen implementieren, sodass einem Dienst nur die Zugriffsberechtigungen erteilt werden, die für den geregelten Ablauf nötig sind. Insbesondere verhindert dies, dass bei einer Kompromittierung des Dienstes der Angreifer Betriebssystemberechtigungen erhält.

Problematisch ist dabei jedoch, dass neue Dienste meistens standardmäßig unter den Berechtigungen *Local System* ablaufen. Dies gilt auch für die Windows Standarddienste. Außerdem ist es oft unklar, ob diese Dienste auch unter einem dedizierten Dienstkonto ablauffähig sind und welche Berechtigungen diesem Konto eingeräumt werden müssen. Dies kann im Regelfall nur durch Tests herausgefunden werden.

- Werden für Dienste dedizierte Dienstkonten genutzt, so sollten diese Konten für den interaktiven Zugang zum System gesperrt werden. Das Anmelden als Dienst muss hingegen erlaubt werden. Außerdem ist ein sicheres Passwort für das Dienstkonto zu vergeben. Zur Verwaltung von Dienstkonten existieren Produkte von Drittherstellern, die auch ein Passwortmanagement erlauben.

komplexe Dienste auf dedizierten Rechnern betreiben

- Für komplexe Dienste, die meist über eine lokale Datenhaltung verfügen, empfiehlt sich die Nutzung dedizierter Rechner. Beispiele hierfür sind u. a. der RAS-Dienst und die Internet Information Services (IIS). Je nach Funktion empfiehlt es sich auch, eine eigene Windows Domäne für gleichartige Dienstrechner, wie z. B. für Internetserver zu erzeugen, sodasss auch auf Domänenebene eine Trennung erfolgen kann. Je nach Einsatzszenario können dann Zugriffsbeschränkungen für diese Domänenmitglieder eingerichtet werden, wie beispielsweise der Entzug der Vertrauensstellung.

Zugriffsrechte auf Netzfreigaben

- Werden durch einen Server Netzfreigaben angeboten, wie beispielsweise durch einen Dateiserver, so ist auf die Vergabe geeigneter Zugriffsrechte zu achten. Dies betrifft sowohl die Netzfreigabe, als auch die durch die Freigabe angebotenen Verzeichnisse und Dateien (siehe dazu auch M 4.149 *Datei- und Freigabeberechtigungen unter Windows 2000/XP*).

Angriffe protokollieren

- Generell empfiehlt es sich, die Zugriffe auf die Ressourcen eines Servers zu protokollieren. Daher sollten für Server Protokolleinstellungen entworfen und umgesetzt werden, die für die Überwachung im Rahmen der jeweiligen Nutzungsszenarien geeignet sind. Diese müssen in das Überwachungskonzept (siehe M 4.148 *Überwachung eines Windows 2000/XP Systems*) integriert sein. Da hier meist auch benutzerbezogene Daten erfasst werden, sollte sowohl der Datenschutzbeauftragte als auch der Personal- bzw. Betriebsrat rechtzeitig in die Planung einbezogen werden.

Die aufgezeigten Empfehlungen sind als Anregung für weitere Maßnahmen zu verstehen, die in Abhängigkeit spezieller Dienste und deren Funktion durchgeführt werden müssen. Vor Einführung eines neuen Dienstes sollte daher eine geeignete Analyse der Auswirkungen auf die Systemsicherheit sowie eine

Schutzbedarfsfeststellung erfolgen (siehe dazu auch IT-Grundschutz-Vorgehensweise).

Ergänzende Kontrollfragen:

- Werden nur die benötigten Dienste auf einem Server ausgeführt?
- Sind bei Nutzung mehrerer Dienste auf einem Server Abhängigkeiten und Seiteneffekte berücksichtigt worden?
- Ist der lokale Benutzerbetrieb für Server unterbunden worden?
- Werden Dienste - wenn möglich - unter eigenen Konten ausgeführt?
- Werden Zugriffe auf die Server-Ressourcen gemäß des Überwachungskonzeptes protokolliert?
- Sind für Dateiserver bedarfsgerechte und minimale Zugriffsrechte auf die Netzfreigaben und die freigegebenen Ressourcen vergeben?

M 4.140 Sichere Konfiguration wichtiger Windows 2000 Dienste

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Zum geregelten Betrieb eines Windows 2000 Netzes werden neben der reinen Betriebssystemsoftware zusätzliche Dienste benötigt. Als wichtigster Dienst zum Betrieb einer Windows 2000 Domänenstruktur steht der Active Directory Service (ADS) zur Verfügung, der damit eine zentrale Stellung einnimmt. Die Sicherheit eines Windows 2000 Netzes hängt wesentlich von der Konfiguration des Active Directories ab, die daher der sorgfältigen Planung und Umsetzung bedarf (siehe dazu M 2.229 *Planung des Active Directory*, M 2.230 *Planung der Active Directory-Administration*, M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000*, M 3.27 *Schulung zur Active Directory-Verwaltung*). Daneben existieren weitere Windows 2000 Dienste, die je nach Bedarf (siehe M 2.227 *Planung des Windows 2000 Einsatzes*) weitere Funktionen übernehmen können. Beispiele für wichtige Dienste sind:

- DDNS-Dienst und WINS-Dienst zur Namensauflösung,
- DHCP-Dienst zur dynamischen Verwaltung von IP-Adressen,
- DFS-Dienst zum Aufbau virtueller, unternehmensweiter Dateibäume,
- Windows PKI-Dienste zur Verwaltung von Zertifikaten,
- Windows RRAS-Dienst für den Remote-Zugang.

Als Voraussetzung für die Sicherheit eines Windows 2000 Netzes muss die sichere Konfiguration jedes einzelnen eingesetzten Dienstes erfolgen. Dies gilt auch für die sichere Konfiguration der Zusammenarbeit einzelner Dienste (z. B. DDNS und DHCP).

Folgendes ist für die betrachteten Dienste zu berücksichtigen:

DDNS ist für das AD erforderlich

- Der DDNS (Dynamic Domain Name Service) ist zwingend einzusetzen, wenn eine Windows 2000 Domäne aufgebaut werden soll, da das AD auf DNS als Namensdienst angewiesen ist. Daher kommt der Integrität und Konsistenz der Daten des DNS eine besondere Bedeutung unter Windows 2000 zu. Fehler in den DNS-Daten oder ein Ausfall des DNS-Servers haben zur Folge, dass z. B. sämtliche Anmeldeversuche fehlschlagen, wenn keine Ausweichserver zur Verfügung stehen. Betroffen sind hiervon auch die Anmeldeversuche eines Administrators direkt am DC. Hinweise zur sicheren Konfiguration finden sich in M 4.141 *Sichere Konfiguration des DDNS unter Windows 2000*.
- Der WINS (Windows Internet Name Service) Dienst ist zum Betrieb einer reinen Windows 2000 Domäne nicht notwendig und muss daher nicht betrieben werden. Da ein Windows 2000 Netz jedoch meistens durch die Migration eines bestehenden Netzes aufgebaut wird und dadurch zumindest übergangsweise meist auch Altsysteme vorhanden sind, muss WINS in der Regel weiter eingesetzt werden. Dies ist insbesondere dann notwendig, wenn WINS-basierte Applikationen existieren, die nicht migriert werden können. Durch den Parallelbetrieb von DDNS und WINS ergibt

sich zusätzlich das Problem der Konsistenz der jeweils gehaltenen Daten. Hinweise zur sicheren Konfiguration von WINS finden sich in M 4.142 *Sichere Konfiguration des WINS unter Windows 2000*.

Konsistenz von DHCP und DDNS

- DHCP (Dynamic Host Configuration Protocol) bietet die Möglichkeit, Rechner dynamisch mit IP-Adressen zu versehen. Einem so genannten DHCP-Server wird eine Menge von IP-Adressen übergeben, die er auf Anfrage von DHCP-Clients dem anfragenden Rechner zuteilen kann. Die IP-Adressen werden dabei nur für eine bestimmte Zeit, die so genannte Lease-Zeit, zugeteilt. Ist diese abgelaufen, muss eine erneute Anfrage an den DHCP-Server gestellt werden. Hierbei kann eine neue IP-Adresse angefragt oder die Lease-Zeit der alten Adresse verlängert werden. Ein Rechner kann die IP-Adresse auch vor Ablauf der Lease-Zeit wieder freigeben. Aufgrund der dynamischen Zuordnung von IP-Adresse zu Rechner und demzufolge auch zum Rechnernamen, muss bei Änderungen der Zuordnung auch eine Änderung im Namensdienst (DDNS) erfolgen. Aus Sicherheitssicht ergibt sich dabei das Problem, die Konsistenz der Namen zur IP-Adressen-Zuordnung innerhalb des DDNS angesichts ständig wechselnder Zuordnungen zu gewährleisten. Hinweise zur sicheren Konfiguration und Nutzung von DHCP finden sich in M 4.143 *Sichere Konfiguration des DHCP unter Windows 2000*. Wenn es organisatorisch möglich ist, sollte eine feste Bindung von IP-Adressen an die MAC-Adressen der Netzwerkkarten in den einzelnen Rechnern angestrebt werden und keine voll dynamische Vergabe erfolgen. Dies erleichtert zudem die Auswertung von Protokollen auf anderen Systemen, wie z. B. Firewalls.

PKI-Einsatz erfordert Sorgfalt und Zeit

- Neben den Windows 2000 Systemmechanismen zur Authentisierung und Absicherung von Kommunikationskanälen erlaubt Windows 2000 zusätzlich die Verwendung PKI-basierter (Public Key Infrastructure) Verfahren. Zur Verwaltung der dabei eingesetzten Schlüssel und Zertifikate stellt Windows 2000 PKI-Komponenten zur Verfügung. Die Kernkomponente einer PKI-Architektur ist die Ausgabestelle für Zertifikate (Certificate Authority, CA). Hinweise zum Umgang und zur sicheren Konfiguration der Windows 2000 CA finden sich in M 4.144 *Nutzung der Windows 2000 CA*. Es muss jedoch darauf hingewiesen werden, dass die Planung und der Betrieb einer PKI Sorgfalt und Zeit benötigen und auch die lokalen Anforderungen berücksichtigt werden müssen. Die angeführten Empfehlungen beziehen sich daher nur auf die technischen Besonderheiten der Windows CA.

sichere Einwahl über RRAS

- Auch unter Windows 2000 steht mit dem Dienst RRAS (Routing & Remote Access Service) die Möglichkeit zur Verfügung, per Einwahl aus der Entfernung auf Ressourcen eines Windows 2000 Netzes zuzugreifen. Außerdem ist es hiermit möglich, abgesicherte VPN (Virtual Private Networking) Verbindungen zwischen Teilnetzen verschiedener Standorte herzustellen. Wird Benutzern die Möglichkeit zur Einwahl eröffnet, ergeben sich automatisch neue Gefährdungen für ein Windows 2000 Netz. Nun spielt auch die Sicherheit der zur Einwahl benutzten Rechner, z. B. am heimischen Arbeitsplatz (siehe dazu auch Baustein B 5.8 *Telearbeit*), und die Sicherheit bei der Kontaktaufnahme (Authentisierung, Absicherung der

Kommunikation) eine Rolle für die Sicherheit des internen Netzes. Hinweise zur Sicherheit bei der Nutzung von RAS-Diensten finden sich im Baustein B 4.4 *Remote Access*. Weitere Hinweise zu den Windows 2000 spezifischen Aspekten finden sich in M 4.145 *Sichere Konfiguration von RRAS unter Windows 2000*.

Abschließend muss darauf hingewiesen werden, dass die Konfiguration einzelner Dienste immer von lokalen Gegebenheiten oder Anforderungen abhängt. Die Konfiguration muss immer im Kontext gesehen werden. Im Einzelfall muss sogar aufgrund lokaler Gegebenheiten auf weniger sichere Konfigurationen ausgewichen werden. In diesen Fällen ist es jedoch wichtig, dann zusätzliche Schutzmaßnahmen einzusetzen, die geeignet sind, die fehlende Sicherheit in der Dienstkonfiguration auszugleichen. Beispiele hierfür sind der Einsatz einer zusätzlichen Firewall oder auch organisatorische Maßnahmen.

Ergänzende Kontrollfragen:

- Wurden die benötigten Infrastrukturdienste sinnvoll im Netz angesiedelt?
- Wurde eine Anhäufung von Diensten auf wenigen Rechnern vermieden?
- Kann auf den zusätzlichen Einsatz von WINS verzichtet werden?
- Wurde die Konfiguration der Dienste DDNS und DHCP aufeinander abgestimmt?

M 4.141 Sichere Konfiguration des DDNS unter Windows 2000

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der Dienst DDNS (Dynamic Domain Name Service) spielt unter Windows 2000 eine wichtige Rolle, da ohne ihn kein Active Directory (AD) - und damit auch keine Windows 2000 Domäne - betrieben werden kann. DDNS stellt einen Namensdienst zur Verfügung, der u. a. eine Zuordnung von IP-Adressen zu (symbolischen) Rechnernamen erlaubt. DDNS beruht dabei auf dem Internet-Namensdienst DNS und erweitert diesen jedoch um die Möglichkeit, Namen-Adressen-Zuordnungen dynamisch in die DNS-Datenbank des so genannten DNS-Servers einzutragen oder aus dieser zu löschen. Auf diese Weise wird die Nutzung des DHCP (Dynamic Host Configuration Protocol) ermöglicht, welches zur dynamischen Zuordnung von IP-Adressen zu Rechnern verwendet werden kann.

Für die Konfiguration und Nutzung des DDNS muss aus Sicherheitssicht Folgendes berücksichtigt werden:

Zonendaten im AD speichern

- Die von einem DDNS-Server verwalteten Zonendaten können entweder in einer Datei gespeichert werden, wie dies z. B. bei herkömmlichen DNS-Servern der Fall ist, oder aber die Daten werden im AD gespeichert. Man spricht dann von AD-integrierten Zonen. Die AD-integrierte Speicherung bietet sicherheitstechnische Vorteile, so dass dies für alle von einem DDNS-Server verwalteten Zonen empfohlen wird. Die Auswahl, wie die Informationen für eine Zone abgelegt werden, erfolgt entweder beim Anlegen der Zone oder kann nachträglich im Eigenschaftsdialog einer Zone verändert werden.
- Werden Zoneninformationen in Dateien gespeichert, so sind die Dateien auf Dateisystemebene so abzusichern, dass auf diese nicht unbefugt zugegriffen werden kann. Vielmehr darf der Zugriff auf die Dateien nur dem Konto des DNS-Administrators und dem DNS-Server-Prozess, der unter dem lokalen Systemkonto abläuft, möglich sein. Es ist zu beachten, dass diese Dateien nicht mit EFS geschützt werden können, da es sich um Systemdateien handelt.
- Windows 2000 ist nicht zwingend auf den Einsatz eines Windows 2000 DDNS-Servers angewiesen, sondern kann auch mit anderen DNS-Server-Implementationen zusammenarbeiten, solange diese bestimmte Anforderungen erfüllen, wie z. B. Unterstützung von SRV-Records und der dynamischen Update-Möglichkeit. Aus Sicherheitssicht empfiehlt sich jedoch insbesondere beim Betrieb eines Windows 2000 DHCP-Servers die Nutzung von Windows 2000 DDNS-Servern, da diese das Update von der korrekten Domänenidentität eines DHCP-Clients abhängig machen.

kein Zonentransfer an unbekannte Rechner

- Zoneninformationen können zwischen DNS-Servern ausgetauscht und damit aktualisiert werden. Dazu dient der so genannte Zonentransfer. Aus Sicherheitssicht sollte der Zonentransfer nur von und an vertrauenswürdige DNS-Server erlaubt werden. Dazu muss die Liste der DNS-Server erstellt werden, die aktualisierte Zoneninformationen erhalten oder versenden sol-

len. Durch die Zoneninformationen wird das gesamte Netz beschrieben (Rechnernamen und IP-Adressen), sodass diese Information einem Angreifer alle potentiellen Ziele aufzeigt. Aus diesem Grund darf der Zonentransfer nur zwischen bekannten DNS-Servern stattfinden. Insbesondere darf ein Zonentransfer an unbekannte Rechner oder gar an unbekannte Rechner im Internet unter Sicherheitsgesichtspunkten nicht stattfinden.

Für das sichere Zusammenspiel mit einem DHCP-Server zum dynamischen Verwalten von DNS-Einträgen ist Folgendes zu berücksichtigen (siehe auch M 4.143 *Sichere Konfiguration des DHCP unter Windows 2000*):

- Bei Nutzung von DHCP mit dynamischem DNS-Update sollten ausschließlich AD-integrierte Zonen verwendet werden, damit die Option *Secure Update* genutzt und aktiviert werden kann. Die Aktivierung erfolgt über den Eigenschaftsdialog der Zone auf der Registerkarte *Allgemein* durch Auswahl von *Ändern* beim Typeintrag und Auswahl der Option *Active-Directory-integriert*. Dies stellt sicher, dass Veränderungen an dynamisch erzeugten DNS-Einträgen nur durch den berechtigten Besitzer möglich sind. Zusätzlich findet eine Zugriffskontrolle aufgrund der Domänenmitgliedschaft statt.
- Generell muss bei DNS Einträgen zwischen dem so genannten Forward-Mapping (Namen-IP-Addressen-Zuordnung) und dem so genannten Reverse-Mapping (IP-Addressen-Namen-Zuordnung) unterschieden werden. Bei einer Windows 2000 Standardinstallation erfolgt die dynamische Registrierung des Forward-Mappings immer durch den DHCP-Client, das Eintragen des Reverse-Mappings erfolgt durch den DHCP-Server. Der DHCP-Client muss jedoch auf die DNS-Registrierung ausgelegt sein, was für ältere Windows-Versionen nicht der Fall ist: Hier muss auch das Forward-Mapping durch den DHCP-Server erfolgen. Diese Option kann im Eigenschaftsdialog auf der Registerkarte *DNS* aktiviert werden. Es muss für ein Netz generell entschieden werden, ob auch das Forward-Mapping generell für alle DHCP-Clients durch den DHCP-Server erfolgt. Aus Sicherheitssicht muss generell verhindert werden, dass durch "bösartige" DHCP-Clients falsche DNS-Einträge vorgenommen werden (siehe auch M 4.143 *Sichere Konfiguration des DHCP unter Windows 2000*).
- Für wichtige Server sollten keine dynamischen Adressen verwendet werden. Die Adressen wichtiger Server sollten statisch im DNS-Server eingetragen werden. Die Berechtigungen für das DNS-Record können dabei so gesetzt werden, dass ein Überschreiben der Adresse durch ein dynamisches Update nicht möglich ist. Muss DHCP aus zwingenden Gründen auch für zentrale Server eingesetzt werden, so empfiehlt sich auch hier, dass der Eintrag im DNS durch den Administrator vorgenommen wird. Die Berechtigungen auf den DNS-Eintrag können jedoch so gesetzt werden, dass ein Update durch den Server erlaubt ist. Die Option *Secure Update* - die im Eigenschaftsdialog einer Zone aktiviert werden kann - stellt dann die korrekte Rechneridentität sicher.
- Das Löschen "alter" DNS-Einträge erfolgt standardmäßig durch den DNS-Server selbst und nicht durch den jeweiligen DHCP-Client. Dadurch kön-

nen eine Zeit lang nicht aktuelle DNS-Zuordnungen existieren, die von Angreifern ausgenutzt werden könnten. Hier empfiehlt es sich, das Forward-Mapping durch den DHCP-Server nach Ablauf der Lease-Dauer löschen zu lassen, damit inkonsistente Zuordnungen nur möglichst kurz existieren. Diese Funktion lässt sich im Eigenschaftsdialog des DHCP-Servers auf der Registerkarte *DNS* mit der Option *Forward-Lookups (Name zu Adresse) beim Ablauf des Lease löschen* aktivieren. Es ist zu beachten, dass auch hier, z. B. im Falle eines Rechnerausfalles, die Name-IP-Adressen-Zuordnung noch bis zum Ablauf der Lease-Dauer im DNS-Server existiert.

Zusammenfassend ergibt sich, dass DNS-Informationen sicherheitsrelevante, schutzwürdige Daten darstellen. Kann ein Angreifer DNS-Informationen verfälschen, so kann die Sicherheit des gesamten Netzes kompromittiert werden. Insofern erfordert insbesondere die Nutzung von DHCP mit DNS eine sorgfältige Planung unter Sicherheitsgesichtspunkten.

Ergänzende Kontrollfragen:

- Können alle Zonen als AD-integrierte Zonen betrieben werden?
- Ist der *Sichere Update* für alle AD-integrierten Zonen aktiviert?
- Ist für alle Zonen das Übertragen der Zoneninformationen so konfiguriert, dass der Austausch nur mit bekannten DNS-Servern erfolgen kann?
- Sind die DNS-Einträge für wichtige Infrastrukturserver fest vorkonfiguriert?
- Ist der DHCP-Server so konfiguriert, dass durch ihn erzeugte DNS-Einträge nach Ablauf der Lease-Dauer automatisch gelöscht werden?

M 4.142 Sichere Konfiguration des WINS unter Windows 2000

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

möglichst auf WINS verzichten

Der *Windows Internet Naming Service (WINS)* wurde unter Windows NT als primärer Namensdienst zur Namen-Adressen-Auflösung verwandt. Unter Windows 2000 hat der DNS (Domain Name Service) bzw. die Windows 2000 Variante DDNS (Dynamic DNS) diese Rolle vollständig übernommen. Daher ist WINS zum Betrieb eines Windows 2000 Netzes nicht mehr erforderlich. In vielen Fällen ist es jedoch auch in Windows 2000 Netzen notwendig, weiterhin WINS anzubieten, da diese oft heterogen sind und Rechner oder Applikationen enthalten, die nach wie vor auf die Namensauflösung mittels WINS angewiesen sind. Wenn möglich, sollte auf den Betrieb von WINS jedoch verzichtet oder der Betrieb von WINS nur so lange wie unbedingt notwendig aufrecht erhalten werden.

Unter Sicherheitsgesichtspunkten sind beim Betrieb von WINS unter Windows 2000 folgende Aspekte zu beachten:

- Werden zwei Strukturen zur Namensauflösung parallel betrieben, so müssen beide Datenbestände konsistente Informationen enthalten. Da aber jeweils unterschiedliche Mechanismen zur Verwaltung eingesetzt werden, kann dies zu Fehlern in den Datenbeständen führen. Dies muss durch regelmäßige Kontrollen verhindert werden.

Zugriffsrechte auf WINS-Datenbanken

- Die Sicherheit des WINS-Servers muss sichergestellt sein. Dazu gehört auch die Dateisystemabsicherung der WINS-Datenbanken, die unter *%SystemRoot%\System32\WINS* abgelegt sind. Diese sollten auf restriktive Zugriffsrechte überprüft werden. In der Regel benötigt hier nur das Systemkonto selbst Zugriffsrechte (Vollzugriff). Werden die Dateien selbst von Hand gewartet, so müssen auch dem berechtigten Administrator entsprechende Zugriffsrechte eingeräumt werden.

"tomb-stoning"

- Da WINS das dynamische Aktualisieren (z. B. durch DHCP) unterstützt, muss die WINS-Datenbank periodisch nach alten, d. h. ungültigen Einträgen durchsucht werden, die dann gelöscht werden. In Umgebungen mit mehreren Servern kann es passieren, dass durch Replikation ein Eintrag, der gerade auf einem Server gelöscht wurde, wieder auf diesen Server repliziert wird. Dadurch kann das Löschen schwierig werden. Aus diesem Grund kann ein Eintrag zunächst als "veraltet" deklariert werden, sodass er zwar noch vorhanden ist, aber nicht genutzt wird. Durch die Replikation verbreitet sich auch der Zustand eines so markierten Eintrages, sodass nach einiger Zeit ein solcher Eintrag auf allen Servern als "veraltet" markiert ist und dann automatisiert gelöscht werden kann. Dieser auch "tomb-stoning" genannte Prozess kann periodisch ausgeführt werden. Die relevanten Alterungsparameter, die angeben, ab wann ein Eintrag als alt betrachtet wird, müssen im Eigenschaftsdialog des Servers auf der Karte *Intervalle* an die lokalen Gegebenheiten angepasst werden. Neben dem automatischen "tomb-stoning" sollte bei WINS in regelmäßigen Abständen auch ein manuelles "tomb-stoning" durchgeführt werden, indem alle nicht automatisch erkannten alten WINS-Einträge über das Vorgang-Menü als

"veraltet" erklärt werden: *Vorgang/Löschen,* Option *Löschen des Eintrags zu anderen Servern replizieren (veralten)*. Für die Sicherung der Konsistenz stehen über das "Windows 2000 Server Resource Kit" weitere Werkzeuge zur Verfügung, z. B. *winschk.exe*.

WINS-Replikation einschränken

- WINS-Replikation, d. h. Austausch und Update der WINS-Daten zwischen WINS-Servern, sollte nur zwischen bekannten und vertrauten WINS-Servern erlaubt sein. Dazu muss die Liste der WINS-Server, mit denen repliziert werden darf, für jeden WINS-Server konfiguriert werden. Dies verhindert, dass "bösartige" WINS-Server inkonsistente oder verfälschte WINS-Daten in einen WINS-Serververbund einbringen. Insbesondere dürfen WINS-Daten nicht mit Domänen, zu denen keine Vertrauensstellungen existieren (*untrusted*), ausgetauscht werden.

kein Autodiscovery für WINS-Replikation

- WINS erlaubt die automatische Konfiguration der WINS-Replikationspartner und der zur Replikation benutzten Topologie (Autodiscovery-Funktion). Dieser Automatismus sollte nicht genutzt werden. Vielmehr ist die WINS-Replikationstopologie zu planen und explizit über die Replikationspartnerlisten im Eigenschaftsdialog eines WINS-Servers zu konfigurieren. Bei der Planung muss festgelegt werden, wo WINS-Server im Netz angesiedelt werden und welcher Server mit welchem Server repliziert.

Wie bei DNS besteht die Hauptgefahr auch bei WINS darin, dass die Adressen-Namens-Zuordnungen verfälscht werden, wodurch Sicherheitseinstellungen unterlaufen werden. Daher sind diese Daten besonders schutzwürdig und erfordern die Umsetzung der angegebenen Schutzmaßnahmen. Je nach Nutzungsszenario sind jedoch auch weitere Maßnahmen notwendig, wie beispielsweise physikalische oder organisatorische Sicherheitsmaßnahmen.

geregeltes Decommissioning eines WINS-Servers

Wird ein WINS-Server aus dem Betrieb genommen, so muss sichergestellt werden, dass dies nach dem vorgeschriebenen Verfahren geschieht, um zu verhindern, dass dessen WINS-Daten weiter im Netz zwischen den verbleibenden WINS-Servern repliziert werden. Im Wesentlichen muss dazu auf allen WINS-Clients des zu entfernenden Servers die WINS-Konfiguration so geändert werden, dass diese nicht mehr auf den WINS-Server zugreifen. Danach müssen alle WINS-Einträge des Servers, der entfernt werden soll, zunächst als "veraltet" markiert werden (tomb-stoning). Anschließend wird die Replikation zu allen Replikationspartnern von Hand gestartet (für den Eintrag *Replikationspartner* Menü *Vorgang/Jetzt Replizieren*). Nach erfolgreicher Replikation mit allen Partnern kann der Server entfernt werden. Detaillierte Hinweise zum korrekten Entfernen (Decommissioning) eines WINS-Servers finden sich in der Windows 2000 Hilfe.

Ergänzende Kontrollfragen:

- Ist geprüft worden, ob auf den Einsatz von WINS verzichtet werden kann?
- Sind die WINS-Dateien gegen unbefugten Zugriff geschützt?
- Werden die WINS-Daten regelmäßig gewartet?
- Ist die automatische Konfiguration der WINS-Replikationspartner für jeden WINS-Server deaktiviert?
- Ist für jeden WINS-Server die Liste der erlaubten Replikationspartner konfiguriert?

M 4.143 Sichere Konfiguration des DHCP unter Windows 2000

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Mittels DHCP (Dynamic Host Configuration Protocol) lässt sich die Konfiguration von Rechnern beim Boot-Vorgang vornehmen. DHCP ist ein Client-Server Protokoll: Ein DHCP-Server verwaltet einen oder mehrere Pools von IP-Adressen, die er auf Anforderung an DHCP-Clients auf Zeit vergeben kann. Die Client-Anforderung ist Broadcast-basiert und wendet sich an alle DHCP-Server in einem Netz. Der Client wählt aus den verschiedenen Server-Antworten eine beliebige aus; dies ist in der Regel die erste Antwort. Insofern existiert prinzipiell keine feste Client-Server-Bindung. Die IP-Adresse wird einem Client nur auf Zeit, der so genannten Lease-Dauer, zugeordnet. Ist diese abgelaufen, so kann der Client die Verlängerung der Zuordnung beim Server beantragen. Ist die maximale Lease-Dauer abgelaufen, so muss ein Neuantrag erfolgen, wodurch in der Regel eine neue IP-Adresse festgelegt wird. Der DHCP-Server löscht Adressen-Zuordnungen, wenn die Lease-Dauer abgelaufen ist und keine Verlängerung beantragt wurde, oder wenn die maximale Lease-Dauer abgelaufen ist. Die betroffene IP-Adresse wird dann wieder in den Pool der nicht zugeordneten Adressen aufgenommen und kann ab dann an andere Rechner vergeben werden. Der Windows 2000 DHCP-Server kann auch mit dem älteren bootp-Protokoll umgehen, das ursprünglich aus der Unix-Welt stammt. So können auch Rechner, auf denen nicht Windows 2000 installiert ist, mit IP-Adressen versorgt werden.

Häufig wird DHCP nur zur dynamischen Zuordnung von IP-Adressen verwendet, da das feste Eintragen von IP-Adressen auf Clients in einem großen Netz mühsam ist. DHCP erlaubt jedoch auch die Konfiguration vieler weiterer Netz-bezogener Parameter (z. B. DNS-Server). Diese Parameter - insgesamt mehr als 70 - die auch DHCP-Optionen genannt werden, können für jeden Adresspool unterschiedlich konfiguriert werden.

Bei der Verwendung von DHCP ergeben sich mehrere Sicherheitsprobleme, die berücksichtigt werden müssen:

synchronisierte Zeit und konsistente Protokollierung

- Erfolgt die IP-Adressen-Zuordnung dynamisch, kann eine bestimmte IP-Adresse nicht mehr automatisch einem dedizierten Rechner zugeordnet werden. Im Falle eines Angriffes oder bei der nachfolgenden Angriffsrekonstruktion muss daher immer zunächst festgestellt werden, welcher Rechner zum fraglichen Zeitpunkt die entsprechende IP-Adresse erhalten hat. Dies erfordert konsistente Protokolldateien sowie eine synchronisierte Zeit innerhalb des gesamten Netzes, damit eine korrekte zeitliche Zuordnung der Einträge aus Protokolldateien, die auf unterschiedlichen Rechnern erzeugt wurden, möglich ist.
- Die IP-Adressen werden bis zum Ablauf der Lease-Dauer einem bestimmten Rechner zugeordnet. Die Namen-Adressen-Zuordnung wird entsprechend im DNS-Server registriert. Ist ein Rechner ausgeschaltet oder kann ein Angreifer einen Rechner lahm legen, z. B. durch eine Denial-of-

Service-Attacke, so kann er u. U. dessen IP-Adresse übernehmen, solange die Lease-Zeit noch nicht abgelaufen ist. Um die Zeitspanne zu verringern, in der eine illegale Übernahme einer IP-Adresse möglich ist, sollte der DHCP-Server so konfiguriert werden, dass er das Forward-Mapping im DNS-Server nach Ablauf der Lease-Zeit automatisch löscht.

Lange Lease-Zeiten einrichten

- Damit beim Einsatz von DHCP die Zuordnung zu Rechnern möglichst statisch ist, empfiehlt es sich, eine lange Lease-Dauer (z. B. 6 Monate) einzurichten. Auf diese Weise hat ein Rechner eine fast statische IP-Adresse und DHCP kann zum Verteilen von Konfigurationen über DHCP-Optionen verwandt werden. Lange Lease-Zeiten können jedoch bei mobilen Rechnern - je nach DNS-Update-Verfahren - auch zu Problemen führen (siehe unten).
- Die Vergabe von IP-Adressen an DHCP-Clients ist unter Sicherheitsgesichtspunkten eine kritische Aktivität. Aus diesem Grund sollten nur berechtigte DHCP-Server in einem Netz existieren. Unter Windows 2000 können DHCP-Server nur betrieben werden, wenn diese im Active Directory als autorisierte DHCP-Server registriert wurden. Dies erfolgt in der DHCP-Verwaltung (MMC-Snap-In) über *Vorgang/Autorisieren.* Es ist jedoch zu beachten, dass ein Angreifer auch DHCP-Server einsetzen kann, die nicht unter Windows 2000 betrieben werden, beispielsweise Linux DHCP-Server. Solche DHCP-Server unterliegen nicht dieser Einschränkung. Allerdings durchsuchen die Windows 2000 Komponenten automatisch den Netzverkehr nach Nachrichten von nicht autorisierten DHCP-Servern und melden solche. Eine explizite Konfiguration dieses Verhaltens ist nicht notwendig.

DHCP-Server nicht auf Domänen-Controllern betreiben

- DHCP-Server sollten nicht auf einem Windows 2000 Domänen-Controller ablaufen. Alle Betriebssystemkomponenten von Windows 2000 laufen unter den Berechtigungen *Local System* ab. Ein Zugriffsschutz zwischen diesen Komponenten existiert daher nicht. Eine entsprechende Empfehlung wird auch von Microsoft selbst ausgesprochen.

feste IP-Adressen für zentrale Server reservieren

- Wird DHCP auch für zentrale Server eingesetzt (z. B. WWW-Server), so empfiehlt es sich, entsprechende Adressreservierungen im DHCP-Server einzutragen. Dazu wird die so genannte MAC-Adresse, die die eindeutige Identität der Netzkarte des relevanten Rechners darstellt, mit einer IP-Adresse verknüpft. Diese kann dann nur vom Rechner mit der eingetragenen MAC-Adresse erfolgreich angefordert werden. Es ist jedoch zu beachten, dass moderne Netzkarten auch das Ändern der MAC-Adresse zulassen, so dass auch dies keinen vollständigen Schutz gegen die Übernahme von IP-Adressen bietet.
- Generell ist auch für Arbeitsplatzrechner, die im Regelfall nicht ständig im Netz bewegt werden, die Bindung der IP-Adresse an die MAC-Adresse zu empfehlen. Dieses Vorgehen erfordert allerdings das Pflegen der MAC-IP-Adressen-Zuordnung für alle Arbeitsplatzrechner. Dies kann jedoch zentral erfolgen und erleichtert die Auswertung von Protokollen auf anderen Rechnern (z. B. auf einer Firewall), insbesondere in heterogenen Netzen.
- Der Windows 2000 DHCP-Server kann so konfiguriert werden, dass nicht nur das Reverse-Mapping (IP-Adressen-Namen-Zuordnung), sondern auch

das Forward-Mapping (Namen-IP-Adressen-Zuordnung) im DNS-Server eingetragen wird. Dies hat den Vorteil, dass dynamische DNS-Updates nur durch DHCP-Server erfolgen können, sodass Veränderungen immer durch die gleichen und bekannten Rechner ausgelöst werden. Dieses Verfahren besitzt jedoch auch verschiedene Nachteile:

- Die DNS-Records sind dann im Besitz des DHCP-Servers. Fällt dieser aus, so müssen die DNS-Records vom Administrator von Hand entfernt werden.
- Werden DHCP-Clients häufig bewegt, so erhalten sie ihre Adresse ggf. von unterschiedlichen DHCP-Servern, werden jedoch beim gleichen DNS-Server registriert. Dadurch kann das Adressen-Update fehlschlagen, da das DNS-Record noch auf den vorherigen DHCP-Server registriert ist und der aktuelle DHCP-Server nicht die Update-Berechtigung besitzt. Die Wahrscheinlichkeit für das Auftreten dieses Phänomens kann dadurch verringert werden, dass kürzere Lease-Zeiten konfiguriert werden und die DHCP-Server nach Ablauf der Lease-Zeit auch das Forward-Mapping im DNS-Server löschen.
- Tragen DHCP-Server auch das Forward-Mapping im DNS-Server ein, so geschieht dies unter den Berechtigungen des DHCP-Servers, dem diese Erlaubnis aufgrund seiner Domänenzugehörigkeit erteilt ist. Da auf DHCP-Ebene keine Authentisierung erfolgt, können auf diese Weise auch Rechner, die nicht Domänenmitglieder sind, im DNS registriert werden. Erfolgt das Eintragen des Forward-Mappings durch den DHCP-Client selbst und ist die Option *Secure Update* für die relevante DNS-Zone aktiviert, so können nur authentisierte Rechner DNS-Updates vornehmen.

Zusammenfassend muss berücksichtigt werden, dass die Nutzung von DHCP und dynamischen DNS-Updates jeweils mit Vor- und Nachteilen behaftet ist. Die zu verwendende Konfiguration muss daher jeweils für den Einzelfall nach einer sorgfältigen Risikoabschätzung entschieden werden.

Ergänzende Kontrollfragen:

- Ist geprüft worden, ob auf den Einsatz von DHCP verzichtet werden kann?
- Ist der DHCP-Server so konfiguriert, dass er die von ihm erzeugten DNS-Einträge automatisch nach Ablauf der Lease-Dauer wieder löscht?
- Sind für alle nicht mobilen Rechner, die DHCP nutzen müssen, vordefinierte IP-Adressen reserviert und an die jeweilige MAC-Adresse gebunden?
- Ist geprüft worden, ob alle dynamischen DNS-Einträge ausschließlich durch den DHCP-Server erfolgen können?

M 4.144 Nutzung der Windows 2000 CA

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Windows 2000 wird mit eigenen PKI-Komponenten ausgeliefert. Eine Hauptkomponente jeder PKI (Public Key Infrastruktur) bildet dabei die so genannte CA (Certificate Authority, Zertifikatsausgabestelle). Windows 2000 kann generell auch ganz ohne PKI bzw. CA betrieben werden, wenn spezielle Windows 2000 Funktionen, wie z. B. chipkartenbasiertes Logon und SSL-Kommunikation zwischen Betriebssystemkomponenten, nicht genutzt werden. Ist die Entscheidung für den Aufbau einer Windows 2000 PKI gefallen und wurde eine entsprechende PKI-Planung (siehe dazu M 2.232 *Planung der Windows 2000 CA-Struktur*) durchgeführt, so muss eine der Windows 2000 CAs (Enterprise-CA oder Stand-alone-CA) installiert und betrieben werden.

Aus Sicherheitssicht ergeben sich dabei folgende Aspekte, die zu berücksichtigen sind:

Vertrauensstellungen einrichten

- Gemäß der geplanten CA-Struktur müssen die notwendigen Vertrauensstellungen eingerichtet werden. Es ist darauf zu achten, dass kein Fehler in der Vertrauensstruktur existiert, da dies im Betrieb zu Sicherheitsproblemen führen kann, indem bestimmten Zertifikaten fälschlicherweise vertraut wird. Die notwendigen Vertrauensstellungen werden entweder während der Konfiguration als untergeordnete CA oder aber durch das Eintragen von CA-Zertifikaten in die Liste der vertrauten Root-CAs (Cross-Zertifizierung) eingerichtet.

CA-Komponenten schützen

- Rechner, auf denen die CA-Komponenten von Windows 2000 installiert sind, müssen besonders geschützt werden. Insbesondere ist die physikalische Sicherheit und die sichere Konfiguration des Betriebssystems notwendig (siehe auch M 4.137 *Sichere Konfiguration von Windows 2000*, M 4.146 *Sicherer Betrieb von Windows 2000/XP*). Vor der Installation der CA-Komponenten muss berücksichtigt werden, dass nach der Installation der CA-Komponenten keine Veränderungen der Domänenzugehörigkeit und des Namens des benutzten Rechners mehr möglich sind. Der Rechner stellt nun die Identität der CA dar, die nicht verändert werden darf, sodass dies von Windows 2000 auch nicht zugelassen wird.
- Es empfiehlt sich, dedizierte CA-Rechner zu benutzen, auf denen keine weiteren Dienste ablaufen.
- Die Administration der CA darf nur den berechtigten CA-Administratoren möglich sein.

Beim Betrieb einer Stand-alone-CA wird das Ausstellen von Zertifikaten durch den CA-Administrator angestoßen, nachdem die Rechtmäßigkeit der Zertifikatsanforderung durch ihn überprüft wurde. Dieser Autorisierungsschritt fehlt, wenn eine Enterprise-CA eingesetzt wird, die Zertifikatsanfragen automatisch bearbeitet. Für die Enterprise-CA sind daher außerdem die folgenden Aspekte zu berücksichtigen:

- Soll unter Windows 2000 Smartcard-gestütztes Login ermöglicht werden oder sollen für Rechner Zertifikate, z. B. zur Absicherung der Kommuni-

kation von Betriebssystemkomponenten mittels SSL, benutzt werden, so muss eine Enterprise-CA eingesetzt werden.

Enroll Permissions konfigurieren

- Eine Enterprise-CA stellt Zertifikate nur dann aus, wenn das so genannte Zertifikats-Template dem Benutzer, der die Zertifikatsanforderung initiiert hat, entsprechende Zugriffsrechte einräumt. Daher sind für jedes Zertifikats-Template die gemäß CA-Planung korrekten Zugriffsrechte (so genannte *Enroll Permissions*) zu konfigurieren. Die Konfiguration ist zweistufig. Zum einen erfolgt sie über das MMC-Snap-in *Certification authority console.* Hier können über den Eigenschaftsdialog des CA-Serverknotens die generellen Zugriffsberechtigungen auf den Server eingestellt werden. Damit kann den berechtigten Benutzergruppen das Recht *Enroll* eingetragen werden. Zum anderen erfolgt die Konfiguration über das MMC-Snap-in *AD Sites and Services* im Eigenschaftsdialog der einzelnen Zertifikats-Templates unter dem Konsolenpfad *Services/Public Key Services/Certificate Templates*.
- Für die Enterprise-CA erfolgt die Zertifikatsanforderung von Benutzern über spezielle WWW-Seiten, die so genannten *Web Enrollment Pages*, die auf einem separaten Rechner mit installiertem WWW-Server gehalten werden.

  Zugriff auf Web Enrollment Pages absichern

  Für den Zugriff auf diese Seiten sollte die Authentisierung nicht mittels *basic authentication* erfolgen. Diese Methode hat nämlich den Nachteil, dass hier ohne zusätzliche Maßnahmen, wie z. B. durch SSL-Absicherung, das Benutzerpasswort mehrfach ungeschützt übertragen wird. Das Passwort ist zwar Base64-kodiert und damit auf den ersten Blick nicht entzifferbar, aber ohne Probleme auswertbar.

  Außerdem muss der Rechner, der die *Web Enrollment Pages* anbietet, abgesichert werden, da dieser direkt mit dem CA-Rechner kommuniziert. Netztopologisch muss der Rechner, der die *Enrollment Pages* anbietet, von allen Benutzern zugreifbar sein, die berechtigt sind, Zertifikate zu beantragen. Je nach Einsatzszenario kann auch eine Anordnung in einem eigenen Netzsegment sinnvoll sein, wobei der Zugriff auf dieses Segment beispielsweise durch Paketfilter kontrolliert werden kann.
- Soll die Enterprise-CA lediglich Zertifikate für Rechner ausgeben und keine Benutzerzertifikate erstellen, so muss die Unterstützung der *Web Enrollment Pages* deaktiviert werden.

Generell muss auch berücksichtigt werden, dass die Rückruflisten entsprechend dem CA-Konzept erstellt und verteilt werden müssen. Die aufgezeigten Maßnahmen müssen immer auf den konkreten Fall angepasst werden.

Ergänzende Kontrollfragen:

- Wurde eine bedarfsgerechte PKI-Planung durchgeführt?
- Sind alle Rechner, auf denen CA-Komponenten installiert sind, gegen unbefugten Zugriff geschützt?
- Sind alle Rechner, auf denen CA-Komponenten installiert sind, physikalisch geschützt?
- Sind auf Rechnern, auf denen CA-Komponenten installiert sind, keine anderen Infrastrukturdienste installiert?
- Sind für alle CAs alle eingerichteten Vertrauensstellungen geprüft worden?
- Sind für alle Zertifikatsvorlagen die notwendigen Zugriffsrechte für Benutzer eingetragen?
- Ist eine Enterprise-CA installiert worden, wenn eine Benutzerauthentisierung mittels Chipkarte geplant ist oder wenn die Kommunikation zwischen Windows 2000 Systemkomponenten mittels SSL abgesichert werden soll?

M 4.145 Sichere Konfiguration von RRAS unter Windows 2000

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Auch unter Windows 2000 steht eine RAS (Remote Access Service) Komponente zur Verfügung, die jedoch auch als RRAS (Routing & RAS) bezeichnet wird. Der RRAS-Server unterstützt dabei außerdem den Aufbau verschlüsselter Kommunikationsverbindungen, so dass damit ebenfalls VPN (Virtual Private Network) Verbindungen möglich sind. Damit ist es z. B. möglich, zwei Windows 2000 Netze über ein unsicheres Kommunikationsmedium, etwa das Internet, miteinander zu verbinden. Es ist zu berücksichtigen, dass hierbei in der Regel das Firewall-Konzept entsprechend angepasst werden muss, siehe dazu Baustein B 3.301 *Sicherheitsgateway (Firewall)*. Allgemeine Hinweise zu RAS finden sich außerdem im Baustein B 4.4 *Remote Access*, so dass im Folgenden nur die für Windows 2000 spezifischen Empfehlungen aufgeführt sind. Um im konkreten Fall eine sichere RAS-Konfiguration zu erreichen, sind jedoch alle relevanten Maßnahmenbündel auf ihre Anwendbarkeit hin zu überprüfen und entsprechend umzusetzen.

Konfiguration durch RAS-Richtlinien

Der Windows 2000 RRAS-Server erlaubt als Besonderheit die Steuerung der Einwahlberechtigung für Benutzer durch so genannte RAS-Richtlinien (Policies). Hier können vielfältige Beschränkungen für die Einwahl festgelegt werden, z. B. die maximale Leerlaufzeit vor Trennen der Verbindung, die Vorgabe von Rufnummern, von denen aus die Einwahl erfolgen muss, sowie die Vorgabe des Einwahlmediums. Über die RAS-Richtlinien werden jedoch auch die erlaubten Authentisierungsverfahren festgelegt, deren Stärke und Sicherheit maßgeblich für die Sicherheit eines Netzes mit RAS-Einwahlmöglichkeit sind.

Bei der Windows 2000 RRAS Konfiguration ist dabei Folgendes zu berücksichtigen:

- Die Einwahl ist mit den zur Verfügung stehenden Mitteln zu beschränken. Windows 2000 bietet hierfür die folgenden Kriterien an:
  - **Leerlaufzeit**: Zeitdauer ohne Aktivitäten, nach der die Verbindung getrennt wird. Standardmäßig ist diese Eigenschaft nicht eingestellt, und Verbindungen im Leerlauf werden nicht durch den RAS-Server getrennt.
  - **Maximale Sitzungsdauer**: Zeitdauer, über die eine Verbindung maximal besteht. Nach Ablauf der maximalen Zeitdauer für die Sitzung wird die Verbindung getrennt. Standardmäßig ist diese Eigenschaft nicht eingestellt, und beim RAS-Server besteht keine maximale Zeitdauer für Sitzungen.
  - **Tage und Uhrzeiten**: Die Wochentage und Uhrzeiten, zu denen eine Verbindung zulässig ist. Wenn der Wochentag und die Uhrzeit der Verbindung nicht mit den konfigurierten Angaben übereinstimmen, wird die Verbindung verweigert. Standardmäßig ist diese Eigenschaft nicht eingestellt, und beim RAS-Server bestehen keine Einschränkungen hinsichtlich des Wochentags oder der Uhrzeit. Die Überprüfung auf zulässige Verbindungszeiten findet nur beim

Aufbau einer Sitzung statt. Eine aktive Verbindung, die zu einem zulässigen Zeitpunkt aufgebaut wurde, wird auch nach dem Ablauf des zulässigen Zeitfensters nicht durch den RAS-Server getrennt.

- **Einwählnummer**: Eine bestimmte Rufnummer, die ein Anrufer verwenden muss, damit die Verbindung zugelassen wird. Wenn die Einwählnummer der Verbindung nicht mit der konfigurierten Einwählnummer übereinstimmt, wird die Verbindung verweigert. Standardmäßig ist diese Eigenschaft nicht eingestellt, und beim RAS-Server sind alle Einwählnummern zulässig.
- **Einwählmedien**: Arten der Medien, die ein Benutzer verwenden muss, damit eine Verbindung zugelassen wird, wie beispielsweise Modem (asynchron), ISDN oder virtuelles privates Netz (VPN). Wenn das Einwählmedium der Verbindung nicht mit dem vorgegebenen Einwählmedium übereinstimmt, wird die Verbindung verweigert. Standardmäßig ist diese Eigenschaft nicht eingestellt, und beim RAS-Server sind alle Medienarten zulässig.

Generelle Empfehlungen zu den vorgenannten Parametern sind nicht möglich. Entsprechende Festlegungen müssen sich am Schutzbedarf des Netzes und dem beabsichtigten Einsatzzweck orientieren.

- Zur Authentisierung sollten nur starke Verfahren unter Verwendung ausreichend langer Schlüssellängen eingesetzt werden. Welche Schlüssellängen als ausreichend sicher erachtet werden, hängt vom Einsatzszenario ab und sollte in der RAS-Sicherheitsrichtlinie (siehe auch M 2.187 *Festlegen einer RAS-Sicherheitsrichtlinie*) festgelegt werden. Zu beachten ist, dass alle RAS-Clients mindestens eines der festgelegten Verfahren unterstützen müssen. Windows 2000 bietet standardmäßig folgende Authentisierungsverfahren an: EAP-TLS, MS-CHAP v2, MS-CHAP, CHAP, SPAP, PAP sowie nicht authentisierte Zugriffe.

  starke Authentisierung

  - Nicht authentisierte Verbindungen dürfen nicht angenommen werden.
  - Die Verfahren PAP, SPAP sowie MS-CHAP (in beiden Versionen) werden als unsicher eingestuft und sollten daher nicht verwendet werden.
  - Muss MS-CHAP als Authentisierungsverfahren eingesetzt werden, so sollte die Version 2 genutzt werden, da diese sicherer ist als Version 1. Da auch in der Version 2 Sicherheitsprobleme gefunden wurden, sollte auf eine neuere Version zurückgegriffen werden, sobald eine solche verfügbar ist.
  - EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) ist nur für einen RAS-Server verfügbar, der Mitglied in einer Windows 2000 Domäne ist. EAP-TLS erlaubt standardmäßig die zertifikats- und chipkartenbasierte Authentisierung, wobei Microsoft aus Sicherheitsgründen nur die Verwendung der chipkartenbasierten Variante empfiehlt.

- Die Nutzung von RADIUS erlaubt die zentrale Verwaltung von RAS-Zugangsberechtigungen.

- RAS-Verbindungen sollten grundsätzlich verschlüsselt sein, um ein hohes Maß an Sicherheit zu gewährleisten. Dazu sollten möglichst sichere

  Verschlüsselung aktivieren

Verfahren zum Einsatz kommen. Die Möglichkeit, unverschlüsselte Verbindungen aufzubauen, sollte deaktiviert werden. Folgende Möglichkeiten werden durch Windows 2000 angeboten:

- **Keine Verschlüsselung**: Diese Option ermöglicht eine unverschlüsselte Verbindung und sollte nicht eingesetzt werden.
- **Basisverschlüsselung**: Bei DFÜ-Verbindungen und PPTP-basierten VPN-Verbindungen wird die Microsoft Punkt-zu-Punkt-Verschlüsselung (MPPE) mit einem 40-Bit-Schlüssel verwendet. Bei VPN-Verbindungen, die auf L2TP und IPSec basieren, wird eine 56-Bit-DES-Verschlüsselung eingesetzt. Diese Option sollte nicht verwendet werden.
- **Starke Verschlüsselung**: Bei DFÜ-Verbindungen und PPTP-basierten VPN-Verbindungen wird MPPE mit einem 56-Bit-Schlüssel verwendet. Bei VPN-Verbindungen, die auf L2TP und IPSec basieren, wird eine 56-Bit-DES-Verschlüsselung eingesetzt. Diese Option kann für Verbindungen eingesetzt werden, die vor zufälligem Mitlesen geschützt werden sollen. Für den Schutz vertraulicher Informationen während der Netzübertragung sollte diese Option nicht verwendet werden.
- **Stärkste Verschlüsselung**: Bei DFÜ-Verbindungen und PPTP-basierten VPN-Verbindungen wird MPPE mit einem 128-Bit-Schlüssel verwendet. Bei VPN-Verbindungen, die auf L2TP und IPSec basieren, wird die 3DES-Verschlüsselung (Triple DES) eingesetzt. Diese Option ist nur nach Einspielen des "High-Encryption-Pack" und des Service Pack 1 oder 2 verfügbar. Diese Option sollte für die Netzabsicherung gewählt werden, wenn vertrauliche Informationen übertragen werden.

- Die ausschließliche Steuerung der Einwahl über RAS-Richtlinien, z. B. in Abhängigkeit der Zugehörigkeit zu einer Benutzergruppe, ist nur in Domänen möglich, die im *Native Mode* betrieben werden.
- Die Einwahlberechtigung kann nicht über eine Gruppenrichtlinie (GPO) aktiviert werden. Dies muss für jeden Benutzer einzeln erfolgen.

Die hier aufgezeigten Empfehlungen und Hinweise können nur allgemeine Anhaltspunkte zur sicheren RAS-Konfiguration liefern, da die konkrete Konfiguration sehr vom Einsatzszenario und den damit verbundenen Sicherheitsanforderungen abhängt. Insofern ist eine entsprechende Anpassung auch unter Berücksichtigung der unternehmens- bzw. behördenweiten Sicherheitsleitlinie notwendig.

Ergänzende Kontrollfragen:

- Wurde ein bedarfsgerechtes RAS-Konzept entworfen und umgesetzt?
- Wurde das RAS-Konzept auf das Firewall-Konzept abgestimmt?
- Ist der RAS-Server so konfiguriert, dass er nicht authentisierte Verbindungen verweigert?
- Werden nur starke Authentisierungsmechanismen eingesetzt?
- Werden die übertragenen Daten verschlüsselt?

M 4.146 Sicherer Betrieb von Windows 2000/XP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Nach der Installation und initialen Konfiguration gemäß den im Vorfeld geplanten Windows 2000/XP Konzepten und Sicherheitsrichtlinien erfolgt der Betrieb von Windows 2000/XP Rechnern in der Regel im Netzverbund. Die Sicherheit eines solchen Netzes hängt dabei einerseits von den eingestellten Konfigurationsparametern ab. Sie wird aber auch andererseits maßgeblich durch die Art und Weise der Konfigurationsänderungen bestimmt, die im laufenden Betrieb erfolgen müssen. Dabei sind insbesondere auch Seiteneffekte zu berücksichtigen, die unter Umständen unbeabsichtigt zu Sicherheitslücken führen können.

Windows 2000/XP bietet eine Reihe von Werkzeugen und Mechanismen an, die die Administratoren bei der Aufrechterhaltung der Sicherheit eines laufenden Systems unterstützen können.

- *Windows File Protection* ist ein Systemmechanismus von Windows 2000/XP, der sicherstellt, dass Systemdateien unverändert im Originalzustand vorhanden sind. Der Mechanismus nutzt zwei Komponenten: den so genannten *SystemFileChecker* (*sfc.exe*), der die Systemdateien auf ihre Unverändertheit hin überprüft (z. B. beim Systemstart) und veränderte Dateien durch zwischengespeicherte Originaldateien ersetzt. Weiterhin existiert ein Überwachungsmechanismus, der beim schreibenden Zugriff auf Systemdateien diese wieder durch die Originalversion ersetzt. Der Mechanismus kann so konfiguriert werden, dass das Überschreiben nach einer entsprechenden Bestätigung erfolgreich ist und die veränderte Datei beibehalten wird. Die Konfiguration erfolgt über die Kommandozeile durch die Kommandos:
  - *sfc /enable*: Veränderungen werden nach einer Bestätigung übernommen.
  - *sfc /quiet*: Veränderte Dateien werden ohne Nachfrage durch die Originale ersetzt.
- Mit Windows XP wurde eine neue Technologie eingeführt: die automatische Systemwiederherstellung. Dieser Mechanismus kann zum Wiederherstellen eines früheren Systemzustands verwendet werden, wenn beispielsweise eine Softwareinstallation fehlschlug und sich das System in einem instabilen Zustand befindet. In Abhängigkeit von lokalen Umständen und insbesondere von der implementierten Softwareverteilungs-Strategie kann der Einsatz der automatischen Systemwiederherstellung z. B. im Testumfeld vorteilhaft sein.

- Windows 2000/XP bietet mit dem kommandozeilenbasierten Sicherheitseditor *secedit.exe* bzw. dem MMC-Snap-in *Sicherheitskonfiguration und -analyse* Werkzeuge zur Konfiguration der Sicherheitseinstellungen von Windows 2000/XP Rechnern. Die Sicherheitskonfiguration kann auch in einer Datenbank gespeichert werden, gegen die dann ein Rechner auf Konformität getestet werden kann. Dazu wird zunächst eine Datenbank neu erzeugt (*Vorgang/Datenbank öffnen*, neuen oder existierenden Datenbanknamen eingeben). Diese kann dann mit einer Sicherheitsvorlage (.inf-Datei, siehe MMC-Snap-in *Sicherheitsvorlagen*) initialisiert werden. Mittels *Vorgang/Computer jetzt analysieren* bzw. *Vorgang/System jetzt konfigurieren* kann eine Analyse oder Konfiguration des Systems anhand der Einstellungen der Datenbank erfolgen. Die Datenbank selbst liegt in Dateiform vor (.sdb-Datei) und kann auch auf andere Systeme übertragen werden. Allerdings sind die Aussagen bei Abweichungen von Zugriffsrechten auf Datei- oder Registry-Ebene wenig hilfreich, da lediglich eine Abweichung dokumentiert wird, nicht jedoch, welche Zugriffsrechte abweichen.
- Die Sicherheitseinstellungen eines Windows 2000/XP Rechners erfolgen beim Betrieb in einer Domäne in der Regel durch die Anwendung von Gruppenrichtlinienobjekten bzw. den in einem Objekt enthaltenen Einstellungen. Auf diese Weise lassen sich nicht nur die Sicherheitseinstellungen effizient und zentral auch für große Windows 2000/XP Netze verwalten. Im täglichen Betrieb sind in der Regel auch Änderungen von GPO-Einstellungen zu erwarten. Die Änderungen finden zentral an einem Domänen-Controller statt und werden dann an die betroffenen Rechner verteilt. Dazu kann der GPO-Mechanismus so konfiguriert werden, dass periodisch ein Update der GPO-Einstellungen erfolgt, so dass die veränderten Einstellungen wirksam werden können (siehe auch M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000* und M 2.326 *Planung der Windows XP Gruppenrichtlinien*).
- Die Sicherheit des Systemzugangs kann durch die Verwendung von Smartcard-basiertem Logon erhöht werden. Die Authentisierung erfolgt dann nicht über einen Benutzernamen und ein möglicherweise schwaches Passwort, sondern über ein Zertifikat, welches auf einer Chipkarte gespeichert ist. Windows 2000/XP kann so konfiguriert werden, dass Anmeldungen alternativ über Benutzername und Passwort bzw. mit Chipkarte oder ausschließlich mit Chipkarte möglich sind. Generell können hier nur Microsoft-konforme Zertifikate genutzt werden sowie Chipkarten, die von Windows 2000/XP unterstützt werden.

Die Sicherheit eines Rechnersystems basiert immer auch auf der physikalischen Sicherheit der Rechner und Netzkomponenten. Diese muss auch für den Betrieb eines Windows 2000/XP Systems sichergestellt sein. Für den sicheren Betrieb eines Windows 2000/XP Systems ist generell Folgendes zu beachten:

- Die Sicherheit von Windows 2000/XP hängt wesentlich von der Sicherheit des Active Directories ab. Die hier enthaltenen Informationen müssen einerseits vor unberechtigter Veränderung geschützt und andererseits konsistent gehalten werden. Dies erfordert insbesondere bei Veränderungen entsprechende Sorgfalt. Es empfiehlt sich dringend, im Rahmen der Sicherheitsplanung nicht nur Werte oder Wertbereiche für Parameter festzulegen, sondern auch (innerbetriebliche oder administrative) Abläufe zu definieren, die geeignet sind, die festgelegte Sicherheitsrichtlinie umzusetzen. So sollte z. B. festgelegt werden, welche Schritte beim Anlegen eines neuen Benutzer-Kontos durchzuführen sind, damit die notwendigen Veränderungen vollständig ausgeführt werden.

  Auch die Installation eines neuen zusätzlichen Domänen-Controllers ist eine sicherheitskritische AD-Veränderung, da dieser eine Kopie des AD erhält. Die physikalische Sicherheit sowie die konsistente und sichere Konfiguration des zukünftigen Domänen-Controllers muss daher vor der Eingliederung sichergestellt sein.

  Windows 2000 erlaubt es, Domänen-Controller im so genannten *Active Directory Restore Modus* zu betreiben. In diesem Modus ist der Active Directory Service nicht gestartet und es können Reparaturarbeiten an der AD-Datenbank erfolgen, indem bestimmte AD-Zweige von einem Backup-Medium zurückgespielt werden. Die Veränderungen können so eingespielt

  werden, dass sie in der gesamten Domäne verteilt werden. Daher muss dieser Vorgang unter größter Sorgfalt erfolgen. Es empfiehlt sich, den AD-Restore-Modus nur im Vier-Augen-Prinzip zu nutzen, da Eingabefehler die Integrität des AD zerstören können.

Sicherheit der Systemdienste

- Neben der Sicherheit des Active Directories und die durch die im AD festgelegten Parameter bedingte Systemsicherheit muss auch die Sicherheit wichtiger Systemdienste gewährleistet werden. Hierbei spielt die Sicherheit von DNS, WINS, DHCP, RAS sowie Kerberos eine besondere Rolle. Auch hier muss bei Änderungen sichergestellt werden, dass die für Windows 2000 geltenden und festgelegten Sicherheitsrichtlinien nicht verletzt werden. Hinweise zur Konfiguration dieser Dienste finden sich in der Maßnahme M 4.140 *Sichere Konfiguration wichtiger Windows 2000 Dienste* und den darin referenzierten Maßnahmen.

Zugriff auf Verwaltungstools beschränken

- Für die Verwaltung eines Windows 2000/XP Systems stehen standardmäßig die so genannten Snap-ins der Microsoft Management Console (MMC-Snap-ins) zur Verfügung. MMC-Snap-ins stellen Verwaltungsmodule dar, die über eine standardisierte Schnittstelle in die MMC integriert werden können. Der Zugriff auf die verschiedenen MMC-Snap-ins muss daher reglementiert werden. Normalen Benutzern sollte der Zugriff auf Systemverwaltungswerkzeuge generell untersagt werden. Als Ausnahme ist hier jedoch das MMC-Snap-in zur Verwaltung von Zertifikaten zu nennen, welches auch von normalen Benutzern zum Verwalten der eigenen Zertifikate genutzt werden muss. Der Zugriff auf die einzelnen MMC-Snap-ins lässt sich dabei feingranular über GPO-Einstellungen regeln.

- Die Verwaltungstools zum Zugriff auf die lokale Registry eines Rechners (*regedt32* und *regedit*) sollten nicht für normale Benutzer zugreifbar sein. Auch dies lässt sich durch GPO-Einstellungen erreichen.

- **neue Applikationen testen**

  Die Sicherheit eines Windows 2000/XP Netzes hängt von vielen Faktoren ab. Insbesondere können Sicherheitslücken auch durch Zusatzapplikationen entstehen, die entweder fehlkonfiguriert sind oder Fehler in der Programmierung enthalten. Oft ergeben sich Probleme auch erst durch den gemeinsamen Betrieb mehrerer Anwendungen. Aus diesem Grund sind vor Einführung einer neuen Applikation Tests durchzuführen, die einen ersten Hinweis darauf geben, ob offensichtliche Probleme bestehen. Eine vollständige Sicherheit kann hier jedoch nicht erreicht werden, da insbesondere der Test auf Fehler durch Seiteneffekte in anderen Applikationen schwierig durchzuführen und extrem aufwendig ist.

- **Überwachung des Systems**

  Auch wenn Änderungen sorgfältig und unter Einhaltung aller Vorsichtsmaßnahmen erfolgen, kann die Existenz von Sicherheitslücken in einem komplexen System nie ganz ausgeschlossen werden. Aus diesem Grund sollte immer eine geeignete Systemüberwachung stattfinden (siehe auch M 4.148 *Überwachung eines Windows 2000/XP Systems*). Dabei muss die Stärke und Genauigkeit der Überwachung der Gefährdungslage angepasst sein. Die Art und Weise der Überwachung kann dabei immer nur im konkreten Fall festgelegt werden. Generell sollten auch die Tätigkeiten von Administratoren durch die Überwachung erfasst werden. Zusätzlich empfiehlt sich eine regelmäßige Überprüfung, damit eventuelle Lücken,

  die durch Veränderungen des Systems entstehen können, möglichst aufgedeckt werden.

- **Domänenstruktur stabil halten**

  Unter Sicherheitsgesichtspunkten sind auch Änderungen in der Domänenstruktur kritisch. Daher sind diese nur nach sorgfältiger Planung durchzuführen. Es ist schon bei der initialen Planung zu berücksichtigen, dass eine Windows 2000 Domänenstruktur (Aufteilung in Domänen, Trees, Forests) nachträglich nur wenige Veränderungen erlaubt.

- **Regelungen dokumentieren**

  Auch unter Sicherheitsgesichtspunkten ist es wichtig, dass alle den Betrieb eines Windows 2000/XP Systems betreffenden Richtlinien, Regelungen und Prozesse dokumentiert werden. Dazu sollten Betriebshandbücher erstellt werden, die auch bei Systemänderungen aktualisiert werden müssen. Da die Betriebshandbücher sicherheitsrelevante Informationen enthalten, sind sie so aufzubewahren, dass einerseits Unbefugte keinen Zugriff auf sie erlangen können, jedoch andererseits für befugte Administratoren ein einfacher Zugriff besteht.

Die aufgeführten Empfehlungen können an dieser Stelle nur allgemeinen Charakter besitzen, da die Aufrechterhaltung der Systemsicherheit auch von lokalen Gegebenheiten abhängt. Daher müssen schon in der Planungsphase eines Windows 2000/XP Netzes entsprechende Richtlinien zum sicheren Betrieb erstellt werden, die die lokalen Anforderungen berücksichtigen. Unter Umständen kann es auch vorkommen, dass gewisse Sicherheitsmechanismen nicht optimal sicher konfiguriert werden können. Dies ist z. B. der Fall, wenn "alte" Applikationen weiter betrieben werden müssen, die nur auf schwache oder keine Authentisierung ausgelegt sind. Hier muss dann durch entsprechend ausgleichende Gegenmaßnahmen an anderer Stelle - oder auf organisatorischer Ebene - eine zufrieden stellende Sicherheit garantiert werden.

Administratoren schulen

Die Sicherheit eines Windows 2000/XP Systems im laufenden Betrieb hängt dabei auch wesentlich vom Kenntnisstand der Administratoren ab. Daher ist die Schulung und Fortbildung der Systemverwalter eine wichtige Schutzmaßnahme (siehe auch M 3.27 *Schulung zur Active Directory-Verwaltung*), da potentielle Sicherheitslücken nur von kompetenten Administratoren entdeckt bzw. vermieden werden können. Daneben müssen auch die normalen Benutzer in Sicherheitsaspekten geschult werden (siehe auch M 3.28 *Schulung zu Windows 2000/XP Sicherheitsmechanismen für Benutzer*), damit potentielle Gefahren bekannt sind und die zur Verfügung stehenden Sicherheitsmechanismen richtig eingesetzt werden können.

Ergänzende Kontrollfragen:

- Sind alle Betriebsabläufe dokumentiert?
- Findet eine regelmäßige Kontrolle der Systemprotokolldaten statt?
- Ist sichergestellt, dass Änderungen am AD nur von berechtigten Benutzern vorgenommen werden können?
- Ist der Zugriff auf alle Administrationswerkzeuge für Benutzer unterbunden worden?
- Werden die Administratoren regelmäßig geschult?

M 4.147 Sichere Nutzung von EFS unter Windows 2000/XP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Unter Windows 2000/XP steht das Dateisystem EFS (Encrypting File System - verschlüsselndes Dateisystem) zur Verfügung, das die Verschlüsselung einzelner Dateien unterstützt, die dafür gekennzeichnet werden müssen. Die Dateiverschlüsselung mittels EFS basiert auf einem hybriden Mechanismus, der asymmetrische und symmetrische Verschlüsselungsverfahren gemischt einsetzt:

- Zur reinen Datenverschlüsselung wird ein schnelles symmetrisches Verfahren benutzt. Der dabei benutzte Schlüssel (der sogenannte File Encryption Key, FEK) wird zufällig erzeugt.
- Windows 2000 und Windows XP vor Service Pack 1 setzen standardmäßig das DESX-Verfahren ein, eine abgewandelte Form des DES-Algorithmus. Windows XP kann aber auch auf das Triple-DES-Verfahren nach FIPS 140-1 umgestellt werden. Der Einsatz des Triple-DES Verschlüsselungsalgorithmus ermöglicht vor allem Verschlüsselung mit größeren Schlüssellängen. Die Aktivierung des Algorithmus erfolgt in Gruppenrichtlinien unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Systemkryptographie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden*. Ab Windows XP Service Pack 1 kommt der AES-Algorithmus mit 256-Bit langen Schlüsseln zum Einsatz. Durch den Registry-Eintrag *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS\AlgorithmID* kann der verwendete Verschlüsselungsalgorithmus festgelegt werden: 0x6603 für Triple-DES, 0x6604 für DESX und 0x6610 für AES.
- Die Aktivierung des Triple-DES Verschlüsselungsalgorithmus betrifft standardmäßig nicht nur das EFS, sondern auch IPSec. Durch einen neuen Eintrag in die Registrierungsdatenbank (DWORD Name: *AlgorithmID*, Wert *0x6603*, unter *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS*) wird die Benutzung von Triple-DES auf EFS beschränkt.

- Beim Einsatz in einer gemischten Umgebung (Windows 2000 und Windows XP) ist zu beachten, dass Windows 2000 Systeme ohne High Encprytion Pack (bzw. vor Service Pack 2) nicht auf mit dem Triple-DES Algorithmus verschlüsselte Dateien zugreifen können. Dokumente, die mit AES verschlüsselt wurden, können nicht von Windows 2000 Systemen und Windows XP Systemen ohne Service Pack 1 gelesen werden. Diese Probleme treten im Normalbetrieb jedoch nur selten auf: wenn die verschlüsselten Daten nicht auf dem Originalrechner entschlüsselt werden (z. B. beim Verwenden von Wechsellaufwerken mit NTFS oder WebDAV mit EFS möglich).- Zur Verschlüsselung des FEK wird das asymmetrische RSA-Verfahren eingesetzt. Die Verschlüsselung des FEK erfolgt mit dem öffentlichen Schlüssel des Benutzers, der die Datei verschlüsselt. Damit kann der FEK nur noch mit dem privaten Schlüssel dieses Benutzers entschlüsselt und zum Entschlüsseln der Dateiinhalte verwendet werden.

Hibernation Modus nicht benutzen

Alle zur Ver- oder Entschlüsselung benötigten Schlüssel werden von Windows 2000/XP bei der Benutzung in einem Hauptspeicherbereich abgelegt, der nicht in die Auslagerungsdatei verlagert wird. Dadurch soll gewährleistet werden, dass die Schlüssel nicht kompromittiert werden können, wenn ein unberechtigter Dritter Zugriff auf die Auslagerungsdatei erhält. Kritisch ist jedoch in diesem Zusammenhang die Verwendung des Ruhezustandes (*Hibernation Modus*), da hier der gesamte Hauptspeicherbereich in eine Datei gespeichert wird, die dann notwendigerweise auch das Schlüsselmaterial enthält. Daher sollte der Ruhezustand bei Verwendung von EFS nicht benutzt werden. Dies ist besonders bei Laptops wichtig.

Benutzer schulen

Die Verschlüsselung mittels EFS kann jeder Benutzer pro Datei oder Verzeichnis einstellen. Über den korrekten Umgang mit EFS sollten die Benutzer geschult werden, ebenso sind sie über die potentiellen Schwächen dieser Art der Verschlüsselung zu informieren.

Durch die Nutzung von EFS wird ein Sicherheitsgewinn erzielt. Die Benutzer sollten sich allerdings darüber bewusst sein, dass trotz des Verschlüsselns von Klartextdateien ein Restrisiko besteht, dass die Daten der gelöschten Klartext-datei teilweise oder ganz wiederhergestellt werden können. Dazu ist jedoch spezielle Software und der Zugriff auf die Festplatte des jeweiligen Rechners notwendig.

Damit die mittels EFS verschlüsselten Dateien beim Verlust des privaten Schlüssels nicht vollständig verloren sind, kann eine zusätzliche Verschlüsselung des FEK mit dem öffentlichen Schlüssel des so genannten Wiederherstellungsagenten (englisch *Recovery Agent*) erfolgen. Dadurch ist eine Entschlüsselung der Daten auch unter dem Benutzerkonto des Wiederher-stellungsagenten möglich. Prinzipiell kann ein beliebiges Benutzerkonto als Wiederherstellungsagent eingesetzt werden. Unter Windows 2000 ist die Angabe eines Wiederherstellungsagenten obligatorisch, unter Windows XP dagegen nicht. Als Standardvorgabe wird von Windows 2000 das Administratorkonto genutzt.

Beim Einsatz von EFS ist Folgendes aus Sicherheitssicht zu beachten:

- EFS ist völlig transparent für den Benutzer. Unter Windows 2000 bemerkt ein Benutzer damit jedoch auch keinen Unterschied zwischen verschlüsselten und unverschlüsselten Dateien. Daher ist besondere Aufmerksamkeit gefordert, dass sensitive Dateien auch tatsächlich verschlüsselt werden. Unter Windows XP werden die verschlüsselten Dateien im Windows Explorer standardmäßig in einer anderen Farbe angezeigt. Dies kann im Windows Explorer durch die die Option *Verschlüsselte oder komprimierte NTFS-Dateien in anderer Farbe anzeigen* unter *Extras* | *Ordneroptionen* | *Ansicht* gesteuert werden.

starke Benutzerpasswörter verwenden

- Aufgrund der Transparenz für Benutzer ist der Schutz der EFS-Dateiverschlüsselung so stark wie das Passwort des jeweiligen Benutzerkontos. Kann sich ein unbefugter Dritter erfolgreich unter einem Benutzerkonto anmelden, so kann er auch auf alle verschlüsselten Dateien dieses Benutzerkontos zugreifen. Wird EFS eingesetzt, empfiehlt es sich, generell starke Passwörter für jedes Benutzerkonto zu benutzen. Da auch Windows 2000/XP es erlaubt, eigene Passwortfilter zu nutzen, kann auf diesen Mechanismus zurückgegriffen werden, um die Verwendung starker Passwörter technisch zu erzwingen.
- EFS ist eine Dateiverschlüsselung und keine Ordnerverschlüsselung. Allerdings kann ein Ordner zur Verschlüsselung markiert werden, und es werden dann alle im Ordner befindlichen Dateien oder auch Dateien, die neu in einem solchen Ordner erzeugt werden, verschlüsselt. Es ist jedoch prinzipiell möglich, auch unverschlüsselte Dateien in einem solchen Ordner zu halten bzw. zu erzeugen. Verschlüsselte Dateien können außerdem an jeder Stelle im Dateibaum existieren und sind damit nicht an Ordner gebunden, die zur Verschlüsselung gekennzeichnet sind.
- Das Verschlüsselungsmerkmal ist ein Dateiattribut, das wie alle anderen Dateiattribute behandelt wird, d. h. beim Verschieben von Dateien bleiben die Dateiattribute unverändert. Dies führt dazu, dass Dateien, die in einen Ordner verschoben werden, der für die Verschlüsselung gekennzeichnet ist, nicht automatisch verschlüsselt werden. Dieses Verhalten lässt sich für den Windows Explorer über eine Gruppenrichtlinie steuern und damit abschalten, so dass auch verschobene Dateien verschlüsselt werden. Dies ist die Voreinstellung. Allerdings gilt dies gilt nicht für das Arbeiten unter der Kommandozeile von Windows. Benutzer müssen auf die Gefahr hingewiesen werden, dass Dateien in Ordnern, die für die Verschlüsselung gekennzeichnet sind, auch unverschlüsselt sein können.

spezielle Ordner für verschlüsselte Dateien verwenden

- Obwohl EFS keine Ordnerverschlüsselung ist, empfiehlt es sich, verschlüsselte Dateien in speziellen Ordnern vorzuhalten bzw. Ordner für die Verschlüsselung zu kennzeichnen. Dies erleichtert das Arbeiten mit verschlüsselten Dateien.
- Die Verschlüsselung einer Datei bietet keine Zugriffskontrolle. Insbesondere können verschlüsselte Dateien durch Dritte auch gelöscht werden, falls die Zugriffsrechte dies erlauben. Neben der Verschlüsselung einer Datei müssen daher auch entsprechende Einstellungen für die Zugriffskontrolle vorgenommen werden.

- Der zentral gesteuerte Einsatz von EFS wird durch die Verwendung von Gruppenrichtlinien ermöglicht, die unter anderem zur Definition der Wiederherstellungsagenten eingesetzt werden.
- Damit EFS unter Windows 2000 eingesetzt werden kann, muss immer ein Wiederherstellungsagent definiert sein. Es empfiehlt sich, dafür ein spezielles Konto anzulegen, das ausschließlich für diesen Zweck genutzt wird. Insbesondere sollte dafür kein Administratorkonto verwendet werden, um den Schutz vor dem Administrator zu erhöhen. In Abhängigkeit vom ermittelten Schutzbedarf sollte darüber nachgedacht werden, für die Benutzung des entsprechenden Kontos ein Vier-Augen-Prinzip einzuführen, z. B. durch Passwortteilung.
- Ein unter Windows 2000 mit Mitteln einer leeren Wiederherstellungsrichtlinie durchgesetztes Verschlüsselungsverbot funktioniert unter Windows XP nicht mehr. Das Verschlüsselungsverbot wird unter Windows XP durch das Deaktivieren der Option *Benutzer dürfen das verschlüsselnde Dateisystem benutzen* in Eigenschaften der Richtlinie *Computerkonfiguration* | *Windows Einstellungen* | *Sicherheitseinstellungen* | *Richtlinien öffentlicher Schlüssel* | *Dateisystem wird verschlüsselt* | *Eigenschaften* | *Benutzer dürfen das verschlüsselnde Dateisystem benutzen* erreicht.
- Die Nutzung eines separaten Wiederherstellungsagenten bietet keinen vollständigen Schutz vor dem Administrator, da dieser immer das Passwort eines Benutzer zurücksetzen kann, um sich nachfolgend als Benutzer anzumelden und auf dessen verschlüsselte Dateien zuzugreifen. Unter Windows XP gilt dies jedoch nur für Domänenkonten. Wird unter Windows XP das Kennwort für ein lokales Benutzerkonto zurückgesetzt, so wird der Zugriff auf seine verschlüsselten Dateien für alle gesperrt. Um den Verlust der verschlüsselten Daten eines lokalen Benutzers zu vermeiden, bietet Windows XP mit der sogenannten Kennwortrücksetzungs-Diskette (Password Reset Disk, PRD) einen neuen Mechanismus an. Die Erstellung einer solchen Kennwortrücksetzungs-Diskette für ein Domänen-Benutzerkonto ist laut Microsoft nicht möglich.
- Der private Schlüssel des Wiederherstellungsagenten sollte vom System gelöscht werden, nachdem er auf ein Speichermedium exportiert worden ist. Das Speichermedium muss an einem sicheren Ort aufbewahrt werden. Der Zugriff auf das Speichermedium sollte nach dem Vier-Augen-Prinzip erfolgen. Es empfiehlt sich, eine gesondert und sicher aufbewahrte Sicherungskopie des Schlüssels anzulegen.

Vier-Augen-Prinzip für Recovery Agent

- Das Sichern aller privaten Schlüssel beim Einsatz von EFS ist wichtig. Hierzu müssen alle Profil-Daten auf allen Rechnern, das heißt alle Verzeichnisse unterhalb von *Dokumente und Einstellungen/<Benutzername>*, die auch alle Benutzerschlüssel und Zertifikate enthalten, durch den Backup-Mechanismus erfasst werden.

alle privaten Schlüssel sichern

- Wird EFS ohne serverseitig gespeichertes Benutzerprofil (*roaming profile*) eingesetzt, so werden in Abhängigkeit von unterschiedlichen lokalen Profilen unterschiedliche Schlüssel zum Ver- und Entschlüsseln des FEK benutzt, da diese im Profil eines Benutzer (verschlüsselt) gespeichert werden. In diesem Fall ist es wichtig, alle Schlüssel zu sichern. Insbesondere können verschlüsselte Daten von einem Rechner, die auf Band gesichert wurden, nicht auf einem anderen Rechner wieder eingespielt werden, da eine erfolgreiche Entschlüsselung aufgrund unterschiedlicher Schlüssel dann nicht möglich ist.
- Der Einsatz einer PKI zum Ausstellen von EFS Zertifikaten in einem Unternehmen bzw. einer Behörde sollte überlegt werden. Insbesondere bei der Verwendung von serverseitig gespeicherten Benutzerprofilen verspricht dies eine einfachere Schlüsselverwaltung und -Sicherung.
- Das Verschlüsseln von Systemdateien (Dateien mit gesetztem Systemattribut) und komprimierten Dateien ist nicht möglich.
- Die Windows Boot-Datei *autoexec.bat* muss vor Verschlüsselung geschützt werden, indem für Benutzer der Schreibzugriff unterbunden wird, da sonst eine Denial-of-Service-Attacke möglich ist.

autoexec.bat nicht verschlüsseln

- Werden verschlüsselte Daten mit Programmen, wie z. B. einem Texteditor, bearbeitet oder gedruckt, so werden dabei in der Regel temporäre Dateien erzeugt, die dann Daten im Klartext enthalten. Diese können dann je nach Programm auch nach der Bearbeitung weiter bestehen. Damit ist je nach Speicherort, z. B. Temp-Verzeichnisse oder Spool-Bereich, und Zugriffsberechtigung auch ein Zugriff durch unautorisierte Dritte möglich.
- Um eine größere Sicherheit bei der Verarbeitung von EFS-verschlüsselten Dateien zu erreichen, sollte überlegt werden, ob es zweckmäßig ist, auch Verzeichnisse, die typischerweise temporäre Daten enthalten (Temp, Spool), für die Verschlüsselung zu kennzeichnen. Es ist dabei zu berücksichtigen, welche Datenmengen in diesen Verzeichnissen abgelegt werden und welche Programme diese Verzeichnisse nutzen. Bei sehr häufigen Zugriffen auf große Datenmengen kann dies zu einem Performanceverlust führen. Es ist jedoch zu bedenken, dass die Verschlüsselung des Temp-Verzeichnisses unter Umständen Probleme bei Updates verursachen kann.
- EFS bietet derzeit über die graphische Oberfläche von Windows 2000 keine Möglichkeit an, Dateien so zu verschlüsseln, dass verschiedene Benutzer darauf zugreifen können. Generell ist es jedoch mit EFS möglich, eine Datei für eine ganze Liste von Benutzern zu verschlüsseln. Dazu muss allerdings auf die EFS Programmierschnittstelle (EFS-API) zurückgegriffen und ein entsprechendes Programm geschrieben werden.

- Mit der Einführung von Windows XP steht die Mehrbenutzer-Verschlüsselung auch in der graphischen Oberfläche zur Verfügung. Es ist zu beachten, dass es nicht möglich ist, in den Verschlüsselungsoptionen eines Ordners mehrere Benutzer anzugeben. Ebensowenig kann eine einzelne Datei für eine Windows-Benutzergruppe verschlüsselt werden. Unter Windows XP können lediglich einzelne Dateien für mehrere Benutzer bzw. alle Dateien in einem Ordner für einen einzelnen Benutzer verschlüsselt werden.
- Unter Windows XP wurde die Möglichkeit zur Verschlüsselung von Offlinedateien eingeführt. Der gesamte Speicher für Offlinedateien, der Dateien aller Benutzer beinhaltet, wird mit einem computerspezifischen Schlüssel verschlüsselt. Die Verschlüsselung ist transparent für Benutzer und kann nur von Administratoren aktiviert/deaktiviert werden. Die Aktivierung erfolgt in Einstellungen des Windows Explorers oder durch die Definition der entsprechenden Gruppenrichtlinie (*Computerkonfiguration* | *Administrative Vorlagen* | *Netzwerk* | *Offlinedateien* | *Offlinedateicache verschlüsseln*).
- Mit EFS verschlüsselte Daten werden auf dem Rechner ver- und entschlüsselt, der die Daten gespeichert hat. Dies bedeutet insbesondere, dass Daten, die auf einem Server verschlüsselt gespeichert werden, beim Zugriff durch einen Client im Klartext über das Netz übertragen werden (SMB-Protokoll). Müssen die Daten in Abhängigkeit vom ermittelten Schutzbedarf auch während der Übertragung geschützt werden, so sind zusätzliche Maßnahmen zur Absicherung der Netzkommunikation erforderlich. Hierfür kann z. B. EFS mit WebDAV (Web Digital Authoring and Versioning), SSL oder IPSec verwendet werden, siehe dazu auch M 5.90 *Einsatz von IPSec unter Windows 2000/XP*.
- Windows XP führte mit WebDAV einen neuen Mechanismus zum Arbeiten mit Dateien über das Web-Sharing ein. Wird EFS mit WebDAV verwendet, so wird eine lokal verschlüsselte Datei in verschlüsselter Form zum Server übertragen und dort gespeichert. Eine über WebDAV angeforderte Datei wird ebenfalls in verschlüsselter Form vom Server übertragen und lokal entschlüsselt. Somit ist durch die Verwendung von WebDAV eine verschlüsselte Übertragung über das Netz möglich.
- Wird EFS für lokale Benutzerkonten eingesetzt, so muss die Registry-Verschlüsselung mittels des Kommandos *syskey* unter Verwendung eines Passwortes erfolgen. Nur so können die lokalen Kontenpasswörter vor dem Zurücksetzen durch "Hacker-Werkzeuge" geschützt werden.

EFS ist nur bei richtiger Anwendung eine kostengünstige Alternative zur Dateiverschlüsselung mit anderen Werkzeugen. EFS kann beispielsweise auf Laptops eingesetzt werden, um die fehlende physikalische Sicherheit auszugleichen, so dass Daten vor dem unbefugten Zugriff an den Betriebssystemmechanismen vorbei geschützt werden können. Der Einsatz von EFS ist jedoch nicht in jedem Fall zweckmäßig, so dass für den jeweiligen Einsatzzweck entschieden werden muss, ob EFS benutzt werden soll.

Ergänzende Kontrollfragen:

- Wird die Nutzung von EFS im Datensicherungskonzept berücksichtigt?
- Sind die Benutzer im korrekten Umgang mit EFS geschult?
- Sind mit EFS verschlüsselte Dateien zusätzlich durch restriktive Zugriffsrechte geschützt?
- Wurde ein dediziertes Konto für den Wiederherstellungsagenten erzeugt und dessen privater Schlüssel gesichert und aus dem System entfernt?
- Wird die *syskey*-Verschlüsselung mit Passwort verwendet, wenn EFS mit lokalen Konten eingesetzt wird?

M 4.148 Überwachung eines Windows 2000/XP Systems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Revisor

Die Überwachung von Rechnersystemen ist ein wichtiges Mittel zur Aufrechterhaltung der Systemsicherheit und Systemintegrität. Nur so können mögliche Sicherheitslücken, Verstöße gegen die geltenden Sicherheitsrichtlinien oder gar Angriffe durch Außen- und Innentäter entdeckt und geeignete Gegenmaßnahmen eingeleitet werden.

Die Überwachung eines Windows 2000/XP Systems muss schon in der Planungsphase berücksichtigt werden, damit die relevanten Parameter entsprechend den Anforderungen festgelegt werden können. Damit unter Windows 2000/XP eine Überwachung erfolgen kann, muss diese zunächst generell aktiviert werden. Dies gilt insbesondere für die Datei- und Registry-Überwachung. Die Aktivierung und die Konfiguration der Überwachungskomponenten erfolgt dabei über folgende Gruppenrichtlinienparameter:

- Allgemeine Aktivierung der Überwachungsfunktionen:

  Es können jeweils die Werte *Keine Überwachung* oder *Erfolgreich* und/oder *Fehlgeschlagen* eingestellt werden.

Computer Richtlinien / Lokale Richtlinien / Überwachungsrichtlinien	
Parameter	**Empfehlung**
Prozessverfolgung überwachen	Die Prozessverfolgung ist im allgemeinen nicht sinnvoll und sollte nur für Debugging-Zwecke aktiviert werden.
Rechteverwendung überwachen	Die Verwendung von Benutzerrechten sollte überwacht werden.
Richtlinienänderungen überwachen	Das Verändern von Richtlinieneinstellungen (GPOs) ist eine sicherheitskritische Operation und sollte überwacht werden.
Systemereignisse überwachen	Aktiviert die Protokollierung der Boot-Ereignisse.
Anmeldeereignisse überwachen	Die Protokollierung der Anmeldeereignisse auf dem lokalen Rechner (z. B. Arbeitsplatzrechner) sollte aktiviert sein.
Anmeldeversuche überwachen	Die Protokollierung der Anmeldeversuche auf dem Domänen-Controller, der die Authentisierung des Benutzers durchführt, sollte aktiviert sein.
Kontenverwaltung überwachen	Änderungen in den Konteneinstellungen sind sicherheitskritische Ereignisse und sollten überwacht werden.

Objektzugriff überwachen	Diese Option sollte aktiviert werden, da hierdurch die Protokollierung von Datei- und Registry-Zugriffen möglich wird.
Active Directory Zugriff überwachen	Dies ist nur auf Domänen-Controllern relevant. Änderungen am AD sollten überwacht werden.

Tabelle: Computer-, Lokale-, Überwachungsrichtlinien

- Einstellungen für die Protokolldateien:

1. Computer Richtlinien / Lokale Richtlinien / Zuweisen von Benutzerrechten	
Parameter	**Empfehlung**
Verwalten von Überwachungs- und Sicherheitsprotokollen	Dieses Recht ermöglicht - die Konfiguration der Audit-Einstellungen für die einzelnen Objekte (Dateien, Registry, Active Directory), - das Ansehen bzw. Löschen des Sicherheitsprotokolls. Welcher Benutzergruppe (bzw. -gruppen) dieses Recht eingeräumt wird, hängt vom Überwachungskonzept ab. Prinzipiell sollte dieses Recht restriktiv vergeben werden. Es sollte dabei jedoch beachtet werden, dass - auch zur Diagnose und Behebung von nicht sicherheitsrelevanten Problemen der Zugriff auf das Sicherheitsprotokoll notwendig sein kann, - Administratoren sich dieses Benutzerrecht auch selbst einräumen können, wenn es ihnen entzogen wird. Es empfiehlt sich daher, diesen Vorgang zu protokollieren (Option *Rechteverwendung überwachen*).
2. Computer Richtlinien / Lokale Richtlinien / Ereignisprotokoll	
- Aufbewahrungsmethode des Anwendungsprotokolls - Aufbewahrungsmethode des Sicherheitsprotokolls - Aufbewahrungsmethode des Systemprotokolls	Je nach Protokollierungskonzept kann gewählt werden zwischen *Nach ... Tagen*, *Überschreiben* und *Nicht überschreiben*.

- Anwendungsprotokoll aufbewahren für - Sicherheitsprotokoll aufbewahren für - Systemprotokoll aufbewahren für	Anzahl der Tage, wenn die Aufbewahrungsmethode *Nach ... Tagen* gewählt wurde.
Windows 2000: - Gastkontozugriff auf Anwendungsprotokoll einschränken - Gastkontozugriff auf Sicherheitsprotokoll einschränken - Gastkontozugriff auf Systemprotokoll einschränken Windows XP: - Lokalen Gastkontozugriff auf Anwendungsprotokoll verhindern - Lokalen Gastkontozugriff auf Sicherheitsprotokoll verhindern - Lokalen Gastkontozugriff auf Systemprotokoll verhindern	Die Zugriffsbeschränkung für das Gastkonto sollte aktiviert werden.
- Maximale Größe des Anwendungsprotokolls - Maximale Größe des Sicherheitsprotokolls - Maximale Größe des Systemprotokolls	Die Größe muss so gewählt werden, dass je nach Aufbewahrungsmethode auch bei überdurchschnittlicher Systemaktivität genügend Platz zur Verfügung steht. Dies ist besonders wichtig für das Sicherheitsprotokoll, da sonst eine zeitliche Lücke in der Sicherheitsüberwachung des Systems entstehen kann. Vorschläge für die hier vorzunehmenden Einstellungen finden sich in M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000* bzw. M 4.xp5 *Sichere Windows XP Systemkonfiguration*. Diese müssen jedoch den realen Bedingungen (Tests im Probebetrieb) angepasst werden.

Windows 2000: System bei Erreichen der max. Sicherheitsprotokollgröße herunterfahren	Im Normalbetrieb ist dies mit Vorsicht zu behandeln. Diese Option ist jedoch in Hochsicherheitsbereichen sinnvoll, wenn Nachweisführung vor Verfügbarkeit geht. In jedem Fall muss der Einsatz genau abgewogen werden.

Tabelle: Einstellungen für Protokolldateien

Im Rahmen der Überwachung sind allgemein auch folgende Aspekte zu berücksichtigen:

DS-Beauftragten und Personalvertretung beteiligen

- Der Datenschutzbeauftragte und der Personal- bzw. Betriebsrat sollten frühzeitig in die Planung mit einbezogen werden, da bei einer Überwachung meist auch personenbezogene Daten erfasst werden, um im Falle einer Sicherheitsverletzung zuverlässig den Verursacher feststellen zu können.
- Damit die Überwachungskomponenten Protokolleinträge generieren, muss die Überwachung über die relevanten Gruppenrichtlinieneinstellungen aktiviert werden.
- Windows 2000/XP stellt zur Überwachung lediglich eine Protokoll-Funktionalität zur Verfügung: Systemkomponenten und Applikationen erzeugen Statusmeldungen, die in drei Protokolldateien (System-, Applikations- und Sicherheitslog) gesammelt werden. Eine dedizierte Auditing-Architektur zur Online-Überwachung existiert nicht. Die Protokolldateien werden jeweils lokal gespeichert und müssen im Wesentlichen von Hand ausgewertet werden.
- Der Aufbau einer zentralen Sammelstelle von Protokolldateien mit entsprechend automatisierter Auswertung kann durch Produkte von Drittherstellern erreicht werden. Wird ein Werkzeug zum Netz- und Systemmanagement eingesetzt (siehe auch Baustein B 4.2 Netz- und Systemmanagement), so ist es - je nach Produkt - möglich, die Windows 2000/XP Protokolle direkt in dieses Werkzeug zu importieren.
- Über die Windows 2000/XP Auditing-Einstellungen können Zugriffe auf Dateien oder Registry-Schlüssel im Sicherheitsprotokoll aufgezeichnet werden.

Überwachungsparameter erst testen

- Durch die Überwachung fallen je nach Einstellung große Datenmengen an. Zusätzlich führt eine intensive Überwachung zu Performanceverlusten. Dadurch kann im Extremfall ein System so überlastet werden, dass ein geregelter Betrieb nicht mehr möglich ist. Aus diesem Grund müssen die geeigneten Überwachungsparameter im Rahmen eines Testbetriebes überprüft und gegebenenfalls angepasst werden. Es ist zu beachten, dass die Anpassung auch Einfluss auf das gesamte Überwachungskonzept haben kann, da bestimmte Überwachungsaufgaben nicht mehr durchführbar sind. Dies gilt insbesondere dann, wenn zusätzliche Produkte eingesetzt werden, die hohe Anforderungen an die protokollierten Ereignisse stellen. Dies sind z. B. Programme, die eine automatische Analyse der Protokolldaten auf Verhaltensanomalien, etwa für die Erkennung von Angriffen, durchführen.

Im Rahmen der Überwachung von Systemfunktionen empfiehlt sich auch die regelmäßige Kontrolle der AD-Replikation, durch die Konfigurationsänderungen weitergereicht werden. Dazu können einerseits AD-Werkzeuge, wie *repadmin.exe* oder *showreps.exe*, genutzt werden, andererseits sollten das ADS-Log (Active Directory Service) und das FRS-Log (File Replication Service) auf Fehlermeldungen hin überprüft werden. Fehler in der Replikation haben meist zur Folge, dass Konfigurationsänderungen nicht überall durchgeführt werden. Dadurch besteht die Gefahr, dass einem Benutzer ungeeignete oder zu viele Rechte zugestanden werden.

Systemzeit synchronisieren

Die Systemzeit spielt eine wichtige Rolle bei der Systemüberwachung und der Auswertung protokollierter Daten. Insbesondere wenn mehrere Systeme überwacht werden, sollte die Systemzeit auf allen Rechnern synchronisiert werden. Windows 2000 führte den Zeitdienst *W32Time* (Windows-Zeitgeber) ein. Dieser Dienst ist für die Zeitsynchronisierung verantwortlich.

In einer Active Directory-Umgebung ist der autorisierende Domain Controller der Zeitgeber für die Domänenmitglieder. Der Windows Zeitdienst ist hierarchisch aufgebaut: Der Domain Controller der Stammdomäne (Root Domain), der die PDCE FSMO Rolle innehat, wird zum zentralen Zeitgeber für die gesamte Active Directory-Infrastruktur. Der Domain Controller kann mit dem Kommando net time /setsntp:<zeitquelle> so konfiguriert werden, dass er eine externe Zeitquelle zum Synchronisieren verwendet. Die Zeitquelle kann sich innerhalb oder außerhalb des eigenen Netzes befinden, wobei eine interne Zeitquelle bevorzugt eingesetzt werden sollte. Wird eine Zeitquelle außerhalb des eigenen Netzes verwendet, muss ihre Vertrauenswürdigkeit sichergestellt sein.

Client-Rechner, die keine Domänenmitglieder sind, benutzen standardmäßig den Microsoft Zeitserver *time.windows.com*. Sie können aber auch mit dem Kommando *net time* oder über die Registrierung (*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \DateTime\Servers*) so konfiguriert werden, dass sie eine andere Zeitquelle verwenden.

Ergänzende Kontrollfragen:

- Wurde ein bedarfsgerechtes Überwachungskonzept entworfen und umgesetzt?
- Wurde die Möglichkeit zur Protokollierung aktiviert?
- Werden wichtige Systemereignisse protokolliert?
- Wurden Überwachungseinstellungen für wichtige Systemdateien und Registry-Einträge konfiguriert?
- Wie wird die Synchronisierung der Systemzeit sichergestellt?

M 4.149 Datei- und Freigabeberechtigungen unter Windows 2000/XP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Das Dateisystem von Windows 2000/XP ist die Weiterentwicklung des Windows NT Dateisystems. Die Mechanismen zur Zugriffssteuerung unterscheiden sich dabei kaum. Die folgende Tabelle gibt einen Überblick der möglichen Zugriffsrechte auf Dateien. Diese erlauben unter Windows 2000/XP eine wesentlich detailliertere Konfiguration, als dies unter Windows NT möglich ist.

Zugriffsrechte für Ordner	Zugriffsrechte für Dateien
Ordner durchsuchen	Datei ausführen
Ordner auflisten	Daten lesen
Attribute lesen	Attribute lesen
Erweiterte Attribute lesen	Erweiterte Attribute lesen
Dateien erstellen	Daten schreiben
Ordner erstellen	Daten anhängen
Attribute schreiben	Attribute schreiben
Erweiterte Attribute schreiben	Erweiterte Attribute schreiben
Unterordner und Dateien löschen	
Löschen	Löschen
Berechtigungen lesen	Berechtigungen lesen
Berechtigungen ändern	Berechtigungen ändern
Besitzrechte übernehmen	Besitzrechte übernehmen

Tabelle: Überblick der Zugriffsrechte für Ordner und Dateien

Die Zugriffrechte können dabei auf Dateien oder Ordner angewandt werden. Im Rahmen der Rechtevererbung ist es möglich, dass Rechte eines Ordners an Dateien und/oder Unterordner weitergereicht werden, so dass eine einfache Möglichkeit besteht, die Zugriffsberechtigungen in einem ganzen Teildateibaum durch die Änderung an einer Stelle zu wechseln. Das Weiterreichen, d. h. das Vererben, an die Objekte in einem Verzeichnis kann gezielt durch folgende sieben Einstellungen kontrolliert werden, die angeben, auf welche Objekte die Zugriffsrechte angewandt bzw. vererbt werden sollen:

- Nur diesen Ordner
- Diesen Ordner, Unterordner und Dateien
- Diesen Ordner, Unterordner
- Diesen Ordner, Dateien
- Nur Unterordner und Dateien
- Nur Unterordner

- Nur Dateien

Durch die Option *Berechtigungen nur für Objekte und/oder Container in diesem Container übernehmen* kann zudem erreicht werden, dass die Rechte nicht rekursiv in den jeweiligen Unterbaum weitervererbt werden, sondern nur auf die Objekte im aktuellen Verzeichnis.

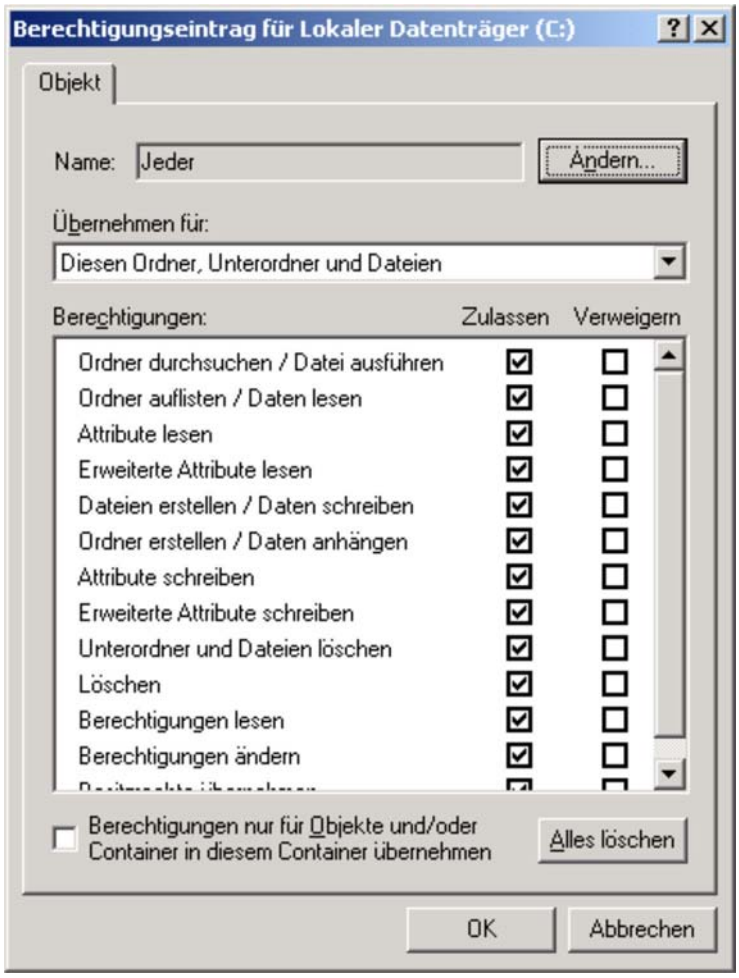


Abbildung: Berechtigungseintrag für Lokaler Datenträger (C:)

Zur Steuerung der Rechteübernahme auf Objekte beim Einsatz des Vererbungsmechanismus stehen zwei weitere Optionen zur Verfügung:

- Das Übernehmen vererbter Rechte kann für Objekte mit der Option *Vererbbare übergeordnete Berechtigungen übernehmen* erlaubt oder blockiert werden.
- Das Übernehmen vererbter Rechte durch Objekte im Unterbaum kann mit der Option Berechtigungen in allen untergeordneten Objekten zurücksetzen und die Verarbeitung vererbbarer Berechtigungen aktivieren erzwungen werden.

Stehen die beiden Rechte in Konflikt miteinander, so wird die erzwungene Übernahme der vererbten Rechte durchgesetzt.

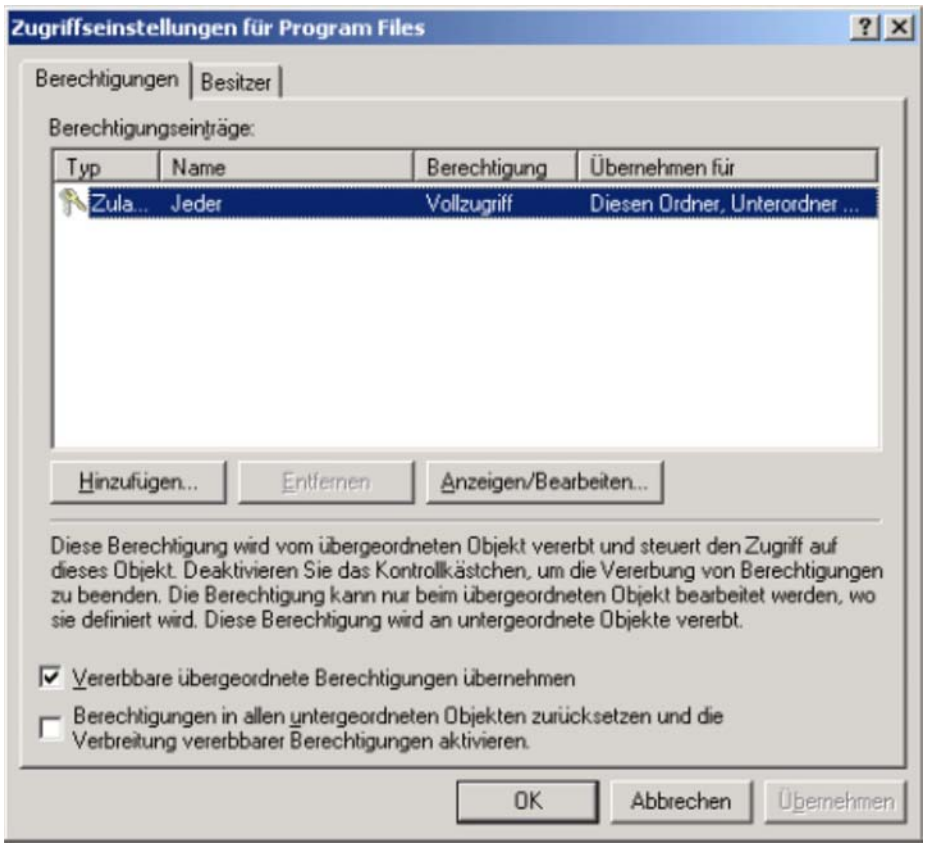


Abbildung: Zugriffseinstellungen für Program Files

Diese Fülle an unterschiedlichen Dateiberechtigungen im Zusammenspiel mit den unterschiedlichen Vererbungsmechanismen macht die Verwaltung von Zugriffsrechten für den Benutzer unübersichtlich. Im Normalfall empfiehlt sich daher, nur die zusammengesetzten Standardzugriffsrechte zu verwenden:

Ordner	**Dateien**	**entspricht**
Vollzugriff	Vollzugriff	*alle Einzelberechtigungen*
Ändern	Ändern	*Lesen, Ausführen* ergänzt um *Löschen*
Lesen, Ausführen	Lesen, Ausführen	*Lesen* ergänzt um *Datei ausführen*
Ordnerinhalt auflisten	-	
Lesen	Lesen	Daten lesen, Attribute lesen, erweiterte Attribute lesen, Berechtigungen lesen
Schreiben	Schreiben	Daten schreiben, Daten anhängen, Attribute schreiben, erweiterte Attribute schreiben

Tabelle: Standardzugriffsrechte

Im Rahmen der Planung des Windows 2000/XP Einsatzes ist auch das Zugriffskonzept für Dateien und Ordner zu entwerfen, durch das die detaillierten Zugriffsrechte festgelegt werden. Dabei sind die organisatorischen und geschäftlichen Anforderungen zu berücksichtigen. Generell empfiehlt es sich, für die Windows 2000/XP Systemdateien restriktive Rechte zu vergeben.

Als Ausgangskonfiguration für Windows 2000 können folgende Berechtigungsvorgaben genutzt werden, die jedoch auf jeden Fall an die lokalen Gegebenheiten angepasst werden müssen. Die vorgeschlagenen Einstellungen gehen davon aus, dass die Benutzerkennung *Hauptbenutzer* (*Power-User*) nicht verwendet wird, da administrative Belange durch Administratoren mit entsprechenden Berechtigungen im Rahmen des Administrationskonzeptes abgedeckt werden. Aus diesem Grund ist die Kennung *Hauptbenutzer* aus allen Zugriffslisten zu entfernen. Zusätzlich empfiehlt sich im Rahmen des Administrationskonzeptes eine Gewaltenteilung, so dass die administrativen Berechtigungen auf entsprechende Konten aufgeteilt werden. Im Folgenden wird jedoch davon ausgegangen, dass jeweils die Gruppe *Administratoren* die gesamte administrative Gewalt hat. Die Berechtigungen gelten nur für die angegebenen Verzeichnisse oder Dateien und sind nicht für die Vererbung gedacht.

Verzeichnis	**Rechte**
Stammverzeichnis der Systempartition	Administratoren: Vollzugriff SYSTEM: Vollzugriff Benutzer: Lesen
\WINNT	Administratoren: Vollzugriff SYSTEM: Vollzugriff ERSTELLER-BESITZER: Vollzugriff Benutzer: Lesen, Ausführen
WINNT\REPAIR	Administratoren: Vollzugriff
WINNT\SYSTEM32\CONFIG	Administratoren: Vollzugriff SYSTEM: Vollzugriff Benutzer: Lesen
WINNT\SYSTEM32\SPOOL	Administratoren: Vollzugriff SYSTEM: Vollzugriff ERSTELLER-BESITZER: Vollzugriff Benutzer: Lesen

Tabelle: Berechtigungsvorgaben für Verzeichnisse unterWindows 2000

Verzeichnis / Datei	Rechte
boot.ini ntldr	Administratoren: Vollzugriff SYSTEM: Vollzugriff
autoexec.bat config.sys	Administratoren: Vollzugriff SYSTEM: Vollzugriff Benutzer: Lesen
TEMP	Administratoren: Vollzugriff SYSTEM: Vollzugriff Benutzer: Ändern
PROGRAMME	Administratoren: Vollzugriff SYSTEM: Vollzugriff Benutzer: Lesen, Ausführen
Dokumente und Einstellungen	Administratoren: Vollzugriff SYSTEM: Vollzugriff Benutzer: Lesen

Tabelle: Berechtigungsvorgaben für Dateien unter Windows 2000

Bei einer Aktualisierung eines Windows NT Rechners auf Windows 2000/XP werden nicht die Windows 2000/XP Standardberechtigungen installiert, sondern es werden die vorhandenen Einstellungen übernommen. Daher muss bei solchen Systemen immer überprüft werden, ob die Berechtigungen konform zum entworfenen Berechtigungskonzept sind.

Auch Windows 2000/XP erlaubt es, Verzeichnisse und die darin enthaltenen Dateien über eine Freigabe für den Netzzugriff zur Verfügung zu stellen. Dabei erfolgt die Zugriffskontrolle zweistufig. Zum einen können Zugriffsberechtigungen auf die Netzfreigabe selbst eingerichtet werden, die bestimmen, wer generell auf die Netzfreigabe zugreifen darf. Zum anderen greifen die oben beschriebenen, auf Dateisystemebene angegebenen Zugriffsrechte auf Dateien und Verzeichnisse. Berechtigungen auf Netzfreigaben können nur über die Rechte

- Vollzugriff,
- Ändern und
- Lesen

gesteuert werden. Eine feinere Kontrolle ist jedoch an dieser Stelle nicht notwendig.

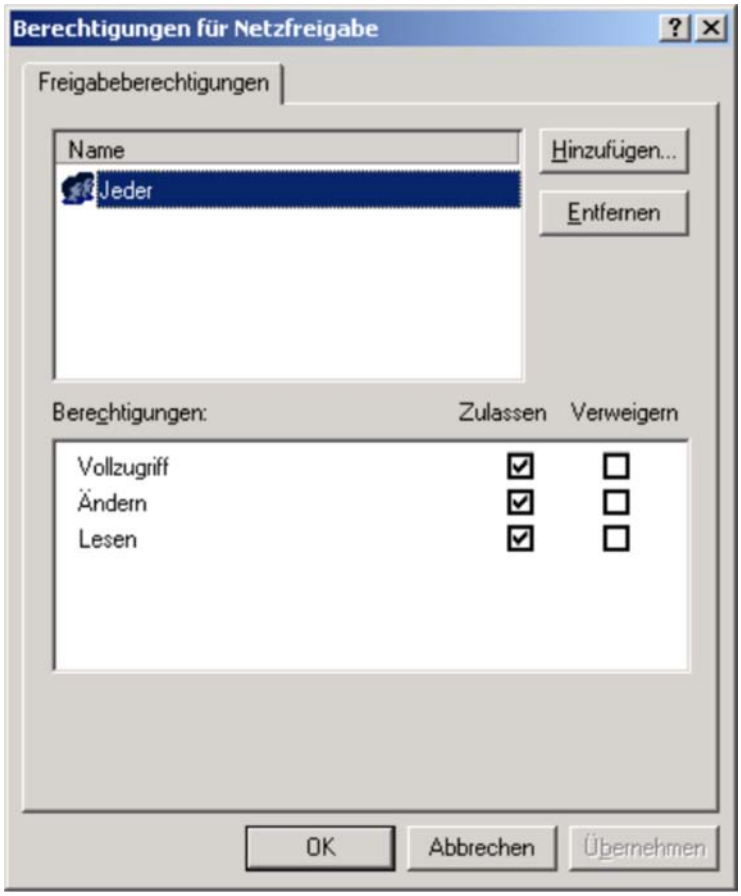


Abbildung: Berechtigungen für Netzfreigabe

Um Datei-, Verzeichnis- und Freigabeberechtigungen festzulegen, sollten folgende Regeln beachtet werden:

Freigaben durch APCs und DCs vermeiden

- Freigaben durch Arbeitsplatzrechner sind zu vermeiden (siehe auch M 5.37 *Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz*, die analog für Windows 2000/XP gilt).
- Freigaben durch Domänen-Controller sind ebenfalls zu vermeiden, da Domänen-Controller sensitive Daten speichern.
- Freigaben auf Arbeitsplatzrechnern und Domänen-Controllern sind zu begründen und zu dokumentieren und sollten nur nach einer vorherigen Risikoabwägung erfolgen.
- Für alle Freigaben und die dadurch zugreifbaren Daten müssen die Zugriffsberechtigungen so restriktiv wie möglich vergeben werden.
- Das Zugriffskonzept muss dokumentiert sein.

Ergänzende Kontrollfragen:

- Wurde ein bedarfsgerechtes Berechtigungskonzept entworfen?
- Sind die Berechtigungen aller Verzeichnisse und Dateien auf allen aktualisierten Rechnern überprüft worden?
- Sind die eingestellten Datei- und Verzeichnisberechtigungen von freigegebenen Verzeichnissen für den Netzzugriff geeignet?

M 4.150 Konfiguration von Windows 2000 als Workstation

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Verwendung von Windows 2000 auf Arbeitsplatzrechnern stellt neben den allgemeinen Sicherheitsanforderungen an die Grundkonfiguration von Windows 2000 (siehe M 4.137 *Sichere Konfiguration von Windows 2000*) auch spezifische, arbeitsplatzbezogene Sicherheitsanforderungen. Die auf Arbeitsplatzrechnern eingesetzte Version ist in der Regel Windows 2000 Professional, das als Clientsystem mit Windows 2000 Servern und Domänen-Controllern kommuniziert.

Für die Konfiguration als Workstation sind folgende Aspekte aus Sicherheitssicht zu berücksichtigen:

Lokale Daten vermeiden

- Es empfiehlt sich, keine lokalen Daten auf Arbeitsplatzrechnern zu halten. Dies hat einerseits Vorteile bei der Datensicherung und bietet zudem den Sicherheitsvorteil, dass bei Kompromittierung des Systems lokal keine sensitiven Daten vorzufinden sind. Kann eine vorgefertigte Standardkonfiguration eingesetzt werden, so ist im Fehlerfall sehr einfach eine Neuinstallation möglich, ohne dass dabei Rücksicht auf lokale Datenbestände genommen werden muss.
- In Einzelfällen kann es notwendig sein, dass Daten aus Sicherheitsgründen lokal auf dem Arbeitsplatz gespeichert werden müssen, da z. B. nur der Arbeitsplatzbenutzer darauf zugreifen darf und eine Übertragung über das Netz nicht erfolgen soll. In diesen Fällen ist der Arbeitsplatz jedoch nicht als Standardarbeitsplatz anzusehen, so dass besondere Regelungen für diese Art Arbeitsplatz geplant und umgesetzt werden müssen. Beispiele für entsprechende Maßnahmen sind starke Absicherung sowohl lokal als auch im Netz, Einsatz von Plattenverschlüsselung und die Einbindung in das Backup-Konzept.

Benutzer darf nicht administrieren

- Ein Arbeitsplatzrechner sollte so konfiguriert sein, dass ein Benutzer keine administrativen Tätigkeiten ausführen kann. Dies betrifft einerseits die Zugriffsrechte auf Dateien und die Registry und andererseits die Berechtigung zum Starten der Konfigurationswerkzeuge, wie z. B. der MMC-Konsole oder auch der Registry-Editoren. Diese Einstellungen können über Gruppenrichtlinien verwaltet werden, so dass dies bei der Planung der Gruppenrichtlinien berücksichtigt werden muss (siehe M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000*).
- Falls auf einem Arbeitsplatz sensitive Daten verarbeitet werden, empfiehlt es sich, regelmäßig Verzeichnisse, in denen temporäre Dateien abgelegt werden, wie *Temp*, *Tmp* und das Drucker-Spool-Verzeichnis, zu bereinigen und auch die Auslagerungsdatei beim Herunterfahren des Systems zu löschen. Nur so kann gewährleistet werden, dass sensitive Informationen oder Restinformationen nicht zufällig zugreifbar sind. Um das Löschen der Auslagerungsdatei beim Herunterfahren zu aktivieren, muss die Einstellung *Auslagerungsdatei des virtuellen Arbeitsspeichers beim Herunterfahren des Systems löschen* aktiviert werden. Diese findet sich unter

Sicherheitseinstellungen/Lokale Richtlinien/Sicherheitsoptionen in der Verwaltung der lokalen Sicherheitsrichtlinien oder aber in Gruppenrichtlinienobjekten unter *Computerkonfiguration/Windows Einstellungen/ Sicherheitseinstellungen/Lokale Richtlinien/Sicherheitsoptionen*.

Einschränkung der Oberfläche kann umgangen werden

- Windows 2000 erlaubt es, die Arbeitsoberfläche eines Benutzers in ihrer Funktionalität einzuschränken. Dies kann sehr detailliert durch entsprechende Konfiguration der Gruppenrichtlinien (GPO-Einstellung) geschehen. Es ist dabei zu beachten, dass diese Einschränkungen nicht als starke Sicherheitsmechanismen anzusehen sind. So kann zwar das Starten von nicht durch den Administrator freigegebenen Programmen über eine GPO-Einstellung für den Windows Explorer verhindert werden. Dies stellt jedoch nicht sicher, dass nicht freigegebene Programme nicht doch durch andere Mechanismen gestartet werden können. Beispiele hierfür sind Start durch den Taskmanager, von der Kommandozeile oder durch ein anderes Programm.
- Im Rahmen des Überwachungskonzeptes (siehe M 4.148 *Überwachung eines Windows 2000/XP Systems*), welches auch die Protokollauswertung beinhaltet, sollten wichtige lokale Systemdateien und Registry-Schlüssel überwacht werden.

Freigaben vermeiden

- Arbeitsplatzrechner sollten neben den administrativen Standardfreigaben keine Verzeichnisfreigaben zur Verfügung stellen. Werden Daten nicht lokal gehalten, so ist dies auch nicht notwendig. Werden Verzeichnisfreigaben verwendet, müssen auch Netzzugriffe zugelassen werden, was als potentielle Gefährdung angesehen werden muss (siehe auch M 5.37 *Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz*).
- Es sollte verhindert werden, dass Benutzer auf Arbeitsplatzrechnern Software installieren können.
- Wird ein Arbeitsplatzrechner in eine Domäne integriert, so muss dies in der Regel unter den Berechtigungen des Domänen-Administrators erfolgen. Wird administrative Delegation eingesetzt, so muss dazu ein entsprechend berechtigtes Konto benutzt werden.

Laptops besonders schützen

- Für Laptops bestehen besondere Gefahren durch die fehlende physikalische Sicherheit. Hier müssen besondere Vorkehrungen getroffen werden (siehe auch Baustein B 3.203 *Laptop*). Windows 2000 bietet hier als zusätzlichen Schutz von Daten die Verschlüsselung von Dateien mittels EFS (Encrypting File System) an. Hinweise zur sicheren Nutzung von EFS sind in M 4.147 *Sichere Nutzung von EFS unter Windows 2000/XP*.

Zusammenfassend muss darauf hingewiesen werden, dass die Sicherheit von Arbeitsplatzrechnern direkten Einfluss auf die Sicherheit des Gesamtsystems hat und dieser damit ein hoher Stellenwert zukommt.

Ergänzende Kontrollfragen:

- Ist sichergestellt, dass auch lokal gehaltene Daten durch das Datensicherungskonzept erfasst werden?
- Wurde der Arbeitsplatzrechner so konfiguriert, dass durch Benutzer keine administrativen Tätigkeiten ausgeführt werden können?
- Werden temporäre Dateien und Verzeichnisse regelmäßig gelöscht?
- Ist EFS für alle Rechner, die Dateien verschlüsselt vorhalten sollen, aktiviert?
- Werden Zugriffe auf wichtige Systembereiche überwacht?

M 4.151 Sichere Installation von Internet-PCs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsbeauftragter

Verantwortlich für Umsetzung: Administrator

Bei der Installation des Internet-PC müssen eine Reihe von Entscheidungen getroffen werden, die Auswirkungen auf die IT-Sicherheit des Systems haben.

Hardware

Die Hardware des Internet-PCs ist so zu konfektionieren, dass nur die im Einsatzkonzept vorgesehenen Komponenten vorhanden sind. Gegebenenfalls müssen nicht vorgesehene Laufwerke oder Schnittstellen, z. B. Diskettenlaufwerke oder interne Modems, entfernt oder deaktiviert werden (siehe auch M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*).

Die Boot-Reihenfolge sollte im System-BIOS so eingestellt werden, dass der Computer immer zuerst versucht, von der Festplatte zu starten, z. B. *C: A:, C only* oder *Harddisk first/only*.

BIOS-Passwort

Der Zugang zum System-BIOS sollte durch ein Passwort geschützt werden. Falls ein Betriebssystem ohne zwingende Benutzer-Authentisierung zum Einsatz kommt, z. B. Windows 9x/ME, kann darüber nachgedacht werden, auch ein Boot-Passwort im BIOS zu aktivieren. Dies bietet einen gewissen Schutz vor Missbrauch durch Gelegenheitstäter.

Betriebssystem

Im Anschluss an die Installation der Hardware wird das im Einsatzkonzept vorgesehene Betriebssystem installiert. Zu beachten ist dabei, dass gängige Betriebssysteme unterschiedliche Sicherheitsfunktionen bieten. Windows NT/2000 und Linux verfügen beispielsweise über eine wirksame Benutzertrennung und Zugriffsrechte. Diese Funktionen stehen bei Windows 9x/ME nur ansatzweise oder gar nicht zur Verfügung, sind jedoch wichtig für die Trennung von Administrator- und Benutzerbereichen.

nur benötigte Komponenten installieren

Grundsätzlich sollten nur die Betriebssystem-Komponenten installiert werden, die auch wirklich für den festgelegten Einsatzbereich benötigt werden. Besonders kritisch zu prüfen sind hierbei "Dienste" (Windows) bzw. "Daemons" (Linux). Ein Internet-PC sollte in der Regel keine Dienste im Internet anbieten (siehe auch M 5.43 *Sichere Konfiguration der TCP/IP-Netzdienste unter Windows NT* und M 5.72 *Deaktivieren nicht benötigter Netzdienste*).

Nach der Installation des Betriebssystems müssen alle evtl. vergebenen Standardpasswörter geändert werden. Unter Linux betrifft dies insbesondere das *root*-Passwort, sofern die verwendete Distribution hierfür ein Standardpasswort vergibt.

sicherheitsrelevante Patches einspielen

Vor der Inbetriebnahme müssen alle aktuellen sicherheitsrelevanten Patches bzw. Updates eingespielt werden. Für Windows-Betriebssysteme sind entsprechende Informationen auf den WWW-Seiten der Firma Microsoft (*www.microsoft.com*) erhältlich. Falls Linux eingesetzt wird, sollte zunächst beim Hersteller der verwendeten Distribution nach verfügbaren Patches und Updates gesucht werden. Falls das Angebot des Herstellers unzureichend ist, sollten weitere Quellen hinzugezogen werden, z. B. *www.linuxdoc.org*.

Weitere Empfehlungen hierzu finden sich in M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems* und M 4.107 *Nutzung von Hersteller-Ressourcen*.

Für Windows-Betriebssysteme gelten darüber hinaus folgende Empfehlungen:

- Das jeweils aktuelle Service Pack sollte eingespielt werden.
- Als einziges Netzprotokoll sollte TCP/IP installiert werden.
- An das TCP/IP-Protokoll für den Internet-Zugang sollten keine Dienste gebunden werden.
- Die Datei- und Druckerfreigabe sollte deaktiviert werden. Es sollten keine *Shares* zur Verfügung gestellt werden.
- Bei Verwendung des Internet Explorers sollte unter *Extras* | *Internetoptionen* | *Verbindungen* die Funktion *Vor dem Wählen Systemsicherheit prüfen* aktiviert werden, falls diese Option angeboten wird.
- Der Windows Scripting Host (WSH) sollte deinstalliert werden, wenn dies bei der verwendeten Konfiguration möglich ist. Anderenfalls sollten die dem WSH zugeordneten Dateitypen, beispielsweise *.vbs* und *.js*, einem Editor zugewiesen werden.
- Der Microsoft Personal Web Server sollte deaktiviert, möglichst sogar deinstalliert werden.
- Die automatische CD-ROM-Erkennung sollte deaktiviert werden (siehe auch M 4.57 *Deaktivieren der automatischen CD-ROM-Erkennung*).
- Falls die verwendete Windows-Version eine Benutzertrennung unterstützt, sollten alle nicht benötigten Benutzerkonten, z. B. *Gast*, deaktiviert oder gelöscht werden. Unter Windows NT kann dies über den *Benutzer-Manager* erfolgen. Das *Administrator*-Konto sollte umbenannt und mit einem starken Passwort geschützt werden.
- Beim Einsatz von Windows 9x/ME kann darüber nachgedacht werden, einen passwortgeschützten Bildschirmschoner zu verwenden. Dies bietet einen gewissen Schutz gegen unberechtigte Zugriffe.
- Als Standardvorgang beim Doppelklick auf eine Datei vom Typ *.reg* sollte *Bearbeiten* (mit Editor öffnen) und nicht *Zusammenführen* eingestellt werden. Unter Windows ME kann das entsprechende Dialogfeld über den Explorer via *Extras* | *Ordneroptionen* | *Dateitypen* erreicht werden.
- Es sollte geprüft werden, ob anstelle der Standardnamen für System- und Datenverzeichnisse bzw. -dateien abweichende Pfadnamen verwendet werden können. Schadprogramme suchen in vielen Fällen nach bestimmten Dateien in Standardverzeichnissen, so dass durch diese Änderung ggf. ein zusätzlicher Schutz erreicht werden kann. Es ist jedoch zu berücksichtigen, dass dies zu Inkompatibilitäten mit bestimmten Programmen führen kann.

Bei der Verwendung von Linux sollten folgende Empfehlungen berücksichtigt werden:

- Der Daemon *inetd* sollte nicht gestartet werden. Je nach Distribution wird dies über Änderungen an den rc-Startdateien oder über spezielle Administrationstools konfiguriert.
- Der *Portmap Daemon* und der *Name Service Caching Daemon* sollten nicht gestartet werden.
- Falls die verwendete Distribution spezielle Dienste zur Fernadministration installiert, z. B. *linuxconf* oder *swat*, so sollten diese deaktiviert werden.

- *Apache* oder andere WWW-Server-Software sollte deinstalliert werden.
- Das Programm *sendmail* sollte nicht im Server-Modus gestartet werden. Auch andere Daemons für den Empfang von E-Mail über das Protokoll SMTP sollten deinstalliert oder zumindest deaktiviert werden. Sofern benötigt, sollte E-Mail stattdessen via POP3 oder IMAP abgeholt werden.
- Als zusätzliche Sicherheitsmaßnahme gegen Angriffe aus dem Internet kann die Paketfilterfunktion *ipchains* bzw. *iptables* von Linux eingesetzt werden. Einige Distributionen enthalten hierfür vorkonfigurierte Pakete.

Als zusätzliche Sicherheitsmaßnahme kann eine so genannte *Personal Firewall* installiert werden. Damit diese auch wirksam ist, muss sie sorgfältig für den jeweiligen Einsatzzweck konfiguriert werden. Insbesondere muss das Programm so eingestellt werden, dass die Benutzer nicht mit einer Vielzahl von Warnmeldungen belästigt werden, die sie nicht interpretieren können. Weitere Empfehlungen finden sich in M 5.91 *Einsatz von Personal Firewalls für Internet-PCs*.

Client-Programme

Neben dem eigentlichen Betriebssystem sollten auf dem Internet-PC nur die zusätzlichen Programme installiert werden, die für die Nutzung der im Einsatzkonzept festgelegten Internet-Dienste erforderlich sind.

Falls die Nutzung des World Wide Web im Einsatzkonzept vorgesehen ist, muss ein WWW-Browser installiert werden. Gängige Browser-Programme sind der *Internet Explorer*, *Netscape Navigator* und *Opera*. Empfehlungen zur sicheren Konfiguration dieser Browser finden sich der Maßnahme M 5.93 *Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs*.

Falls vom Internet-PC aus E-Mails gesendet oder empfangen werden sollen, muss entweder ein E-Mail-Client installiert werden oder es muss auf einen WWW-basierten E-Mail-Dienst (z. B. GMX oder Web.de) zurückgegriffen werden. Gängige E-Mail-Clients sind *Outlook, Outlook Express, Netscape Messenger* oder *KMail*. Empfehlungen zur sicheren Konfiguration dieser Programme finden sich in der Maßnahme M 5.94 *Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs*.

Falls im Einsatzkonzept vorgesehen ist, weitere Internet-Dienste zu nutzen, z. B. News oder Instant Messaging, müssen ggf. weitere Client-Programme installiert werden.

Alle Programme sollten so konfiguriert werden, dass sie optimale Sicherheit bieten, und die Benutzer sollten in deren sichere Nutzung eingewiesen werden.

Tools

Im Hinblick auf den sicheren Betrieb eines Internet-PCs müssen in der Regel zusätzliche Tools installiert werden, die nicht Bestandteil des Betriebssystems sind.

Viren-Schutz

Unverzichtbar ist der Einsatz eines Viren-Schutzprogramms auf jedem Internet-PC. Solche Programme sind von verschiedenen Herstellern erhältlich. Wichtig ist, dass die zugehörigen Datenbanken, auf deren Grundlage diese Tools arbeiten, regelmäßig aktualisiert werden. Gängige Viren-Schutz-

programme stellen hierfür spezielle Funktionen zur Verfügung. Dabei ist zu beachten, dass dies nicht zentral gesteuert werden kann, wenn die Internet-PCs nicht untereinander vernetzt sind. Weitere Empfehlungen zum Schutz vor Computer-Viren finden sich in M 4.3 *Regelmäßiger Einsatz eines Viren-Schutzprogramms*.

Datensicherung nicht vergessen!

Zur Datensicherung für einen Internet-PC gibt es unterschiedliche Konzepte (siehe auch M 6.79 *Datensicherung beim Einsatz von Internet-PCs*). In vielen Fällen wird hierfür jedoch ein eigenständiges Tool benötigt, dass das erforderliche Backup automatisch oder halbautomatisch erledigt. Oft lassen sich Datensicherung und Datentransport vom oder ins Hausnetz über das gleiche Medium realisieren. Wichtig ist hierbei eine ordnungsgemäße Verwaltung der evtl. benötigten Datenträger.

Bei der Übertragung über das Internet können Daten u. U. mitgelesen oder manipuliert werden. Um diesen Gefährdungen entgegenzuwirken, können kryptographische Verfahren eingesetzt werden. Beispielsweise existieren eine Reihe von Tools, mit denen E-Mails verschlüsselt und signiert werden können. Weiterhin besteht die Möglichkeit, sichere Kanäle zu bekannten Kommunikationspartnern aufzubauen, beispielsweise über so genannte Virtuelle Private Netze (VPNs). Planungshinweise zum Einsatz kryptographischer Verfahren finden sich in Baustein B 1.7 *Kryptokonzept*.

Informationen im Internet werden nicht nur im HTML-Format angeboten, sondern z. B. auch als Word-, Excel-, PowerPoint- oder PDF-Dateien. Wenn solche Dateien direkt auf dem Internet-PC betrachtet werden sollen, müssen hierfür geeignete Viewer-Programme installiert werden. Diese Viewer sollten nach Möglichkeit nicht in der Lage sein, Makro-Befehle auszuführen. Insbesondere sollte nach Möglichkeit kein Office-Paket auf dem Internet-PC installiert werden. Falls dies dennoch zwingend erforderlich ist, sollten alle integrierten Funktionen zum Schutz vor Makro-Viren aktiviert werden.

Für alle installierten Betriebssystem- und Software-Komponenten sollten die jeweils verfügbaren sicherheitsrelevanten Patches bzw. Updates eingespielt werden. Diese sollten aus vertrauenswürdigen Quellen, beispielsweise direkt vom Hersteller, bezogen werden (siehe auch M 4.152 *Sicherer Betrieb von Internet-PCs*).

Nachdem alle Betriebssystem- und Software-Komponenten installiert sind, sollte ein Abbild ("Image") dieser Grundkonfiguration gesichert werden. Dies erlaubt es, das System schnell wiederherzustellen, wenn die Installation durch Abstürze, fehlgeschlagene Konfigurationsänderungen oder Manipulationen unbrauchbar wird (siehe auch M 6.79 *Datensicherung beim Einsatz von Internet-PCs*).

Ergänzende Kontrollfragen:

- Wurden alle nicht benötigten Dienste bzw. Daemons des Betriebssystems deinstalliert oder deaktiviert?
- Wurden nur die Client-Programme installiert, die für die Nutzung der benötigten Internet-Dienste erforderlich sind?

M 4.152 Sicherer Betrieb von Internet-PCs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsbeauftragter

Verantwortlich für Umsetzung: Administrator

Um den sicheren Betrieb eines Internet-PCs zu gewährleisten, müssen Maßnahmen zur Wartung und Pflege des Systems umgesetzt werden. Anderenfalls besteht die Gefahr, dass beispielsweise durch Veränderungen an der Konfiguration Sicherheitslücken entstehen oder bekannt gewordene Software-Schwachstellen für Angriffe von innen oder außen ausgenutzt werden. Beim Betrieb eines Internet-PCs sollten daher die folgenden Aufgaben wahrgenommen werden:

- **Installation von Patches und Updates zur Behebung sicherheitsrelevanter Schwachstellen**

  Häufig werden Fehler in Software-Produkten bekannt, die dazu führen können, dass die Sicherheit der IT-Systeme, auf denen diese Produkte installiert sind, beeinträchtigt wird. Diese Software-Schwachstellen müssen so schnell wie möglich behoben werden, damit sie nicht durch interne oder externe Angreifer ausgenutzt werden können. Die Hersteller von Betriebssystem- oder Software-Komponenten veröffentlichen hierzu in der Regel so genannte Patches oder Updates, die auf dem jeweiligen IT-System installiert werden müssen, um den oder die Fehler zu beheben.

  Die Administration des Internet-PCs sollte sich daher regelmäßig über bekannt gewordene Software-Schwachstellen informieren und dagegen veröffentlichte Patches bzw. Updates installieren (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*). Wichtig ist dabei, dass Patches und Updates - wie jede andere Software - nur aus vertrauenswürdigen Quellen bezogen werden dürfen, möglichst direkt vom Hersteller bzw. Anbieter. Vor der Installation sollten sie außerdem mit Hilfe eines Computer-Virenschutzprogramms geprüft werden.

- **Regelmäßige Kontrolle und Überwachung des Internet-PCs**

  Die Installation und Konfiguration eines Internet-PCs ist in der Regel nicht statisch, sondern ändert sich im laufenden Betrieb. Benutzer können beispielsweise Lesezeichen auf besuchte Internet-Seiten anlegen, E-Mails oder Downloads abspeichern und Dateitypen mit Anzeigeprogrammen verknüpfen. Viele Programme nehmen teilweise auch selbständig erhebliche Änderungen an der Konfiguration vor. Schließlich können sich auch Angriffe oder Angriffsversuche durch Änderungen an der Installation oder Konfiguration des Internet-PCs bemerkbar machen.

  Die Administration muss daher regelmäßig überprüfen, ob die Installation und die Konfiguration des Internet-PCs den Vorgaben bzw. Sollwerten entspricht. Hierzu ist z. B. zu prüfen,

  - ob die Hardware-Konfiguration des Internet-PCs verändert wurde,
  - ob Software-Komponenten entfernt oder zusätzlich installiert wurden,

- ob Einstellungen des BIOS, des Betriebssystems oder der Programme unerlaubt verändert wurden und
- ob es Hinweise darauf gibt, dass lokal gespeicherte Daten nicht den Richtlinien entsprechen, z. B. aufgrund der Pfad- oder Dateinamen.

Weiterhin sollten sporadisch die zur Verfügung stehenden Protokollierungsmechanismen, z. B. *Ereignisanzeige* unter Windows NT, *syslog* unter Linux, *Verlauf* im Internet Explorer, ausgewertet werden. Diese Protokolle können Hinweise auf Angriffe, Angriffsversuche und missbräuchliche Nutzung des Internet-PCs, z. B. Zugriffe auf unerlaubte Internet-Seiten, liefern. Dabei ist jedoch zu berücksichtigen, dass einige dieser Protokolle leicht manipuliert werden können.

Bewusste Verstöße gegen die Sicherheitsrichtlinien werden naturgemäß ungern in der Öffentlichkeit unternommen. Um einen Missbrauch zusätzlich zu erschweren, kann der Internet-PC daher auch an einem Ort mit Publikumsverkehr aufgestellt werden, beispielsweise in einer Bibliothek.

Bei der Kontrolle oder Überwachung des Internet-PCs müssen die Bestimmungen zum Datenschutz und zur betrieblichen Mitbestimmung beachtet werden. Daher sollten alle Maßnahmen hierzu frühzeitig mit dem Personalrat und dem Datenschutzbeauftragten abgestimmt werden.

- **Regelmäßige Neuinstallation des Systems**

  Eine weitere Möglichkeit, unerwünschten Veränderungen an der Installation oder Konfiguration des Internet-PCs entgegenzuwirken, ist die regelmäßige Neuinstallation des Systems. Solche Neuinstallationen beugen auch Systemabstürzen vor, die durch beschädigte oder instabile Installationen verursacht werden. Die Zeitabstände zwischen den Neuinstallationen müssen individuell anhand der Anforderungen an die Integrität des Internet-PCs festgelegt werden.

  Falls solche Neuinstallationen in kurzen Zeitabständen durchgeführt werden sollen, empfiehlt es sich, ein Abbild ("Image") des Systems herzustellen, das dann als ganzes installiert werden kann. Andernfalls entsteht u. U. ein erheblicher Arbeitsaufwand, da jedes Mal das System anhand der einzelnen Software-Komponenten und der Konfigurationsparameter rekonstruiert werden muss.

  Die Vorgehensweise bei der Neuinstallation muss auf jeden Fall mit dem Datensicherungskonzept für den Internet-PC (siehe M 6.79 *Datensicherung beim Einsatz von Internet-PCs*) abgestimmt sein. Andernfalls besteht die Gefahr, dass bei der Neuinstallation Daten verloren gehen, die nicht rekonstruiert werden können.

Ergänzende Kontrollfragen:

- Ist sichergestellt, dass Patches und Updates gegen bekannt gewordene Sicherheitslücken zeitnah installiert werden?
- Werden die Protokolldateien regelmäßig im Hinblick auf Angriffsversuche oder missbräuchliche Nutzung ausgewertet?

M 4.153 Sichere Installation von Novell eDirectory

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Nach erfolgter Planung eines eDirectory-Verzeichnissystems (siehe M 2.236 *Planung des Einsatzes von Novell eDirectory*) muss eDirectory auf den relevanten Servern installiert werden. Während der Installationsphase ist ein eDirectory-Server nicht vollständig konfiguriert, sodass auch die gewünschten Sicherheitseinstellungen noch nicht aktiviert sind. Es empfiehlt sich daher, die erstmalige Konfiguration entweder in einer geschützten Umgebung durchzuführen oder alternativ eine vorbereitete Standardkonfiguration aufzuspielen.

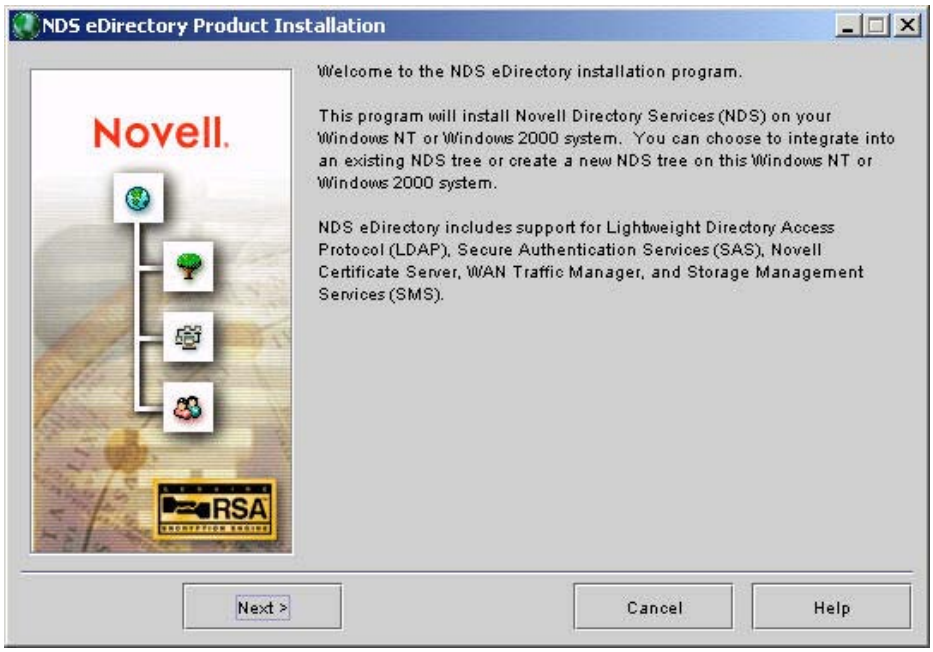


Abbildung: eDirectory Installationsprogramm

Bei der Installation eines eDirectory-Servers in einen bereits bestehenden Verzeichnisbaum muss dessen genauer Kontext spezifiziert werden. Eine spätere Verschiebung des Servers innerhalb des Baums ist nur mit größerem Aufwand zu bewerkstelligen.

Während der Installation erfolgt u. a. auch die erstmalige Konfiguration der lokalen Sicherheitseinstellungen. Die wichtigsten Grundeinstellungen beziehen sich auf

- die Definition des eDirectory-Baums,
- die eDirectory-Zugriffsberechtigungen,
- die eDirectory-Vererbungseinstellungen und
- die Sicherheitseinstellungen für den LDAP-Zugriff.

Während der Installation lassen sich diese Einstellungen zum Teil vorgeben, ein Teil wird jedoch zunächst mit Standardwerten initialisiert. Bei Servern, die

als Erstes einen neuen eDirectory-Baum repräsentieren, muss zunächst die Zertifikatsserver-Komponente von eDirectory installiert werden, bevor ein durch SSL geschützter LDAP-Zugriff verwendet werden kann. Die Alternative hierzu ist, dass der eDirectory-Server einem bereits bestehenden eDirectory-Baum beitritt.

Sicherheit auch während der Installation

Je nachdem, welche eDirectory-Module zum Einsatz kommen, ist für jedes Modul eine sichere Installationskonfiguration einzurichten, die den Zugriff verhindert, solange sich der Server in der erstmaligen Konfigurationsphase befindet und bis die festgelegten Sicherheitsrichtlinien umgesetzt worden sind. Weitere Empfehlungen hierzu finden sich in M 4.155 *Sichere Konfiguration von Novell eDirectory*.

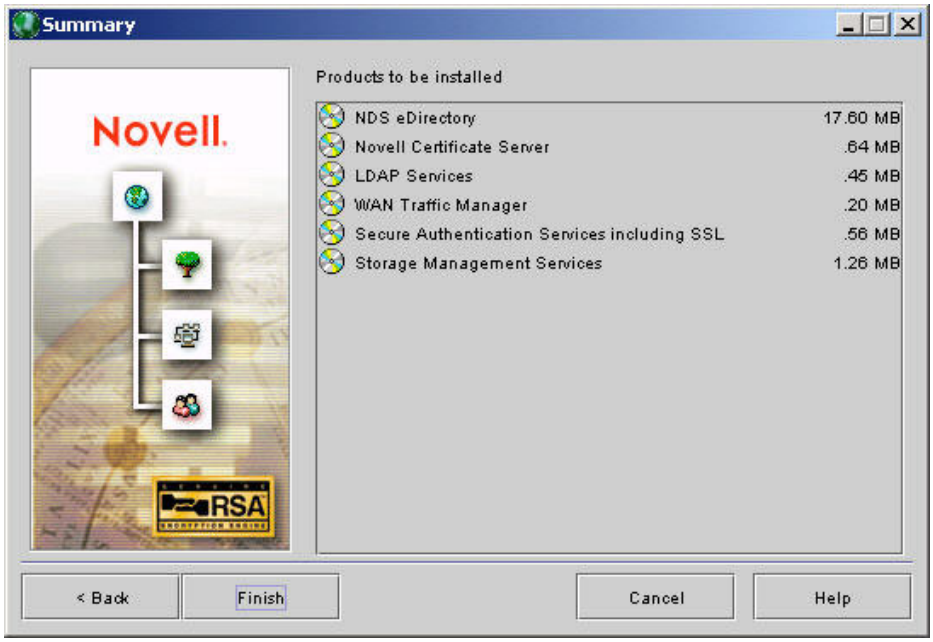


Abbildung: Zusammenfassung der Installation

Generell ist bei der Installation aus Sicherheitssicht Folgendes zu beachten:

- Die geltenden Zugriffseinstellungen für das Verzeichnissystem nach einer eDirectory-Installation hängen davon ab, ob die Software neu installiert wurde oder ob ein Upgrade erfolgt ist.
- Weitere Upgrade-Mechanismen können die Standardeinstellungen verändern, z. B. die Einbeziehung einer Windows NT-Domäne in einen eDirectory-Baum.
- Soll ein neuer Server in einen existierenden eDirectory-Baum aufgenommen werden, so erlaubt es der implizite Vererbungsmechanismus, die erstmalige Konfiguration deutlich abzukürzen.
- Bei der Installation der eDirectory-Server ist besondere Sorgfalt erforderlich, da diese im späteren Betrieb sensitive Daten speichern.

eDirectory-Server dürfen nur auf Servern installiert und betrieben werden, die sich in einer physikalisch sicheren Umgebung befinden (siehe auch M 1.29 *Geeignete Aufstellung eines IT-Systems*). Dies gilt insbesondere für eDirectory-Server, auf denen die Partition mit dem Security-Container abgelegt ist.

Ergänzende Kontrollfragen:

- Befinden sich die eDirectory-Server in einer physikalisch geschützten Umgebung, z. B. einem Serverraum oder einem Serverschrank?
- Wurden die installierten Administrations- und Zugriffsberechtigungen bedarfsgerecht geplant?
- Sind die Zugriffsrechte für eDirectory-Objekte bei Systemen, die von Vorgängerversionen aktualisiert bzw. von anderen Verzeichnissystemen übernommen wurden, ebenfalls aktualisiert worden?

M 4.154 Sichere Installation der Novell eDirectory Clientsoftware

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Nach der Planung eines eDirectory-Systems (siehe M 2.236 *Planung des Einsatzes von Novell eDirectory*) und der Installation der eDirectory-Server (siehe M 4.153 *Sichere Installation von Novell eDirectory*) muss die eDirectory-Clientsoftware auf den relevanten Rechnern installiert werden. Während der Installationsphase ist die eDirectory-Clientsoftware noch nicht vollständig konfiguriert, sodass auch die gewünschten Sicherheitseinstellungen noch nicht aktiviert sind. Es empfiehlt sich daher, die erstmalige Konfiguration entweder in einer geschützten Umgebung durchzuführen oder alternativ eine vorbereitete Standardkonfiguration aufzuspielen.

Die Installation der eDirectory-Clientsoftware erfolgt naturgemäß nicht unabhängig von den eDirectory-Servern. Die Installation kann erst dann als abgeschlossen gelten, wenn die Server-Anbindung erfolgt ist.

Schon bei der Installation der eDirectory-Clientsoftware sind sicherheitsrelevante Aspekte zu berücksichtigen. In der Regel genügt eine Standardinstallation nicht den geltenden Sicherheitsanforderungen, sodasss direkt danach eine sichere Konfiguration der Software erfolgen sollte.

Je nach eingesetztem Betriebssystem gibt es verschiedene Clientsoftware: Windows (der Novell Client), Linux sowie Sun Solaris. Nach erfolgter Installation wird dem Benutzer die Eingabemaske für das eDirectory-Login angezeigt (unter Windows der Novell Client):

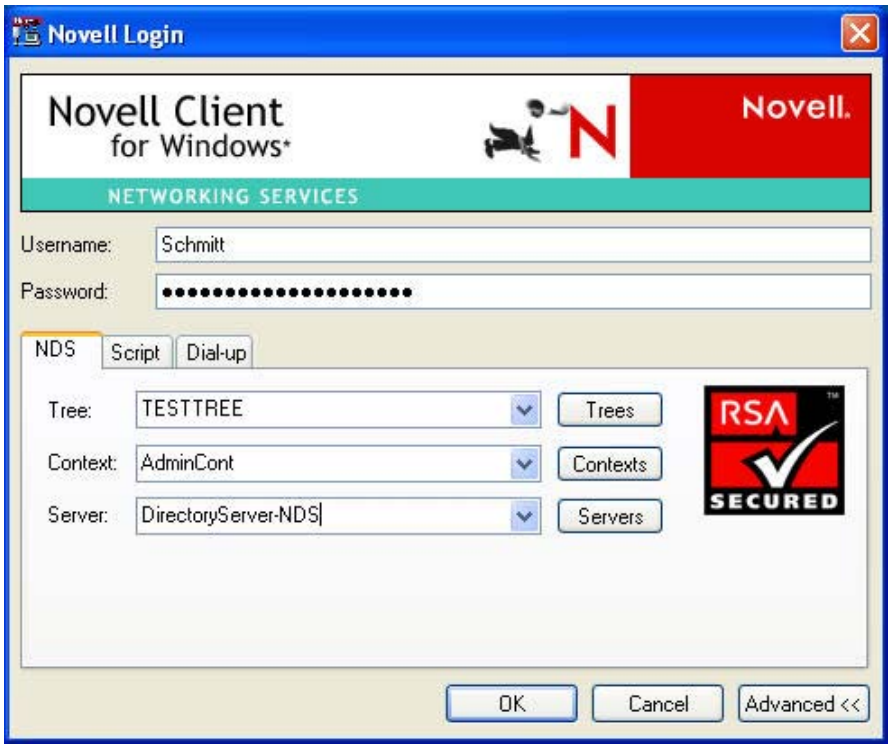


Abbildung: Eingangsmaske des eDirectory-Login

Die Installation beschränkt sich nicht nur auf die Clientsoftware, sondern betrifft in der Regel auch die zugrunde liegenden Betriebssysteme. Auch hierbei gilt, dass der Installationsprozess erst dann als abgeschlossen betrachtet werden kann, wenn direkt nach der Betriebssystem-Installation eine sichere Konfiguration erfolgt. Empfehlungen zur sicheren Installation und Konfiguration des Betriebssystems finden sich in den entsprechenden Bausteinen.

Für jedes Modul ist eine sichere Installationskonfiguration einzurichten, die den Zugriff verhindert, solange sich der Rechner in der erstmaligen Konfigurationsphase befindet und bis die festgelegten Sicherheitsrichtlinien umgesetzt worden sind. Weitere Empfehlungen hierzu finden sich in M 4.156 *Sichere Konfiguration der Novell eDirectory Clientsoftware*.

Ergänzende Kontrollfragen:

- Werden bei der sicheren Installation der eDirectory-Clientsoftware auch das unterliegende Betriebssystem und alle verwendeten Zusatzmodule berücksichtigt?

M 4.155 Sichere Konfiguration von Novell eDirectory

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Konfiguration von eDirectory kann um eine Vielzahl weiterer Module erweitert werden, deren Funktionen über einen reinen Verzeichnisdienst hinausgehen. Dazu gehören:

- das *LDAP-Servermodul*, das einen Zugriff auf die Benutzerinformationen für LDAP-Clients erlaubt,
- das *iMonitor-Tool*, welches den administrativen Zugriff über einen Web-Browser gestattet,
- das *SLP-Modul* (Service Location Protocol), welches Service-URLs verwaltet und in das Ressourcenmanagement einbezieht,
- die *ConsoleOne* als Administrationsplattform des eDirectory,
- der *Zertifikatsserver*, der stets bei der Erstinstallation eines eDirectory-Servers innerhalb eines eDirectory-Baums installiert wird,
- eventuell eingesetzte Zusatzmodule, wie z. B. das Modul zur Unterstützung von *Groupwise*.

Daraus ergibt sich ein Bündel an Konfigurationsaufgaben, das noch durch folgende Themen ergänzt wird:

- Konfiguration der Verzeichnisbaumhierarchie,
- Konfiguration der Objekt-Zugriffsrechte,
- Konfiguration der Vererbungsfilter,
- Konfiguration der Sicherheitsäquivalenzen zwischen einzelnen Objekten bzw. Objektklassen,
- Konfiguration der Administrationsrollen,
- Konfiguration der Delegation von Administrationsaufgaben,
- Konfiguration der Benutzer und der Benutzergruppen,
- Verteilung der Key Management Objekte (KMOs),
- Konfiguration des Client-Zugriffs auf das eDirectory,
- Konfiguration der Partitionierung der eDirectory-Verzeichnisdatenbank,
- Konfiguration der Repliken des eDirectory-Verzeichnisdienstes,
- Konfiguration der DirXML-Schnittstelle zur Synchronisation mit fremden Verzeichnisdiensten,
- Konfiguration der Systemüberwachung.

Dies alles betrifft originär die eDirectory-Software. Es darf jedoch nicht vergessen werden, dass auch das zugrunde liegende Betriebssystem sicher konfiguriert werden muss, insbesondere was den Serverzugriff, die Netzanbindung und das Dateisystem betrifft.

nur genutzte Module installieren

Je nach Einsatzszenario und dem vom eDirectory-Server angebotenen Funktionsumfang muss überprüft werden, welche Zusatzmodule für den Betrieb von eDirectory benötigt werden und genutzt werden sollen. Nicht genutzte Module sollten nicht installiert werden, da jedes installierte Modul bei Fehlkonfiguration Sicherheitsprobleme verursachen kann.

Sicherheitsplanung für Module

Für jedes aktivierte Modul muss eine entsprechende Sicherheitsplanung durchgeführt werden. Anschließend ist diese durch geeignete Konfigurationsparameter umzusetzen (siehe auch M 2.238 *Festlegung einer Sicherheitsrichtlinie für Novell eDirectory*).

eDirectory bietet weitgehende Möglichkeiten zur Konfiguration des Benutzerzugangs für die einzelnen im Verzeichnis angelegten Benutzerkonten. Neben der individuellen Konfiguration einzelner Benutzerkonten können auch Templates verwendet werden, um eine Vielzahl von Benutzerkonten identisch zu konfigurieren. Die vorhandenen Einstellungsmöglichkeiten umfassen u. a.

- eine Beschränkung der Zeiten, zu denen eine Anmeldung an das Benutzerkonto möglich ist,
- eine Beschränkung der IP-Adressen, von denen aus eine Anmeldung möglich ist,
- eine Begrenzung der Anzahl gleichzeitiger Anmeldungen an ein Benutzerkonto,
- Anforderungen an die Passwortlänge und die Gültigkeitsdauer von Passwörtern.

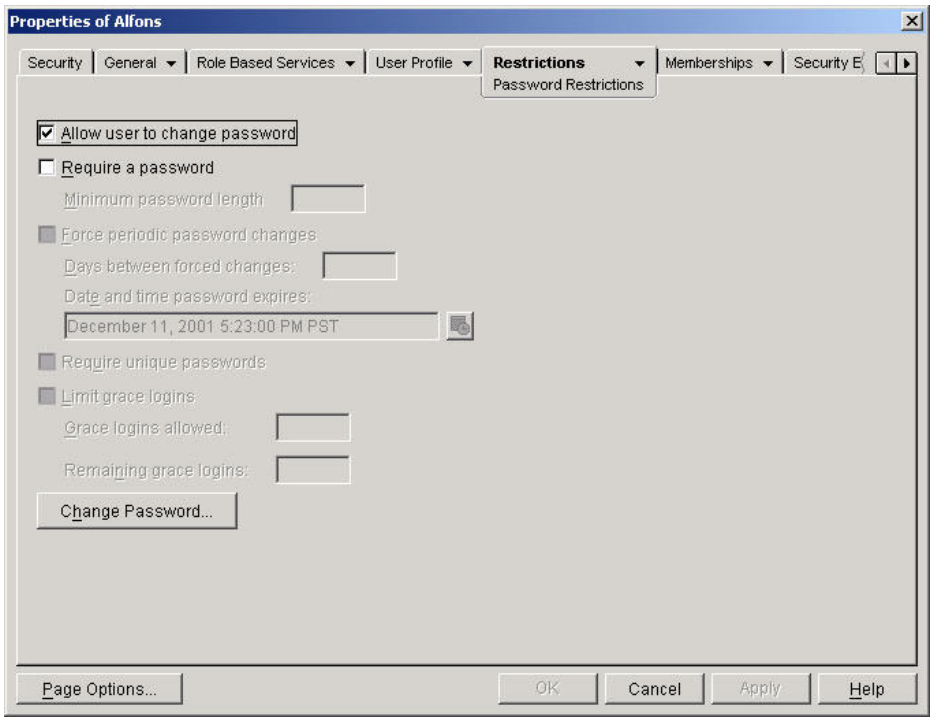


Abbildung: Eigenschaften von Alfons

Außerdem gibt es die Möglichkeit, Benutzerkonten direkt zu deaktivieren oder sie nach Ablauf einer bestimmten Zeit automatisch deaktivieren zu lassen.

Clientsoftware sicher konfigurieren

Die Sicherheit eines eDirectory-Systems hängt außerdem von der Sicherheit der zum Zugriff benutzten Clientsoftware ab. Daher müssen für die sichere Konfiguration eines eDirectory-Systems auch die Client-seitigen Rechner und Programme einbezogen werden. Empfehlungen hierzu sind gesondert in Maßnahme M 4.156 *Sichere Konfiguration der Novell eDirectory Clientsoftware* zusammengefasst. Besondere Schutzmaßnahmen sind für die administrativen Zugänge zum eDirectory zu realisieren.

Replikationskonzept erstellen

Ein eDirectory-System besteht in der Regel nicht nur aus einem eDirectory-Server, sondern aus einem ganzen Serververbund (siehe auch M 2.236 *Planung des Einsatzes von Novell eDirectory*). Die Verzeichnisdatenbank kann dabei in Form von einzelnen Partitionen auf verschiedene Server verteilt werden. Weiterhin können die einzelnen Server die Verzeichnisdatenbanken untereinander replizieren. Dadurch, dass mehrere Kopien einer Datenbank-Partition auf unterschiedlichen Servern vorliegen, kann eine Lastverteilung erreicht werden. Damit die Aktualität der Verzeichniskopien sichergestellt ist, müssen Veränderungen an den Daten zwischen den Servern ausgetauscht werden. Es muss daher ein Replikationskonzept erstellt werden. Unter anderem sind dabei folgende Aspekte zu berücksichtigen:

- Welcher Server hält die Master-Replica einer eDirectory-Partition?
- Welche Replikationstypen werden konfiguriert?
- Auf welche Server soll das eDirectory-Verzeichnis repliziert werden?
- Welche Informationen des eDirectory-Verzeichnisses sollen repliziert werden (Definition von Filtern)?
- Sollen Änderungen an Replikaten des Verzeichnisses erlaubt sein und sollen diese auf das Original übertragen werden (Definition als Typ *Read/Write* oder als *Read-Only*)?

Da ein System in der Regel ständig Veränderungen durch den laufenden Betrieb unterworfen ist, muss auch die Sicherheit permanent überprüft und neu konfiguriert werden. Hinweise dazu finden sich in M 4.159 *Sicherer Betrieb von Novell eDirectory*.

Ergänzende Kontrollfragen:

- Sind alle Server gemäß der ihnen zugedachten Rolle konfiguriert?
- Werden die geplanten Protokolleinstellungen umgesetzt?
- Sind notwendige Änderungen an den Zertifikats-Parametern umgesetzt und getestet?

M 4.156 Sichere Konfiguration der Novell eDirectory Clientsoftware

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Nach der Planung und Installation eines eDirectory-Systems (siehe M 2.236 *Planung des Einsatzes von Novell eDirectory*) muss das Verzeichnissystem inklusive seiner Clientsoftware auf den relevanten Rechnern konfiguriert werden.

Aufgrund der Vielzahl möglicher Applikationen und Dienste, die als Clientsoftware für eDirectory in Betracht kommen, wird im Folgenden nicht detailliert auf spezifische Konfigurationsmöglichkeiten eingegangen. Unter anderem ist es auch möglich, eigene Clientsoftware zu erstellen, die mit eDirectory über die standardisierte LDAP-Schnittstelle kommuniziert.

Die folgenden, generischen Hinweise sollten in jedem Fall beachtet werden:

- Zur Absicherung der jeweiligen Client-Installation sind die relevanten Maßnahmen der IT-Grundschutzhand-Kataloge für das jeweilige zugrunde liegende Betriebssystem anzuwenden.
- Soll die Clientsoftware zum eDirectory eine mittels SSL geschützte LDAP-Verbindung aufbauen, muss der Client ein entsprechendes Wurzelzertifikat erhalten, anhand dessen er die Authentizität des SSL-Serverzertifikats überprüfen kann.

Die Administration von eDirectory erfolgt über das Programm *ConsoleOne* von einem Client aus. Die Sicherheit der eDirectory-Installation hängt auch von der Integrität der zur Administration verwendeten Clients ab. Die Absicherung dieser Clients ist daher besonders wichtig.

Integrität des Betriebssystems

Zum einen muss für administrativ genutzte Clientsoftware die Integrität der jeweiligen Betriebssystemplattform geschützt werden. Dafür können z. B. Zugriffsbeschränkungen auf Systemdateien eingerichtet werden, sofern solche Beschränkungen nicht bereits in der Voreinstellung des Betriebssystems vorhanden sind. Neben dem Schutz der unterliegenden Betriebssystemplattform des Clients ist auch ein Schutz der Administrationssoftware selbst erforderlich. Durch die Vergabe geeigneter Zugriffsbeschränkungen müssen die Verzeichnisse, in denen die *ConsoleOne* und die entsprechende Zusatzsoftware installiert sind, vor Manipulationen oder Überschreiben geschützt werden.

Speziell für den *Novell Client für Windows* ist das Zusatzmodul NMAS (Novell Modular Authentication Services) verfügbar. Dies erlaubt die Konfiguration zusätzlicher Authentisierungsmethoden (z. B. mittels Smartcard, Biometrie, RADIUS-Protokoll) für den Zugriff auf das eDirectory. Auch Kombinationen von Authentisierungsmethoden sind nutzbar. Auf Seite des eDirectory lassen sich bei Verwendung dieses Moduls Zugriffsrechte in Abhängigkeit der verwendeten Authentisierungsmethode konfigurieren.

M 4.157 Einrichten von Zugriffsberechtigungen auf Novell eDirectory

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der Verzeichnisdienst eDirectory speichert in der Regel sehr viele sensitive Unternehmens- und Benutzerdaten. Es ist deshalb unerlässlich, diese Informationen nur ausdrücklich autorisierten Applikationen, Benutzern und Administratoren zugänglich zu machen. Dazu ist es notwendig, eine zuvor erstellte Sicherheitsrichtlinie, die Regelungen für die Zugriffsberechtigungen enthalten muss (siehe M 2.238 *Festlegung einer Sicherheitsrichtlinie für Novell eDirectory*), konsequent und konsistent umzusetzen.

Access Control

Die Rechtevergabe erfolgt bei eDirectory über *Access Control Lists* (ACLs). Zugriffsberechtigungen können dabei sowohl auf Objekt- als auch auf Attributsebene vergeben werden. Folgende Objektrechte (bzw. Privilegien) stehen zur Verfügung: *Browse, Create, Delete, Rename* und *Supervisor*. Attributsrechte sind: *Compare, Read, Add or Delete Self, Write, Supervisor* sowie *Inheritance Control*. Rechte können grundsätzlich nur im positiven Sinne vergeben werden, d. h. der Zugriff wird explizit erlaubt. Ein ausdrücklicher Ausschluss eines Benutzers mittels einer Zugriffsliste kann nicht definiert werden.

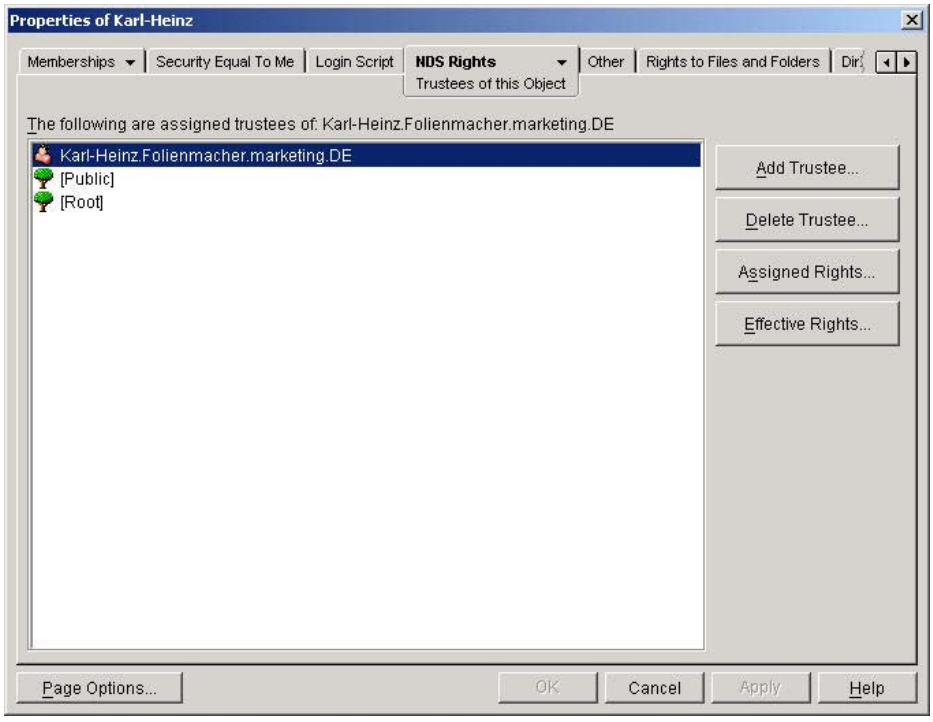


Abbildung: Rechtevergabe unter Novell eDirectory

Trustee Assignments

Zugriffsberechtigungen werden explizit durch so genannte *Trustee-Assignments* vergeben. Für ein Zielobjekt wird dabei eingetragen, welche weiteren Objekte darauf zugreifen dürfen, d. h. *Trustees* dieses Zielobjekts sind. Umgekehrt kann man auch die Sicht eines zugreifenden Objekts einnehmen und so ablesen, auf welche Zielobjekte dieses Objekt zugreifen darf.

Inherited Rights Filter

Zugriffsberechtigungen vererben sich entsprechend der Baumhierarchie des Verzeichnisdienstes. Dies gilt allerdings zunächst nur für die Objektrechte, die Attributsrechte vererben sich nur, wenn dies explizit konfiguriert wird. Die automatische Vererbung von Zugriffsberechtigungen von Objekten auf deren Kindobjekte kann reglementiert werden durch die Konfiguration so genannter Masken oder *Inherited Rights Filter* (IRF). Damit lässt sich die Vererbung der Zugriffsberechtigungen einschränken. Da über das *Self*-Recht eigene Attributswerte verändert werden können, ist es aus Sicherheitssicht kritisch und sollte ebenfalls mit Hilfe des Filters kontrolliert werden.

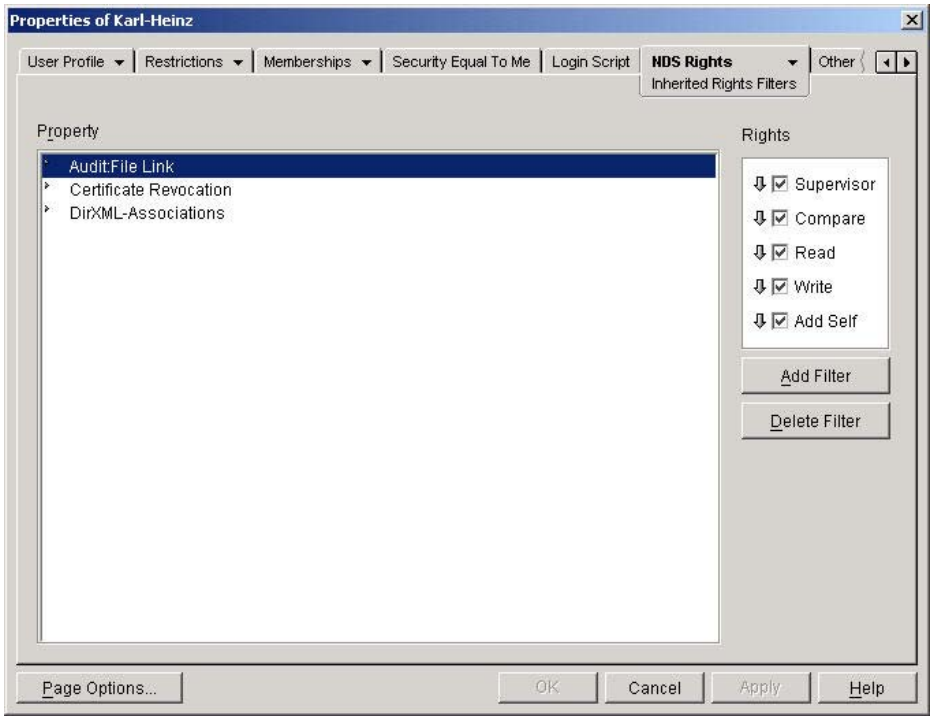


Abbildung: Rechte zuweisen

Bei einer Partitionierung des Verzeichnisbaums entsteht zunächst eine Lücke in der Vererbungskette, welche allerdings automatisch durch das Anhängen einer *inherited ACL* geschlossen wird.

Sicherheitsäquivalenz

Eine weitere Möglichkeit zur Vergabe von Zugriffsberechtigungen auf eDirectory-Objekte besteht in der Zuweisung einer so genannten Sicherheitsäquivalenz eines Objektes zu einem anderen Objekt. So kann definiert werden, dass auf Objekt X zumindest die gleichen Zugriffsmöglichkeiten existieren wie auf Objekt Y. Sämtliche Trustees von Objekt Y werden damit automatisch auch zu Trustees von Objekt X.

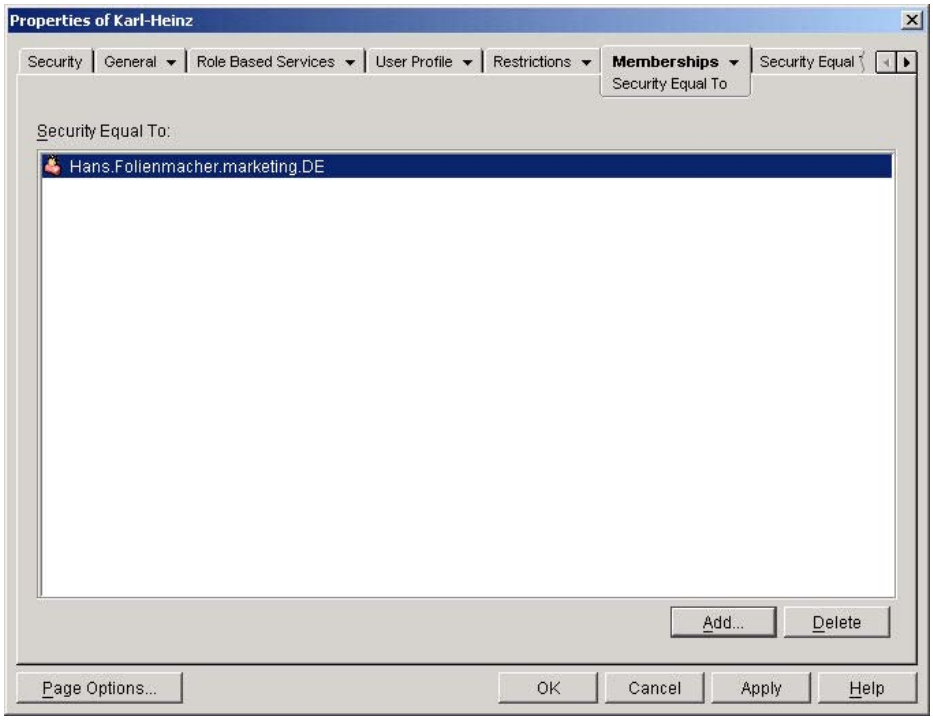


Abbildung: Gruppen-Mitgliedschaften einrichten

effektive Rechte

Wirksam bei einem Zugriffsversuch werden die so genannten *effektiven Rechte*, d. h. diejenigen Zugriffsberechtigungen, die sich gemäß den oben genannten Mechanismen als Endresultat ergeben. Diese effektiven Rechte werden bei jedem Zugriff dynamisch berechnet bzw. im Cache des Servers gehalten. Der Administrator hat über die Managementkonsole *ConsoleOne* die Möglichkeit, sich diese aktuell gültigen effektiven Rechte auf einzelne Objekte anzeigen zu lassen.

Organizational Roles verwenden

Ein wichtiger Aspekt bei der Rechtevergabe im eDirectory ist die Konfiguration der Benutzer und der Benutzergruppen (Organizational Roles). Durch geeignete Definition der Benutzer- und Administratorgruppen lässt sich die Rechtevergabe transparenter und einfacher gestalten. Dies ist zu empfehlen, da generell eine hohe Komplexität in der Administration die Gefahr durch Fehlkonfigurationen erhöht. Zur vereinfachten und konsistenten Konfiguration der Benutzer und Benutzergruppen (Organizational Roles) sollten *Templates* (Vorlagen) verwendet werden.

Role Based Service

eDirectory erlaubt eine rollen- und funktionsbasierte Administration. Dazu werden so genannte RBS-Objekte (*Role Based Service*) und anschließend RBS-Jobobjekte sowie RBS-Funktionsobjekte definiert. Dies erfordert eine Schemaerweiterung des Verzeichnisdienstes. Mit Hilfe der RBS-Funktionsobjekte werden die Aufgaben definiert, die von Mitgliedern einer zugewiesenen Benutzergruppe (Administratorengruppe) durchgeführt werden können. Auf diese Weise wird auch die Delegation von Administrationsaufgaben ermöglicht.

Bei einer eventuellen Zusammenführung zweier oder mehrerer eDirectory-Bäume zu einem Gesamtbaum sind anschließend die resultierenden effektiven Rechte zu kontrollieren. Auch bei der Verschiebung von Partitionen innerhalb eines eDirectory-Baums ist dies zu berücksichtigen. Ebenso müssen die Zugriffsberechtigungen kontrolliert und eventuell nachkonfiguriert werden, wenn z. B. eine Windows NT-Domäne in einen eDirectory-Baum durch Migration übernommen wurde.

Ergänzende Kontrollfragen:

- Wurden die Zugriffsrechte der Benutzer- und Administratorgruppen gemäß der erstellten Sicherheitsrichtlinie konfiguriert?
- Wurden die sich tatsächlich ergebenden effektiven Rechte auf die Zielobjekte stichprobenartig kontrolliert?
- Sind die Administratorrollen und die Delegation von Administrationsrechten konsistent konfiguriert?

M 4.158 Einrichten des LDAP-Zugriffs auf Novell eDirectory

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

LDAP (Lightweight Directory Access Protocol) ist ein Protokoll zum Zugriff auf Daten eines Verzeichnisdienstes. LDAP wurde ursprünglich als Alternative zu DAP (Directory Access Protocol) entwickelt, das im Rahmen des X.500-Directory-Standards definiert wurde. Das zugrunde liegende Datenmodell und die innerhalb des Protokolls möglichen Operationen wurden dabei im Wesentlichen vom X.500-Standard übernommen. Die aktuelle Version des Protokolls, LDAP Version 3, hat sich inzwischen zum dominierenden Standard für den Zugriff auf Verzeichnisdienste entwickelt.

eDirectory verfügt über eine LDAP-Schnittstelle. Dies ermöglicht z. B. die folgenden Einsatzszenarien:

Einsatz im Internet

- eDirectory wird im Internet platziert, z. B. als so genannte eBusiness-Plattform oder einfach als Zertifikatsdatenbank. Die Benutzer greifen über das Internet mit Hilfe eines geeigneten, LDAP-fähigen Software-Clients darauf zu.

Einsatz im Intranet

- eDirectory wird im Intranet einer Organisation zur Verwaltung von Benutzerkonten oder Ressourcen im Netz eingesetzt. Dann sind neben direkten Benutzerzugriffen über einen LDAP-Client auch Zugriffe von Netzapplikationen möglich. Außer über die Novell-eigenen Protokolle können diese Zugriffe ebenso über die LDAP-Schnittstelle erfolgen.

In beiden Fällen ist der LDAP-Zugriff entsprechend der zuvor definierten Sicherheitsrichtlinie (siehe M 2.238 *Festlegung einer Sicherheitsrichtlinie für Novell eDirectory*) zu konfigurieren.

Anonymer LDAP-Zugriff

eDirectory erlaubt prinzipiell eine anonyme Anmeldung von LDAP-Clients. In der Voreinstellung hat dabei der LDAP-Client die Zugriffsrechte, die für das Objekt [Public] im eDirectory eingetragen sind. Das Objekt [Public] ist ein virtuelles Objekt, das lediglich der Rechtevergabe im eDirectory dient. Jeder Zugriff auf Objekte im Verzeichnisbaum erfolgt automatisch mindestens mit den Rechten, die diesem Objekt eingeräumt werden.

In der Voreinstellung verfügt [Public] über das Recht *Browse* auf dem gesamten Baum.

Proxy-User

Sollen anonymen Benutzern auf einzelne Teilbereiche des Verzeichnisbaums weitergehende Zugriffe eingeräumt werden, so sollte dafür ein gesondertes Benutzerkonto angelegt werden. Dieses Benutzerkonto muss dann als so genannter *Proxy-User* für den anonymen LDAP-Zugriff eingetragen werden. Dieses Konto darf kein Passwort erfordern, damit ein anonymer Zugang möglich ist. Es muss ferner darauf geachtet werden, dass dieses Benutzerkonto auch kein Passwort einrichten kann, da der anonyme Zugang sonst durch einen einzelnen Client blockiert werden könnte.

Bereits bei der Planung des Einsatzes eines Verzeichnisdienstes muss entschieden werden, welche Daten über eine anonyme Anmeldung zugänglich sein dürfen (siehe auch M 2.238 *Festlegung einer Sicherheitsrichtlinie für Novell eDirectory*). Entsprechend dieser Entscheidung müssen die Zugriffsrechte für den Proxy-User im eDirectory konfiguriert werden.

Abbildung: Zugriffsrechte für Proxy-User

Einsatz von Novell eDirectory als LDAP-Server im Internet

LDAP-Server durch Firewall schützen

Wird eDirectory als LDAP-Server im Internet eingesetzt, so sollten die entsprechenden Server durch eine Firewall geschützt werden. Diese sollte so konfiguriert werden, dass nur die zum Betrieb der LDAP-Server notwendigen Datenpakete zu den LDAP-Servern weitergeleitet werden. Meist wird es sich dabei um TCP-Pakete an die Ports 389 und 636 handeln, die standardisierten Port-Nummern für LDAP bzw. LDAP über SSL.

Für Daten, auf die nicht anonym zugegriffen werden darf, ist eine Authentisierung des jeweiligen LDAP-Clients notwendig. Das Ergebnis einer erfolgreichen Authentisierung ist ein *NDS User Bind* des LDAP-Clients an das eDirectory. Der jeweilige Client authentisiert sich also als im eDirectory-Verzeichnis eingetragener Benutzer.

Keine Klartext-Kennwörter über das Internet übertragen

Um zu verhindern, dass Kennwörter im Klartext über das Internet übertragen werden, sollte für die entsprechende LDAP-Gruppe der Schalter *allowing cleartext passwords* nicht gesetzt sein (siehe auch M 5.97 *Absicherung der Kommunikation mit Novell eDirectory*). Dies entspricht auch der Voreinstellung von eDirectory. Mit dieser Einstellung sind anonyme LDAP-Verbindungen ebenso möglich wie eine Benutzeranmeldung mit LDAP über SSL.

Grundsätzlich wird empfohlen, SSL für die Kommunikation und Übertragung einzusetzen. Hierbei werden die Optionen *ein-* sowie *zweiseitige Authentisierung* unterstützt. Zweiseitige Authentisierung bedeutet, dass auch der Client in Besitz eines gültigen Zertifikats sein muss und dass auf Basis des zugehörigen privaten Schlüssels ein *Session-Key* generiert wird. Dies ist die sicherste Konfiguration. Alternativ kann die Client-Authentisierung jedoch auch über ein Passwort erfolgen. Durch die Verwendung einer verschlüsselten SSL-Verbindung zum Server ist die Vertraulichkeit des Passworts bei der Übertragung gewährleistet. In jedem Fall müssen die Benutzer das CA-Wurzelzertifikat in ihren LDAP-Client, z. B. einen Browser, importieren, damit die eingerichteten Vertrauensbeziehungen auch lokal nachvollzogen werden können.

Wird kein SSL verwendet, so können die Benutzerpasswörter im Klartext über das Internet an das eDirectory übertragen werden (siehe auch M 5.97 *Absicherung der Kommunikation mit Novell eDirectory*). Dies sollte aber vermieden werden. Um es ausdrücklich zu unterbinden, muss die Option *allowing cleartext passwords* auf *disabled* geschaltet sein.

Konfiguration des LDAP-Zugriffes bei Schemaänderungen

Welche LDAP-Objekte entsprechen welchen eDirectory-Objekten?

eDirectory bietet die Möglichkeit, die innerhalb von LDAP verwendeten standardisierten Objektklassen auf andere im eDirectory intern verwendete Objektklassen abzubilden. Diese Eigenschaft wird relevant, wenn LDAP-Clients bei der Suche standardisierte LDAP-Objektklassen verwenden, die entsprechenden Daten sich jedoch in Attributen von eDirectory-Objektklassen mit anderen Namen befinden. Bei der erstmaligen Verwendung von LDAP-Clients oder bei Änderungen des eDirectory-Schemas sollte daher überprüft werden, ob die Abbildung der LDAP-Objektklassen auf eDirectory-Objektklassen schlüssig ist und die verwendeten LDAP-Applikationen damit korrekt funktionieren.

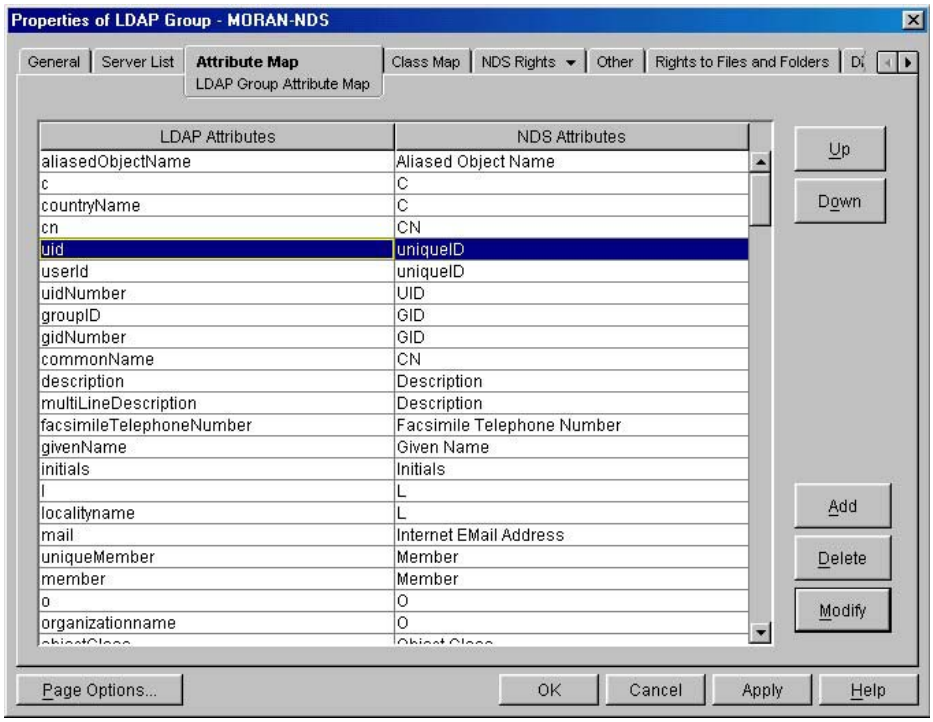


Abbildung: Eigenschaften der LDAP-Gruppe

Ergänzende Kontrollfragen:

- Sind alle eDirectory-Server, die vom Internet aus über LDAP angesprochen werden können, durch eine Firewall geschützt?
- Auf welche Bereiche des eDirectory-Verzeichnisdienstes hat das Benutzerkonto [Public] Zugriff?
- Falls ein Proxy-User für die LDAP-Gruppe konfiguriert wurde, sind die Zugriffsrechte für diesen Proxy-User hinreichend restriktiv vergeben?

M 4.159 Sicherer Betrieb von Novell eDirectory

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Die Sicherheit eines komplexen Systems muss im Betrieb permanent aufrecht erhalten werden, da sich im laufenden Betrieb notwendige Veränderungen ergeben. Es genügt daher nicht, eine sichere Anfangskonfiguration einzustellen (siehe M 4.153 *Sichere Installation von Novell eDirectory*, M 4.155 *Sichere Konfiguration von Novell eDirectory* sowie die entsprechenden Maßnahmen M 4.154 *Sichere Installation der Novell eDirectory Clientsoftware* und M 4.156 *Sichere Konfiguration der Novell eDirectory Clientsoftware*).

Nach der Installation und erstmaligen Konfiguration gemäß den im Vorfeld festgelegten eDirectory-Konzepten und Sicherheitsrichtlinien erfolgt der Betrieb von eDirectory-Servern in der Regel im Netzverbund. Die Sicherheit eines solchen Netzes hängt dabei einerseits von der anfangs eingestellten Konfiguration ab. Sie wird jedoch auch maßgeblich durch die Art und Weise der Konfigurationsänderungen bestimmt, die im laufenden Betrieb erfolgen müssen. Dabei sind insbesondere auch Seiteneffekte zu berücksichtigen, die unter Umständen unbeabsichtigt zu Sicherheitslücken führen können.

Folgende Aspekte sind im laufenden Betrieb für ein eDirectory-Verzeichnissystem aus Sicht der IT-Sicherheit zu beachten:

Verfügbarkeit des eDirectory-Zertifikatsservers sicherstellen

- Der eDirectory-Zertifikatsserver spielt eine wesentliche Rolle für die Zugriffskontrollmechanismen des Verzeichnisses. Der Zertifikatsserver wird auf dem ersten eDirectory-Server eines eDirectory-Baums installiert. Für jedes neue Objekt im eDirectory wird automatisch ein eigenes Schlüsselpaar generiert und auf dem Zertifikatsserver abgelegt. Der sichere Betrieb dieses "ersten eDirectory-Servers" im Baum ist deshalb besonders wichtig. Zu schützen sind nicht nur die sensitiven Daten, die sich auf diesem befinden, sondern vor allem auch dessen Verfügbarkeit. Es ist deshalb dringend anzuraten, die Replizierung des eDirectory auf verschiedene Server zu konfigurieren, insbesondere sollte wenigstens eine vollständige *Read/Write-Replica* existieren. Wird der "Hauptserver" aus einem wichtigen Grund heruntergefahren oder fällt dieser dauerhaft aus, so kann die nächstgelegene *Read/Write-Replica* zur *Master-Replica* erklärt und der Betrieb damit aufrecht erhalten werden.

Sichere Aufstellung der Server und Netzkomponenten

- Die Sicherheit eines IT-Systems basiert immer auch auf der physikalischen Sicherheit der Server und Netzkomponenten. Diese muss auch für den Betrieb von eDirectory sichergestellt sein. Entsprechende Maßnahmen finden sich in Schicht 2, beispielsweise in den Bausteinen B 2.4 *Serverraum* oder B 2.9 *Rechenzentrum*.

Sicherheitseinstellungen nach Änderungen anpassen

- Veränderungen in einem eDirectory-Verzeichnissystem ergeben sich insbesondere dann, wenn fremde eDirectory- oder LDAP-Verzeichnisse in einen bestehenden eDirectory-Baum importiert werden. Diese neu importierten Verzeichnisse sind in der Regel noch nicht in die bestehenden Sicherheitsstrukturen eingebunden. Damit die definierte

Sicherheitsrichtlinie auch weiterhin konsistent umgesetzt ist, muss die Konfiguration der Sicherheitseinstellungen umgehend nachgeholt werden. Die Berechtigungen zum Import neuer Verzeichnisse und zum Erzeugen von Verzeichnis-Repliken müssen restriktiv vergeben werden.

- Um den Sicherheitszustand eines Systems nachvollziehen zu können, ist es notwendig, dieses zu überwachen. Ziel einer solchen Überwachung ist es, Verstöße gegen die geltenden Sicherheitsvorschriften zu entdecken, bestehende Sicherheitslücken aufzudecken oder Fehlkonfigurationen, die potentiell zu Sicherheitslücken führen können, zu erkennen. Ein entsprechendes Überwachungskonzept ist dabei auch als Teil des Sicherheitskonzeptes anzusehen. Komplexe Systeme wie eDirectory können in der Regel nicht mehr durch einzelne Administratoren überwacht werden, sondern die Überwachung muss automatisch durch entsprechende Systemkomponenten oder Produkte von Drittherstellern erfolgen. Dabei ist auch die Konfiguration der Systemüberwachung regelmäßig an das sich verändernde System anzupassen. Die Empfehlungen zur Überwachung sind in M 4.160 *Überwachen von Novell eDirectory* zusammengefasst.

Überwachung von eDirectory

- Ein wichtiger Aspekt der Systemsicherheit eines eDirectory-Systems ist die konsistente Verwaltung von Benutzern und Berechtigungen. Das administrative Konzept hat dabei Auswirkungen auf die Komplexität der durchzuführenden Aufgaben. Da es bei komplexen Abläufen leicht zu Fehlern kommen kann, sollten die administrativen Aufgaben möglichst einfach gestaltet werden. Dies trägt zur Aufrechterhaltung eines sicheren Systemzustands bei. Deshalb ist ein gruppenbasiertes Zugriffskonzept unerlässlich. Dadurch wird die Verwaltung von Zugriffsrechten auf Datenbanken wesentlich vereinfacht und weniger fehleranfällig.

gruppenbasiertes Zugriffskonzept

Auch unter Sicherheitsgesichtspunkten ist es wichtig, dass alle den Betrieb eines eDirectory-Systems betreffenden Richtlinien, Regelungen und Prozesse dokumentiert werden. Dazu sollten Betriebshandbücher erstellt und bei Systemänderungen aktualisiert werden. Da die Betriebshandbücher sicherheitsrelevante Informationen enthalten, sind sie so aufzubewahren, dass Unbefugte keinen Zugriff auf sie erlangen können. Befugte Administratoren sollten die Handbücher jedoch leicht einsehen können.

Dokumentation aller Regelungen und Arbeitsvorgänge

Die aufgeführten Empfehlungen können an dieser Stelle nur allgemeinen Charakter haben, da die Aufrechterhaltung der Systemsicherheit auch von lokalen Gegebenheiten abhängt. Daher müssen schon in der Planungsphase eines eDirectory-Verzeichnisbaums entsprechende Richtlinien zum sicheren Betrieb erstellt werden, die die lokalen Anforderungen berücksichtigen. Unter Umständen kann es auch vorkommen, dass bestimmte Mechanismen nicht optimal sicher konfiguriert werden können. Dies ist z. B. der Fall, wenn "alte" Applikationen weiter betrieben werden müssen, die nur auf schwache oder keine Authentisierung ausgelegt sind. Hier muss dann durch alternative Gegenmaßnahmen an anderer Stelle, z. B. auf organisatorischer Ebene, eine angemessene Sicherheit erreicht werden.

Potentielle Sicherheitslücken können nur von kompetenten Administratoren entdeckt bzw. vermieden werden. Daher ist die Schulung und Fortbildung der Systemverwalter eine wichtige Schutzmaßnahme (siehe auch M 3.29 *Schulung zur Administration von Novell eDirectory*). Daneben müssen auch

Konsequente Schulung aller Administratoren

die normalen Benutzer in Sicherheitsaspekten geschult werden (siehe auch M 3.30 *Schulung zum Einsatz von Novell eDirectory Clientsoftware*), damit potentielle Gefahren bekannt sind und die zur Verfügung stehenden Sicherheitsmechanismen richtig eingesetzt werden können.

Sicherheitseinstellungen regelmäßig prüfen

Die Sicherheitseinstellungen und die Protokolldateien eines Servers sollten regelmäßig überprüft werden. Dies kann manuell oder werkzeuggestützt erfolgen. Anderenfalls besteht die Gefahr, dass Abweichungen von den Sicherheitsrichtlinien und Sicherheitsprobleme nicht frühzeitig erkannt und dadurch auch nicht rechtzeitig behoben werden (siehe auch M 4.160 *Überwachen von Novell eDirectory*).

Beispiel: gruppenbasiertes Zugriffskonzept

Ein Mitarbeiter wechselt die Abteilung, wodurch eine Anpassung der Zugriffsrechte erforderlich ist. Werden benutzerbezogene *Access Control Lists* (ACLs) genutzt, so muss jedes Verzeichnis überprüft werden, um den Benutzer gegebenenfalls aus der ACL auszutragen bzw. neu einzutragen. Werden dagegen gruppenbezogene ACLs verwendet, so muss der Benutzer lediglich in der Benutzerverwaltung aus den relevanten Gruppen aus- bzw. eingetragen werden. Die Änderung kann zentral am Benutzer-Objekt erfolgen.

Ergänzende Kontrollfragen:

- Sind alle Betriebsabläufe dokumentiert?
- Werden die Systemprotokolle regelmäßig kontrolliert?
- Ist der Zugriff auf alle Administrationswerkzeuge für normale Benutzer unterbunden worden?

M 4.160 Überwachen von Novell eDirectory

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator, Revisor

Um den Sicherheitszustand eines Systems nachvollziehen zu können, ist es notwendig, dieses kontinuierlich zu überwachen. Ziel einer solchen Überwachung ist es, Verstöße gegen die geltenden Sicherheitsvorschriften zu entdecken, bestehende Sicherheitslücken aufzudecken oder Fehlkonfigurationen, die zu Sicherheitslücken führen können, zu erkennen. Ein entsprechendes Überwachungskonzept ist dabei auch als Teil des Sicherheitskonzeptes anzusehen.

automatische Überwachung

Komplexe Systeme wie eDirectory können dabei in der Regel nicht mehr durch einzelne Administratoren überwacht werden, sondern die Kontrolle muss automatisch durch entsprechende Systemkomponenten oder Produkte von Drittherstellern erfolgen. Dabei ist auch die Konfiguration der Systemüberwachung regelmäßig an das sich verändernde System anzupassen.

eDirectory stellt für die Systemüberwachung das Werkzeug *iMonitor* zur Verfügung. Dies ist eine Client-Server-Anwendung, bei der auf einigen (oder allen) eDirectory-Servern der iMonitor-Dienst läuft. Die Clients können über einen Browser darauf zugreifen, der hierfür HTML Version 3 unterstützen muss. Der Zugreifende muss sich gegenüber den iMonitor-Services authentisieren und erhält nach erfolgreicher Erkennung Zugriff auf die iMonitor-Daten, wobei die für ihn konfigurierten Rechte gelten.

Monitor-Zugruff nur über SSL

Die Informationen, die der iMonitor-Dienst über einen eDirectory-Server zur Verfügung stellt, könnten u. U. von Unbefugten dazu genutzt werden, gezielt nach Sicherheitslücken in einer bestehenden eDirectory-Installation zu suchen. Aus diesem Grund wird empfohlen, den Zugriff auf den iMonitor-Dienst nur mit aktivierter SSL-Verschlüsselung zu erlauben, besonders wenn von außerhalb des eigenen Behörden- bzw. Unternehmensnetzes aus zugegriffen werden kann. Dazu muss auf dem Client das entsprechende Server-Zertifikat in den Browser importiert werden.

direkter Modus oder Proxymodus für iMonitor-Zugriff

Es gibt zwei verschiedene Operationsmodi des iMonitor-Zugriffs: den *direkten Modus* und den *Proxymodus*. Beim direkten Modus ist der Browser direkt mit dem eDirectory-Server verbunden, dessen Statusdaten abgefragt werden. Auf dem eDirectory-Server müssen dabei die iMonitor-Services aktiviert sein. Beim Proxymodus wird auf einen Server zugegriffen, auf dem die iMonitor-Services zur Verfügung stehen, die eigentliche Information wird aber von einem anderen Server abgefragt.

Der direkte Modus besitzt gegenüber dem Proxymodus u. a. den Vorteil, dass er weniger Bandbreite benötigt und die serverzentrierten Funktionalitäten in vollem Umfang zur Verfügung stehen. Aus Sicht der IT-Sicherheit ist jedoch der Proxymodus zu bevorzugen, damit nicht alle eDirectory-Rechner diese direkte Zugriffsmöglichkeit gestatten. Dabei sollte eine feste Einwahladresse verwendet werden, die dann entsprechend kontrolliert und geschützt werden muss.

Das *NDS Trace Utility* dient der Erfassung eDirectory-spezifischer Ereignisse in eine eigene Protokolldatei. Damit kann eine Protokollierung sämtlicher

eDirectory-Ereignisse erreicht werden. Ferner gibt es das Zusatzmodul NAAS (Novell Advanced Auditing Service), womit sich eine automatisierte Auswertung der eDirectory-spezifischen Ereignisse realisieren lässt.

Im Rahmen der Überwachung sind auch folgende Aspekte zu beachten:

- Der Datenschutzbeauftragte und der Personal- bzw. Betriebsrat sollten frühzeitig in die Planung mit einbezogen werden, da eine Überwachung meist auch personenbezogene Daten erfassen muss, damit im Fall einer Sicherheitsverletzung zuverlässig der Verursacher festgestellt werden kann.
- Neben den eDirectory-spezifischen Ereignissen müssen auch Ereignisse des Betriebssystems beobachtet und protokolliert werden, um ein vollständigeres Bild über die Systemabläufe zu erhalten. Empfehlungen und Hinweise zur Protokollierung auf Betriebssystem-Ebene finden sich in den jeweiligen Bausteinen.
- Eine zentrale Sammelstelle für Protokolldateien mit entsprechend automatisierter Auswertung kann durch Produkte von Drittherstellern aufgebaut werden. Wird ein Werkzeug zum Netz- und Systemmanagement eingesetzt (siehe auch Baustein B 4.2 *Netz- und Systemmanagement*), so ist es - je nach Produkt - möglich, die eDirectory-Protokolle direkt in dieses Werkzeug zu integrieren.

Tools können Auswertung erleichtern

- Durch die Überwachung fallen je nach Einstellung große Datenmengen an. Diese müssen nicht nur regelmäßig ausgewertet, sondern aus Platzgründen auch gelöscht oder auf andere Datenträgern ausgelagert werden. Zusätzlich führt eine intensive Überwachung u. U. zu Performanceverlusten. Dadurch kann ein Server unter Umständen so überlastet werden, dass ein geregelter Betrieb nicht mehr möglich ist. Aus diesem Grund müssen die geeigneten Überwachungsparameter im Rahmen eines Testbetriebs überprüft und gegebenenfalls angepasst werden. Es ist zu beachten, dass die Anpassung auch Einfluss auf das gesamte Überwachungskonzept haben kann, da bestimmte Überwachungsaufgaben u. U. nicht mehr durchführbar sind. Dies gilt besonders, wenn zusätzliche Produkte eingesetzt werden, die hohe Voraussetzungen an die protokollierten Ereignisse stellen. Beispiele hierfür sind Programme, die eine automatische Analyse der Protokolldaten auf Verhaltensanomalien, etwa für die Erkennung von Angriffen, durchführen.

Nicht zu viel und nicht zu wenig protokollieren!

Im Rahmen der Überwachung der Systemfunktionen empfiehlt sich außerdem eine regelmäßige Kontrolle der eDirectory-Replikation, durch die Konfigurationsänderungen weitergeleitet werden. Fehler in der Replikation haben meist zur Folge, dass Konfigurationsänderungen nicht überall durchgeführt werden und so z. B. einem Benutzer zu viele Rechte zugestanden werden.

Ergänzende Kontrollfragen:

- Wurde ein bedarfsgerechtes Überwachungskonzept entworfen und umgesetzt?
- Werden wichtige Systemereignisse protokolliert?
- Wurden Überwachungseinstellungen für wichtige Systemdateien konfiguriert?

M 4.161 Sichere Installation von Exchange/Outlook 2000

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Eine sichere Software-Installation ist immer eine Grundvoraussetzung für den reibungslosen und sicheren Betrieb des Systems. Vor der Installation von Exchange/Outlook sollte zunächst eine Sicherungskopie der bestehenden E-Mail-Daten angelegt und sorgfältig verwahrt werden. Dies ist sowohl auf der Server-Seite (z. B. durch ein Backup der Daten einer früheren Exchange-Version) als auch auf der Client-Seite notwendig.

In diesem Dokument werden Empfehlungen zu folgenden Themen in Bezug auf Exchange gegeben:

- Vorbereitung der Installation
- Installation
- Abschluss der Installation

Weiterhin werden in dieser Maßnahme auch Empfehlungen zur Installation von Outlook 2000 gegeben. Diese betreffen vor allem die Vorkonfiguration von Outlook 2000 mittels des Microsoft Office 2000 *Custom Installation Wizard*s.

Vorbereitung der Installation von Exchange 2000

Updates und Patches einspielen

Eine der Voraussetzungen für einen sicheren Betrieb von Exchange/Outlook 2000 ist die sichere Konfiguration des jeweils zugrunde liegenden Betriebsystems - Windows 2000 Server bzw. Professional. Das aktuelle Service Pack und alle verfügbaren Sicherheitsupdates bzw. -patches müssen installiert werden. Mehr über die sichere Installation, Konfiguration und Betrieb von Windows 2000 Server bzw. Professional kann den entsprechenden Bausteinen zu Windows 2000 entnommen werden (z. B. M 4.150 *Konfiguration von Windows 2000 als Workstation* oder M 4.139 *Konfiguration von Windows 2000 als Server)*.

Aus Integritätsgründen wird empfohlen, die Exchange-Installation auf einer eigenen Partition oder, wenn möglich, auf einer separaten Festplatte vorzunehmen. Als Dateisystem muss NTFS zum Einsatz kommen.

Installation als Member-Server

Es wird empfohlen, den Exchange-Server als Member-Server einer Domäne zu installieren. Der Exchange Server darf unter keinen Umständen auf einem Domänen-Controller installiert werden, da dies negative Auswirkungen auf die Sicherheit des gesamten Windows-Systems hätte.

Es wird dringend empfohlen, keine deutsche, sondern die englische Originalversion der Exchange 2000 Software zu installieren. Dies hat vor allem den Vorteil, dass Sicherheits-Updates, -Patches und Service Packs erfahrungsgemäß für die Originalversion früher veröffentlicht werden als für die lokalisierten Versionen der Software.

Keine weiteren Dienste auf dem Exchange-Rechner

Die Einrichtung eines dedizierten Servers für Exchange 2000 ist aus Sicherheitssicht vorteilhaft. Auf diesem sollten also nur die für den Betrieb von Exchange 2000 unbedingt notwendigen Dienste in Betrieb genommen werden.

Benutzung eines dedizierten Installationskontos

Die Installation von Exchange 2000 sollte nicht unter einem bereits vorhandenen Benutzerkonto mit Administratorrechten durchgeführt werden. Da dem Installationskonto nach der Installation volle administrative Rechte auf Exchange eingeräumt werden, wird empfohlen, ein dediziertes Benutzerkonto für die Installation von Exchange 2000 anzulegen. Dieses Installationskonto muss administrative Rechte für den lokalen Rechner besitzen sowie Mitglied in den Gruppen der Enterprise- und Schema-Administratoren sein. Nach erfolgreicher Installation sollte der Benutzer wieder aus den Gruppen der Enterprise- und Schema-Administratoren entfernt werden.

Bei der Installation weiterer Exchange-Server sollten ebenfalls jeweils dedizierte Benutzerkonten verwendet werden. Für die Installation weiterer Exchange-Server sind jedoch keine Enterprise- bzw. Schema-Administratorrechte notwendig. Es ist ausreichend, wenn diese dedizierten Konten die Rechte voller Exchange-Administratoren sowie Domain-Administratoren besitzen.

Unbeaufsichtigte Installation der zusätzlichen Exchange-Server

Bei der Installation zusätzlicher Exchange-Server empfiehlt sich eine so genannte unbeaufsichtigte Installation von Exchange. Dies führt einerseits zu einer Verminderung des Installationsaufwands und ermöglicht es andererseits, die Installation an weitere Personen zu delegieren.

Die Grundlage für die Installation ohne Aufsicht ist eine Setup-Initialisierungsdatei. Diese kann beispielsweise mit *e:\...\exchange-install-cd\...\setup.exe /CreateUnattend c:\temp\setup.ini* erstellt werden. Die so erstellte Initialisierungsdatei *setup.ini* ist eine lesbare Textdatei mit Einstellungen für die einzelnen Exchange Komponenten, und kann daher auch zur Dokumentation einer Installation benutzt werden. Die Installation auf einem weiteren Rechner wird dann mit *e:\...\exchange-install-cd\...\setup.exe /UnattendFile c:\temp\setup.ini* angestoßen.

Die Initialisierungsdatei kann sensitive Informationen in den Einstellungen für die Exchange-Komponenten beinhalten. Ist dies der Fall, sollte die Initialisierungsdatei verschlüsselt werden.

Verschlüsselung der Setup-Initialisierungsdatei

Um sensitive Informationen, wie z. B. Kennwörter für den Schlüsselverwaltungsdienst, vor dem Zugriff durch unberechtigte Personen zu schützen, kann die Initialisierungsdatei auch in einer verschlüsselten Form erzeugt werden. Von dieser Möglichkeit sollte vor allem bei der Delegation einer Exchange-Installation Gebrauch gemacht werden.

Die Erstellung einer verschlüsselten Initialisierungsdatei erfolgt beispielsweise mit dem Kommando *e:\...\exchange-install-cd\...\setup.exe /EncryptedMode /UnattendFile c:\temp\setup.ini*. Die Installation wird mit *e:\...\exchange-install-cd\...\setup.exe /UnattendFile c:\temp\setup.ini* genauso wie bei einer unverschlüsselten Initialisierungsdatei angestoßen.

Installation von Exchange 2000

Während der eigentlichen Exchange-Installation sind folgende sicherheitsrelevante Aspekte zu berücksichtigen:

- Auswahl der zu installierenden Komponenten
- Installationspfad
- Existenz der Windows 2000 Sicherheitsgruppe *Pre-Windows 2000 Compatible Access*

Der letzte Aspekt ist nur dann zu berücksichtigen, wenn der Domain-Controller der aktuellen Domäne mit Pre-Windows 2000 kompatiblen Einstellungen aufgesetzt wurde. Dies ist während der Installation von Exchange Server an der Meldung des Installationsassistenten zu erkennen, dass die Domäne aufgrund der exstierenden Pre-Windows 2000 kompatiblen Einstellungen als unsichere Domäne erkannt wurde.

Abbildung: Installations Wizard

unnötige Gruppen-Mitgliedschaften entfernen

In diesem Fall wird empfohlen, die Zusammensetzung der Gruppe *Pre-Windows 2000 Compatible Access* zu überprüfen und alle Mitglieder aus dieser Gruppe zu entfernen, die nicht unbedingt dieser Gruppe angehören müssen.

Bei der Auswahl der zu installierenden Komponenten sollen nur die absolut notwendigen Komponenten ausgewählt werden. Soll zu einem späteren Zeitpunkt die Funktionalität des Exchange-Servers erweitert werden, so können fehlende Komponenten jederzeit nachinstalliert werden.

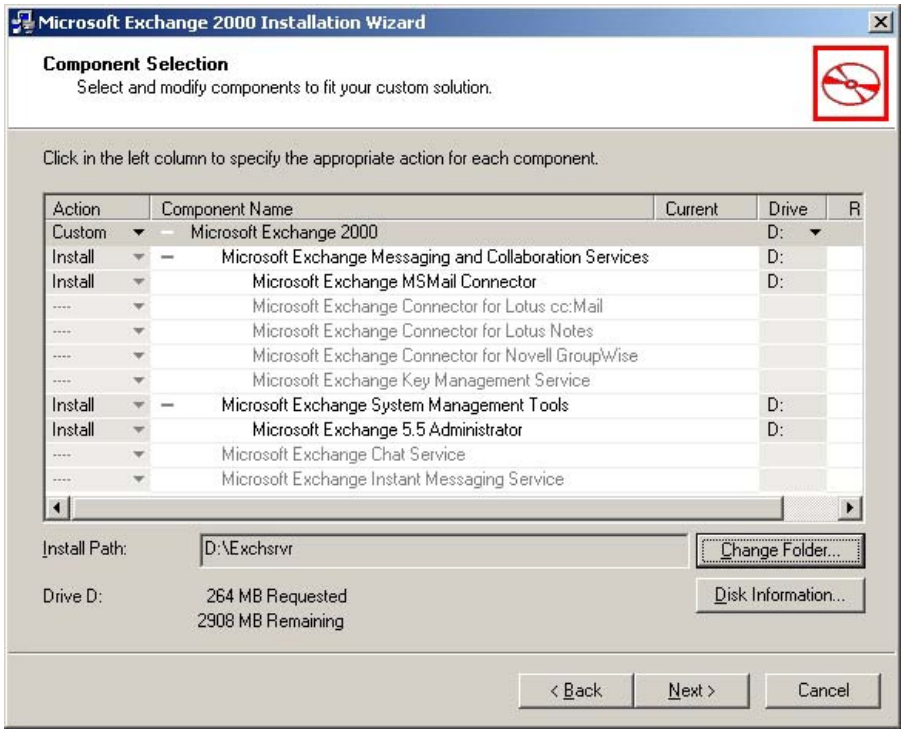


Abbildung: Installationspfad einrichten

Der Installationspfad muss auf die neu eingerichtete und mit NTFS formatierte Partition gesetzt werden. Eine dedizierte Partition sollte, wie bereits erwähnt, in der Phase der Installationsvorbereitung angelegt werden.

Wichtig ist, dass die Information über die einzurichtende Exchange-Organisation, die während der Installation des primären Exchange-Servers eingegeben wird, später nicht mehr geändert werden kann.

Abschluss der Exchange-Installation

Service Packs, Sicherheits-Updates und -Patches

auch Patches für IIS einspielen

Nach der erfolgten Installation von Exchange 2000 müssen alle verfügbaren Service Packs, Sicherheits-Updates und -Patches für Exchange 2000 eingespielt werden. Da Exchange 2000 den Microsoft Internet Information Server (IIS) benutzt, müssen auch alle entsprechenden Service Packs, Sicherheits-Updates und -Patches für den IIS installiert werden.

Grundsätzlich gilt, dass alle auf dem Exchange-Rechner laufenden Dienste und Anwendungen aktualisiert und auf den neuesten Stand gebracht werden müssen.

Anzeige der Administrativ- und Routinggruppen

Nach der Installation von Exchange 2000 werden die existierenden Administrativ- und Routing-Gruppen standardmäßig nicht angezeigt. Um ihre Anzeige zu aktivieren, müssen die Optionen *Display administrative groups* und *Display routing groups* in den generellen Eigenschaften der Exchange-Organisation aktiviert werden. Die Eigenschaften der Exchange-Organisation

können mit dem Exchange-spezifischen Werkzeug *System-Manager* eingesehen werden.

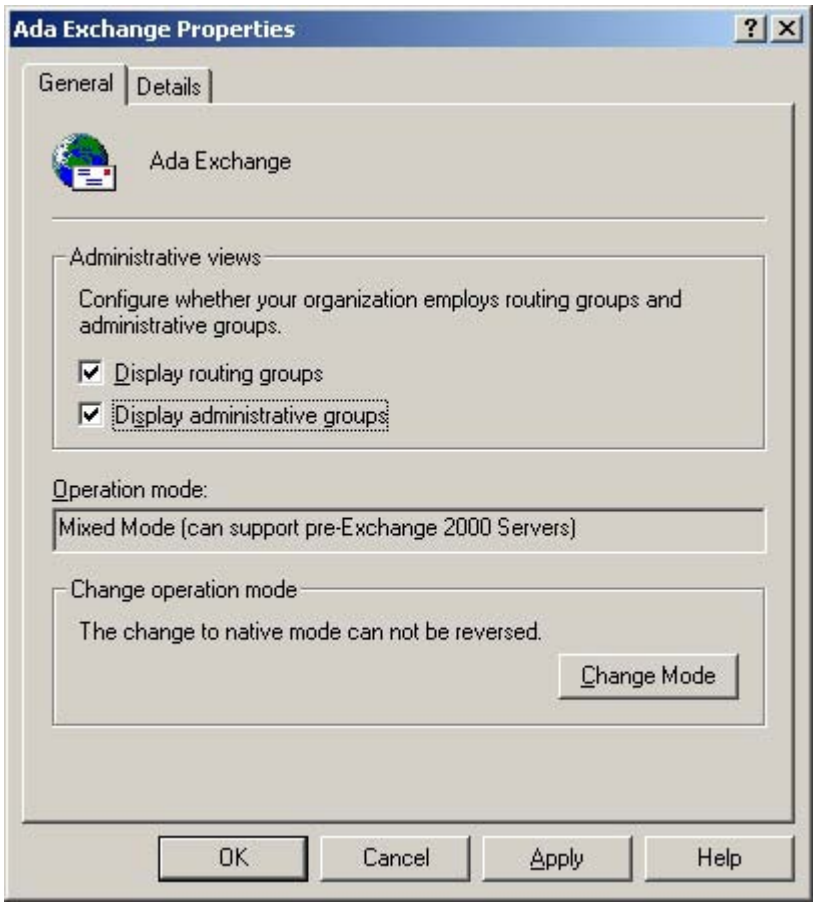


Abbildung: Ada Exchange Einstellungen

Allgemeines zur Installation von Outlook 2000

Microsoft Outlook kann in einer der folgenden Installationsarten installiert werden:

- ohne Internet-Mail-Unterstützung
- mit Internet-Mail-Unterstützung
- mit Unterstützung für Unternehmens- und Arbeitsgruppenumgebungen, d. h. als Exchange-Client

Die erste Variante gestattet nur die Pflege von Kontakten, Terminen und Dokumenten. Die Internet-Unterstützung ermöglicht das Versenden und Empfangen von E-Mail-Nachrichten über E-Mail-Protokolle - wie POP3, SMTP und IMAP. Um jedoch in einer Exchange 2000 Umgebung spezifische Exchange-Funktionen nutzen zu können, muss Outlook 2000 explizit als Exchange-Client installiert werden. Diese letzte Installationsart wird hier betrachtet.

vorkonfigurierte Version erzeugen

Es besteht die Möglichkeit mit Administrationswerkzeugen aus dem Office 2000 Resource Kit, eine vorkonfigurierte Version von Outlook 2000 für die

spätere Verteilung/Installation zentral durch den Administrator zu erzeugen. Die Erstellung einer vorkonfigurierten Version verhilft zu einem gleichmäßigen Sicherheitsniveau.

Für ein Unternehmen wird empfohlen, angepasste und vorkonfigurierte Versionen von Outlook 2000 zu erstellen und zu verteilen. Für die Erstellung einer an die Bedürfnisse des Unternehmens angepassten Version von Outlook 2000 wird der Office 2000 *Custom Installation Wizard* aus dem Microsoft Office 2000 Resource Kit benutzt.

Vorkonfiguration von Outlook 2000 mit dem *Custom Installation Wizard*

Mit Hilfe des Office 2000 *Custom Installation Wizard*s kann nicht nur Outlook 2000, sondern das ganze Microsoft Office Paket vorkonfiguriert werden. Das Ergebnis des Microsoft Office 2000 *Custom Installation Wizard* ist ein *Windows Installer Transform* - eine MST-Datei mit Installationsangaben für den Microsoft Installer.

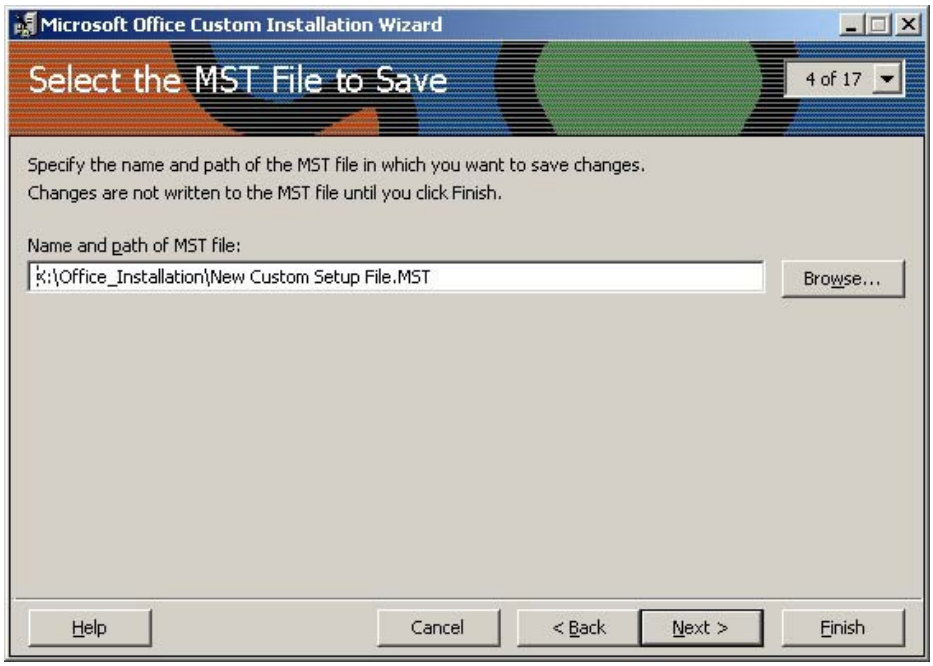


Abbildung: MST Datein Einstellungen

alte Version von Outlook entfernen

Der *Custom Installation Wizard* bietet bei der Installation einer neuen Version an, alte Versionen der Office-Komponenten - wie Outlook, Word, PowerPoint, Excel oder Access - zu deinstallieren. Es wird empfohlen, die alten Versionen von Outlook bei der Installation von Outlook 2000 zu entfernen.

Auswahl der zu installierenden Outlook 2000 Komponenten

EFD nicht installieren

Es wird empfohlen, den elektronischen Formulardesigner (EFD) den Outlook-Benutzern nicht zur Verfügung zu stellen, da die Verwendung von Formularen mit aktiven Inhalten eine potentielle Bedrohung für das Intranet der Organisation darstellt. Diese Komponente sollte während der Erstellung einer angepassten Version von Outlook 2000 nicht in das Installationspaket aufgenommen werden. Ebenso wird empfohlen, die Komponenten *Collaboration Data Objects* und *Netzordner* nicht zu installieren.

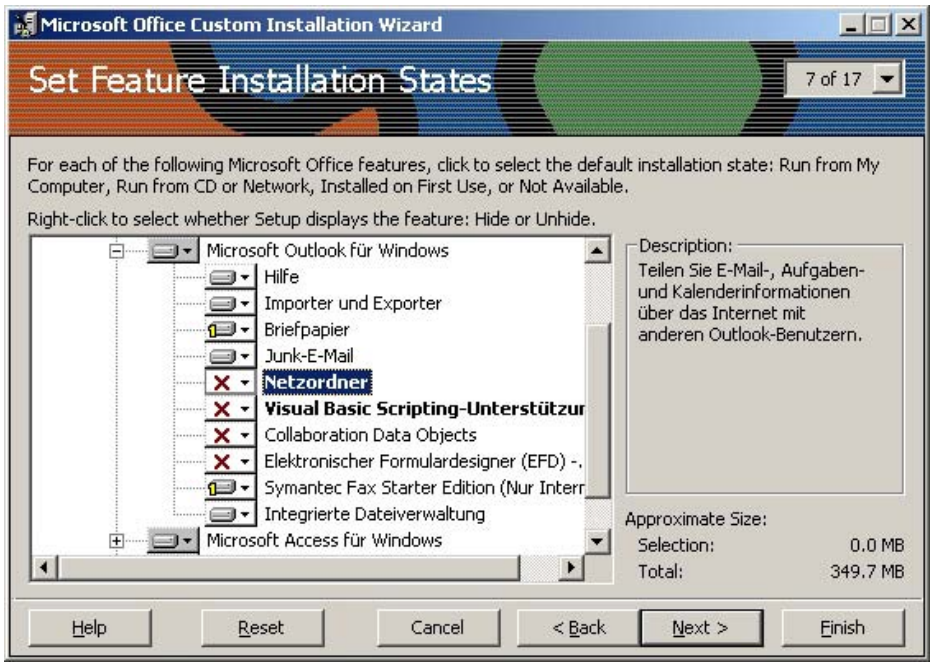


Abbildung: Anpassung der Anwendungseinstellungen

Der Installation Wizard bietet die Möglichkeit, bereits bestehende Einstellungen von Microsoft Office als Vorlage für die Anpassung zu benutzen. Um die Einstellungen des Office-Pakets in eine Datei zu exportieren, wird das Werkzeug Office 2000 Profile Wizard eingesetzt. Wird im *Custom Installation Wizard* kein existierendes Office-Profil als Vorlage angegeben, so werden die Standard-Einstellungen von Office 2000 benutzt. Es wird empfohlen, das Profil einer bestehenden, geeignet konfigurierten Installation von Outlook 2000 zu benutzen (siehe Maßnahme M 4.165 *Sichere Konfiguration von Outlook 2000*).

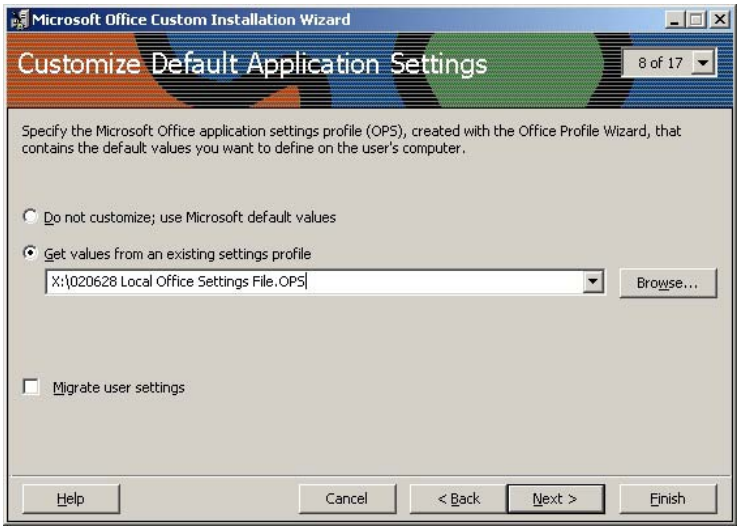


Abbildung: Vorkonfiguration der Einstellungen

Je nach Betriebsart von Outlook 2000 (als Exchange-Client oder nur als Internet-Mail-Client) sind entsprechende Einstellungen vorzunehmen.

optimale Verschlüsselung der Personal Folder

Für Outlook 2000 als Exchange-Client können Einstellungen für Standardprofile, Exchange-Server, persönliche Outlook-Ordner, POP3- und SMTP-Protokolle vorgenommen werden. Für Standardprofile können Dienste (wie z. B. MS Exchange Server Service, Personal Folder Service oder Address Book Service) angegeben werden, die in einem Standardprofil enthalten sein sollen. In den Einstellungen für persönliche Outlook-Order (Personal Folder) sollte die optimale Verschlüsselung ausgewählt werden (siehe Maßnahme M 4.165 *Sichere Konfiguration von Outlook 2000*). In den POP3- bzw. SMTP-Einstellungen sollten die sichere Kennwort-Authentisierung und die Benutzung von SSL aktiviert werden. Dies erfordert selbstverständlich auch eine entsprechende Konfiguration des Exchange-Servers.

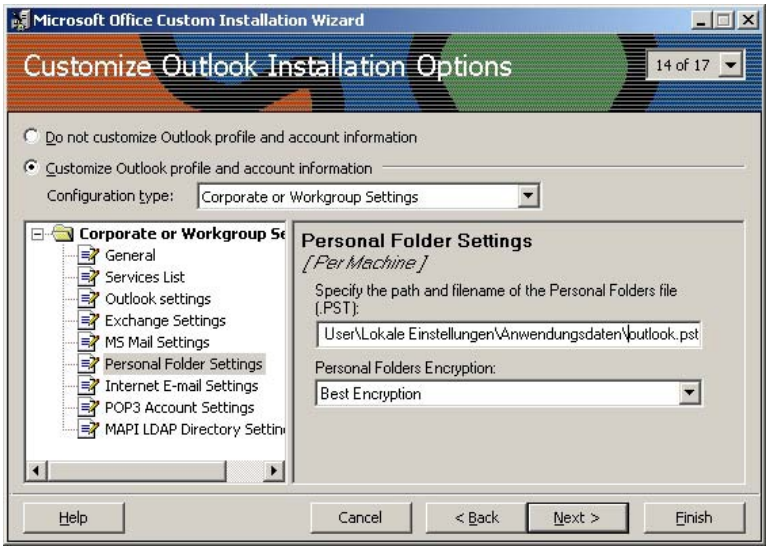


Abbildung: Outlook Installation anpassen

Für Outlook 2000 als Internet-Mail-Client können unter anderem Einstellungen für POP3, SMTP und LDAP vorgenommen werden. Es wird für alle Protokolle empfohlen, die sichere Kennwort-Authentisierung und die Benutzung von SSL zu aktivieren. Dies erfordert selbstverständlich auch eine entsprechende Konfiguration der Server-Seite.

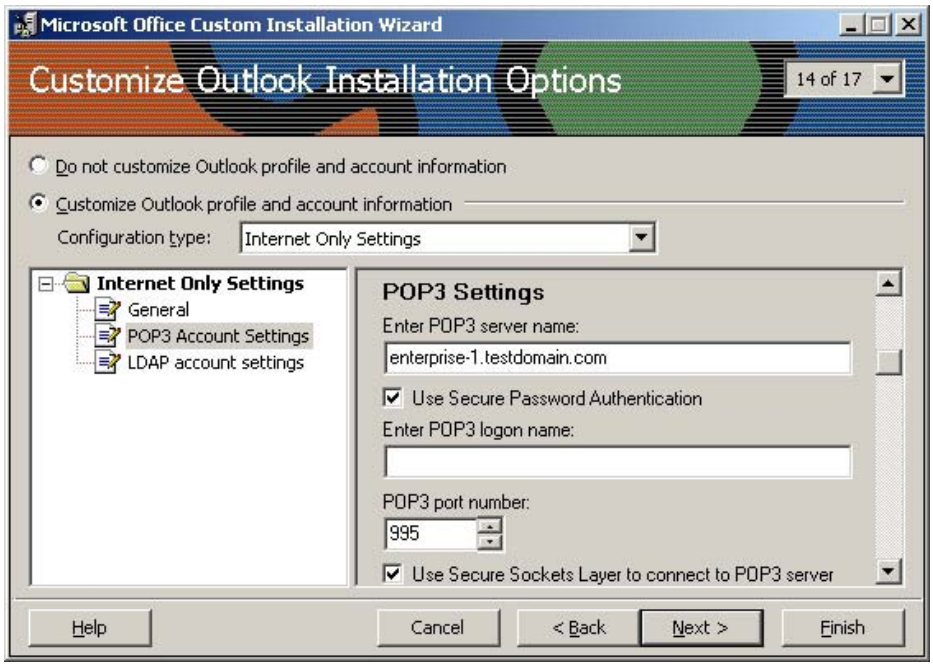


Abbildung: Anpassungen des Internet Explorers

Internet Explorer Adminstration Kit

Der *Custom Installation Wizard* bietet auch eine Möglichkeit, die alte Version des Internet Explorers auf die Version 5 zu aktualisieren. Hierbei wird empfohlen, für den Internet Explorer auch eine an die Bedürfnisse des Unternehmens bzw. der Behörde angepasste Version der Browser-Software zu erstellen. Dies ist mit dem *Internet Explorer Adminstration Kit* (IEAK) möglich. Mit dem IEAK können unter anderem auch die Einstellungen für die Internet-Zonen des Internet Explorers anpasst werden, welche direkten Einfluss auf der Sicherheit von Outlook 2000 bezüglich der Verarbeitung von E-Mail-Anlagen haben (siehe Maßnahme M 4.165 *Sichere Konfiguration von Outlook 2000*).

Installation/Verteilung von Outlook 2000

Nach der Installation und der Konfiguration der Exchange 2000 Systeme werden die Outlook 2000 Clients verteilt. Die Installation der Clients erfolgt in der Regel über einen Software-Verteilungsmechanismus, so können z. B. die *msi-Packages* auch über das Active Directory an die Clients verteilt werden.

Einzelplatzinstallation von Outlook 2000

Bei einer Einzelplatzinstallation von Outlook 2000 ist der administrative Aufwand für die Erstellung eines angepassten Installationspakets zu hoch. So kann die Outlook 2000 Software auch lokal installiert werden. Bei solch einer Installation sollten dieselben Empfehlungen (z. B. Auswahl der zu installierenden Komponenten) wie oben beschrieben beachtet werden. Weiterhin sind die Empfehlungen aus der Maßnahme M 4.165 *Sichere Konfiguration von Outlook 2000* bereits bei der Installation umzusetzen.

Ergänzende Kontrollfragen:

- Befinden sich die Exchange 2000 Server in einer physikalisch geschützten Umgebung, z. B. einem Serverraum oder einem Serverschrank?
- Wurden die Administrations- und Zugriffsberechtigungen bedarfsgerecht geplant und umgesetzt?
- Sind die Zugriffsrechte für Objekte, sofern diese von Exchange 5.5 übernommen wurden, ebenfalls aktualisiert worden?

M 4.162 Sichere Konfiguration von Exchange 2000 Servern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Nach der Installation von Exchange 2000 muss die Software sicher konfiguriert werden. Diese Maßnahme gibt Empfehlungen für die geeignete Konfiguration von Exchange 2000. Bevor ein Administrator nach der erfolgreichen Installation von Exchange 2000 mit der Konfiguration fortfährt, sollten allgemeine Empfehlungen zur Administration umgesetzt werden, wie z. B. das Einrichten geeigneter Gruppen zur Verwaltung von Exchange. Bei der eigentlichen Konfiguration von Exchange 2000 ist dann vor allem auf folgendes zu achten:

- Umsetzung der administrativen Maßnahmen,
- Einschränkung der Zugriffsberechtigungen,
- Konfiguration der Exchange-Connectors und anderer Komponenten,
- Konfiguration virtueller SMTP-Server und der POP3, IMAP4 und NNTP Kommunikationsprotokolle und
- Protokollierung.

Verwendung des einheitlichen Modus (native mode)

Wegen der Abwärtskompatibilität mit Exchange 5.5 befindet sich ein Exchange 2000 Server nach der Installation im so genannten *gemischten Modus* (*mixed mode*). Es ist darauf zu achten, die im Exchange-Umfeld benutzten Bezeichnungen *native mode* und *mixed mode* nicht mit den analogen Bezeichnungen für Windows 2000 Domänen Controller zu verwechseln.

Der Betrieb der Exchange-Server im *gemischten Modus* wird generell nicht empfohlen. Der *einheitliche Modus* sollte verwendet werden, sobald sämtliche Exchange-Server auf Exchange 2000 migriert wurden bzw. wenn eine Eingliederung von Exchange 5.5 Servern in das Exchange-System nicht vorgesehen ist.

Die Umschaltung eines Exchange 2000 Servers in den *einheitlichen Modus* geschieht im *Exchange System-Manager* in den Eigenschaften des Exchange-Organisationsobjektes. Dazu muss die Schaltfläche *Change Mode* auf der Registerkarte *General* betätigt werden. Durch das Umschalten in den *einheitlichen Modus* geht die Abwärtskompatibilität zu früheren Versionen (Exchange 5.5) irreversibel verloren.

Administratives

Einrichtung dedizierter Benutzergruppen für die Exchange-Administration

Die Exchange-Administration kann auf mehrere administrative Gruppen verteilt werden. Als Basis hierfür dienen drei vordefinierten Exchange Administrationsrollen:

- Die Rolle *Exchange Full Administrator* dient der Verwaltung der Exchange-Informationen und der Exchange-Berechtigungen.
- Die Rolle *Exchange Administrator* dient nur der Verwaltung der Exchange-Informationen.

- Die Rolle *Exchange View Only Administrator* darf lediglich die Exchange-Informationen einsehen.

Berechtigungen an Gruppen vergeben

Es wird empfohlen, drei dedizierte Sicherheitsgruppen zu erstellen, die dann jeweils eine der oben aufgeführten Exchange-Rollen zugewiesen bekommen. Grundsätzlich sollte die Administration auf dem Gruppen- und nicht dem Personenprinzip aufgebaut werden: Berechtigungen sollten für Gruppen und nicht für einzelne Benutzerkonten vergeben werden. Dadurch wird die Verwaltung erheblich erleichtert und übersichtlicher gestaltet - eine mögliche Fehlerquelle wird beseitigt. Die Exchange-Administratoren werden dabei über Gruppenmitgliedschaften verwaltet.

Die Zuweisung der Rollen zu den erstellten Administrativgruppen erfolgt mit Hilfe des Delegationsassistenten (Delegation Wizard) im *Exchange System-Manager*.

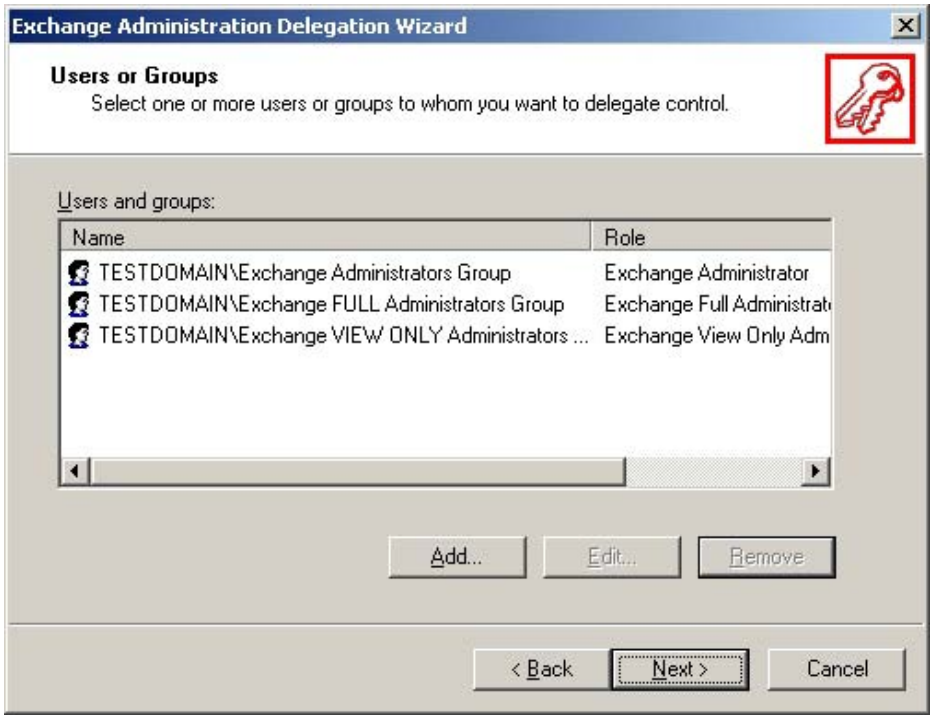


Abbildung: Benutzerkonten und serverseitige Benutzerprofile

Werden Newsgroups eingerichtet?

Die Benutzerkonten und Newsgroups müssen gemäß den für diesen Punkt vorgesehenen Sicherheitsrichtlinien (siehe M 2.248 *Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook* 2000) eingerichtet werden. Vor allem sollte hier entschieden werden, welche Benutzer mit einem Exchange-Postfach ausgestattet und ob Newsgroups überhaupt eingerichtet werden.

Es wird empfohlen, serverseitige Benutzerprofile zu verwenden. Besitzt ein Benutzer ein serverseitiges Profil, werden die Benutzereinstellungen bei jeder Anmeldung an der Domäne in die lokale Konfiguration (*Registry*) der Arbeitsstation übernommen. Somit kann ein rechnerunabhängiger Zugriff auf Exchange-Daten erreicht werden.

Systemkonten für die Exchange 2000 Dienste

Exchange 2000 besteht aus mehreren Diensten, welche miteinander kommunizieren. Diese Kommunikation erfordert eine Authentisierung auf der Grundlage des Kerberos-Protokolls. Die Dienste laufen dabei standardmäßig unter dem Windows 2000 Konto *LocalSystem*. Windows 2000 ändert das Kennwort dieses Kontos automatisch alle 7 Tage.

Exchange 2000 nicht in Exchange 5.5 Umgebung integrieren

Ein benutzerähnliches Dienstkonto muss eingerichtet werden, wenn ein Exchange 2000 Server in eine Exchange 5.5 Umgebung integriert wird. Innerhalb eines Standortes müssen die Exchange-spezifischen Dienste für ihre Kommunikation ein gemeinsames Standortdienstkonto zur Authentisierung verwenden. Die Integration eines Exchange 2000 Servers in eine Exchange 5.5 Umgebung wird generell nicht empfohlen.

Die für Exchange relevanten Dienste - vornehmlich der *Information Store Service*, der *Routing Engine Service* sowie der *System Attendant Service* - laufen nach der Standardinstallation unter dem Konto *Local System*, das weitreichende Rechte auf dem lokalen Server besitzt. Für diese Exchange-Dienste können optional eigene Konten mit angepassten Rechten erstellt werden (siehe M 4.139 *Konfiguration von Windows 2000 als Server*). Es wird jedoch darauf hingewiesen, dass dies unter Umständen einen großen Test- und Konfigurationsaufwand erfordert.

Einsatz der Exchange-Systemrichtlinien

Die Exchange 2000 Systemrichtlinien ermöglichen es, gleichzeitig mehrere Exchange-Server zu konfigurieren. Es existieren drei unterschiedliche Typen von Systemrichtlinien: Server-, Mailbox-Store-Richtlinien und Richtlinien für öffentlichen Ordner. Der Einsatz der Richtlinien ermöglicht eine einheitliche Konfiguration und vermindert somit das Risiko einer Fehlkonfiguration. Es wird daher empfohlen, Exchange-Richtlinien einzusetzen und sie pro definierter Administrativgruppe festzulegen.

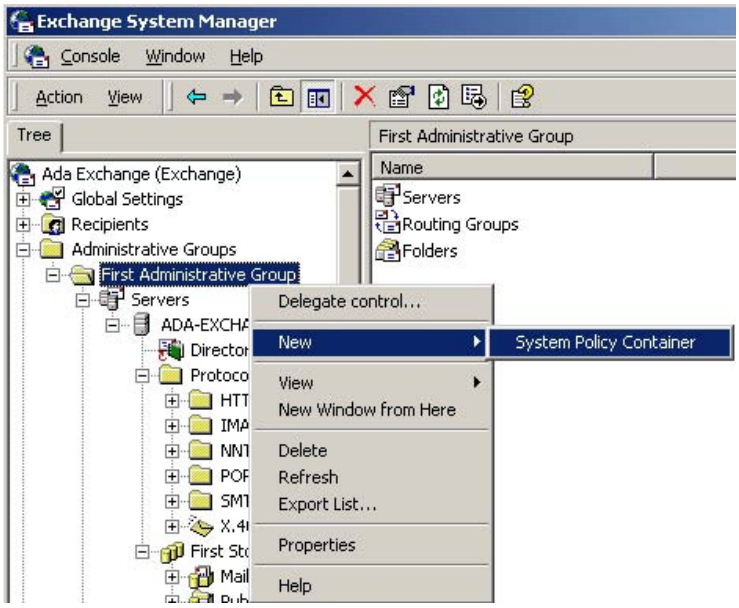


Abbildung: Exchange-Systemrichtlinien

In den Mailbox-Store-Richtlinien und den Richtlinien öffentlicher Ordner können Speicherbeschränkungen definiert werden. Bei Erreichen des Limits können Warnungen ausgegeben, Senden oder Senden und Empfangen von Nachrichten untersagt werden. Die Größenbeschränkungen sollten hierbei den jeweiligen Anforderungen im Unternehmen bzw. in der Behörde angepasst werden.

gelöschte Nachrichten erst nach Backup löschen

Weiterhin ist in den Mailbox-Store-Richtlinien und den Richtlinien öffentlicher Ordner die Einstellung vorzunehmen, dass die gelöschten Nachrichten erst nach einem Backup endgültig gelöscht werden dürfen.

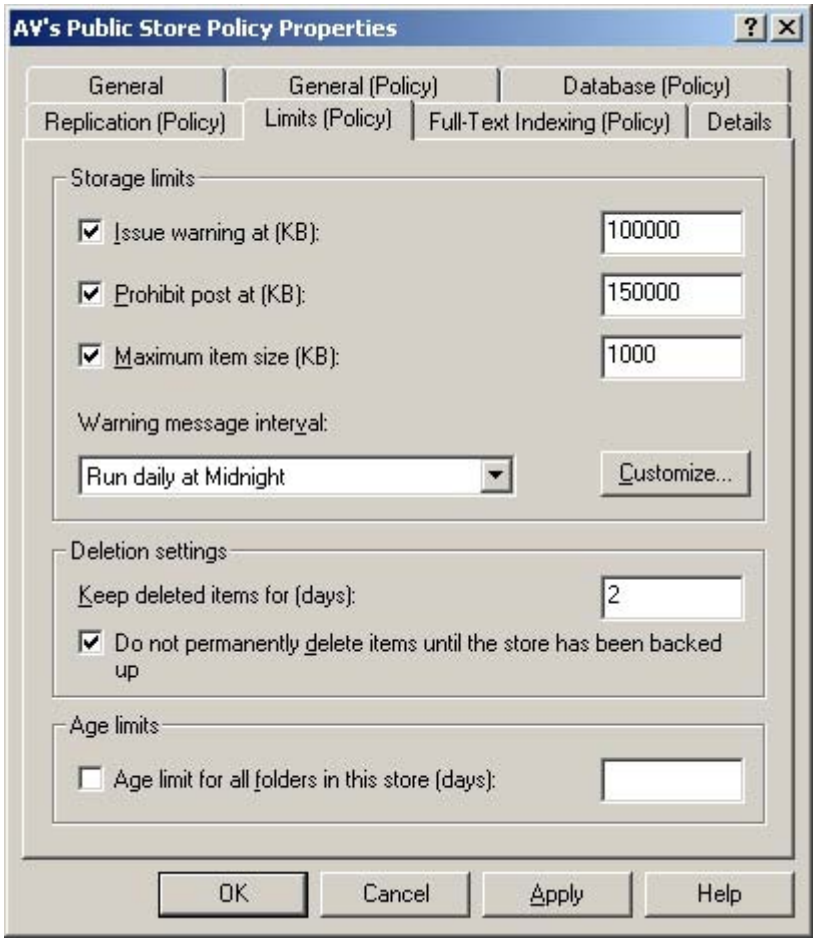


Abbildung: Mailbox-Store-Richtlinien

In den Server-Richtlinien sollten die Optionen für die Nachrichtenverfolgung und -Protokollierung aktiviert werden. Die Protokolldateien dürfen hierbei nicht gelöscht werden.

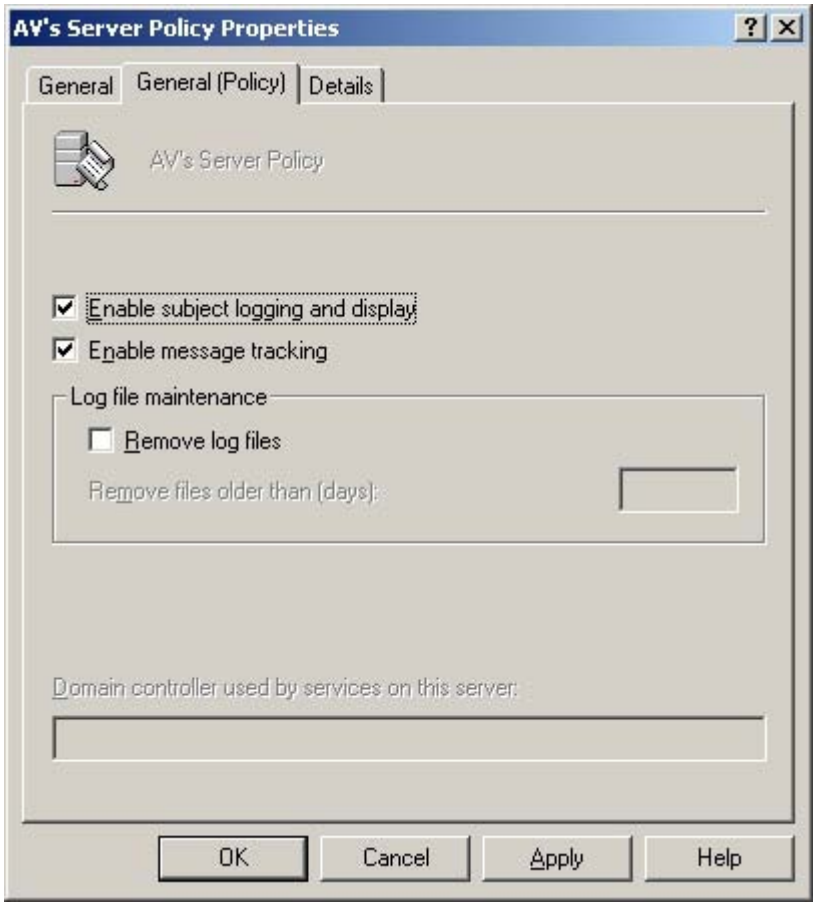


Abbildung: Einschränkung der Zugriffsrechte

Zugriffseinschränkung auf das Exchange-Verzeichnis

Die Standard-NTFS-Berechtigungen auf das Exchange-Verzeichnis müssen angepasst werden, so dass nur autorisierten Administratoren und Systemkonten der Zugriff auf sensitive Daten in diesem Verzeichnis (z. B. Datenbanken und Transaktionsprotokolle) erlaubt ist. Die Standard-Einstellungen sind daher wie folgt anzupassen:

- Zugriff der Mitglieder der Gruppe *Everyone* (*Jeder*) auf den Verzeichnisbaum verbieten (d. h. bestehende Berechtigungen entfernen)
- Alle Berechtigungen sollten für folgende Gruppen eingerichtet werden:
  - SYSTEM
  - CREATOR OWNER
  - Domain Admins
  - <Exchange Administrator Groups> (eingerichtet wie im vorherigen Abschnitt beschrieben)
- Ist die Benutzung von *Outlook Web Access* (OWA) geplant, muss für die Gruppe der authentisierten Benutzer (*Authenticated Users*) Lese- und Ausführrecht gewährt werden.

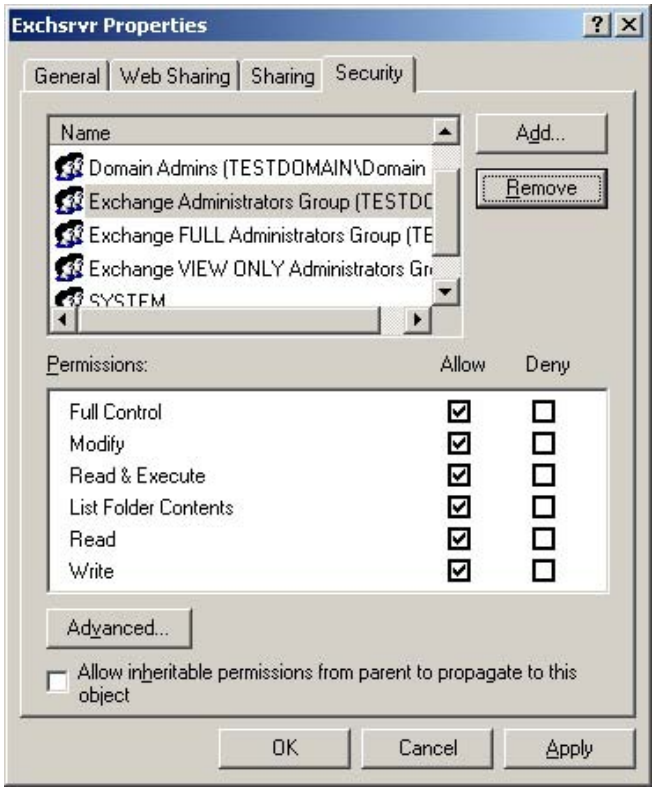


Abbildung: Zugriffsbeschränkungen einrichten

Zugriffseinschränkungen auf Exchange-Netzfreigaben

Die Zugriffsberechtigungen der während der Installation erstellten Exchange-Netzfreigaben müssen ebenfalls angepasst werden. Zusätzlich zu den oben aufgelisteten Zugriffsrechten muss das lokale Computerkonto vollen Zugriff auf diese Freigaben erhalten. Die Zugriffsberechtigungen für das Konto *Everyone* (*Jeder*) sollten generell entfernt werden.

Unter anderem werden folgende Netzfreigaben eingerichtet:

- *<Exchange-Pfad>\Address*, freigegeben als *Address*. Damit wird der Zugriff auf die Adressgenerator-DLLs ermöglicht. Standardmäßig verfügen die Administratoren und das lokale Computerkonto über Vollzugriff auf diese Freigabe. Der Zugriff für das Konto *Everyone* ist nach der Installation auf lesenden Zugriff beschränkt.
- *\Programme\Exchsrvr\<servername>.log*, freigegeben als *<servername>.log*. Die für das Nachrichtentracking relevanten Protokolldateien werden in diesem Verzeichnis gespeichert. Diese Protokolldateien enthalten Informationen zu Nachrichtenempfängern, Nachrichtengrößen, Absendern, Übermittlungszeiten und möglicherweise die Betreffzeilen der Nachrichten. Standardmäßig verfügen die Administratoren und das lokale Computerkonto über Vollzugriff auf diese Freigabe. Der Zugriff für das Konto *Everyone* ist nach der Installation auf lesenden Zugriff beschränkt.
- *\Programme\Exchsrvr\Connect\Msmcon\Maildata*, freigegeben als *Maildat$*. Damit wird der Zugriff auf die versteckte Netzfreigabe auf den MS Mailconnector ermöglicht. Standardmäßig nach der Installation

verfügen die Administratoren, das lokale Computerkonto sowie das Konto *Everyone* über Vollzugriff auf diese Freigabe.

Einschränkung der Zugriffsrechte auf Exchange 2000 Objekte

Zur Einschränkung der Zugriffsrechte auf Exchange 2000 Objekte wird auf die Maßnahme M 4.163 *Zugriffsrechte auf Exchange 2000 Objekte* verwiesen.

Globale Exchange-Einstellungen

Nachrichtenfilterung

Exchange 2000 bietet die Möglichkeit, die Nachrichtenfilterung serverseitig zu aktivieren. Da nur einzelne Absender gesperrt und keine Inhaltsfilter definiert werden können, bietet diese Maßnahme keinen guten Schutz gegen E-Mail-Spam. In Einzelfällen ist die Nachrichtenfilterung jedoch ein sinnvolles Instrument. Wenn sie benutzt werden soll, wird empfohlen, alle ausgefilterten Nachrichten zu protokollieren und den Verfasser einer ausgefilterten Nachricht nicht über die stattgefundene Filterung zu informieren.

Weiterhin sollten auch Nachrichten mit einem leeren Absender-Feld ausgefiltert werden. Diese Konfigurationen werden in der Registerkarte *Filtering* in den Einstellungen für die Nachrichtenzustellung (*Message Delivery Properties*) der Exchange-Gesamtorganisation vorgenommen.

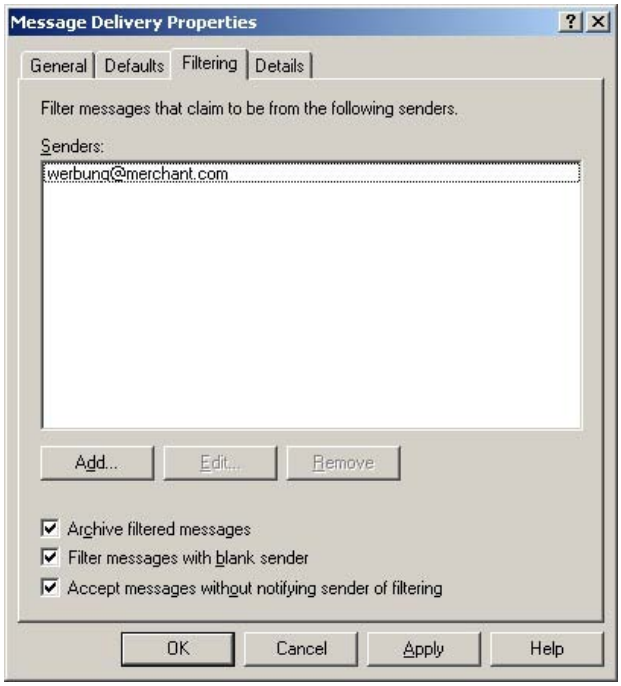


Abbildung: Einstellung für Nachrichtenzustellung

Begrenzung der maximalen Nachrichtengröße

Als eine der möglichen Maßnahmen zum Schutz gegen DoS-Attacken (*Denial of Service*) können maximal zulässige Größen sowohl für eingehende als auch für ausgehende Nachrichten definiert werden. Es wird empfohlen, die Größe eingehender Nachrichten zu begrenzen. Dies kann in der Registerkarte

Defaults in den Einstellungen für die Nachrichtenzustellung (*Message Delivery Properties*) eines virtuellen SMTP-Servers vorgenommen werden.

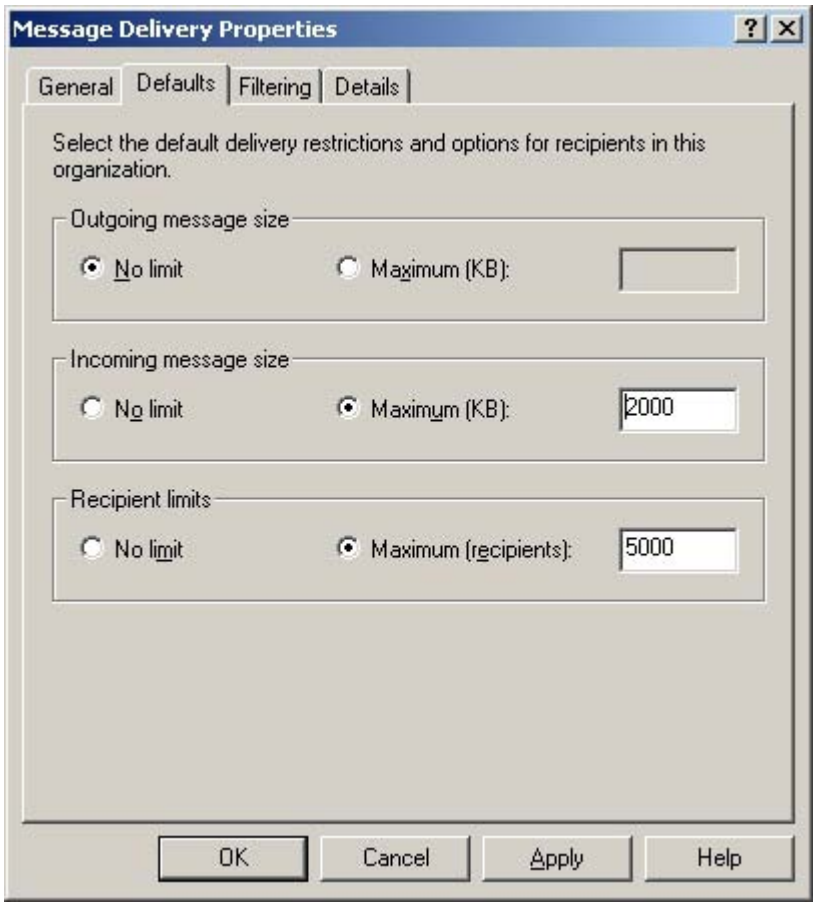


Abbildung: Eigenschaften der Nachrichtenzustellung

Umgang mit Sondernachrichten

Automatische Lese- und Empfangsbestätigungen, sowie *Out-of-Office*-Meldungen können zu (eventuell unbeabsichtigten) Denial-of-Service-Attacken führen. Sofern im Unternehmen bzw. in der Behörde die Verwendung von E-Mail-Bestätigungen und *Out-of-Office*-Meldungen nicht explizit gewünscht ist, wird empfohlen, den Einsatz dieser Sondernachrichten in der Exchange-Gesamtorganisation komplett zu verbieten. In den Standardeinstellungen der Exchange-Gesamtorganisation (Registerkarte *Advanced*) sollten alle Sondernachrichtentypen deaktiviert werden.

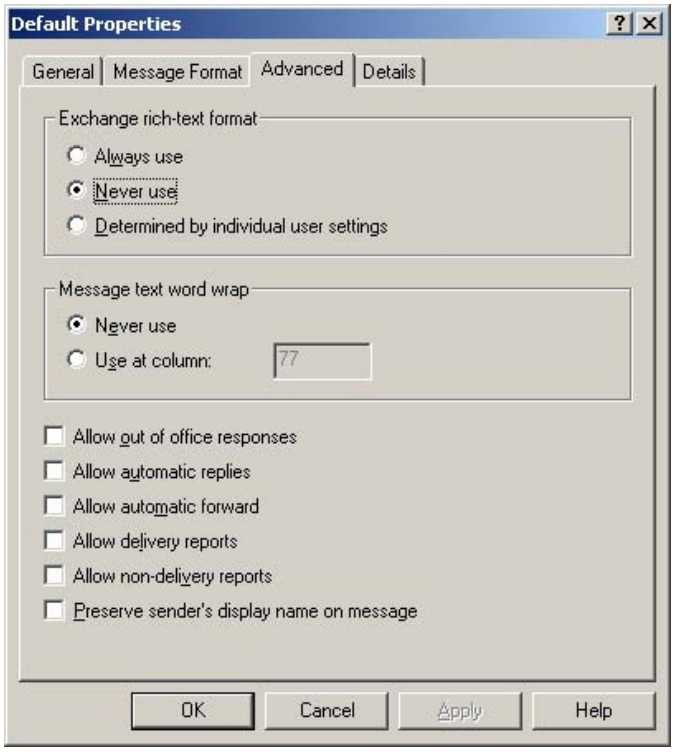


Abbildung: Standard Einstellungen

Konfiguration der Exchange-Connectors

In einer Umgebung mit mehreren Servern muss die Sicherheit der Nachrichtenübertragung gewährleistet werden, was eine entsprechende Konfiguration der Routing-Connectors bedeutet. Die Verbindungen zwischen Servern einer Routing-Gruppe werden während der Installation automatisch konfiguriert. Die Einstellungen der einzelnen Connectors müssen jedoch manuell angepasst werden, um ein höheres Sicherheitsniveau zu erreichen.

Es ist zu beachten, dass für die Konfiguration der Exchange-Connectors nicht nur Exchange-Administratorrechte, sondern auch Windows-Administratorrechte erforderlich sind.

Einrichtung redundanter Verbindungen

Aus Verfügbarkeitsgründen sollten redundante Verbindungen eingerichtet werden. So ist es beim Einsatz von SMTP- oder Routing-Group-Connectors möglich, mehrere sogenannte Bridgehead-Server (lokal und entfernt) zu spezifizieren. Bei Verbindungen zu X.400-Systemen empfiehlt es sich, mehrere X.400-Connectors einzurichten.

Allgemeine Connector-Einschränkungen

Nachrichtengröße beschränken

Für alle Exchange-Connectors können allgemeine Einschränkungen in bezug auf die Größe der Nachrichten definiert werden. Diese Größeneinschränkungen sollten als eine Maßnahme zum Schutz vor Denial-of-Service-Attacken aktiviert werden. Dies erfolgt in den Einstellungen des jeweiligen Connectors auf der Registerkarte *Content Restrictions*.

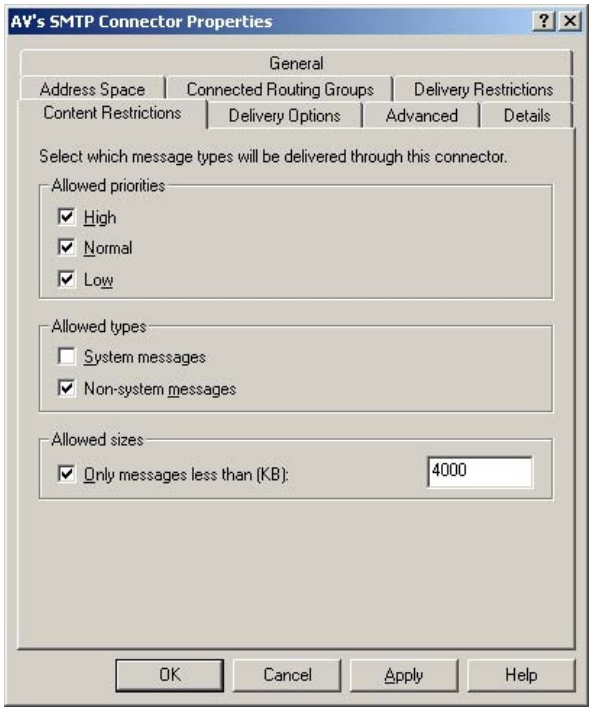


Abbildung: Einschränkungen für den Inhalt

Weiterhin können Exchange-Connectors so konfiguriert werden, dass der Zugriff durch bestimmte Benutzer oder Gruppen gestattet oder verwehrt wird. Dies wird in den Einstellungen eines Connectors auf der Registerkarte *Delivery Restrictions* eingestellt. Damit alle beschriebenen Einschränkungen wirksam werden, ist in der Windows-Registrierungsdatenbank unter

HKEY_LOCAL_MACHINE / System / CurrentControlSet / Services / Resvc / Parameters

der Schlüssel *CheckConnectorRestrictions* mit Datentyp *REG_DWORD* und Wert *1* einzutragen.

Routing-Group-Connector

Der Routing-Group-Connector wird eingesetzt, um verschiedene Routinggruppen miteinander zu verbinden. Das Standardprotokoll in Routing-Gruppen ist SMTP. Werden Exchange-Server im *gemischten Modus* betrieben, so findet die Kommunikation mit Exchange 5.5 Servern über RPC statt.

Da Routing-Group-Connectors keine Verschlüsselung anbieten, sollten sie, sofern sensitive Daten über unsichere Strecken übertragen werden, nur in Verbindung mit IPSec eingesetzt werden. Als eine Alternative zu Routing-Group-Connectors werden SMTP-Connectors empfohlen, die auch eine Verschlüsselung ermöglichen.

X.400-Connector

Der X.400-Connector kann für die Verbindung mit X.400-Systemen benutzt werden. Da der X.400-Connector nur die Authentisierung mit Kennwörtern im

Klartext und *HTTP Basic Authentisierung* kennt, stellt der Einsatz eines solchen Connectors über eine unsichere Kommunikationsstrecke ein Sicherheitsrisiko dar. Daher wird von der Verwendung des X.400-Connectors abgeraten.

SMTP-Connector

Ein SMTP-Connector kann nicht nur zur Verbindung zweier Routing-Gruppen, sondern auch zur Verbindung verschiedener Exchange-Organisationen sowie zur Einbindung fremder (nicht-Exchange-) Server benutzt werden.

Genauso wie der Routing-Group-Connector ist der SMTP-Connector unidirektional. Authentisierungs- und Verschlüsselungseinstellungen für ausgehende Verbindungen können in den Eigenschaften des jeweiligen Connectors vorgenommen werden (Registerkarte *Advanced*, Schalter *Outbound Security*). Die Verschlüsselung des Nachrichtenverkehrs kann durch die Aktivierung der TLS-Verschlüsselungsoption erreicht werden. Die Verschlüsselung sollte aktiviert werden, wenn sensitive Daten über unsichere Strecken übertragen werden.

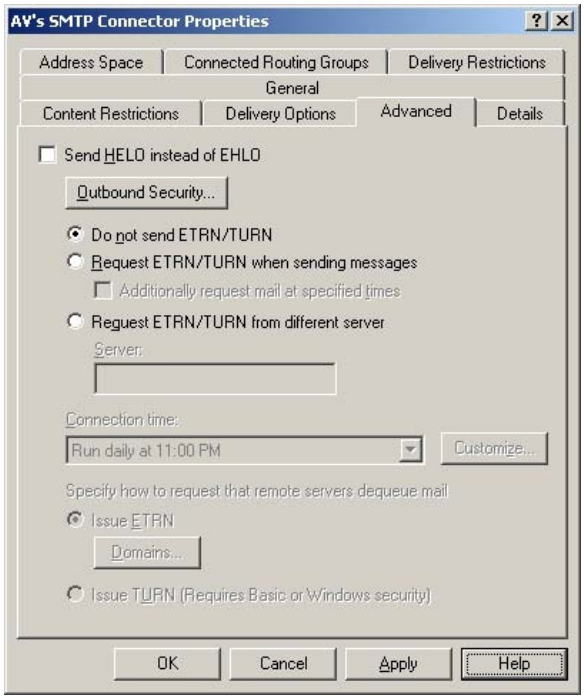


Abbildung: Erweiterte Einstellungen

Authentisierung

Es stehen drei Authentisierungsoptionen zur Verfügung: anonymer Zugriff, HTTP Basic Authentisierung und integrierte Windows 2000 Authentisierung. Standardmäßig findet keine Authentisierung statt (anonymer Zugriff). Sofern die Kommunikation zwischen Exchange Servern einer Windows-Domäne (z. B. innerhalb einer Routing-Gruppe) erfolgt, wird die integrierte Windows-Authentisierung zum Einsatz empfohlen. Die HTTP Basic Authentisierung sollte ausschließlich zusammen mit TLS benutzt werden. Sofern dies möglich ist, sollte auf den anonymen Zugriff verzichtet werden.

Abbildung: Sicherheit ausgehender Nachrichten

Weitere Exchange-Connectors

Außer den oben beschriebenen Exchange-Connectors existieren noch weitere, wie z. B. für cc:Mail, GroupWise oder MsMail. Die Notwendigkeit des Einsatzes dieser Exchange-Connectors sollte in jedem Einzelfall geprüft werden. Wenn solche Exchange-Connectors eingesetzt werden sollen, sollten die Einstellungen für die Authentisierung und die Verschlüsselung so vorgenommen werden, dass ein möglichst hohes Sicherheitsniveau erreicht wird (falls hierfür Einstellungsmöglichkeiten vorhanden sind).

Komponentenkonfiguration

dedizierte Front- and Back-End-Server

Wenn es den Benutzern möglich sein soll, über das Internet auf ihre Postfächer zuzugreifen, empfiehlt sich der Einsatz von dedizierten Front-End-Servern. Die Front-End-Server befinden sich in der DMZ und leiten eingehende Client-Verbindungen zu den Back-End-Systemen, auf denen sich die Postfächer der Benutzer befinden. Die Front-End-Server selbst enthalten keine privaten Postfächer.

Ein Exchange-Server kann als Front-End-Server konfiguriert werden, indem die Option *This is a Front-End-Server* in den Eigenschaften des Servers aktiviert wird. Ist diese Option nicht gesetzt, ist der aktuelle Exchange-Server ein Back-End-Server. Dies ist die Standardeinstellung.

Authentisierung zwischen Exchange-Servern und SMTP-Relay-Hosts

Für die Weiterleitung einkommender und ausgehender Nachrichten kann in der DMZ eines Unternehmens ein SMTP-Relay-Host eingerichtet werden. Öffentliche SMTP-Verbindungen (von außen zum SMTP-Relay-Host) können prinzipiell nicht verschlüsselt werden, wenn fremde SMTP-Server mit dem SMTP-Relay-Host in der DMZ im Klartext kommunizieren. Zwischen dem Relay-Host in der DMZ und den Servern im internen Netz sollte jedoch von

der Authentisierung der Server Gebrauch gemacht werden. Der SMTP-Connector muss entsprechend konfiguriert werden.

Zugriff auf den Exchange-Server über HTTP (Outlook Web Access - OWA)

Von der Benutzung der OWA-Funktionalität im Exchange-Umfeld wird grundsätzlich abgeraten. Soll den Benutzern der Zugriff auf Exchange-Server über HTTP dennoch ermöglicht werden, müssen die Empfehlungen aus der Maßnahme M 4.164 *Browser-Zugriff auf Exchange 2000* umgesetzt werden.

Zugriff von MAPI-Clients auf Exchange 2000 Server über das Internet

Es wird empfohlen, den Benutzern keinen direkten Zugriff auf die Exchange-Postfächer und den globalen Katalog über das Internet zu gestatten. Sollte dies aus anderen Gründen doch erlaubt werden, so muss die Firewall entsprechend konfiguriert werden: MAPI verwendet für die Kommunikation RPC und dynamische Portzuweisungen.

Konfiguration von Instant Messaging und Chat

Beim Einsatz der Funktionalität für Instant Messaging und Chat von Exchange 2000 muss die Benutzerauthentisierung gewährleistet werden. Empfohlen wird hierfür die integrierte Windows-Authentisierung. Die HTTP-Authentisierung sollte nicht eingesetzt werden, da es die reversible Kennwortverschlüsselung unter Windows 2000 erfordert, was unter gar keinen Umständen aktiviert werden darf. Dies impliziert jedoch, dass sich diejenigen Benutzer, die über Firewalls oder HTTP-Proxies arbeiten, wahrscheinlich nicht authentisieren können.

Konfiguration des Transports Outlook-Client zu Exchange 2000 Server

Der Exchange-Transportdienst für die Client/Server-Kommunikation stützt sich auf RPCs. Die folgenden RPC-Mechanismen werden für die Kommunikation zwischen Outlook und Exchange 2000 Server unterstützt:

- Banyan Vines: für die Kommunikation über Banyan Vines-Netze
- LPC: sofern Client und Server auf dem gleichen Rechner installiert sind
- Named Pipes: zum Verbindungsaufbau unter Verwendung des NetBIOS-basierten Named Pipes-Protokolls
- NetBIOS: zum Verbindungsaufbau via NetBIOS über NetBEUI, IPX/SPX oder TCP/IP
- IPX/SPX: um echte Novell Netware-Arbeitsstationen über IPX/SPX und die Winsock-Schnittstelle zu unterstützen
- TCP/IP: zur Verwendung von Winsock über TCP/IP

Die Verbindungsreihenfolge kann konfiguriert werden, was speziell in heterogenen Netzen von Bedeutung ist. Die Standardreihenfolge ist LPC, TCP/IP, IPX/SPX, Named Pipes, NetBIOS und schließlich Banyan Vines. Die Änderung der Verbindungsreihenfolge erfolgt über die Windows-Registrierungsdatenbank. Unter

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Exchange \ Exchange Provider

Verbindungsreihenfolge anpassen

enthält der Schlüssel *Rpc_Binding_Order* eine durch Kommata getrennte Aufzählung der RPC-Kommunikationsmethoden: *ncalrpc* (für LPC), *ncacn_ip_tcp* (für TCP/IP), *ncacn_spx* (für SPX), *ncacn_np* (für Named Pipes), *netbios* (für NetBIOS) sowie *ncacn_vns_spp* (für Banyan Vines). Es wird empfohlen, die Reihenfolge der Kommunikationsmechanismen anzupassen.

Konfiguration des Exchange-Transportdienstes

Verschlüsselung aktivieren

Die Informationen, die vom Client zum Exchange-Server übertragen werden, sollten kryptographisch geschützt werden. Die Verschlüsselung der Daten wird auf der Registerkarte *Advanced* aktiviert. Bei der Benutzung einer Einwählverbindung ist die Verschlüsselung besonders wichtig.

Die Windows 2000-Kennwortauthentisierung sollte als Authentisierungsmethode eingesetzt werden. Dies erfolgt ebenso auf der Registerkarte *Advanced*.

Soll der Zugriff auf Exchange-Server über eine Einwählverbindung möglich sein, wird empfohlen, dies nur auf Basis eines dedizierten Kontos zuzulassen.

Konfiguration virtueller SMTP-Server

Exchange 2000 ermöglicht die Definition mehrerer virtueller SMTP-Server. Die Sicherheitseinstellungen betreffen an dieser Stelle die Sicherheit der ein- und ausgehenden SMTP-Verbindungen: Authentisierung, Verschlüsselung, Einschränkungen der Weiterleitungsfunktionalität und Vergabe der Zugriffsberechtigungen auf Basis der IP-Adressen oder der Domänennamen.

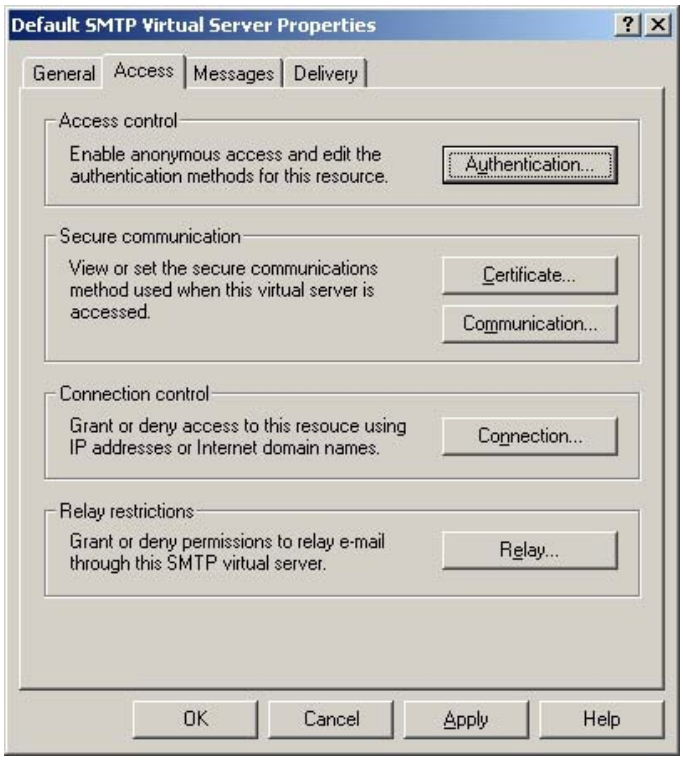


Abbildung: Vergabe der Zugriffsberechtigungen

Für die Authentisierung eingehender Verbindungen stehen in den Eigenschaften eines SMTP-Servers (Registerkarte *Access*, Schalter *Authentication*) drei Optionen zur Verfügung, die alle standardmäßig aktiviert sind: anonymer Zugriff, HTTP Basic Authentisierung und integrierte Windows 2000 Authentisierung. Es wird empfohlen, entweder die integrierte Windows Authentisierung oder HTTP Basic Authentisierung in Verbindung mit TLS-Verschlüsselung zu benutzen. Nach Möglichkeit ist die Windows Authentisierung vorzuziehen. Müssen anonyme SMTP-Zugriffe auf den Server möglich sein (d. h. dieser Server ist ein öffentlicher SMTP-Server), so empfiehlt sich der Einsatz eines SMTP-Relay-Hosts in der DMZ.

Abbildung: Authentikation

Für die Authentisierung ausgehender Verbindungen stehen in den Eigenschaften eines SMTP-Servers dieselben drei oben genannten Optionen zur Verfügung (einstellbar in der Registerkarte *Delivery*, Schalter *Outbound security*). Müssen Verbindungen zu unterschiedlichen externen SMTP-Servern mit verschiedenen Anmeldedaten aufgebaut werden, empfiehlt sich die Einführung unterschiedlicher SMTP-Connectors.

Abbildung: Sicherheit ausgehender Nachrichten

Die Verschlüsselung der Verbindungen wird empfohlen, wenn sensitive Daten über ungeschützte Kommunikationswege übertragen werden. Ebenso wird die

Verschlüsselung empfohlen, wenn die HTTP Basic Authentisierung zum Einsatz kommen soll. Die TLS-Verschlüsselung für eingehende Verbindungen wird in den Eigenschaften eines SMTP-Servers in der Registerkarte *Access*, Bereich *Secure communication* aktiviert. Bei der Übertragung besonders schützenswerter Daten sollte die 128-Bit-Verschlüsselung eingesetzt werden. Es ist zu beachten, dass für die Aktivierung der Verschlüsselung eingehender Verbindungen ein entsprechendes Server-Zertifikat benötigt wird. Die Verschlüsselung ausgehender Verbindungen wird durch die Aktivierung der TLS-Option in der Registerkarte *Delivery*, Schalter *Outbound security* erreicht. Hier ist darauf zu achten, dass die Gegenseite natürlich ebenfalls TLS unterstützen muss.

default deny policy

Sind alle SMTP-Server bekannt, mit denen der zu konfigurierende virtuelle Server kommuniziert, so wird empfohlen, Zugriffseinschränkungen auf Basis der IP-Adressen oder der Domänennamen festzulegen. Hierbei sollte die Definition der Einschränkungen auf Basis der IP-Adressen bevorzugt werden. Weiterhin wird empfohlen, nur erlaubte IP-Adressen (oder Domänennamen) anzugeben, dem Rest sollte der Zugriff implizit verweigert werden (so genannte *default deny policy*). Die Zugriffseinschränkungen werden in den

Eigenschaften des Servers in der Registerkarte *Access*, Bereich *Connection control* vorgenommen.

Abbildung: Zugriffseinschränkungen

Die Weiterleitungsfunktionalität, die anderen SMTP-Servern zur Verfügung gestellt wird, kann eingeschränkt werden (Registerkarte *Access*, Bereich *Relay restrictions* in Servereinstellungen). Es wird empfohlen, dies durch die Definition einer Liste berechtigter SMTP-Server zu realisieren (*default deny policy*).

Die Nachrichtengröße sowie die Anzahl der Nachrichten pro Verbindung und die Anzahl der Nachrichtempfänger pro Nachricht können in den Einstellungen des jeweiligen virtuellen SMTP-Servers eingeschränkt werden (Registerkarte *Messages*). Die Definition der Größeneinschränkungen wird generell empfohlen, da es eine der möglichen Maßnahmen für die Abwehr von DoS-Attacken ist. Die Maximalwerte sollten hierbei den Anforderungen des jeweiligen Unternehmens bzw. der Behörde angepasst werden.

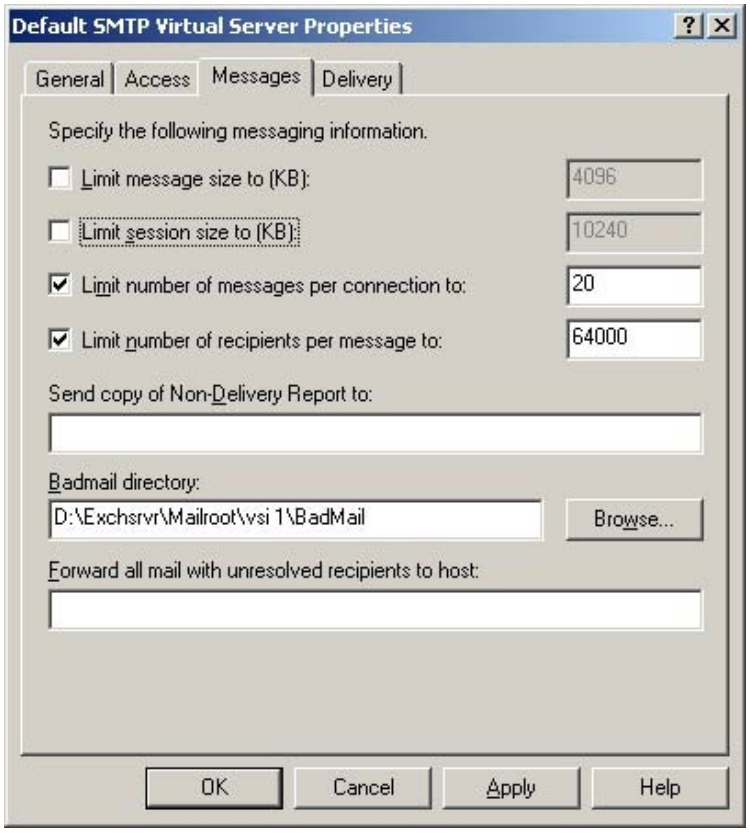


Abbildung: Maximalwerte des Virtual Servers

Banner-Information bereinigen

Der SMTP-Dienst von Exchange meldet sich beim Aufbau einer SMTP-Verbindung standardmäßig mit einem Banner, das unter anderem auch Informationen über die Softwareversion preisgibt. Es wird dringend empfohlen, solche Informationen aus dem Banner zu entfernen, etwa mit dem Werkzeug MetaEdit aus der IIS-Metabase. Die Informationen im Banner sollten keine Rückschlüsse auf die Art der eingesetzten Software und ihrer Version ermöglichen.

Konfiguration der POP3, IMAP4 und NNTP Netzprotokolle

Der Zugriff auf einen Exchange-Server kann unter anderem über die Protokolle POP3, IMAP4 oder NNTP stattfinden. Entscheidet sich eine Institution, diese Protokolle einzusetzen, so sollten Einstellungen zur Authentisierung und Verschlüsselung vorgenommen sowie Zugriffseinschränkungen auf Basis der IP-Adressen oder Domänennamen definiert werden. Dies erfolgt in den jeweiligen Protokolleinstellungen.

Die benutzerbezogenen Einstellungen, wie z. B. die Aktivierung bzw. Deaktivierung des POP3- bzw. IMAP-Zugriffs, werden mit dem MMC-Snap-In *Active Directory Users and Computers* vorgenommen (Registerkarte *Exchange advanced*, Schaltfläche *Protokolleinstellungen* | *Protokolle*).

Authentisierung

Als Authentisierungsmechanismus sollte die integrierte Windows Authentisierung der HTTP Basic Authentisierung vorgezogen werden. Die HTTP Basic

Authentisierung sollte nur in Verbindung mit TLS-Verschlüsselung eingesetzt werden. Für das NNTP-Protokoll muss überlegt werden, ob ein anonymer Zugriff auf den Server erlaubt werden soll. In jedem Fall wird empfohlen, für das NNTP-Protokoll Einschränkungen bezüglich der Maximalgröße der zu veröffentlichenden Nachrichten zu definieren (Registerkarte *Settings*).

Verschlüsselung

Die Verschlüsselung der Verbindungen wird empfohlen, wenn sensitive Daten über ungeschützte Kommunikationswege übertragen werden oder HTTP Basic Authentisierung zum Einsatz kommen soll. Die TLS-Verschlüsselung für eingehende Verbindungen wird in den Protokolleinstellungen in der Registerkarte *Access*, Bereich *Secure communication* aktiviert. Bei der Übertragung besonders schützenswerter Daten sollte die 128-Bit-Verschlüsselung eingesetzt werden. Es ist jedoch zu beachten, dass für die Aktivierung der Verschlüsselung eingehender Verbindungen ein entsprechendes Server-Zertifikat benötigt wird.

Zugriffseinschränkungen

Es wird empfohlen, die Zugriffseinschränkungen auf Basis der IP-Adressen oder der Domänennamen zu definieren, sofern die Menge der Clients festgelegt werden kann.

Nachrichtenformat

einfache Textnachrichten

Nachrichten im HTML-Format können auch aktive Elemente enthalten, was ein Sicherheitsrisiko für Clients darstellt. Deshalb wird empfohlen, die Nachrichten über POP3 und IMAP4 als einfache Textnachrichten auszuliefern (*message body as plain text*, Registerkarte *Message Format*). Von der Verwendung des Rich-Text-Formats (RTF) wird abgeraten.

Protokollierung

Aus Sicht der IT-Sicherheit muss der Betrieb eines Exchange-Systems protokolliert werden. Hierzu wird auf die Maßnahme M 4.167 *Überwachen eines Exchange-Systems* verwiesen.

Generelles

Zusätzlich zu den hier beschriebenen Maßnahmen müssen die im Baustein 6.9 Windows 2000 Server empfohlenen Maßnahmen zur Absicherung des Windows 2000 Systems (speziell Active Directory) umgesetzt werden.

Sobald die Installation und die Konfiguration eines Exchange-Servers abgeschlossen ist, sollte eine Datensicherung durchgeführt werden.

Ergänzende Kontrollfragen:

- Wurden die Routing Groups im Vorfeld der Konfiguration definiert?
- Wurden die Administrativen Gruppen der Exchange 2000 Installation festgelegt?
- Ist organisationsintern geklärt, ob der Zugriff via Outlook Web Access auf E-Mail-Konten erlaubt werden soll?

M 4.163 Zugriffsrechte auf Exchange 2000 Objekte

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Sicherheit von Exchange 2000 wird unter anderem von der Sicherheit des Active Directory von Windows 2000 bestimmt. Ein wesentlicher Bestandteil der Installation von Exchange 2000 ist die Schema-Erweiterung des Active Directory, bei der Exchange-spezifische Objekte und zusätzliche Attribute zu bereits bestehenden Objekten dem Verzeichnisdienst hinzugefügt werden. Die wichtigsten Objekte sind: *Mailbox, Custom Recipient, Distribution List, Connectors, Public Folder* sowie *Server.*

Zugriffsrechte auf Exchange-Objekte

Diese Objekte speichern zum großen Teil personen- und organisationsbezogene Daten, steuern die Verteilung von E-Mails und müssen daher vor unberechtigten Zugriffen geschützt werden. Die Vergabe der Zugriffsrechte auf die Exchange-Objekte ist von zentraler Bedeutung für die Sicherheit einer Exchange-Installation. Die Zugriffssteuerung erfolgt über Access Control Lists (ACLs). Die Vergabe der Zugriffsberechtigungen auf die Exchange-Objekte geschieht wie im Active Directory üblich. Deshalb sei in diesem Zusammenhang auf folgende Maßnahmen des Bausteins Windows 2000 Server verwiesen:

- M 2.229 *Planung des Active Directory*
- M 2.230 *Planung der Active Directory-Administration*
- M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000*
- M 4.137 *Sichere Konfiguration von Windows 2000*

Konfigurationswerkzeuge

Microsoft Management Console

Die Administration der Exchange 2000 Objekte erfolgt - wie bei Windows 2000 üblich - über die sogenannte *Microsoft Management Console* (MMC) und zugehörige Snap-Ins: Exchange System, Exchange Message Tracking System und Exchange Advanced Security.

Das Dienstprogramm *ADSI Edit* kann zur Anzeige der Informationen im Active Directory verwendet werden.

Administration der Zugriffsrechte

gesondertes Benutzerkonto verwenden

Nach der Standardinstallation von Exchange 2000 unter dem Administratorkonto besitzen Domänen- und Enterprise-Administratoren volle Administrationsrechte über die Exchange-Organisation. Dies ist jedoch unerwünscht, da so keine klare Trennung der Administrationsaufgaben möglich ist. Daher wird empfohlen, die Installation unter einem gesonderten Benutzerkonto durchzuführen, wie es in der Maßnahme M 4.161 *Sichere Installation von Exchange/Outlook* 2000 beschrieben wird.

Auf der Ebene der Organisation oder der administrativen Gruppen sollte für die Zuweisung von Berechtigungen stets der *Assistent für die Zuweisung von Verwaltungsberechtigungen auf Exchange-Objekte* im Exchange System Manager verwendet werden.

Konfiguration von Exchange 2000 spezifischen Benutzerberechtigungen

Die Exchange 2000 spezifischen Berechtigungen können individuellen Benutzer- und Gruppenkonten zugewiesen werden (über die Registerkarte *Security* in den jeweiligen Benutzer-Objekteinstellungen). Eine gruppenorientierte Berechtigungsvergabe ist dabei grundsätzlich vorzuziehen.

Die folgenden Berechtigungen sollten grundsätzlich nur die Exchange-Administratoren besitzen:

- *Add PF to Admin Group* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, den öffentlichen Ordner zu einer administrativen Gruppe hinzuzufügen.
- *Administer Information Store* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, den Informationsspeicher zu verwalten.
- *Create named Properties in the Information Store* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, Eigenschaften mit eigenen Bezeichnungen anzulegen (wie Anzeigename, Vorname, Nachname, Markierungen für gelöschte Einträge, usw.).
- *Create Public Folder* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, öffentliche Ordner unterhalb des momentan ausgewählten Ordners anzulegen.
- *Create Top-Level Public Folder* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, öffentliche Ordner auf der obersten Ebene in der Ordnerhierarchie anzulegen.
- *Full Store Access* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, in vollem Umfang auf die Datenbanken des Informationsspeichers zuzugreifen.
- *Mail-Enable Public Folder* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, einem öffentlichen Ordner E-Mail-Adressen zuzuweisen.
- *Modify Public Folder ACL* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, die ACLs eines öffentlichen Ordners zu modifizieren.
- *Modify Public Folder Admin ACL* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, die ACLs eines öffentlichen Ordners für Administratoren zu verändern.
- *Modify Public Folder Deleted Item Retention* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, die Zeitspanne in Tagen festzulegen, die gelöschte Objekte im öffentlichen Ordner erhalten bleiben sollen.
- *Modify Public Folder Expiry* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, eine Altersgrenze für die Objekte im öffentlichen Ordner festzulegen.
- *Modify Public Folder Quotas* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, eine Größenbeschränkung für den öffentlichen Ordner festzulegen.
- *Modify Public Folder Replica List* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, die Liste der Replikate des Ordners zu modifizieren. Der Administrator muss diese Berechtigung sowohl

auf der administrativen Gruppe als auch auf der öffentlichen Ordnerdatenbank besitzen, um ein Replikat erfolgreich anlegen und die Replikation von öffentlichen Ordnern verwalten zu können.
- *Open Mail Send Queue* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, die ein- und ausgehenden Nachrichtenwarteschlangen des Informationsspeichers anzeigen zu können.
- *Read All Metabase Properties* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, die Metabase der Internet Information Services zu lesen.
- *Remove PF from Admin Group* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, einen öffentlichen Ordner aus der administrativen Gruppe zu entfernen.
- *View Information Store Status* gibt an, ob das Benutzerkonto über die Berechtigung verfügt, die Statusinformationen des Informationsspeichers anzuzeigen. Beispiele solcher Statusinformationen sind Informationen zu den momentan angemeldeten Benutzern und den ihnen zugeordneten Ressourcen.

Mailbox-Speicher

Es wird empfohlen, das "lockdown"-Skript (*edslock.vbs*) auf allen Exchange 2000 Servern auszuführen. Dadurch werden Implementierungsfehler behoben und Zugriffsmöglichkeiten auf die Mailbox-Stores des lokalen Servers eingeschränkt. **lockdown**

Zugriffsrechte auf die privaten Postfächer (Mailbox)

Die standardmäßig vergebenen Zugriffsrechte auf ein privates Postfach eines Benutzers brauchen im Allgemeinen nicht angepasst werden, da nur dem Postfach-Besitzer Leseberechtigungen und voller Zugriff auf das Postfach eingeräumt werden. Es ist zu beachten, dass diese Berechtigungen nicht über den *Exchange System-Manager* sondern mit Hilfe des MMC-Snap-Ins *Active Directory Users and Computers* in den Eigenschaften des jeweiligen Benutzerkontos vergeben werden (Registerkarte *Exchange Advanced*).

Einschränkung der Zugriffsrechte auf öffentliche Ordner

Die standardmäßig nach der Installation von Exchange 2000 vergebenen Zugriffsrechte erlauben den Mitgliedern der Gruppe *Jeder* (*Everyone*) das Erstellen von neuen öffentlichen Ordnern aus Outlook heraus. Dieses Recht sollte jedoch soweit wie möglich eingeschränkt werden, da der Besitzer eines öffentlichen Ordners dort auch Formulare veröffentlichen kann, die aktive Inhalte enthalten können. Da dies u. U. ein Sicherheitsrisiko darstellt, sollten nur wenige Personen das Recht besitzen, neue öffentliche Ordner anzulegen.

Es wird daher empfohlen, folgende Rechte nur vertrauenswürdigen Personen zu gewähren:

- Create Top-Level Public Folders
- Create Public Folders
- Create Named Properties

Der Gruppe *Jeder* sollten außerdem auch die administrativen Berechtigungen (z. B. das Recht, ACLs oder andere Eigenschaften eines Ordners zu ändern) explizit verwehrt werden.

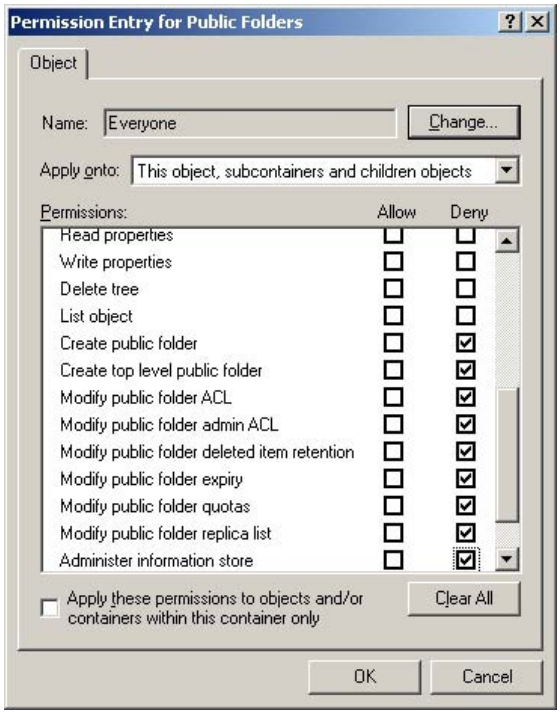


Abbildung: Berechtigungen

Die Vergabe der Berechtigungen *Create Public Folder*, *Create Top Level Public Folder*, *Modify Public Folder ACL*, *Modify Public Folder Admin ACL* geschieht im *Exchange System-Manager* in den Eigenschaften des jeweiligen öffentlichen Ordners (Registerkarte *Security*). Weitere Zugriffsberechtigungen auf öffentliche Ordner werden in der Registerkarte *Permissions* vergeben. Dort befinden sich die drei Schaltflächen *Client permissions*, *Directory rights* und *Administrative rights*.

Sicherheitseinstellungen für Organisationsformularbibliotheken (OFL)

Ordnerformularbibliotheken werden bei der Erstellung eines Nachrichtenordners implizit angelegt. Diese erben die Einstellungen der Ordnerkonfiguration und die Benutzerberechtigungen. Auf der Ebene des Systemordners (der verborgen ist) liegt die Organisationsformularbibliothek. Standardmäßig kann nur der Administrator, der die Organisationsformularbibliothek erstellt hat, Outlook-Formulare dort registrieren.

Es wird empfohlen, die Berechtigungen für die Registrierung der Outlook-Formulare sehr restriktiv zu vergeben, da die Formulare auch mit aktiven Inhalten ausgestattet werden können. Sollen weitere Benutzer diese Berechtigungen besitzen, so kann dies mit Hilfe des *Exchange System-Managers* festgelegt werden: mit der rechten Maustaste unter *EFORMS REGISTRY* auf den Ordner der Organisationsformularbibliothek klicken, *Properties* wählen, zur Registerkarte *Permissions* wechseln und auf die Schaltfläche *Client Permissions* klicken, um weitere Benutzer anzugeben.

Vergabe der Berechtigung *send on behalf* und ähnlicher Berechtigungen

Folgende Exchange 2000 spezifische Berechtigungen sind bei der Festlegung von Stellvertretern für Benutzer von Bedeutung: *Senden als* (*send as*), *Senden im Auftrag* (*send on behalf*) und *Empfangen als* (*receive as*). Diese Berechtigungen werden mit dem MMC-Snap-In *Active Directory Users and Computers* in den Eigenschaften des jeweiligen Benutzers vergeben (*send as* und *receive as* auf der Registerkarte *Security*, *send on behalf* auf der Registerkarte *Exchange General*).

Berechtigung "send as" verwenden

Von der Vergabe der Berechtigung *send as* an Benutzer wird grundsätzlich abgeraten. Falls notwendig, sollte stattdessen die Berechtigung *send on behalf* vergeben werden, die auch dann gesetzt wird, wenn ein Benutzer auf der Registerkarte *Delegation* in den Outlook-Einstellungen einen Benutzer als seinen Stellvertreter angibt.

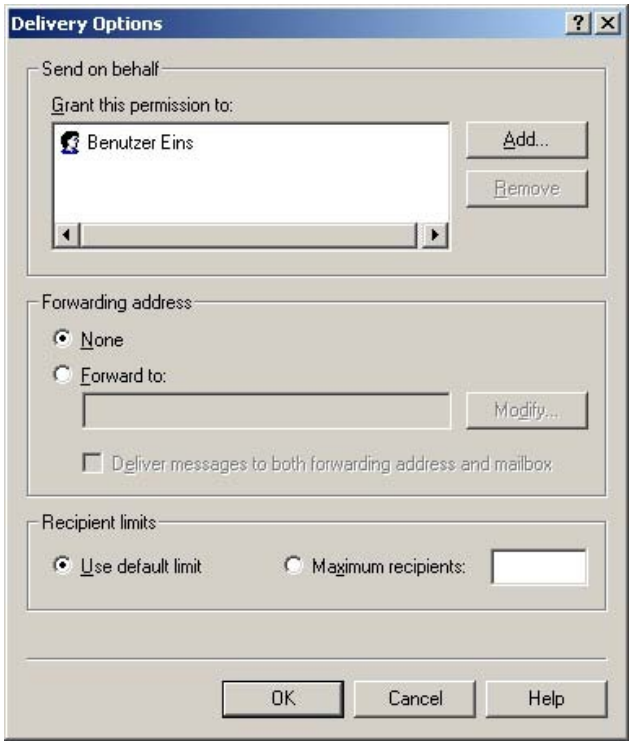


Abbildung: Vergabe der Berechtigung *sennd on behalf*

Diese Berechtigungen sind in hohem Maße sicherheitsrelevant. Die Berechtigungen *send on behalf* und *receive as* sollten nur sehr restriktiv und die Berechtigung *send as* sollte gar nicht vergeben werden.

Ergänzende Kontrollfragen:

- Wurde die Rolle eines Exchange-Administrators definiert und eine entsprechende Benutzergruppe eingerichtet?
- Wurden die Zugriffsberechtigungen auf Exchange-Objekte auf der Grundlage der Sicherheitsrichtlinie festgelegt?
- Werden die Exchange-Objekte im Rahmen der Replikation des Active Directory geeignet verteilt?

M 4.164 Browser-Zugriff auf Exchange 2000

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Outlook Web Access

Exchange 2000 bietet die Möglichkeit, auf Exchange-Server über das HTTP-Protokoll zuzugreifen. Benutzer erhalten damit über einen Web-Browser eine Oberfläche, die der von Outlook 2000 entspricht. Diese Zugriffsmöglichkeit trägt in der Exchange-Terminologie den Namen *Outlook Web Access* (OWA).

Web Store

Eine weitere Funktionalität von Exchange 2000 ist der so genannte *Web Store* (*Installable File System* - IFS), der den Benutzern ein Web-basiertes Dateisystem zur Verfügung stellt. Dieses (virtuelle) Dateisystem IFS ist auch über das "normale" Windows-Dateisystem erreichbar. Das Laufwerk M ist dabei standardmäßig dem Web Store zugewiesen.

In der Vergangenheit gab es unter Verwendung der OWA-Funktionalität einige erfolgreiche Angriffe auf Exchange. Bei diesen Angriffen konnten auch Daten des Global Catalog Servers kompromittiert werden. Daher muss bei der Planung des Exchange-Einsatzes entschieden werden, ob die OWA-Funktionalität prinzipiell genutzt werden soll. Da OWA standardmäßig nach der Installation von Exchange 2000 zur Verfügung steht, muss es explizit deaktiviert werden, wenn es nicht benutzt werden soll.

Bei der Verwendung der OWA-Funktionalität sind vor allem die folgenden Aspekte sicherheitsrelevant:

- Authentisierung und
- Datenintegrität und Datenvertraulichkeit.

Während die Authentisierung gewährleistet werden kann, können Datenintegrität und Datenvertraulichkeit nicht wie gewünscht realisiert werden. Unter Verwendung von OWA ist das Signieren und Verschlüsseln der Daten nicht möglich. Die Vertraulichkeit der Datenübertragung kann jedoch durch die Nutzung einer SSL/TLS-Verbindung zum IIS-Server gewährleistet werden.

OWA möglichst nicht nutzen

Aus diesen Gründen sollte auf den Einsatz der OWA-Funktionalität möglichst verzichtet werden.

Konfigurationswerkzeuge

MMC und Exchange System-Manager

Die Konfiguration erfolgt mit drei unterschiedlichen Werkzeugen: mit dem Internetdienst-Manager, dem *Exchange System-Manager* und dem MMC-Snap-In *Active Directory Users and Computers*.

Die Einstellungen der Standard-Webseite (unter anderem auch die Sicherheitseinstellungen) werden mit dem Internetdienst-Manager vorgenommen. Die Zugriffsrechte auf die virtuellen Verzeichnisse von OWA werden dagegen mit dem *Exchange System-Manager* konfiguriert. Die benutzerbezogenen Einstellungen, wie z. B. die Aktivierung/Deaktivierung des Browser-Zugriffs, werden mit dem MMC-Snap-In *Active Directory Users and Computers* vorgenommen (Registerkarte *Exchange advanced*, Schaltfläche *Protocol settings | HTTP Settings*).

Einige Einstellungen lassen sich mit dem *Exchange System-Manager* und mit dem Internetdienst-Manager vornehmen. In solchen Fällen wird empfohlen, den *Exchange System-Manager* zu verwenden.

Zugriffskontrolle, Authentisierung und Verschlüsselung

Anonymen Zugriff verwenden

Jedes virtuelle Verzeichnis, auf das ein Benutzer zugreifen kann, besitzt in seinen Eigenschaften die Registerkarte *Access*, in der Einstellungen für die Zugriffskontrolle, Ausführungsberechtigungen sowie Authentisierung vorgenommen werden können. Jeder Zugriff auf Postfachressourcen muss authentisiert werden. Ebenso ist es ist nicht empfehlenswert, den anonymen Zugriff auf die MAPI-basierte öffentliche Ordnerhierarchie (als *http://<Servername>/public* veröffentlicht) zu erlauben. Denn standardmäßig weist das System den anonymen Benutzern das Gastkonto des IIS zu (*IUSR_<Servername>*), welches ein gültiges Windows 2000-Benutzerkonto ist. Deshalb werden in diesem Fall die Standardberechtigungen für Clients angewendet und nicht die Berechtigungen des Kontos *Anonym*. Man kann jedoch dem Gastkonto des IIS eine E-Mail-Adresse zuweisen und damit die Vergabe expliziter Zugriffsberechtigungen für anonyme Benutzer im *Exchange System-Manager* oder Outlook 2000 ermöglichen.

sichere Authentisierung

Beim Browser-Zugriff auf Exchange-Daten stehen folgende Authentisierungsmethoden zur Verfügung: Anonymer Zugriff, HTTP Basic Authentisierung sowie integrierte Windows 2000 Authentisierung. Die entsprechenden Einstellungen werden in den Eigenschaften des jeweiligen virtuellen HTTP-Serverobjektes in der Registerkarte *Access* vorgenommen. Es wird empfohlen, keinen anonymen Zugriff zu erlauben und die integrierte Windows 2000 Authentisierung zu verwenden. Es ist jedoch zu beachten, dass die integrierte Windows-Authentisierung nur bei Verwendung des Microsoft Internet Explorers als Web-Browser zur Verfügung steht. Beim Einsatz anderer Web-Browser sollte die HTTP Basic Authentisierung zusammen mit einer Verschlüsselung der Übertragungswege benutzt werden.

Bei der Verwendung von OWA wird generell empfohlen, die Verschlüsselung zu aktivieren, wenn Exchange-Daten über nicht vertrauenswürdige Netze transportiert werden (insbesondere im Internet). Die Verschlüsselung wird mit Hilfe des Internetdienst-Managers (IIS-Einstellungen) aktiviert. Es ist zu beachten, dass ein geeignetes Server-Zertifikat benötigt wird.

dedizierte virtuelle Server einrichten

In der Registerkarte *General* kann über den so genannten Exchange-Pfad angegeben werden, ob der virtuelle HTTP-Server für den Zugriff auf Postfächer und öffentliche Ordner oder ausschließlich für den Zugriff auf öffentliche Ordner konfiguriert wird. Es wird empfohlen, für den Zugriff auf öffentliche Ordner dedizierte virtuelle Server einzurichten.

Es wird weiterhin empfohlen, Zugriffseinschränkungen auf Basis von IP-Adressen oder Domänennamen zu definieren, sofern die Menge der Clients festgelegt werden kann. Dies erfolgt in der Registerkarte *Access* (Bereich *Connection control*). Dabei sollten die erlaubten IP-Adressen bzw. Domänennamen angegeben und allen anderen der Zugriff verwehrt werden (*default deny policy*).

Skript-Quellzugriff verbieten

In den Einstellungen des HTTP-Protokolls können in der Registerkarte *Access* auch die Berechtigungen für eingehende Clientverbindungen beschränkt werden (Lesen, Schreiben, Skript-Quellzugriff sowie Verzeichnissuche). Es wird empfohlen, den Skript-Quellzugriff unter keinen Umständen zu gewähren.

Weiterhin sollte die Ausführung von Skripten und ausführbaren Dateien nach Möglichkeit verboten werden.

Deaktivieren virtueller Exchange HTTP-Server

Sämtliche virtuellen HTTP-Server können im *Exchange System-Manager* beendet bzw. angehalten werden. Es sollte beachtet werden, dass der Standard-HTTP-Server den Zugriff auf die Eigenschaften der öffentlichen Ordner über das virtuelle Verzeichnis *Exadmin* gewährleistet. Wenn dieser virtuelle Server beendet wird, können die Einstellungen der öffentlichen Ordner im *Exchange System-Manager* nicht mehr verwaltet werden. Es erscheint eine Fehlermeldung, dass der Zugriff auf die öffentlichen Ordner fehlgeschlagen ist.

Schulung der OWA-Benutzer

Vor der Verwendung der OWA-Funktionalität müssen die Benutzer entsprechend geschult werden. Dabei sollte besonders auf folgende Regeln geachtet werden:

- Nach Beendigung einer OWA-Sitzung sollten die Benutzer den Browser schließen, insbesondere dann, wenn sie sich an einem allgemein zugänglichen Computer befinden. Dadurch werden die Anmeldedaten gelöscht.
- Das Kennwort sollte unter keinen Umständen im Web-Browser gespeichert werden.
- Der lokale Zwischenspeicher des Browsers sollte nicht aktiviert sein. Anderenfalls verbleiben die Informationen auf der lokalen Festplatte und sind unter Umständen für andere Benutzer zugänglich.
- Der Cache des Browsers sollte gelöscht werden (manuell oder automatisch), wenn die Sitzung beendet wird.

Ergänzende Kontrollfragen:

- Ist entschieden, welche Personen Zugriff auf die Exchange-Daten über einen Web-Browser erhalten sollen?
- Findet eine den Sicherheitsanforderungen der Institution angepasste Benutzerauthentisierung statt?
- Gibt es eine Sicherheitsrichtlinie für die Verwendung der Web Stores?

M 4.165 Sichere Konfiguration von Outlook 2000

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Nach der Installation bzw. Verteilung von Outlook 2000 innerhalb einer Institution muss die Client-Software entsprechend konfiguriert werden, um einen sicheren Betrieb der Exchange/Outlook-Umgebung zu gewährleisten. Grundsätzlich ist hier die Maßnahme M 5.57 *Sichere Konfiguration der Mail-Clients* umzusetzen.

Nachfolgend werden Empfehlungen speziell für Outlook 2000 unter anderem zu folgenden Themen beschrieben:

- Administrations-Tools zur Konfiguration von Outlook 2000
- aktive Inhalte in Outlook 2000
- E-Mail-Signaturen und -Verschlüsselung
- Filterregeln als Anti-Spam-Mechanismus
- Umgang mit Makros in Outlook 2000
- Sichere Lagerung der Outlook-Daten
- Zugriffsschutz der Outlook-Objekte (Outlook-Ordner als ganzes bzw. einzelne Objekte, wie Aufgaben oder Kontakte)
- Umgang mit E-Mail-Anhängen
- Umgang mit speziellen Nachrichten (*Out-of-Office*-Meldungen bzw. Empfangsbestätigungen)
- Kommunikationssicherheit aus Sicht von Outlook 2000
- Gebrauch des Outlook 2000 SR-1 Sicherheits-Updates

Es wird dabei davon ausgegangen, dass Outlook 2000 als MAPI-Client zu Exchange 2000 und nicht als Internet-Mail-Client eingesetzt wird.

Allgemeine Empfehlungen

Es wird empfohlen, Einstellungen in der Exchange/Outlook-Umgebung soweit wie möglich durch Administratoren vornehmen zu lassen. Nur in Ausnahmefällen, in denen dies nicht möglich ist, sollten die Einstellungen durch Benutzer vorgenommen werden.

Einstellungen, die durch Administratoren zentral vorgegeben werden, müssen vor Änderungen durch Benutzer geschützt werden, so dass diese das vorgegebene Sicherheitsniveau nicht durch Fehlkonfigurationen abschwächen können. Leider ist dies nicht für alle Einstellungen möglich. Besteht diese Möglichkeit, so wird in den nachfolgenden Empfehlungen darauf hingewiesen.

Sichere Konfiguration des zugrunde liegenden Betriebssystems

Als Voraussetzung für eine sichere Konfiguration von Outlook 2000 ist zunächst das zugrunde liegende Betriebssystem sicher zu konfigurieren. Für Arbeitsplätze mit dem Betriebssystem Windows 2000 ist dazu insbesondere die Maßnahme M 4.150 *Konfiguration von Windows 2000 als Workstation* umzusetzen.

Für die allgemeine Konfiguration und Administration von Clients bietet Windows 2000 den Richtlinien-Mechanismus an. Es wird empfohlen, diese Richtlinien zu nutzen (siehe Baustein B 3.209 *Client unter Windows*), da so eine zentrale Administration erreicht werden kann.

Administrationswerkzeuge

Die Administration bzw. Konfiguration von Outlook 2000 kann zu unterschiedlichen Zeitpunkten stattfinden: noch vor der eigentlichen Verteilung und Installation von Outlook 2000 (sogenannte Vorkonfiguration) oder dann, wenn Outlook bereits verteilt ist. Durch Administrationswerkzeuge für Outlook 2000, wie dem *Custom Installation Wizard*, hat der Administrator beispielsweise die Möglichkeit, eine vorkonfigurierte Version der Outlook 2000 Software für die spätere Verteilung und Installation zentral zu erzeugen.

Für mittle und große Unternehmen bzw. Behörden wird empfohlen, Administrationswerkzeuge zur Konfiguration und Administration von Outlook 2000 Clients zu verwenden. Der Einsatz von Administrationswerkzeugen erleichtert die Arbeit der Administratoren und verhilft zu einem gleichmäßig hohen Sicherheitsniveau in der Institution. Für kleine Unternehmen bzw. Behörden sollte geprüft werden, ob sich der Einsatz von Administrationswerkzeugen lohnt.

Folgende Werkzeuge können von Administratoren benutzt werden:

- *Custom Installation Wizard*: Durch den *Custom Installation Wizard* besteht die Möglichkeit, bei der Installation von Outlook 2000 spezielle Installationspakete zu verwenden, die auf die Anforderungen der Institution angepasst sind. Das Installationspaket kann unter anderem dazu benutzt werden, die Konfiguration der Client-Einstellungen vorzugeben und die zu installierenden Outlook-Komponenten festzulegen. Dadurch können einige der im Folgenden beschriebenen Empfehlungen bereits vor der Installation vom Administrator umgesetzt werden.
- *OutlookSecurity.oft* ist eine Vorlage zum Erzeugen von Sicherheitseinstellungen auf dem Exchange-Server, die dazu dient, das Sicherheits-Update anzupassen.
- Das administrative Template *Outlk9.adm* definiert eine Systemrichtlinie für Windows 2000 Gruppenrichtlinienobjekte, damit Outlook-Sicherheitseinstellungen auf den Clients organisationsweit zentral im Active Directory eingestellt und durchgesetzt werden können.

Verwenden von Benutzerprofilen

Sofern mehrere Benutzer einen PC gemeinsam verwenden, kann für jeden Benutzer ein eigenes Outlook-Profil mit den benutzerspezifischen Einstellungen angelegt werden. In diesem Fall sind die unterschiedlichen Outlook-Profile durch den Administrator einzurichten und gegeneinander abzusichern. Die Benutzerprofile können dabei entweder serverseitig oder auf dem Client abgelegt werden.

Es wird generell empfohlen, serverseitige Benutzerprofile zu verwenden. Meldet sich ein Benutzer an einer Windows 2000 Domäne an, so werden diese automatisch in die Registry (genauer in den Teil *HKEY_CURRENT_USER*) des Clients geladen (vergleiche M 4.162 *Sichere Konfiguration von Exchange 2000 Servern*). Es muss dabei beachtet werden, dass *Offline*-Arbeit (bei der die Daten in einer rechnerlokalen Kopie existieren) nicht möglich ist, wenn serverseitige Profile verwendet werden. Wird dies explizit gewünscht,

müssen die Outlook-Profile auf dem Client abgelegt werden. Es ist dabei zu beachten, dass Veränderungen am Profil dann jeweils nur für den lokalen Rechner gelten, so dass ein Benutzer unter Umständen auf verschiedenen Rechnern mit unterschiedlichen Profilen arbeitet.

Auch wenn Outlook-Profile lokal abgelegt werden, wird empfohlen, die Benutzerprofile von dem Exchange-Administrator erzeugen und verteilen zu lassen, damit eine sichere und konsistente Vorkonfiguration erfolgen kann. Der Exchange-Administrator erstellt dazu mit Hilfe des *Custom Installation Wizard* eine Profildatei (*outlook.prf*). Dieses Profil muss dann später in das Windows 2000 Systemverzeichnis - in der Regel *\Winnt* - des Zielrechners kopiert werden und dient als Basis für neue Benutzerprofile.

Schutz sensitiver Daten in Outlook 2000

Outlook-relevante Daten sicher lagern

Outlook-Daten werden in erster Linie im Postfachordner auf dem Exchange-Server gehalten. Es ist jedoch auch möglich, Outlook-Daten lokal auf dem Client zu speichern, wenn z. B. mit Offline-Ordnern (d. h. mit einer lokalen Kopie des serverseitigen Postfachordners) gearbeitet wird oder wenn der Benutzer lokal eigene persönlichen Ordner angelegt hat. Die auf den Clients gehaltenen Outlook-Daten sind generell einem höheren Risiko ausgesetzt als die serverseitig abgelegten Informationen, da für deren Schutz auch der Benutzer zuständig ist. Dieser muss für eigene persönliche Ordner die Sicherheit (z. B. Dateizugriffsrechte) selbst konfigurieren. Es ist deshalb in der Sicherheitsrichtlinie für Outlook festzulegen, ob Outlook-Daten auf den Benutzersystemen gehalten werden dürfen oder nicht. Es wird empfohlen, Outlook-Daten prinzipiell nicht clientseitig zu speichern. Dies schließt jedoch auch aus, dass mit Offline-Ordnern gearbeitet wird.

Kann auf das Arbeiten mit Offline-Ordnern nicht verzichtet werden, so sind die folgenden Empfehlungen für den Schutz der lokal abgelegten Outlook-Ordner zu berücksichtigen. Outlook speichert Informationen in persönlichen Ordnern (.pst-Dateien) sowie im Offline-Ordner (.ost-Dateien), die in diesem Fall auf der lokalen Festplatte des Clients liegen. Es ist zu beachten, dass zusätzlich Daten in den Systemverzeichnissen, den Installationsverzeichnissen von Outlook sowie in den Windows 2000 Benutzerprofilen (in der Regel *C:\Dokumente und Einstellungen \ <Benutzername> \ Anwendungsdaten \ Microsoft \ Outlook*) abgelegt werden. Diese sind daher mit restriktiven Zugriffsrechten zu versehen.

Datensicherung für lokale Outlook-Ordner

Werden persönliche Outlook-Ordner auf dem Benutzersystem abgelegt, muss gewährleistet sein, dass diese von der Datensicherung erfasst werden, um Datenverlust zu vermeiden. Dies gilt auch für Offline-Ordner.

Lokale Outlook-Ordner verschlüsseln

Es wird empfohlen, lokale Outlook-Ordner (d. h. persönliche Ordner und Offline-Ordner) zu verschlüsseln.

Die Verschlüsselung für Offline-Ordner wird unter *Extras* | *Dienste* | *Microsoft Exchange Server* | *Eigenschaften* auf der Registerkarte *Erweitert* unter *Einstellungen Offlineordnerdatei* aktiviert.

Die Verschlüsselung persönlicher Ordner kann ausschließlich beim Anlegen der Ordner konfiguriert und nachträglich nicht wieder verändert werden. Das Anlegen erfolgt unter *Extras* | *Dienste* | *Hinzufügen*: aus der Liste *verfügbare Informationsdienste* den Dienst *Persönliche Ordner* wählen und mit *OK* bestätigen. Es erscheint das Dialogfeld *Persönliche Ordner erstellen*, wo der Name des anzulegenden Ordners angegeben werden muss. Danach können im Konfigurationsmenü des jeweiligen Ordners die Verschlüsselungsoptionen gewählt werden.

Als Verschlüsselungsart stehen in Outlook 2000 entweder komprimierbare oder optimale Verschlüsselung zur Verfügung. Es wird die optimale Verschlüsselung empfohlen. Bei beiden Verschlüsselungsarten ist zu beachten, dass sie wegen einer bekannt schwachen Mechanismenstärke keinen hohen Schutz der Vertraulichkeit bieten.

Als zusätzlicher Schutz wird empfohlen, den Offline-Ordner bzw. persönliche Ordner in einem eigenen Verzeichnis zu speichern und dieses mit restriktiven Zugriffsrechten zu versehen. Das Verzeichnis sollte nur für den jeweiligen Benutzer zugreifbar sein.

Ein höherer Schutz der Vertraulichkeit der in den Ordnern gespeicherten Informationen lässt sich mit Hilfe der Windows 2000 Dateisystemverschlüsselung (EFS) oder mit Zusatzprodukten erreichen.

Kennwortschutz der lokalen persönlichen Outlook-Ordner nicht nutzen

Für die persönlichen Ordner kann ein Kennwortschutz aktiviert werden, dessen Verwendung jedoch wenig sinnvoll ist. Dieser Kennwortschutz ist schwach und kann mit im Internet verfügbaren Werkzeugen ausgehebelt werden.

Verlangt die Sicherheitsrichtlinie der Organisation zusätzlich, dass Passwörter zentral hinterlegt werden müssen, so steht der mit dem Kennwortschutz verbundene Sicherheitsgewinn in keinem Verhältnis zum administrativen Aufwand.

Von der Verwendung des Kennwortschutzes wird deshalb abgeraten.

Abbildung: Lokale Ordner verschlüsseln

Zugriffsberechtigungen auf zentrale Outlook-Ordner

In einer Exchange-Umgebung können persönliche Ordner für andere Benutzer zugreifbar gemacht werden. Dazu stehen insgesamt acht Berechtigungsstufen zur Verfügung, von der höchsten Berechtigungsstufe 8 (für den Besitzer des Ordners) bis hin zu keinen Berechtigungen.

Es wird generell empfohlen, Zugriffsberechtigungen restriktiv zu vergeben, so dass nur die unbedingt notwendigen Berechtigungen bestehen. Als sichere Grundeinstellung wird empfohlen, nur dem Besitzer den Zugriff zu gestatten. Insbesondere sollten dem Benutzer *Standard* keine Berechtigungen erteilt werden. Es ist zu beachten, dass sich die Zugriffsberechtigungen von übergeordneten Ordnern auf die untergeordneten Ordner vererben.

Sicherer Umgang mit dem Outlook 2000 Journal

Das Journal erfasst auf einer Zeitskala Aktivitäten, die mit Outlook 2000 durchgeführt wurden. Dazu gehören nicht nur gesendete und empfangene E-Mails, Termine und Aufgaben, sondern auch Aktivitäten im Zusammenhang mit Kontakten und Office-Dokumenten.

Journaleinträge können manuell erstellt oder auch automatisch generiert werden. Aus Sicherheitssicht muss beachten werden, dass die im Journal eingetragenen oder automatisch generierten Einträge vertrauliche Informationen und Datei-Verknüpfungen enthalten können. Daher wird empfohlen, Einträge nicht automatisch zu erzeugen. Dies kann unter *Extras* | *Optionen* auf der Registerkarte *Einstellungen* über die Schaltfläche *Journaloptionen* konfiguriert werden: Keiner der Einträge darf mit einem Häkchen versehen sein.

Wird ein Eintrag manuell erzeugt und haben andere Benutzer Zugriff auf den Outlook-Ordner, so wird empfohlen, den Eintrag als *Privat* zu markieren. Als *Privat* markierte Einträge werden anderen Benutzern nicht angezeigt. Es ist zu beachten, dass dies nur ein einfacher Schutzmechanismus ist, der lediglich das "zufällige Lesen" verhindert.

Im Rahmen der organisatorischen Sicherheitsrichtlinien sollte festgelegt werden, welche Dateien als Verknüpfungen in den Journaleinträgen zugelassen sind.

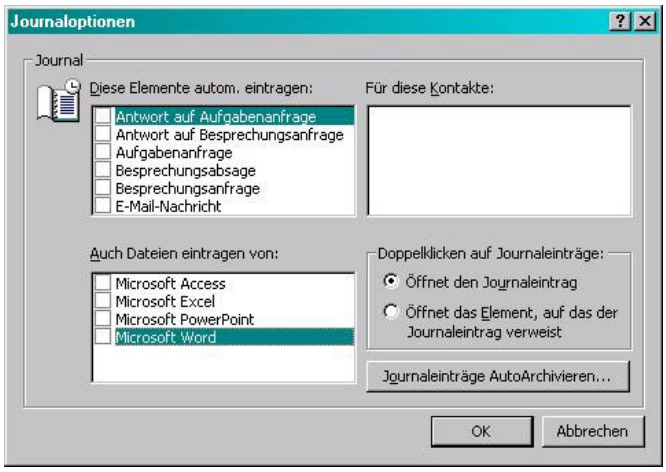


Abbildung: Journaloptionen

Schutz persönlicher Daten gegenüber Systemadministratoren

Lokal gehaltene persönliche Outlook-Daten (.pst-Dateien) sind durch Administratoren jederzeit einsehbar. Vertraulichkeit gegenüber den Administratoren kann daher nur durch Verschlüsselung erreicht werden. Dazu kann die Outlook-eigene (schwache) Verschlüsselung oder aber ein dateibasiertes Verschlüsselungssystem (EFS unter Windows 2000 oder ein Zusatzprodukt) eingesetzt werden. Wird Windows 2000 EFS genutzt, muss beachtet werden, dass der definierte Wiederherstellungsagent Zugriff auf die verschlüsselten Informationen hat. Bei einer Standardinstallation ist der Administrator automatisch als Wiederherstellungsagent definiert.

Beim Einsatz eines dateibasierten Verschlüsselungssystems wird empfohlen, eine Sicherheitsrichtlinie für das Hinterlegen der verwendeten Schlüssel zu definieren, damit der Zugriff auf die verschlüsselten Daten in Notsituationen möglich ist.

Schutz der Outlook/Exchange Kommunikation

Authentisierung

Die Authentisierungsmethode, die von Outlook 2000 als MAPI-Client gegenüber dem Exchange-Server genutzt wird, wird unter *Extras* | *Dienste* | *Microsoft Exchange Server* | *Eigenschaften* auf der Registerkarte *Erweitert* im Feld *Anmeldung-Netzwerksicherheit* eingestellt.

Es wird empfohlen, nicht auf die automatischen Anmeldeverfahren *NT Kennwortauthentifizierung* und *Verteilte Kennwortauthentifizierung* zurückzugreifen, sondern die Einstellung *Keine* zu verwenden. In diesem Fall

wird der Benutzer beim Zugriff auf den Exchange Server aufgefordert, seinen Benutzernamen und sein Passwort anzugeben.

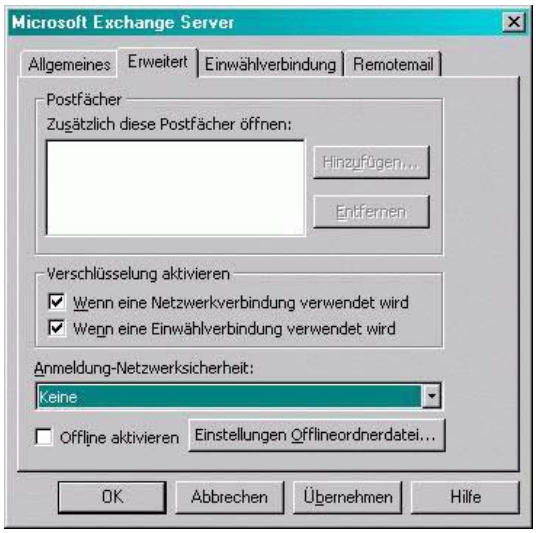


Abbildung: Anmeldung-Netzwerksicherheit

Wird Outlook 2000 als POP3/IMAP4/SMTP-Client zum Zugriff auf einen Exchange-Server oder einen anderen E-Mail-Server verwendet, wird empfohlen, die Methode *Anmeldung durch gesicherte Kennwortauthentifizierung* (*Extras* | *Dienste* | *Internet E-Mail* | *Eigenschaften* | *Server*) zu nutzen, sofern der E-Mail-Server dies unterstützt.

Zusätzlich wird die Einstellung *Server erfordert Authentifizierung* für den Postausgangs-Server empfohlen, die an der gleicher Stelle konfiguriert werden kann. In den Einstellungen sollte außerdem das Kontrollkästchen *Anmeldung durch gesicherte Kennwortauthentifizierung (SPA, Secure Password Authentication)* gesetzt werden. Der Postausgangs-Server muss dabei jedoch so konfiguriert sein, dass eine Authentisierung angefordert wird.

In keinem Fall darf das Benutzerkennwort gespeichert werden, d. h. das Kontrollkästchen *Kennwort speichern* ist zu deaktivieren. Anderenfalls besteht die Gefahr, dass die gespeicherten Kennwörter bei einem lokalen Zugriff auf das Benutzersystem mit öffentlich im Internet verfügbaren Werkzeugen ausgelesen werden.

Verschlüsselung der Kommunikation

Wenn Outlook 2000 als MAPI-Client eines Exchange-Servers eingesetzt wird, kann die in diesem Fall genutzte RPC-Kommunikation (*Remote Procedure Call*) zwischen Client und Exchange-Server durch Verschlüsselung geschützt werden. Ob diese Kommunikationsverschlüsselung genutzt wird, muss durch die Sicherheitsrichtlinie für Outlook festgelegt werden.

Die Verschlüsselung ist besonders dann zu empfehlen, wenn die Kommunikation zwischen den Outlook-Clients und dem Exchange-Server über unsichere Netze erfolgt. Die RPC-Verschlüsselung wird unter *Extras* | *Dienste* | *Micro*

soft Exchange Server | *Eigenschaften* auf der Registerkarte *Erweitert* im Feld *Verschlüsselung aktivieren* konfiguriert. Es wird empfohlen, beide angebotenen Optionen *Wenn eine Netzwerkverbindung verwendet wird* und *Wenn eine Einwählverbindung gewählt wird* zu aktivieren, damit die Kommunikation für beide Zugriffsarten abgesichert wird.

Werden die IP-basierten Protokolle POP3, IMAP4 und SMTP genutzt, so sollte SSL/TLS eingesetzt werden. Dies wird unter *Extras* | *Dienste* | *Internet*

E-Mail | *Eigenschaften* auf der Registerkarte *Erweitert* über das Kontrollkästchen *Dieser Server erfordert eine sichere Verbindung (SSL)* aktiviert.

Aktive Inhalte in Outlook 2000

Generell können in E-Mails die folgenden zwei Typen von aktiven Inhalten enthalten sein:

- Skripte in HTML-Mails
- Aktive Inhalte als E-Mail-Anhänge

Aktive Inhalte stellen eine Gefährdung für den Outlook-Client, den lokalen Rechner und für das gesamte lokale Netz dar, wenn diese unkontrolliert bewusst oder unbewusst ausgeführt werden. Der Schutz vor aktiven Inhalten kann dabei unter Outlook 2000 wie folgt konfiguriert werden.

Konfiguration der Sicherheitszonen

Die Einstellungen der Sicherheitszonen des Microsoft Internet Explorers sind auch für die Beschränkungen bei der Ausführung aktiver Inhalte in Outlook 2000 maßgeblich. Sie legen das Verhalten von Outlook 2000 beim Empfang von E-Mails oder beim Anzeigen von Web-Seiten (z. B. als Inhalt einer HTML-E-Mail) fest. Es ist zu beachten, dass die Einstellungen der Sicherheitszonen nicht Outlook 2000 spezifisch sind, sondern für das lokale System gelten. Veränderungen haben daher immer Auswirkungen auf alle anderen Programme, die diese Einstellungen nutzen (z. B. auf den Microsoft Internet Explorer).

Outlook-E-Mails können entweder der Zone *Internet* oder der Zone *Eingeschränkte Sites* zugeordnet werden. Es wird empfohlen, die Nachrichten der Zone *Eingeschränkte Sites* zuzuordnen, indem dies unter *Extras* | *Optionen* auf der Registerkarte *Sicherheit* im Abschnitt *Inhalt sichern* unter der Option *Zone* ausgewählt wird. Die Zoneneinstellung sollte gemäß den folgenden Empfehlungen angepasst werden.

Die Konfiguration der Sicherheitszonen kann generell durch Windows 2000 Gruppenrichtlinien für eine Gruppe von Rechnern bzw. Benutzern oder direkt auf einem Client in Outlook 2000 erfolgen. Es wird empfohlen, die Sicherheitszonen ausschließlich mittels Windows 2000 Richtlinien zu konfigurieren, um einheitliche Einstellungen zu erreichen. Ein weiterer Vorteil ist dabei die Möglichkeit, die vorgenommenen Einstellungen vor Veränderungen durch den Benutzer zu schützen.

Die Sicherheitseinstellungen für Internetzonen werden benutzerbezogen in der Richtlinie *Benutzerkonfiguration* | *Windows-Einstellungen* | *Internet Explorer-Wartung* | *Sicherheit* | *Sicherheitszonen und Inhaltsfilter* vorgenommen. Um

die vorgenommenen Einstellungen vor Änderungen durch Benutzer zu schützen, kann die Richtlinie *Computerkonfiguration* | *Administrative Vorlagen* |*Windows-Komponenten* | *Internet Explorer* | *Sicherheitszonen: Benutzer können Einstellungen nicht ändern* aktiviert werden.

Zusätzlich wird empfohlen, die Richtlinie *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Internet Explorer* | *Sicherheitszonen: Benutzer können Sites nicht hinzufügen oder entfernen* zu aktivieren, so dass der Gültigkeitsbereich der Zonen nicht durch Benutzer verändert werden kann.

Unter Outlook 2000 können die Sicherheitszonen unter *Extras* | *Optionen* auf der Registerkarte *Sicherheit* konfiguriert werden, sofern dies aufgrund der lokalen Sicherheitsrichtlinie für Outlook erlaubt ist.

Abbildung: Sicherheitseinstellungen

Die ausgewählte Sicherheitszone des Internet Explorers kann über die Schaltfläche *Zoneneinstellungen* aufgerufen werden.

Für die Zone sollte als Vorlage die Sicherheitsstufe *Hoch* gewählt werden, die dann weiter entsprechend der nachfolgenden Tabelle angepasst wird (Schaltfläche *Stufe anpassen*).

Option	Einstellung
ActiveX Steuerelemente ausführen, die für Scripting sicher sind	deaktiviert
ActiveX Steuerelemente initialisieren und ausführen, die nicht sicher sind	deaktiviert
ActiveX Steuerelemente und Plugins ausführen	deaktiviert
Download von signierten ActiveX Steuerelementen	deaktiviert
Download von unsignierten ActiveX Steuerelementen	deaktiviert
Anmeldung	Eingabe-auf-forderung
Dateiendownload	deaktiviert
Schriftartendownload	deaktiviert
Java permissions	Disable Java
Active Scripting	deaktiviert
Einfügeoperationen über ein Skript zulassen	deaktiviert
Scripting von Java Applets	deaktiviert
Auf Datenquellen über Domänengrenzen hinweg zugreifen	deaktiviert
Dauerhaftigkeit der Benutzerdaten	deaktiviert
Gemischte Inhalte anzeigen	deaktiviert
Installieren von Desktopobjekten	deaktiviert
Keine Aufforderung zur Clientzertifikatsauswahl, wenn kein oder nur ein Zertifikat vorhanden ist	deaktiviert
META REFRESH zulassen	deaktiviert
Programme und Dateien in einem iFrame starten	deaktiviert
Subframes zwischen verschiedenen Domänen bewegen	deaktiviert
Unverschlüsselte Formulardaten übermitteln	deaktiviert
Ziehen und Ablegen oder Kopieren und Einfügen von Dateien	deaktiviert
Zugriffsrechte für Softwarechannel	hoch

Tabelle: ActiveX-Steuerelemente und Plugins einrichten

Es ist zu beachten, dass die eingestellten Restriktionen der Zone für alle Programme gelten, die die Sicherheitszonen des Internet Explorers nutzen. Die angegebene Konfiguration ist sehr restriktiv, da verhindert werden soll, dass jegliche aktive Inhalte innerhalb von Outlook ausgeführt werden. Wird diese Zoneneinstellung durch den Internet Explorer auf Internet-Seiten angewandt,

so ist eine korrekte Anzeige der Seite unter Umständen nicht möglich, wenn sie Skripte oder sonstige aktive Inhalte enthält. Es ist derzeit nicht möglich, zusätzliche Sicherheitszonen zu definieren, so dass die Zone *Eingeschränkte Sites* auf die restriktiven Anforderungen von Outlook zugeschnitten werden muss.

Umgang mit potentiell gefährlichen Dateianhängen

Dateianhänge dürfen prinzipiell nicht automatisch aus E-Mails heraus geöffnet werden. Um dies zu verhindern, ist die Stufe *Hoch* für die Konfiguration der Anlagensicherheit (unter *Extras* | *Optionen* | *Sicherheit* auf der Schaltfläche *Anlagensicherheit*) auszuwählen.

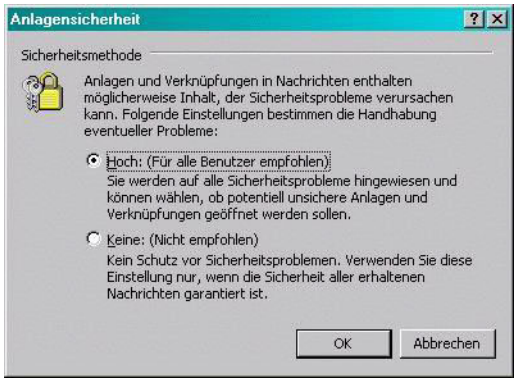


Abbildung: Anlagensicherheit

Um die Anlagensicherheit zu erhöhen, bietet Microsoft das Sicherheits-Update *Outlook 2000 SR-1 E-Mail Security Update International Release* (siehe

entsprechenden Abschnitt) an. Dies kann aber aufgrund der damit verbundenen Funktionseinschränkung aus praktischer Sicht nicht empfohlen werden.

Generell kann der Einsatz eines Filters auf einem E-Mail-Gateway oder einer Firewall empfohlen werden, um E-Mails auf potentiell gefährliche E-Mail-Anhänge zu kontrollieren und wenn nötig auszufiltern. Wird jedoch E-Mail-Verschlüsselung eingesetzt, so sind die auf einem E-Mail-Gateway eingesetzten Filter nicht mehr wirksam. In diesem Fall können E-Mail-Filter auf den Clients eingesetzt werden, die E-Mails nach der Entschlüsselung kontrollieren. Ob lokale E-Mail-Filter eingesetzt werden, muss im Einzelfall entschieden werden. Es ist zu beachten, dass hierdurch zusätzlicher Administrationsaufwand für die Verteilung, Installation und Wartung der Filter-Software anfällt.

Der zusätzliche Einsatz sogenannter *Personal Firewalls* kann das erreichbare Sicherheitsniveau erhöhen. Diese erlauben Beschränkungen für das Ausführen auf Betriebssystemebene und stellen für ausführbare E-Mail-Anhänge *Quarantäne-Bereiche* oder *Sandboxen* (d. h. kontrollierte Ablaufumgebungen) zur Verfügung. Auch hier muss der Einsatz eines solchen Produktes sorgfältig geprüft werden, da zusätzlicher Administrationsaufwand anfällt.

Vom Einsatz lokal installierter Produkte, wie E-Mail-Filter oder Personal Firewalls, wird abgeraten, wenn

- diese nicht zentral konfiguriert und administriert werden oder

- die vorgegebene Konfiguration durch den Benutzer geändert werden kann oder
- die Konfiguration sogar durch den Benutzer erfolgen muss.

Vorschaufenster deaktivieren

Wird das Vorschaufenster bzw. die Autovorschau von Outlook genutzt, werden E-Mails automatisch angezeigt und damit die in ihnen vorhandenen aktiven Inhalte automatisch ausgeführt. Es wird daher empfohlen, das Vorschaufenster und die Autovorschau zu deaktivieren. Dazu sind in Outlook die Optionen *Ansicht* | *Vorschaufenster* und *Ansicht* | *AutoVorschau* zu deaktivieren.

Sicherheitseinstellungen für die Makroverarbeitung in Outlook

Es wird empfohlen, die Sicherheitsstufe für Visual Basic (VBA) Makros unter *Extras* | *Makro* | *Sicherheit* | *Sicherheitsstufe* auf *Hoch* einzustellen. Dadurch können nur signierte Makros ausgeführt werden, deren Signaturen mit Hilfe bestimmter Zertifikate überprüft werden können. Die Liste der vertrauten Zertifikate kann unter *Extras* | *Makro* | *Sicherheit* | *Vertrauenswürdige Quellen* eingesehen werden.

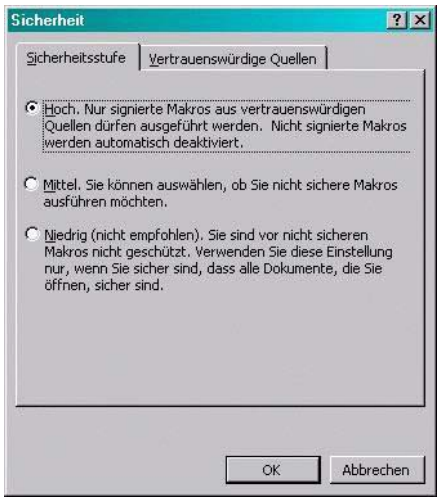


Abbildung: Sicherheitsstufe

Es muss beachtet werden, dass auch hier auf die sogenannten Authenticode-Einstellungen des Microsoft Internet Explorers zurückgegriffen wird. Änderungen wirken sich dadurch auf alle Programme aus, die diese Einstellungen nutzen.

Es wird empfohlen, die Liste der vertrauten Herausgeber zentral zu verwalten und diese mittels Windows 2000 Gruppenrichtlinien zu verteilen. Die zugehörige Richtlinie ist eine Benutzerrichtlinie, so dass für verschiedene Benutzergruppen unterschiedliche Voreinstellungen festgelegt werden können. Die Richtlinie findet sich in einem Gruppenrichtlinienobjekt unter *Benutzerkonfiguration / Windows-Einstellungen / Internet Explorer-Wartung / Sicherheit / Authenticode-Einstellungen*.

Es wird empfohlen, die Voreinstellungen gegen Veränderungen durch den Benutzer zu sperren, indem in den Authenticode-Einstellungen die Option *Sperrung für vertrauenswürdige Herausgeber aktivieren* eingeschaltet wird.

Abbildung: Authenticode-Einstellungen

Es muss beachtet werden, dass die Makro-Einstellungen nur für VBA Makros gelten, nicht jedoch für Visual Basic Script (Beschränkungen dazu erfolgen über die Einstellungen der Sicherheitszone).

Dürfen Benutzer die Liste der vertrauenswürdigen Herausgeber selbst aufbauen und verändern, so zeigt sich folgendes Verhalten: Wird ein signiertes VBA Makro geöffnet und befindet sich das zugehörige Zertifikat nicht in der Liste der vertrauenswürdigen Quellen, kann der Benutzer entscheiden, ob das Zertifikat in die Liste aufgenommen werden soll oder nicht. In der Liste vorhandener Zertifikate kann auch durch den Benutzer gelöscht werden. Diese Entscheidungen sind sicherheitsrelevant und sollten in der Regel nicht von den Benutzern getroffen werden. Für den Einsatz in Unternehmen und Behörden wird dieses Vorgehen daher nicht empfohlen.

E-Mail-Signaturen und E-Mail-Verschlüsselung

Für die Konfiguration der Ver- und Entschlüsselung sowie Signatur von E-Mails stehen unter Outlook generell zwei Mechanismen zur Verfügung:

- Exchange Server Security
- S/MIME

Die Einstellung *Exchange Server Security* setzt voraus, dass die *Key Management Services* von Windows 2000 verfügbar sind (siehe Baustein B 3.106

Server unter Windows 2000). In einem homogenen Windows 2000 Umfeld wird diese Einstellung empfohlen.

Ist dies nicht der Fall oder soll die E-Mail-Verschlüsselung über eine Windows-Domäne hinweg betrieben werden, so wird der Einsatz von S/MIME empfohlen.

Die Optionen zum Ver- und Entschlüsseln und zur digitalen Signatur von E-Mails werden unter *Extras* | *Optionen* auf der Registrierkarte *Sicherheit* über die Schaltfläche *Sicherheitseinstellung* konfiguriert. In dem Dialogfeld zu den Sicherheitsoptionen ist der Name einer Sicherheitseinstellung festzulegen. Weiterhin kann über die Option *Sicherheitsformat* zwischen S/MIME und *Exchange Server Security* gewählt werden. Die Zertifikate, die benutzt werden sollen, wenn Signaturen erstellt werden und wenn Verschlüsselt wird, können an dieser Stelle ausgewählt werden. Ebenso kann konfiguriert werden, welche Algorithmen zum Signieren und zum Verschlüsseln genutzt werden sollen. Welche Zertifikate und Algorithmeneinstellungen zu wählen sind, muss in der unternehmens- bzw. behördenweiten Sicherheitsrichtlinie für Outlook festgelegt werden.

Werden verschiedene Sicherheitseinstellungen verwendet, so muss für eine der Konfigurationen das Kontrollkästchen *Standardsicherheitseinstellung für dieses Sicherheitsformat für Nachrichten* aktiviert sein. Damit werden die Standardeinstellungen für das ausgewählte Sicherheitsformat festgelegt.

Werden sowohl *Exchange Server Security* als auch *S/MIME* genutzt, so kann das Kontrollkästchen *Standardeinstellung für alle sicheren Nachrichten* aktiviert werden, um die gewählten Sicherheitseinstellungen für beide Sicherheitsformate als Standardeinstellungen festzulegen. Auf diese Weise können die gleichen Zertifikate und Verfahren sowohl bei *Exchange Server Security* als auch bei *S/MIME* genutzt werden. Dazu müssen jedoch kompatible Zertifikate und Verfahren verfügbar sein.

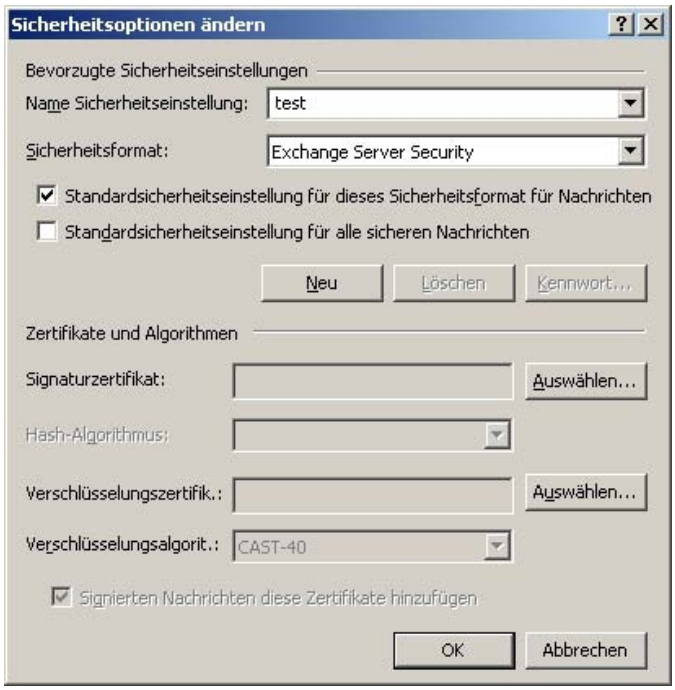


Abbildung: Sicherheitsoptionen ändern

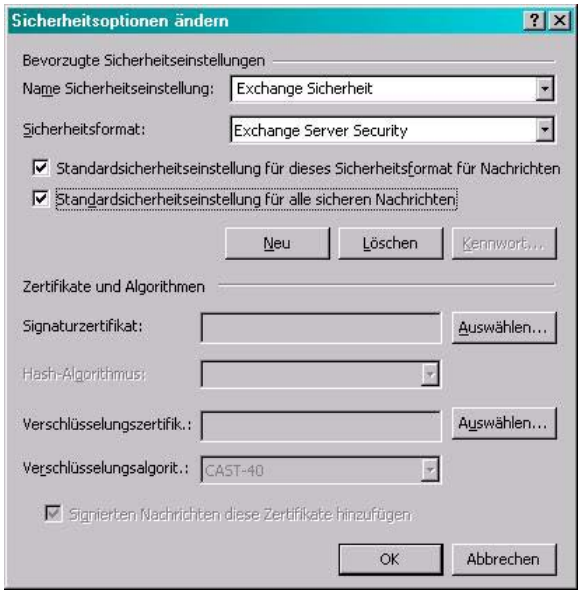


Abbildung: Standardsicherheitseinstellungen

Konfiguration der E-Mail-Filterregeln

Unerwünschte E-Mails (so genannte Spam-E-Mails) können das produktive Arbeiten stören. Outlook 2000 bietet die Möglichkeit, solche unerwünschten E-Mails mittels spezieller Filterregeln auszufiltern. Es wird jedoch empfohlen, Filtereinstellungen nicht durch Benutzer in der Outlook 2000 Client-Software vornehmen zu lassen, sondern das Filtern auf dem Server durchzuführen. Dies hat den Vorteil, dass alle E-Mails konsistent gefiltert werden und beschränkt den administrativen Aufwand auf einen definierten Punkt.

Ist eine serverseitige Filterung nicht erwünscht, so wird empfohlen, dass der Administrator die Filterregeln zentral erzeugt. Die Benutzer können diese dann über *Extras* | *Regel-Assistent* | *Optionen* importieren. Benutzereigene Regeln sollten dann nur zusätzlich erzeugt werden.

Abbildung: Regel-Assistent

Restriktive Stellvertreterberechtigungen

Outlook/Exchange erlaubt es, für Zeiten der Abwesenheit (z. B. Urlaub oder Krankheit) Stellvertreter zu definieren, die dann die Bearbeitung von E-Mails im Namen des Benutzers übernehmen können. Diese Stellvertreter erhalten Zugriff auf das Postfach bzw. einzelne Outlook-Ordner des jeweiligen Benutzers und können "im Auftrag" E-Mails verschicken.

Es wird empfohlen, dass Stellvertreter nur durch Postfachadministratoren und nicht durch Benutzer definiert werden. Die Gefahr eines Daten- bzw. Vertraulichkeitsverlusts durch Fehlkonfiguration wird dadurch verringert. Die Zugriffsberechtigungen für Stellvertreter können für die einzelnen Bestandteile des Outlook-Ordners (Kalender, Kontakte, Posteingang etc.) separat vergeben werden. Die Konfiguration erfolgt in den jeweiligen Objekteigenschaften. Die Stellvertreter-Regelungen sollten in den unternehmens- bzw. behördenweiten Richtlinien verankert sein.

Postfachadministratoren können die Berechtigung *Im Auftrag senden* mit dem Dienstprogramm *Active Directory-Benutzer und -Computer* konfigurieren.

Stellvertreter für Benutzer werden unter *Eigenschaften* | *Exchange-Allgemein* | *Zustelloptionen* definiert.

Stellvertreterberechtigungen können in Outlook 2000 im Bedarfsfall über *Extras* | *Optionen* auf der Registrierkarte *Stellvertretungen* mit *Hinzufügen* vergeben werden. Stellvertreter werden hierbei aus dem Adressbuch ausgewählt. Jedem Benutzer, dem der Stellvertreterzugriff auf ein fremdes Postfach gewährt wurde, wird automatisch die Berechtigung *Im Auftrag senden* erteilt. Dies bedeutet, dass die Stellvertreter die "Von"-Schaltfläche verwenden können, um den jeweiligen Namen im "Von"-Feld einer Nachricht hinzuzufügen. Die Nachrichtenempfänger werden dann den Hinweis "im Auftrag von" und den Namen des Kontoinhabers neben dem Namen des Stellvertreters in der "Von"-Zeile finden.

E-Mails nicht automatisch weiterleiten und verschieben

Der Regelassistent, mit dem die Filterregeln eingestellt werden, kann auch benutzt werden, um E-Mails automatisch an andere Benutzer weiterzuleiten und in bestimmte Ordner zu verschieben. Durch unbedacht eingerichtete Weiterleitungen oder Verschiebungen besteht jedoch die Gefahr des Daten- bzw. Vertraulichkeitsverlustes. Dies kann z. B. dann vorkommen, wenn E-Mails unerwartet vertrauliche Mitteilungen enthalten oder wenn der Ordner, in den E-Mails verschoben werden, keine restriktiven Zugriffsrechte besitzt.

Es wird daher empfohlen, E-Mails nicht automatisiert weiterzuleiten oder automatisch in Ordner zu verschieben.

Weitere Sicherheitsmaßnahmen für Benutzer

Absender- bzw. Empfängeradresse überprüfen

Wird die E-Mail-Adresse eines Absenders mit einem Anzeigenamen versehen, z. B. *BSI-Verteiler <falsche@adresse>*, so zeigt Outlook 2000 nicht immer die vollständige E-Mail-Adresse, sondern nur den Anzeigenamen an, in diesem Fall *BSI-Verteiler*. Durch diese Eigenschaft von Outlook 2000 besteht die Gefahr, dass manipulierte E-Mail-Adressen nicht als solche erkannt und

dadurch unter Umständen vertrauliche Informationen an unberechtigte Empfänger versandt werden.

Es wird daher empfohlen, die E-Mail-Adresse des Absenders (bzw. des Empfängers, wenn die "Antworten"-Funktion benutzt wurde) explizit anzuzeigen und zu kontrollieren. Die E-Mail-Adresse kann durch Doppelklicken auf den angezeigten Namen im "Von"- bzw. "An"-Feld angezeigt werden. Diese Überprüfung muss durch den Benutzer erfolgen.

Anzeigen der Header-Informationen

Bestehen Zweifel an der Herkunft einer E-Mail, so sollten die in einer E-Mail enthaltenen Header-Informationen überprüft werden. Diese sind im Feld *Internetkopfzeilen* unter *Ansicht* | *Optionen* zu finden. Neben zusätzlichen Informationen über den Absender ist hier auch der Weg vermerkt, auf dem die E-Mail vom Sender zum Empfänger übertragen wurde.

Es ist jedoch zu beachten, dass ein Angreifer die in seiner Nachricht enthaltenen E-Mail-Header verändern kann.

Erweiterte Funktionalität von Outlook 2000 deaktivieren

Deaktivieren des Outlook-Formulardesigners auf Clients

Der Outlook-Formulardesigner stellt eine Entwicklungsumgebung für Workflow-Anwendungen auf Basis von Outlook-Verzeichnissen dar. Hierdurch

können Sicherheitsprobleme entstehen, da dem Formularentwickler z. B. ActiveX-Steuerelemente zur Verfügung stehen. Normale E-Mail-Anwender benötigen diese Möglichkeit nicht. Es wird daher empfohlen, den Outlook-Formulardesigner auf den Clients zu deaktivieren.

Dazu stehen zwei Möglichkeiten zur Verfügung. Es kann ein angepasstes Installationspaket erstellt werden (*Customized Installation*), in dem der Formulardesigner nicht enthalten ist (siehe auch M 4.161 *Sichere Installation von Exchange/Outlook 2000*). Alternativ kann der Formulardesigner über eine Registry-Einstellung deaktiviert werden. Dazu ist unter *HKEY_USERS* \ *.DEFAULT* \ *Software* \ *Microsoft* \ *Office* \ *9.0* \ *Outlook* ein *REG_DWORD* namens *NoOutlookFormsDesigner* anzulegen. Der Wert muss auf *1* gesetzt sein, damit der Formulardesigner nicht mehr zur Verfügung steht. Der Registry-Eintrag wird dann automatisch in die benutzerspezifischen Registry-Zweige kopiert.

Es wird empfohlen, die angepasste Installation zu verwenden, wenn Outlook neu verteilt wird. Für bestehende Installationen kann der Registry-Eintrag über Windows 2000 Gruppenrichtlinien verteilt werden.

Nutzung von Folder-Add-Ins und COM-Add-Ins untersagen

Outlook 2000 gestattet es seinen Benutzern standardmäßig, selbständig Add-Ins zu installieren, um den Funktionsumfang von Outlook zu erweitern (Add-In-Manager und COM-Add-Ins unter *Extras* | *Optionen* auf der Registerkarte *Weitere* im Abschnitt *Allgemeines* | *Erweiterte Optionen*). Da dabei in der Regel ausführbarer Code in Form von EXE- oder DLL-Dateien eingebunden wird, müssen Erweiterungen immer zur Verwendung freigegeben werden.

Es muss organisatorisch geregelt werden, dass Benutzer keine eigenen Add-Ins aus dem Internet laden und verwenden.

Ordner *Gelöschte Objekte* automatisch Leeren

Wird der Ordner *gelöschte Objekte* automatisch geleert, wenn Outlook beendet wird, so hat dies Vor- und Nachteile. Der Hauptvorteil liegt darin, dass der Ordner dann keine "gelöschten" vertraulichen Daten enthält und kein zusätzlicher Speicherplatz verbraucht wird. Der wesentliche Nachteil besteht darin, dass dadurch Daten verloren gehen können. In Umgebungen, in denen häufig vertrauliche Daten über E-Mail ausgetauscht werden, sollte der Ordner *gelöschte Objekte* automatisch geleert werden.

Das automatisierte Leeren kann aktiviert werden, indem unter *Extras* | *Optionen* auf der Registerkarte *Weitere* das Kontrollkästchen *Bei Programmbeendigung Ordner "Gelöschte Elemente" leeren* ausgewählt wird.

Es wird in jedem Fall empfohlen, eine Warnung anzeigen zu lassen, bevor Elemente endgültig gelöscht werden. Dies wird unter *Extras* | *Optionen* auf der Registerkarte *Weitere* | *Erweiterte Optionen* über das Kontrollkästchen *Warnung anzeigen, bevor Elemente endgültig gelöscht werden* konfiguriert.

Kein Import von PST-Dateien mit der Option Duplikate durch importierte Elemente ersetzen

Beim Import von PST-Dateien (z. B. Sicherungskopie, Archiv) können Datenverluste durch das Überschreiben aktueller Elemente mit älteren Versionen

auftreten, wenn im Import-Assistenten die Option *Duplikate durch importierte Elemente ersetzen* gewählt wird. Es wird deshalb empfohlen, die Option *Erstellen von Duplikaten zulassen* auszuwählen. Es ist dabei zu beachten, dass keine Warnung ausgegeben wird, wenn Duplikate erzeugt werden, so dass überflüssige Duplikate gegebenenfalls durch den Benutzer gesucht und von Hand gelöscht werden müssen.

Abbildung: Import-Assistent

Outlook 2000 E-Mail Sicherheits-Update

Das von Microsoft empfohlene Sicherheits-Update bietet eine erhöhte Sicherheit bei der E-Mail-Nutzung. Voraussetzung für die Installation ist, dass das

Office 2000 Service Pack 1 oder 1a installiert wurde. Nach der Installation des Sicherheits-Updates ist die Funktion von Outlook im Umgang mit E-Mail-Anhängen stark einschränkt, wenn Outlook als Internet-Mail-Client konfiguriert ist und E-Mails in persönlichen Ordnern (.pst) abgelegt werden. Es muss daher im Einzelfall entschieden werden, ob das Sicherheits-Update in diesem Fall benutzt wird oder nicht.

Als grobe Richtlinie gilt dann:

- In Büroumgebungen, in denen Benutzer z. B. Office-Dokumente über E-Mail versenden, kann die Installation empfohlen werden.
- In Umgebungen, in denen Programmentwickler oder Administratoren oft auch ausführbare Dateien versenden, kann die Installation nicht empfohlen werden. Es sind dann jedoch zusätzliche Maßnahmen (z. B. Virenfilter, Personal Firewall) zum Schutz vor schädlichen ausführbaren E-Mail-Anhängen zu treffen.

Wird das Sicherheits-Update in Umgebungen genutzt, in denen Outlook als Exchange-Client eingesetzt wird, so kann das Verhalten durch den Exchange Administrator eingestellt werden. In diesem Fall wird die Installation des Sicherheits-Updates empfohlen.

Das Sicherheits-Update bewirkt folgendes:

- *E-Mail Anlagensicherheit*: Hierdurch werden die Benutzer daran gehindert, auf E-Mail-Dateianhänge, die gefährlichen ausführbaren Code enthalten können (z. B. .EXE, .BAT, Skripts, siehe Tabelle unten) zuzugreifen. Outlook unterbindet dabei den Zugriff vollständig, so dass auch ein Abspeichern der Anhänge nicht möglich ist. Ob eine E-Mail-Anlage blockiert wird, entscheidet Outlook anhand der Dateinamenserweiterung.
- *Objektmodellschutz*: Hierdurch wird eine Benutzerinteraktion erforderlich, sobald ein externes Programm versucht, auf das Outlook-Adressbuch zuzugreifen oder eigenständig eine E-Mail zu verschicken (analog dem ILOVEYOU-Virus). Dies bedeutet für Situationen, in denen innerhalb einer Benutzersitzung programmgesteuert E-Mails im Hintergrund versendet werden, dass jedes Mal eine Benutzerinteraktion notwendig ist, bevor E-Mails verschickt werden können. Dies ist in der Regel nicht gewünscht.
- *Erhöhte Standard-Sicherheitseinstellungen*: Hierdurch werden die Standardeinstellungen der Sicherheitszone für Outlook von *Internet* zu *Eingeschränkte Sites* angehoben. Gleichzeitig wird aktives Skripting innerhalb dieser Zone ausgeschaltet.

Nachdem der Security-Patch installiert wurde, können Benutzer auf bestimmte Dateianhänge (die so genannten *Dateien der Sicherheitsstufe 1*) nicht mehr zugreifen. Dazu gehören die in der nachfolgenden Tabelle angegebenen Dateitypen.

Dieses Verhalten kann zwar aus Sicht der IT-Sicherheit begrüßt werden, stellt aber in der Praxis eine starke Einschränkung der Funktionalität dar. Um von vertrauenswürdigen Absendern auch weiterhin Dateianhänge der Sicherheitsstufe 1 empfangen und abspeichern zu können, falls dies erforderlich ist, müs-

sen die Absender diese in ein anderes Dateiformat verpacken (z. B. ZIP-Format).

Bezeichnung	Voreingestellte Dateinamenserweiterungen	Empfohlene Erweiterungen
Level 1	.ADE, .ADP, .BAS, .BAT, .CHM, .CMD, .COM, .CPL, .CRT, .EXE, .HLP, .HTA, .INF, .INS, .ISP, .JS, .JSE, .LNK, .MDB, .MDE, .MSC, .MSI, .MSP, .MST, .PCD, .PIF, .REG, .SCR, .SCT, .SHS, .URL, .VB, .VBE, .VBS, .WSC, .WSF, .WSH	Es wird empfohlen, keine Einträge aus der Liste zu streichen. Bei Bedarf kann die Liste erweitert werden. Veränderungen können nur erfolgen, wenn die Daten auf dem Exchange Server gespeichert werden. Werden Daten in lokalen Ordnern gehalten, können keine zusätzlichen Dateinamenserweiterungen definiert werden.
Level 2	Keine	Office Dateien: .DOC, .DOT, .XLS, .XLT, .MDZ, .POT, .PPT, .WIZ, .OFT, .PST, .EML Komprimierte Dateien: .ZIP, .ARC, .ARJ, .CAB Multimedia Dateien: .AVI, .MPEG, .IVF, .MP3, .WAV Internet Seiten: .HTM, .HTML

Tabelle: Dateiformate

Durch den Sicherheits-Patch wird zusätzlich die Klasse der so genannten Dateien der Sicherheitsstufe 2 definiert, diese können nicht mehr direkt aus einer E-Mail heraus geöffnet werden. Um solche Dateien zu bearbeiten, sind diese zunächst abzuspeichern. Welche Dateien zur Sicherheitsstufe 2 gehören, muss vom Administrator definiert und eingerichtet werden.

Es wird empfohlen, zumindest folgende Dateitypen der Sicherheitsstufe 2 zuzuordnen (siehe auch obige Tabelle):

- Microsoft Office-Dateiformate
- Komprimierte Dateiformate
- Multimedia-Dateiformate

- Internetseiten

Eine vollständige Liste der auf einem lokalen Rechner bekannten Zuordnungen von Dateiformaten mit installierten Applikationen findet sich unter dem Registry-Schlüssel *HKEY_CLASSES_ROOT*. Es wird empfohlen, dass der Administrator anhand dieser Registry-Einträge die Liste der Level 2-Dateien festlegt.

Für E-Mail-Anhänge, die nicht durch die Dateiendungen der Level 1 und 2 erfasst werden, erfolgt die normale Verarbeitung: der Benutzer wird gefragt, ob der Anhang geöffnet oder gespeichert werden soll.

Um das Sicherheits-Update anzupassen und auf die Clients verteilen zu können, wird empfohlen, das *Outlook Security Template* (*OutlookSecurity.oft*) zu benutzen.

Umgang mit Sondernachrichten

Lese- und Empfangsbestätigungen

Automatisierte Lese- und Empfangsbestätigungen können zu - gegebenenfalls unbeabsichtigten - Denial-of-Service-Angriffen führen. Sofern die E-Mail-Richtlinie einer Organisation nicht explizit die Verwendung von E-Mail-Bestätigungen vorsieht, wird empfohlen, auf Lese- und Empfangsbestätigungen zu verzichten. Dazu sollte die Option *Nie eine Antwort senden* unter *Extras* | *Optionen* auf der Registerkarte *Einstellungen* über die Schaltflächen *E-Mail-Optionen* | *Verlaufsoptionen* aktiviert werden.

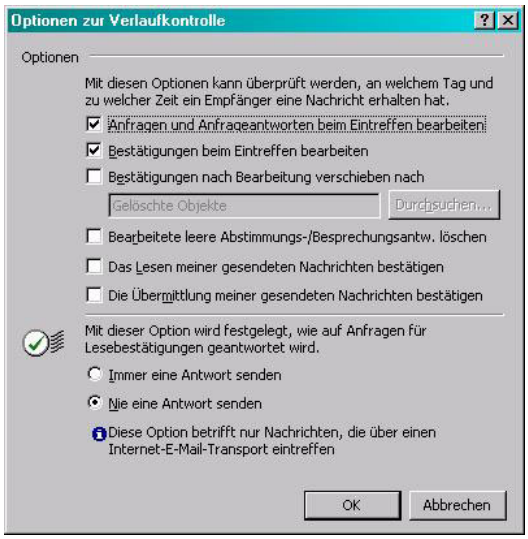


Abbildung: Verlaufskontrolle

Out-of-Office-Meldungen

Automatisch generierte Abwesenheitsnachrichten übermitteln zum einen die Information der Abwesenheit eines Mitarbeiters nach außen und können zum anderen als ein Ansatzpunkt für einen Denial-of-Service-Angriff genutzt werden. Es ist deshalb organisationsintern festzulegen, ob diese Funktionalität genutzt werden soll.

Der Abwesenheitsassistent wird konfiguriert über das Menu *Extras* | *Abwesenheits-Assistent*. Der Abwesenheits-Assistent kann auch für Outlook-Clients deaktiviert werden, indem unter *Extras* | *Optionen* | *Weitere* | *Erweiterte Op-*

tionen | *Add-In-Manager* das Kontrollkästchen *Exchange-Erweiterungsbefehle* deselektiert wird.

E-Mail-Format

Für das Versenden von Nachrichten wird empfohlen, nicht das HTML-Format zu verwenden, da dies auf Empfängerseite u. U. ein Sicherheitsrisiko darstellt. Das E-Mail-Format wird unter *Extras* | *Optionen* auf der Registerkarte *E-Mail-Format* ausgewählt. Es wird empfohlen, als Nachrichtenformat *Nur Text* einzustellen.

Es ist zu beachten, dass dies keinen Schutz vor eingehenden HTML-E-Mails bietet. (Hinweis: Die Nachfolgeversion von Outlook 2000 kann so eingestellt werden, dass alle eingehenden E-Mails beim Empfang in reines Textformat konvertiert werden.)

Abbildung: E-Mail-Format

Word als E-Mail-Editor vermeiden

Wird Microsoft Word als E-Mail-Editor benutzt, werden Nachrichten im RTF-Format (Richt-Text-Format) erstellt. Dies birgt ein Risiko, da nicht alle E-Mail-Anwendungen Nachrichten im RTF-Format darstellen können. Im schlimmsten Fall können dadurch Bestandteile einer E-Mail verloren gehen.

Da auch Word-Makros ein Sicherheitsproblem darstellen, wird davon abgeraten, Word als E-Mail-Editor zu nutzen. Dazu muss unter *Extras* | *Optionen* auf der Registerkarte *E-Mail-Format* das Kontrollkästchen *E-Mail mit Microsoft Word bearbeiten* deaktiviert sein. In der Behörde bzw. im Unternehmen sollte durch eine Richtlinie einheitlich geregelt sein, welcher Editor für E-Mails genutzt wird.

Weitere Aspekte

Kontrollierter Zugriff auf verschlüsselte Backupdaten

Wird eine E-Mail-Verschlüsselung wie S/MIME eingesetzt, so werden die verschlüsselten Nachrichten in der Regel auch verschlüsselt in das Backup übernommen. Um sicherzustellen, dass später auf diese Informationen zuge-

griffen werden kann, z. B. im Rahmen einer Reparaturmaßnahme nach einem Notfall, müssen die verwendeten Schlüssel ebenfalls in die Datensicherung einbezogen werden. Weitere Informationen hierzu finden sich in M 6.82 *Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen*.

Zurücksetzen der Hauptkategorienliste bei gelöschten Aufgaben, Kontakten sowie Kalender- und Journaleinträgen

Beim Anlegen von Aufgaben, Kontakten sowie Kalender- und Journaleinträgen ist es möglich, diesen Kategorien zuzuweisen. Solche Kategorien können aus einer vordefinierten Hauptkategorienliste gewählt oder aber neu definiert werden. Die selbst definierten Kategorien bleiben erhalten, auch wenn die angelegten Aufgaben, Kontakte oder Kalendereinträge bereits gelöscht wurden. Nicht mehr benötigte Kategorien sollten deshalb gelöscht werden, besonders wenn sie Rückschlüsse auf vertrauliche Einträge zulassen.

Die Kategorienliste kann unter *Bearbeiten* | *Kategorien* | *Hauptkategorienliste* eingesehen werden. Dort können einzelne Kategorien gelöscht oder aber die gesamte Hauptkategorienliste auf ihren vordefinierten Stand zurückgesetzt werden, was sämtliche neu angelegte Kategorien entfernt.

Abbildung: Hauptkategorienliste

Entfernen schutzbedürftiger Detailinformationen aus eigenen E-Mail-Headern

Die Header ausgehender E-Mails können Informationen beinhalten, welche nach Möglichkeit nicht nach außen gegeben werden sollten. Dazu zählen beispielsweise Informationen zum Betriebssystem und zur E-Mail-Software des eingesetzten E-Mail-Servers. Dies ist serverseitig zu konfigurieren, siehe auch M 4.162 *Sichere Konfiguration von Exchange 2000 Servern*.

Einsatz eines Virenscanners

Der Einsatz eines Viren-Schutzprogramms wird in jedem Fall empfohlen. Den größten Schutz bietet dabei eine kombinierte Gateway-Client-Lösung, welche sowohl server- als auch clientseitige Komponenten beinhaltet. Es muss ge

währleistet sein, dass alle Dateianhänge einer E-Mail geprüft werden. Dies gilt auch für komprimierte oder verschlüsselte Anhänge.

Software- und Systempflege

Die zuständigen Administratoren sollten sich regelmäßig im Internet über neu entdeckte Schwachstellen in Exchange/Outlook 2000 informieren. Die verfügbaren Patches sollten zunächst innerhalb einer Testumgebung und dann für den Produktivbetrieb eingespielt werden.

Ergänzende Kontrollfragen:

- Wurde eine Liste der Dateitypen der Sicherheitsstufe 2 erstellt?
- Wurden Benutzerprofile erstellt?
- Wird regelmäßig im Internet nach neu erkannten Schwachstellen von Exchange/Outlook 2000 recherchiert?

M 4.166 Sicherer Betrieb von Exchange/Outlook 2000

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Nach der Installation und Konfiguration von Exchange/Outlook 2000 müssen Maßnahmen zur Gewährleistung des sicheren Betriebs ergriffen werden. Folgende sicherheitsrelevante Aspekte sind dabei zu berücksichtigen:

- Umsetzung der Sicherheitsrichtlinien der betreffenden Organisation (siehe M 2.248 *Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000*),
- Sicherer Betrieb des zugrunde liegenden Betriebssystems (siehe M 4.146 *Sicherer Betrieb von Windows 2000/XP*),
- Administrative Aspekte,
- Software- und Systempflege,
- Virenschutz,
- Systemüberwachung,
- Datensicherung und
- Ausfallsicherheit bzw. Schadenbegrenzung bei einem Ausfall.

Administrative Aspekte

Bei der Administration und der Vergabe von Berechtigungen sollte stets das Prinzip des geringsten Privilegs (*least privilege*) beachtet werden. Dies gilt vor allem in Bezug auf die Exchange-Administratoren: Jeder Administrator erhält nur diejenigen Rechte, die zur Wahrnehmung seiner Aufgaben notwendig sind.

Trennung der Administratoraufgaben

Es wird empfohlen, administrative Tätigkeit in Windows und Exchange soweit wie möglich zu trennen. Es sollte jedoch beachtet werden, dass dies nicht uneingeschränkt möglich ist: Für einige Aufgaben benötigen Exchange-Administratoren auch lokale Administratorrechte unter Windows 2000 (so z. B. zum Starten und Stoppen der Exchange-Dienste).

Software- und Systempflege

Updates und Patches testen

Eine wichtige Voraussetzung für den sicheren Betrieb ist, dass alle sicherheitsrelevanten Service Packs, Updates und Patches für das Softwareprodukt eingespielt werden. Es ist daher erforderlich, dass sich die Administratoren regelmäßig über neu bekannt gewordene Schwachstellen in Exchange 2000 und Windows 2000 informieren und ggf. geeignete Maßnahmen zu deren Beseitigung zeitnah umsetzt. Vor dem Einspielen eines Service Packs, Updates oder Patches in das Produktivsystem sollte dies jedoch zunächst in einer Testumgebung geschehen. So kann überprüft werden, ob unerwünschte Seiteneffekte zu erwarten sind. Darüber hinaus sollten die Konfigurationseinstellungen des Gesamtsystems regelmäßig daraufhin überprüft werden, ob sie den Vorgaben entsprechen und den Sicherheitsanforderungen genügen.

Virenschutz

Eine der größten Gefahren für den sicheren Betrieb eines E-Mail-Systems besteht darin, dass unter Umständen Computer-Viren, Würmer und andere Schadprogramme eingeschleust werden können. Zur Abwehr sollte ein Viren-Schutzprogramm eingesetzt werden, dessen Muster-Datenbank periodisch aktualisiert werden muss. Weitere Details zum Virenschutz finden sich in dem entsprechenden Baustein 3.6 Computer-Virenschutzkonzept sowie in den Maßnahmen M 4.33 *Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung* und M 6.23 *Verhaltensregeln bei Auftreten eines Computer-Virus*.

Systemüberwachung

Um die Sicherheit im laufenden Betrieb zu gewährleisten und mögliche Gefährdungen frühzeitig zu erkennen, sollte das Exchange-System permanent überwacht werden. Empfehlungen hierzu finden sich in M 4.167 *Überwachung und Protokollierung von Exchange 2000 Systemen*.

Datensicherung

Als Grundlage für die schnelle Wiederherstellung der Daten - z. B. nach einem Systemausfall - muss regelmäßig eine Datensicherung des Exchange-Systems angelegt werden (siehe M 6.32 *Regelmäßige Datensicherung* und M 6.49 *Datensicherung einer Datenbank*). Zur Datensicherung kann das Windows 2000 Backup Utility verwendet werden (siehe M 6.78 *Datensicherung unter Windows 2000/XP*).

Es wird empfohlen, zumindest den *Mailbox Store*, den *Public Store* sowie die *Transaction Logs* zu sichern. Die Art des Backups (vollständig oder inkrementell) spielt an dieser Stelle keine besondere Rolle. Da Exchange/Outlook-Systeme zum ordnungsgemäßen Betrieb das Windows 2000 Active Directory benötigen, sollte dieses ebenso gesichert werden (siehe dazu M 4.146 *Sicherer Betrieb von Windows 2000*).

Es wird weiterhin empfohlen, bereits gelöschte Exchange-Objekte in Postfächern und öffentlichen Ordnern erst nach einigen Tagen und auch erst nach einer abgeschlossenen Datensicherung permanent zu löschen. Diese Einstellungen können für jeden einzelnen Informationsspeicher vorgenommen werden. Außerdem wird empfohlen, gelöschte Postfächer innerhalb einer bestimmten Zeitspanne nicht permanent zu löschen (die Standardeinstellung beträgt 30 Tage). Diese Werte müssen an die jeweiligen Anforderungen des Unternehmens bzw. der Behörde angepasst werden.

Online-Sicherung

Exchange 2000 Server bietet eine eigene Programmierschnittstelle (API) zur Sicherung und Wiederherstellung der Datenbanken an (*Esebcli2.dll*). Dies ermöglicht dem Sicherungsprogramm von Windows 2000, die Sicherung und Wiederherstellung online durchzuführen, d. h. ohne dass die Exchange-Dienste heruntergefahren werden. Die Online-Sicherung empfiehlt sich für häufig (z. B. täglich) durchgeführte Backups.

Offline-Sicherung

Zur Offline-Sicherung einer Installation von Exchange 2000 Server müssen die Exchange-Dienste heruntergefahren werden. Anschließend ist das Exchange-Verzeichnis (z. B. *c:\Programme\Exchsrvr*) inklusive sämtlicher Unterverzeichnisse zu sichern. Damit werden die gesamten binären Daten des

Exchange-Servers erfasst, unter anderem auch die Nachrichtenwarteschlangen des MTAs und der Gateway-Connectoren. Diese Variante empfiehlt sich für die weniger häufig durchgeführten Sicherungen (z. B. einmal wöchentlich).

Die Automatisierung des Sicherungsprozesses wird über die Einstellungen des Windows 2000 Servers konfiguriert. Sofern keine anderen Automatismen zur Durchführung einer Sicherung innerhalb der Organisation etabliert sind, wird die Verwendung dieses Windows-eigenen Mechanismus empfohlen.

Clients berücksichtigen

Bei der Datensicherung sind auch Clients zu berücksichtigen. Auf lokalen Benutzersystemen abgelegte Daten, wie z. B. persönliche Outlook-Ordner, müssen in die Sicherung einbezogen werden.

Besonderes Augenmerk erfordert das Backup von Daten, die durch Verschlüsselung, Zugangskennwörter oder andere Mechanismen geschützt sind. In der Regel müssen die sensitiven Zugangsinformationen dann ebenfalls gesichert werden, damit sie bei der Wiederherstellung der Daten verfügbar sind.

Ausfallsicherheit

Partitionierung

Für den sicheren und unterbrechungsfreien Betrieb von Exchange 2000 muss der *Global Catalog Server* stets erreichbar sein. Um die Auswirkung des Ausfalls eines Exchange 2000 Servers zu verringern, können Exchange-Daten durch *Partitionierung* auf mehrere Server verteilt werden. Der Ausfall eines einzelnen Servers betrifft dann nur einen Teil der Daten. Die Partitionierung ist bedarfsgerecht zu planen und durchzuführen.

Replizierung

Müssen Daten öffentlicher Ordner stets im vollen Umfang verfügbar sein, sollten *Replikate* angelegt werden, so dass die Daten auf mehrere Server verteilt werden. Beim Ausfall eines einzelnen Servers kann immer noch auf die Replikate auf anderen Servern zugegriffen werden.

Clustering

Durch das so genannte *Clustering* existiert eine Möglichkeit, mehrere physikalische Server als einen virtuellen Server zu betreiben. Beim Ausfall eines Servers erfolgt ein automatisches *Failover* und die restlichen Server des Clusters übernehmen die Aufgaben des ausgefallenen Servers. Ob diese Funktion eingesetzt werden sollte, muss jeweils im Einzelfall entschieden werden.

Redundanz

Bei hohen Anforderungen an die Verfügbarkeit sollte darüber nachgedacht werden, redundante Verbindungen innerhalb der Exchange-Organisation und gegebenenfalls auch von/nach außen einzurichten (siehe M 4.162 *Sichere Konfiguration von Exchange 2000 Servern*).

Notfallplan

Als Vorsorge sollte schließlich ein praktikabler Notfallplan vorliegen (siehe hierzu die Maßnahme M 6.82 *Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen*).

Schutz vor Denial-of-Service-Attacken (DoS)

Als Schutz vor DoS-Attacken wird empfohlen, Einschränkungen der maximal möglichen Nachrichten- bzw. Speichergrößen einzuführen. Dies gilt vor allem für eingehende Verbindungen.

Ein weiterer Mechanismus ist die Filterung von Nachrichten. Damit können zwar keine großangelegten Spam-Angriffe abgewehrt werden, jedoch kann

dieser Mechanismus für die Filterung einzelner Absender sinnvoll eingesetzt werden.

Ergänzende Kontrollfragen:

- Wurde ein Notfallplan für den Ausfall des Exchange-Systems erarbeitet?
- Werden regelmäßig Datensicherungen von Exchange, Outlook und Active Directory durchgeführt?
- Informieren sich die Administratoren regelmäßig über neu entdeckte Schwachstellen?

M 4.167 Überwachung und Protokollierung von Exchange 2000 Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, IT-Sicherheitsmanagement

Die Überwachung und die Protokollierung eines Exchange 2000 Systems sind aus vielen Gründen notwendig: Zum einen hilft die aktivierte Überwachung, potentielle Schwachstellen möglichst frühzeitig zu erkennen und zu beseitigen. Zum anderen dient die Protokollierung dazu, Verstöße gegen die Sicherheitsrichtlinie zu erkennen (siehe M 2.248 *Festlegung einer Sicherheitsrichtlinie für Exchange/ Outlook 2000*) oder Nachforschungen über einen Sicherheitsvorfall anzustellen.

Das Exchange-System sollte gemeinsam mit dem Windows 2000 Betriebssystem überwacht werden. Weitere Informationen zu der Überwachung von Windows 2000 finden sich in M 4.148 *Überwachung eines Windows 2000/XP Systems*.

Um eine hinreichende Überwachung und Protokollierung zu erreichen, sollten Einstellungen in folgenden Bereichen konfiguriert werden:

- Überwachen von Systemressourcen auf kritische Werte,
- Erzeugen automatischer Benachrichtigungen beim Erreichen kritischer Werte,
- Protokollierung der Internet-Protokolle (auf Basis virtueller Server),
- Protokollierung der Dienstkomponenten eines Exchange 2000 Servers (Diagnose-Protokollierung) und
- Nachrichtentracking.

Überwachungswerkzeuge

Für die Überwachung der Exchange-Umgebung stehen dem Systemadministrator eine Reihe von Werkzeugen zur Verfügung:

- Der *Event Viewer* von Windows 2000 hält unter den Rubriken *Application*, *Security* und *System* auch Exchange 2000 Ereignisse fest.
- Spezielle *Exchange Monitors* (*Server & Link Monitors*) erlauben die gezielte Abfrage von Server- und Verbindungsstatus.
- Das *Message Tracking Center (MTC)* erlaubt die Aufzeichnung sämtlicher über einen Exchange-Server übertragenen E-Mails.
- Der Windows 2000 *System Monitor* ermöglicht die graphische Darstellung der Performance einer Vielzahl von Systemparametern.
- Die Microsoft *MADMAN* (*Mail and Directory Management*) *MIB* (*Management Information Base*) erlaubt die Aufzeichnung Exchange-spezifischer Ereignisse auf Basis des standardisierten Protokolls SNMP (Simple Network Management Protocol).

Allgemeines

Protokolle nicht überschreiben

Es wird empfohlen, keine Umlaufprotokollierung für Protokolldateien zu aktivieren. Anderenfalls werden Einträge irgendwann überschrieben, was es einem Angreifer ermöglicht, seine Spuren durch das Erzeugen vieler Protokolleinträge zu verwischen.

System nicht automatisch herunterfahren

Das System sollte außerdem nicht so konfiguriert werden, dass nach dem Vollwerden einer Protokolldatei der Dienst gestoppt oder heruntergefahren wird. Dies kann von einem Angreifer für DoS-Attacken ausgenutzt werden.

Unabhängig von den Überwachungsrichtlinien von Windows 2000 protokolliert der Informationsspeicherdienst im Anwendungsprotokoll, wenn ein Benutzer ein Postfach nicht mit dem primären Konto öffnet.

In einer Exchange 2000 Umgebung stehen mehrere Formate für Protokolldateien zur Verfügung. Es wird empfohlen, das *W3C Extended Log File Format* zu benutzen.

Überwachen der Systemressourcen

Die Systemressourcen, wie z. B. der verfügbare virtuelle Speicherplatz, die CPU-Auslastung, der freie Festplattenplatz oder das Wachstum der Nachrichtenwarteschlangen, können und sollten überwacht werden. Dies wird auf der Registerkarte *Monitoring* in den Eigenschaften eines Exchange-Servers aktiviert.

Es besteht die Möglichkeit, zwei Werte für die jeweilige Ressource anzugeben: einen Wert für den Warnzustand und einen Wert für den kritischen Zustand. Diese Werte sollten an die Anforderungen des Unternehmens bzw. der Behörde angepasst werden.

Zumindest folgende Ressourcen sollten überwacht werden:

- der freie Speicherplatz,
- die CPU-Auslastung und
- der allgemeine Serverzustand (das Ereignis *Stopped*).

Etwa die Hälfte oder mehr des verfügbaren Speicherplatzes sollte frei bleiben. Dieser Festplattenplatz kann dann für die Komprimierung der Datenbanken oder die Offline-Reparatur von beschädigten Datenbanken verwendet werden.

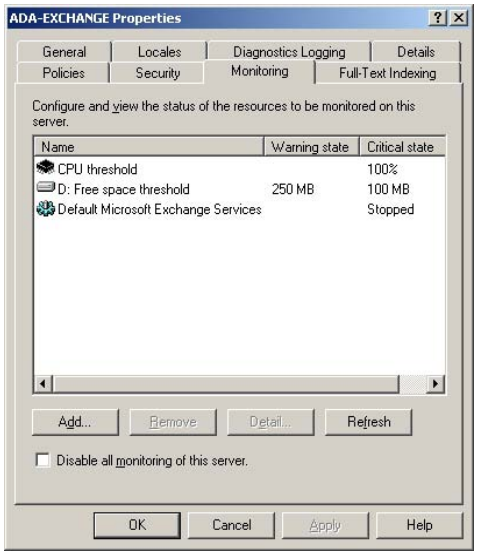


Abbildung: Exchange Eigenschaften

Konfiguration von automatischen Benachrichtigungen

Exchange 2000 kann so konfiguriert werden, dass eine automatische Benachrichtigung verschickt wird, wenn einer der überwachten Parameter einen bestimmten Status erreicht. Es wird empfohlen, die automatische Benachrichtigung für überwachte Exchange-Server zu aktivieren, wenn ein Parameter den kritischen Status erreicht hat.

Eine automatische Benachrichtigung kann über E-Mail oder über ein Skript erfolgen, das vom Administrator definierte Aktionen durchführen kann, wie z. B. Stoppen eines Dienstes oder ähnliches. Da eine E-Mail-Benachrichtigung aus einer Reihe von WMI-Platzhaltern besteht (*Windows Management Instrumentation*), kann sie an die eigenen Anforderungen angepasst werden.

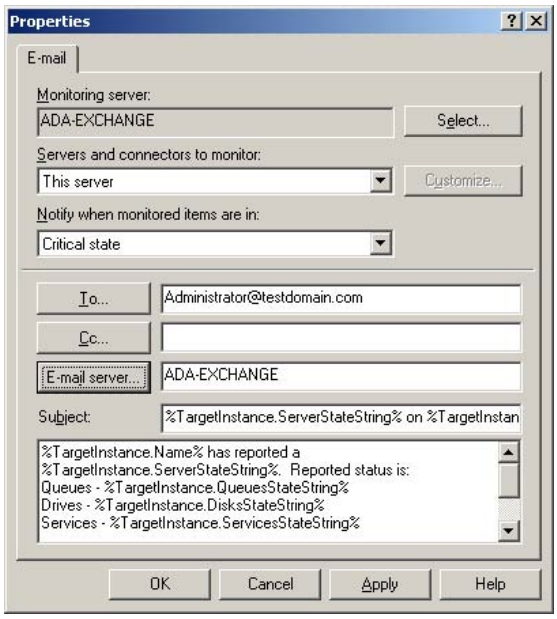


Abbildung: E-Mail Eigenschaften

Wird die E-Mail-Benachrichtigung genutzt, so sollte ein interner SMTP-Server angegeben werden, der anonyme Weiterleitungen (*Relay*) zulässt.

Automatische Benachrichtigungen werden im *Exchange System-Manager* im Bereich *Tools/Monitoring und Logging* der Exchange-Organisation definiert. Bei beiden Arten der automatischen Benachrichtigung muss der zu überwachende Server angegeben werden.

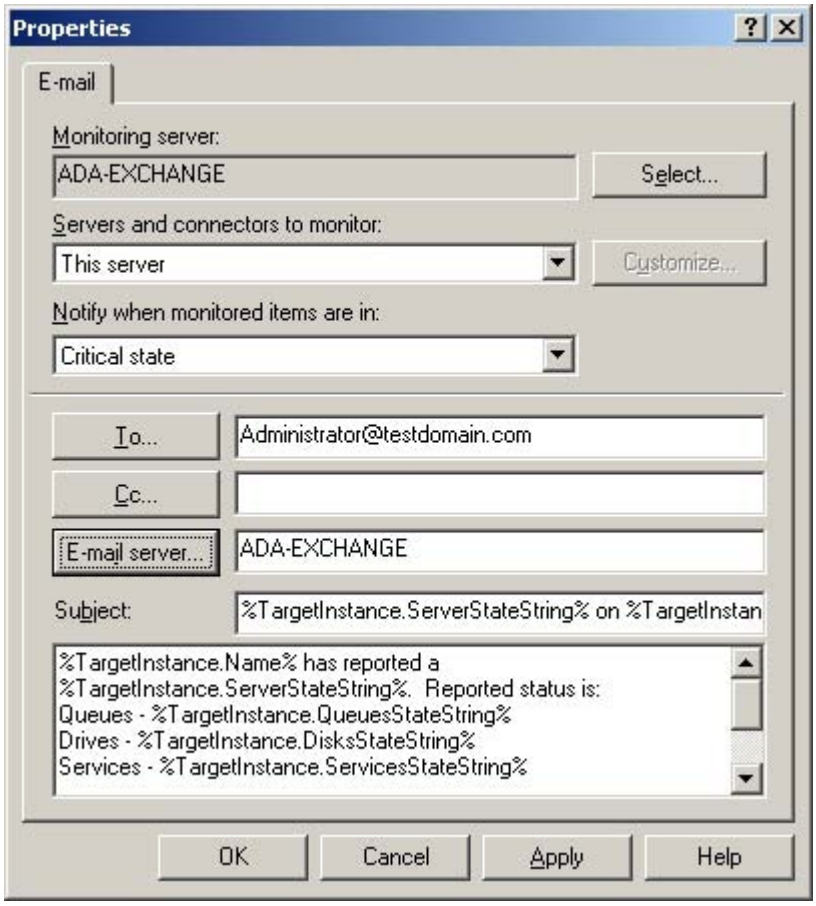


Abbildung: Exchange System Manager

Protokollierung

Diagnose-Protokollierung (diagnostic logging)

Die Diagnose-Protokollierung eines Servers ist nützlich, wenn Nachforschungen über Sicherheitsvorfälle angestellt werden. Diese Art der Protokollierung erfolgt pro Server: Sie wird in den Eigenschaften eines Exchange-Servers auf der Registerkarte *Diagnostic Logging* konfiguriert.

Die Diagnose-Protokollierung sollte für die Protokollierung der POP3- und IMAP4-Ereignisse eingesetzt werden, da für diese Protokolle (im Gegensatz zu SMTP, HTTP und NNTP) keine andere Protokollierungsmöglichkeit existiert. Deshalb sollte für die Komponenten *POP3Svc* und *IMAP4Svc* die Protokollierung der Kategorie *Authentication* auf die maximal mögliche Protokollierungsstufe (*Maximum*) gesetzt werden.

Abbildung: Diagnostics Logging

Nachfolgend werden die empfohlenen Einstellungen für die Protokollierung aufgeführt:

- Die Komponente *MSExchangeMTA* (Microsoft Exchange Message Transfer Agent) in der Kategorie *Security* auf die maximal mögliche Protokollierungsstufe einstellen.
- Die Komponente *MSExchangeIS* (Microsoft Exchange Information Store Service) in folgenden Kategorien auf die maximale Protokollierungsstufe einstellen:
  - Logons
  - Access Control
  - Send On Behalf Of
  - Send As

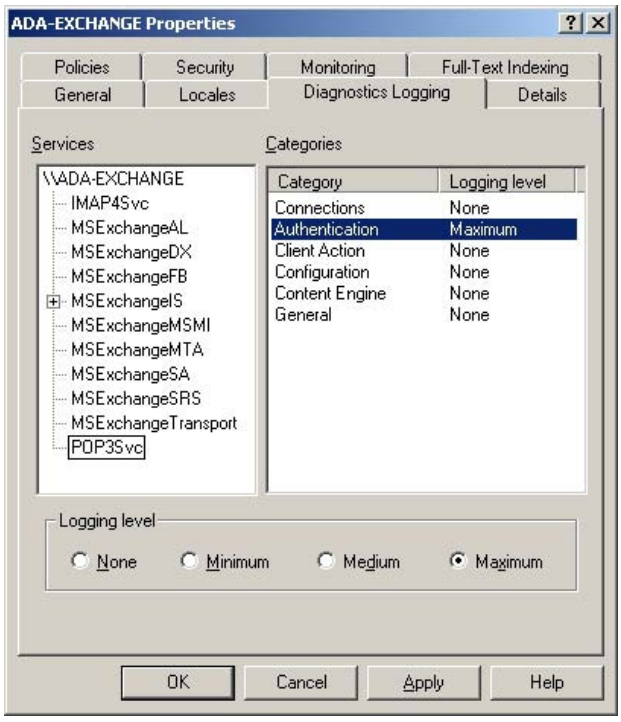


Abbildung: Diagnostics Logging

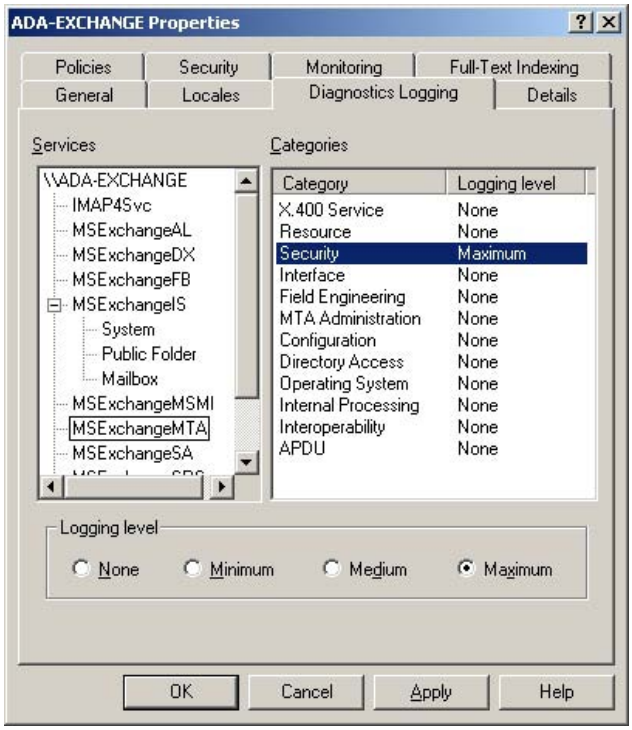


Abbildung: Diagnostics Logging

Protokollierung der Internet-Protokolle

Die Protokollierung der SMTP- und NNTP-Protokolle wird im *Exchange System-Manager* in den Eigenschaften der virtuellen Server auf der Registerkarte *General* aktiviert. Die HTTP-Protokollierung wird im Internetdienst-Manager in den Eigenschaften des zu überwachenden virtuellen HTTP-Servers eingeschaltet.

Die Protokollierung der IMAP4- und POP3-Protokolle wird dagegen nicht mit einem Konfigurationswerkzeug, sondern durch Einträge in die Windows 2000 Registry aktiviert:

- *HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ POP3Svc \ Parameters*
- *HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ IMAP4Svc \ Parameters*

Die relevanten Werte hierbei sind: *POP3 Protocol Log Path* und *POP3 Protocol Log Level* sowie *IMAP4 Protocol Log Path* und *IMAP4 Protocol Log Level*. Der jeweils erste Wert verweist auf das Verzeichnis, in dem die Protokolldateien erstellt werden (das Namensformat ist *L0000001.log*). Der zweite Wert bezieht sich auf den Detailgrad der Protokollierung. Die Skala reicht dabei von 0 (keine Protokollierung) bis hin zu 5 (größter Detailgrad). Damit die Änderungen wirksam werden, ist ein Neustart der Dienste erforderlich.

Protokollierung für Instant Messaging

Um die Protokollierung für Instant Messaging zu aktivieren, sollte im Internetdienst-Manager in den Eigenschaften des virtuellen Verzeichnisses *InstMsg* auf der Registerkarte *Website* das Kontrollkästchen *Enable Logging* ausgewählt werden. Die Protokolldatei befindet sich dann im Verzeichnis *\Winnt\System32\Logfiles\W3svc1*.

Nachrichtentracking

Zugriff für Everyone sperren

Mit dem Nachrichtentracking lassen sich nicht nur vermisste Nachrichten in Warteschlangen aufspüren und Verzögerungen innerhalb des Übertragungspfades erkennen, sondern auch Hinweise darüber finden, ob bestimmte Nachrichten erfolgreich zugestellt wurden. Beim aktivierten Nachrichtentracking werden Statusinformationen in täglichen Protokolldateien aufgezeichnet und im Exchange-Log-Verzeichnis gespeichert (z. B. *\Programme\Exchsrvr \<Servername>.log*). Der Dateiname folgt dabei dem Schema *<JJJJMMTT>.log*. Diese Trackingprotokolle werden auf allen Exchange 2000 Servern über die Freigabe *<Servername>.log* sämtlichen Domänenbenutzern zugänglich gemacht. Die Gruppe *Everyone* sollte aus der Zugriffskontrollliste dieser Freigabe entfernt werden.

Ergänzende Kontrollfragen:

- Wird der freie Speicherplatz überwacht?
- Erfolgt eine automatische Benachrichtigung, wenn ein überwachter Parameter den kritischen Zustand erreicht hat?
- Enthält die Sicherheitsrichtlinie zum Einsatz von Exchange/Outlook detaillierte Vorgaben für die Systemüberwachung?

M 4.168 Auswahl eines geeigneten Archivsystems

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Archivverwalter

Die Auswahl eines Archivsystems erfolgt auf der Grundlage der im Archivierungskonzept (siehe hierzu M 2.243 *Entwicklung des Archivierungskonzepts*) festgeschriebenen Vorgaben.

Typischerweise werden folgende Mindestanforderungen an das einzusetzende Archivsystem gestellt, wobei individuelle organisationsspezifische Anforderungen zu ergänzen sind:

- Anbindung an die vorhandene Systemumgebung

  Das Archivsystem sollte die erforderlichen Schnittstellen zur Anbindung an die vorliegende Systemumgebung (Netz, Server, Clients, Systemmanagement) aufweisen. Systeme zur Datenein- und -ausgabe, wie Scanner, Textverarbeitung, Drucker, etc., sind typischerweise nicht Bestandteil des Archivsystems, sondern werden auf Anwendungsebene bereitgestellt.

- Anbindung an ein Dokumentenmanagementsystem

  Das Archivsystem sollte Schnittstellen zur Anbindung an ein Dokumentenmanagementsystem (DMS) aufweisen.

- Versionierung von Dokumenten

  Das Archivsystem sollte die mehrfache Speicherung von Dokumenten in unterschiedlichen Fassungen unterstützen (Versionierung).

- Zugriffsschutz auf die archivierten Daten

  Durch das Archivsystem sollte ein Zugriffsschutz auf die archivierten Daten und die Funktionen des Archivsystems umgesetzt werden können. Dies sollte auf der Grundlage eines vorgegebenen Berechtigungskonzepts erfolgen.

- Mehrstufiges, rollenbasiertes Berechtigungskonzept

  Beachtung von Rollenkonflikten

  Bei einer rollenbasierten Rechtevergabe werden Zugriffsrechte nicht an konkrete Benutzer vergeben, sondern an definierte Benutzergruppen (Rollen). Im Gegensatz zu normalen Berechtigungsgruppen werden in einem rollenbasierten Zugriffsmodell auch Rollenkonflikte berücksichtigt. Dies bedeutet zum Beispiel, dass eine Person nicht gleichzeitig die Rolle des Administrators und des Revisors einnehmen kann.

- Protokollierung

  Das Archivsystem sollte eine Protokollierung ermöglichen, die alle Vorgänge rund um die Archivierung nachvollziehbar macht (siehe auch M 4.172 *Protokollierung der Archivzugriffe*). Dabei sollte es auch möglich sein, kritische Ereignisse zu definieren und einen Administrator zu benachrichtigen, wenn solche auftreten.

- Einrichtung eines Benutzerkontos für die Revision

  Leserecht für Revision

  Für Zugriffe im Rahmen der regelmäßigen Revision des Archivsystems sollte ein entsprechendes Benutzerkonto mit den für die Revision notwendigen Rechten eingerichtet werden. Die konkrete Rechtevergabe ist organisationsintern festzulegen. Im Rahmen der Revision werden typischerweise Leserechte (read-only) auf Konfigurationsdaten und Protokolldaten eingerichtet.

- Erweiterbarkeit des Archivsystems

  Das Archivsystem sollte erweiterbar sein, damit es bei Änderungen der Anforderungen angepasst werden kann. Die Erweiterbarkeit betrifft vor allem die eingesetzten Speicherkomponenten und Speichermedien, aber auch sonstige Hardware-Änderungen sowie die Archivsystem-Software und Nutzungslizenzen.

- Geringe Zugriffszeit

  Für das Archivsystem wird typischerweise eine geringe Zugriffsverzögerung und gleichzeitig eine hohe Bandbreite bei der Übertragung und Bereitstellung der angeforderten Dokumente verlangt. Die Anforderungen sind organisationsspezifisch zu ermitteln. Hierbei ist neben der Einbindung in die vorhandene Systemumgebung auch das abzusehende Benutzerverhalten zu berücksichtigen.

  Dimensionierung von Cache-Komponenten

  Die festgelegten Anforderungen wirken sich auf die Auswahl der Archivmedien und der Speicherlaufwerke aus. Ebenso können die Anforderungen die Auswahl und Dimensionierung von Cache-Komponenten beeinflussen.

- Ausreichende Kapazität der Archivmedien

  Die Archivmedien sollten eine ausreichende Kapazität aufweisen. Sowohl die mehrfache Speicherung von Dokumenten zur Versionierung als auch die zu erwartende Datenmenge sollten bei der Kapazitätsplanung berücksichtigt werden.

- Systemgesteuertes Einlegen oder Entnehmen von Archivmedien

  mount und unmount

  Das Archivsystem sollte generell eine systemgestützte Entnahme der Archivmedien aus Laufwerken unterstützen. Hierdurch soll gewährleistet werden, dass Archivmedien nur nach kontrollierter Offline-Schaltung (unmount) sowie unter Beachtung entsprechender Zugriffsrechte entnommen werden und die Entnahme protokolliert werden kann. Gleiches gilt für die Online-Schaltung (mount) von Archivmedien. Dies ist erforderlich, damit eine konsistente Verwendung der Archivmedien sichergestellt ist.

  Für Notfälle sehen in der Regel alle Archivsysteme und Laufwerke manuelle Möglichkeiten vor, Archivmedien zu entnehmen.

- Kapazitätsüberwachung der Archivmedien

  Die Restkapazität der in Benutzung befindlichen Archivmedien muss laufend überwacht werden. Bei Unterschreiten einer Restkapazitätsgrenze muss eine Signalisierung bzw. Alarmierung erfolgen.

- Alarmierung und Signalisierung

  Anbindung an das Systemmanagement

  Das Archivsystem muss die Signalisierung von Systemmeldungen an übergreifende Systemmanagement-Umgebungen gestatten. Wenn keine Anbindung an eine Systemmanagement-Umgebung vorgesehen ist, so sollte eine individuelle Alarmierung über E-Mail, SMS oder SNMP möglich sein.

- Einhaltung von Standards

  Die Einhaltung von Standards erleichtert die Interoperabilität zwischen einzelnen Komponenten. Dies ist erforderlich, weil damit gerechnet werden muss, dass im Betriebszeitraum einzelne Komponenten ausgetauscht werden müssen oder das System erweitert werden soll.

  Standards sind in folgenden Bereichen relevant:

  - Archivmedien und Aufzeichnungsverfahren (siehe M 4.169 *Verwendung geeigneter Archivmedien*),
  - Dateiformate und Komprimierungsverfahren (siehe M 4.170 *Auswahl geeigneter Datenformate für die Archivierung von Dokumenten*),
  - Dokumentenmanagementsysteme (siehe M 2.259 *Einführung eines übergeordneten Dokumentenmanagements*).

Verschlüsselung und digitale Signatur

Es sollte überlegt werden, die Daten durch Verschlüsselung und digitale Signatur zu schützen. Dies wird jedoch typischerweise nicht durch das Archivsystem implementiert, sondern auf Anwendungsebene, z. B. durch das Dokumentenmanagementsystem.

Eine Ausnahme bildet die Grundverschlüsselung von Archivmedien durch das Archivsystem. Hierdurch soll ein Missbrauch des Archivmediums außerhalb des Archivsystems verhindert werden. Diese Grundverschlüsselung wird jedoch für den IT-Grundschutz nicht gefordert.

Ergänzende Kontrollfragen:

- Sind die Anforderungen an das Archivsystem dokumentiert?
- Werden die Anforderungen durch das ausgewählte Archivsystem erfüllt?

M 4.169 Verwendung geeigneter Archivmedien

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator

Die dauerhafte elektronische Archivierung von Dokumenten erfordert den Einsatz geeigneter Datenträger (Archivmedien). Für die Wahl der Archivmedien sollten folgende Fragen berücksichtigt werden:

- Welches Datenvolumen soll archiviert werden?
- Welche Zugriffszeiten sind im Mittel zu erbringen?
- Wie hoch ist die Zahl gleichzeitiger Zugriffe im Mittel?
- Welche Aufbewahrungsfristen sollen durch das Archivmedium abgedeckt werden?
- Sollen Daten "revisionssicher" gespeichert werden?

In den folgenden Abschnitten werden typische Archivmedien und deren Einsatzbereiche beschrieben. Für die Datenträger werden üblicherweise magnetische, magnetooptische oder optische Speichertechnologien verwendet. Die Vorzüge und Nachteile der Technologien sind in den jeweiligen Abschnitten beschrieben.

Sämtliche beschriebenen Archivmedien sind anfällig gegenüber physikalischen Beschädigungen, etwa durch

- Wasser,
- Feuer bzw. Hitzeentwicklung,
- Verkratzen des Mediums durch das Laufwerk infolge Verschmutzung oder Herunterfallen,
- Zerknittern und Aufreißen des Mediums im Bandlaufwerk sowie
- Sabotage und Diebstahl.

Schutz vor physikalischen Beschädigungen

Archivmedien müssen daher sorgsam aufbewahrt und vor den genannten Einflüssen geschützt werden. Außerdem muss der unbefugte Zugriff auf die Datenträger verhindert werden. Hierzu wird, abhängig vom konkreten Einsatzszenario des elektronischen Archivs, die Anwendung der im Baustein B 2.5 *Datenträgerarchiv* bzw. B 2.7 *Schutzschränke* beschriebenen Maßnahmen zum Schutz der Datenträger empfohlen.

Digitale magnetische Systeme

Bei magnetischen Speichersystemen wird durch gezielte lokale Veränderung eines magnetisierten Grundmediums ein Speichereffekt erzielt. Die Magnetisierung kann durch ein Lesegerät erfasst, die gespeicherten Daten können dadurch gelesen werden. Durch erneutes Einwirken eines Magnetfeldes können die gespeicherten Daten verändert werden. Dies erfolgt gezielt durch Verwendung eines Schreib-/Lesegerätes oder ungezielt durch starke externe Magnetfelder (z. B. elektromagnetische Felder in der Nähe von Transformatoren oder großen Spulen). Dies kann auch unabsichtlich geschehen.

Magnetische Datenträger sind anfällig gegenüber Angriffen mit starken Magnetfeldern, die auf das Speichermedium einwirken. Da das magnetisierte Grundmedium typischerweise als Verbundwerkstoff aus Kunststoffen sowie einer metallischen (magnetisierbaren) Beschichtung hergestellt wird, ist außerdem auch bei sorgsamer Behandlung mit langfristigen Veränderungen zu rechnen. Diese können z. B. durch Zersetzung (durch Weichmacher in Kunststoffen), Aufquellen (Ablösung von Kunststoff- und Metallschichten) oder Oxydation (der Metallschicht) bedingt sein.

nicht revisionssicher

Aufgrund der verwendeten Technologie sind magnetische Speicher zudem stets wiederbeschreibbar bzw. löschbar und daher ohne zusätzliche Sicherungsverfahren prinzipiell nur für die kurzfristige Archivierung geeignet, bei der kein Schutz gegen Veränderung bzw. Wiederbeschreiben von Dokumenten durch das Medium erbracht werden muss. Dies schließt typischerweise die Verwendung als Archivmedium aus, wenn eine revisionssichere Archivierung gefordert wird. Dagegen können magnetische Systeme für Datensicherungen und als Cachemedien eingesetzt werden.

Die Revisionssicherheit kann mit hohem Aufwand durch den Einsatz kryptographischer Verfahren, die eine Veränderung an den Daten erkennen lassen, erreicht werden (z. B. Signierung).

Typische magnetische Speicher sind Festplatten, Disketten und (Magnet-) Bandmedien.

- **Disketten**

  Disketten, die derzeit in Abmessungen von 3,5 Zoll, früher auch 5,25 Zoll und größer, angeboten werden, weisen eine geringe Kapazität von 1,44 MB auf. Der Einsatz von Disketten als Archivmedium wird nur für sehr kleine Archive empfohlen, in denen keine revisionssichere (schreibgeschützte) Archivierung gefordert wird.

- **Festplatten**

  mechanische Ausfälle

  In Festplatten sind typischerweise das Speichermedium und das Schreib-/Lese-Laufwerk zusammen in einer Einheit untergebracht. Sie sind daher fehleranfällig gegen mechanische Ausfälle, wie z. B. des Laufwerkantriebs. Durch die physikalische Kapselung wird eine dichtere Anordnung der Magnetmedien bei gleichzeitigem Schutz vor Staubpartikeln ermöglicht, so dass Festplatten im Gegensatz zu Disketten-Laufwerken über mehrere Schreib-Lese-Einheiten verfügen.

  Festplatten weisen typischerweise eine hohe Kapazität und eine geringe Zugriffszeit bei hoher Übertragungsrate auf. Aufgrund der verwendeten Speichertechnologie eignen sie sich nicht für eine dauerhafte, revisionssichere Ablage von Dokumenten. Festplatten finden dagegen Verwendung als Datenträger für das Archivsystem selbst und in Cachesystemen.

- **Magnetbänder**

  Magnetbänder bestehen aus einem aufgewickelten Magnetstreifen, der in der Regel an einem Schreib-Lesekopf sequentiell vorbeigeführt wird. Magnetband und Schreib-Lese-Einheit sind typischerweise nicht miteinander verbunden.

Magnetbänder weisen technologisch bedingt eine sehr lange Zugriffszeit und eine sehr geringe Übertragungsrate auf. Ihre Speicherdichte und Platzverbrauch sind jedoch vergleichbar mit Festplatten.

mittelfristige Stabilität

Magnetbänder eignen sich für die Speicherung großer Datenmengen, auf die nur selten und sequentiell zugegriffen werden muss. Sie sind daher geeignet für Backups, bei denen eine mittelfristige, jedoch nicht langfristige Stabilität erwartet wird. Da auch Magnetbänder prinzipiell überschrieben, gelöscht oder durch zufälligen Einfluss von Magnetfeldern verändert werden können, eignen sie sich nicht für die revisionssichere Speicherung von Daten.

Die folgende Tabelle gibt einen kurzen Überblick über die Eignung magnetischer Speichermedien für die elektronische Archivierung:

Medium	Format und Kapazität	Standard	Verwendung
Diskette	3,5 - 5,25 Zoll, bis 1,44 MB	de facto	Kurzfristig für sehr kleine Archive, nicht revisionssicher
Festplatte	2,5 - 5,25 Zoll, über 100 GB	Herstellernormen	Kurzfristig für kleine Archive und Cachesysteme, nicht revisionssicher
Magnetband	über 80 GB	Herstellernormen	Mittelfristig für Archive mittlerer Größe, nicht revisionssicher

Tabelle: Eignung magnetischer Speichermedien

Digitale optische Systeme

Bei optischen Speichersystemen wird ein Speichereffekt dadurch erzielt, dass das optische Verhalten eines Grundmediums gezielt verändert werden kann. Die Speicherung erfolgt typischerweise durch Veränderung des Grundmediums, indem in eine ebene Grundschicht ("Land") gezielt Vertiefungen ("Pits") erzeugt oder simuliert werden, die beim Lesevorgang ein unterschiedliches optisches Verhalten eines gezielt ausgesandten Laserstrahls hervorrufen. Hieraus lassen sich Bitmuster interpretieren.

Während der Lesevorgang typischerweise bei allen optischen Medien gleich ist (die Wellenlänge des verwendeten Lasers kann sich allerdings unterscheiden), bestehen beim Speichervorgang wesentliche technologische Unterschiede.

- **CD-ROM**

nur bei hoher Stückzahl rentabel

Die Erzeugung von CD-ROMs (Compact Disk Read Only Memory) erfolgt mechanisch durch Stempelung mit einem Master-Datenträger. Die auf CD-ROM gespeicherten Daten sind typischerweise nicht mehr nachträglich änderbar (WORM). Die Produktion solcher Datenträger ist jedoch nur bei hoher Stückzahl rentabel. Als Archivmedien eignen sich solche Datenträ-

ger nicht, da in elektronischen Archiven typischerweise nur eine sehr geringe Stückzahl produziert wird, die nicht rentabel ist. Es gibt jedoch Ausnahmen, z. B. "Jahrgangsarchive" als Beilage zu großflächig verteilten Zeitschriften.

Für CD-ROMs sind mehrere Standards definiert, wodurch eine breite Herstellerunterstützung besteht. Ihre Speicherkapazität beträgt typischerweise bis zu 650 MB.

- **CD-Recordables (CD-Rs)**

  CD-Rs bestehen im Gegensatz zu CD-ROMs aus einer zusätzlichen Schicht (typischerweise Cyanin oder Phtalocyanin), bei der durch Auspunkten ("Brennen") mit einem Laser eine Lichtreflexion erzeugt werden kann, so dass beim Lesen des Datenträgers ein ähnlicher optischer Effekt wie bei einer CD-ROM erzielt wird. Die Speicherkapazität beträgt typischerweise bis zu 700 MB. Die einmal "gebrannten" Punkte können nicht wieder gelöscht werden. Vorteil gegenüber der mechanischen Stempelung des Datenträgers ist die individuelle Anpassbarkeit. Die Nachteile sind:

  - CD-Recordables können in beschränktem Umfang nachträglich geändert werden, da es prinzipiell möglich ist, durch Überbrennen der CD-R weitere Brennpunkte zu erzeugen und dadurch unter Umständen auch gezielte Datenveränderungen bis hin zur Unlesbarmachung der CD-R vorzunehmen. Es können jedoch keine bereits ausgepunkteten Bereiche wieder rückgängig gemacht werden. CD-Rs sind demnach gegenüber der allgemeinen Auffassung keine "echten" Write-Once-Medien (WORM), sondern lediglich nichtlöschbare Datenträger.
  - Bei fehlerhaftem Brennvorgang kann eine Lichtreflexion vorgetäuscht werden, die in seltenen Fällen durch eine nur vorübergehende Reaktion der Zwischenschicht erzeugt wird. CD-Rs müssen daher nach einigen Tagen verifiziert werden, um diesen Effekt auszuschließen.
  - Bei CD-Rs besteht ein sehr geringes Restrisiko, dass durch spontane Kristallisation der Oberfläche gespeicherte Daten zufällig verändert werden.

  CD-ROMs sind zwar nur einmal beschreibbar, es können aber in weiteren Brennvorgängen mehrere Sitzungen (Sessions) darauf angelegt werden. Bei der Verwendung als Archivmedien ist hiervon unbedingt abzusehen, da dies die Lesbarkeit und Korrektheit der zuerst archivierten Daten gefährden kann.

  Nur eine Session anlegen!

- **CD-Rewritables (CD-RWs)**

  CD-RWs nutzen ähnlich wie CD-Rs eine Zwischenschicht, die jedoch aus einem aufwändigeren Material (aus Silber, Indium, Antimon und Tellur) besteht, das gezielt in zwei unterschiedlich lichtreflektierende Zustände versetzt werden kann. Dies hängt ab von der Intensität des benutzten Lasers. CD-RWs sind daher mehrfach wiederbeschreibbar bzw. löschbar, bei fehlerhaften Laufwerken auch versehentlich. Sie eignen sich daher nicht für Archive, in denen eine revisionssichere Speicherung der Daten

  nicht revisionssicher

gefordert wird. Die Speicherkapazität beträgt typischerweise bis zu 700 MB.

Als Archivmedium weist die CD-RW-Technologie analog zur CD-R Schwachstellen auf:

- Bei fehlerhaftem Brennvorgang kann eine Lichtreflexion vorgetäuscht werden, die in seltenen Fällen durch eine nur vorübergehende Reaktion der Zwischenschicht erzeugt wird. CD-RWs müssen daher nach einigen Tagen verifiziert werden, um diesen Effekt auszuschließen.
- Bei CD-RWs besteht ein sehr geringes Restrisiko, dass durch spontane Kristallisation der Oberfläche gespeicherte Daten zufällig verändert werden.

- **DVD**

  DVD-Medien (Digital Versatile Disk) sind eine technologische Weiterentwicklung der Compact Disk (CD). DVDs erlauben eine wesentlich höhere Speicherdichte von 4,7 bis zu 17 GB, je nach Hersteller. Das DVD-Format ist im Gegensatz zur CD nicht standardisiert, weshalb derzeit unterschiedliche DVD-Varianten auf dem Markt erhältlich sind.

  Bei einigen DVD-Varianten können Daten übereinander in zwei unterschiedlichen Medienschichten gespeichert werden, die separat mit unterschiedlich fokussierten Lasern gelesen werden können (Dual Layer DVD).

  DVD-Recordable

  DVDs sind derzeit auch als DVD-Recordable (DVD-R) erhältlich. Es wird erwartet, dass künftig auch DVD-RWs am Markt angeboten werden. Für die elektronische Archivierung ist - analog zur CD - insbesondere die Variante DVD-Recordable interessant, da hierdurch eine revisionssichere Ablage bei hoher Speicherkapazität ermöglicht wird. Allerdings sind dabei dieselben Einschränkungen hinsichtlich des Überschreibschutzes wie bei der CD-R zu beachten.

Neben den weitverbreiteten CD- und DVD-Medien gibt es für die elektronische Archivierung weitere standardisierte optische Medien, die von Herstellern großer Speichersysteme verwendet werden. Die folgende Tabelle gibt einen Überblick über erhältliche Medienformate und die zugehörigen Standards:

Format	Kapazität	Normierung
3,5 Zoll		ANSI X3.213
CD (5,25 Zoll)	650 - 700 MB	ISO 9660
DVD (5,25 Zoll)	4,7 - 17 GB	ISO 13346
5,25 Zoll, RW	1 - 2,6 GB	ISO 10089
5,25 Zoll, WORM	1 - 2,6 GB	ISO 9171, ANSI X3.191, ANSI X3.211, ANSI X3.214
12 Zoll	2,6 - 16 GB	herstellerspezifisch, keine Norm
14 Zoll, WORM	6,8 - 25 GB	ANSI X3.200 und ISO/IEC 10885

Tabelle: Erhältliche Medienformate

Herstellergarantie

Die bei diesen Medien verwendete Technologie gleicht grundsätzlich dem bei CD-R (DVD-R) und CD-RW (DVD-RW) verwendeten optischen Verfahren. Die wesentlichen Unterschiede bestehen in der Verarbeitung zuverlässigerer Materialien und erweiterten Garantieerklärungen der Hersteller. Diese garantieren für wiederbeschreibbare Medien eine Datenstabilität zwischen 10 und 100 Jahren und für WORM-Medien zwischen 30 und 100 Jahren, je nach Hersteller und unter jeweiliger Vorgabe optimaler Einsatzbedingungen.

Jukeboxen

Auch bei den hier beschriebenen WORM-Medien kann technologisch bedingt nachträgliches Überschreiben bislang nicht genutzter Bereiche nicht ausgeschlossen werden. Es handelt sich demnach auch hier nicht um "echte" Write-Once-Medien, sondern lediglich um nicht-löschbare Datenträger.

Die betreffenden Hersteller bieten in der Regel nicht einzelne Medien an, sondern komplette Speicherlösungen, bei denen meist eine automatische Datenträgerverwaltung erfolgt. Die Speichermedien sind dann mechanisch an die jeweilige Herstellerlösung angepasst und mit einem Gehäuse versehen, so dass sie in den entsprechenden Robotersystemen (Jukeboxen) verwendet werden können.

Medium	**Format und Kapazität**	**Verwendung in Archiven**	**Revisionssicherheit**
CD-ROM	5,25 Zoll, 650 MB	nicht empfohlen	ja
CD-R	5,25 Zoll, 700 MB	kleine Archive	ja*
CD-RW	5,25 Zoll, 700 MB	kleine Archive	nein
DVD	5,25 Zoll, 4 - 17 GB	nicht empfohlen	ja
DVD-R	5,25 Zoll, 4 - 17 GB	mittelgroße Archive	ja*
DVD-RW	5,25 Zoll, 4 - 17 GB	mittelgroße Archive	nein
ISO 9171-WORM Medien	5,25 Zoll, 1,3 - 2,6 GB	mittelgroße bis große Archive	ja*
ISO 10089-RW Medien	5,25 Zoll, 1,3 - 2,6 GB	mittelgroße bis große Archive	nein
12 Zoll RW, herstellerspezifisch	12 Zoll, 2,6 - 16 GB	große Archive	nein
12 Zoll WORM, herstellerspezifisch	12 Zoll, 2,6 - 16 GB	große Archive	ja*
14 Zoll Medien, herstellerspezifisch	14 Zoll, 6,8 - 25 GB	große Archive	unbekannt

(* Technologisch bedingt ist ein Überschreiben dieser Medien prinzipiell nicht vollständig zu verhindern. WORM-Medien werden jedoch im Allgemeinen als revisionssicher angesehen.)

Tabelle: Überblick über die Eignung optischer Speichermedien für die elektronische Archivierung

Magneto-Optische Systeme

Polarisation

Bei der magneto-optischen (MO) Speichertechnologie werden gespeicherte Daten, ähnlich wie bei optischen Speichern, durch Abtasten eines Speichermediums mit einem Laserstrahl gelesen. Im Gegensatz zu CD-ähnlichen Speichern wird der optische Effekt jedoch nicht durch Vertiefungen in der Oberfläche des Speichermediums verursacht, sondern durch eine Magnetschicht, deren Partikel beim Durchlaufen und Reflexion des Laserstrahls als Polarisationsfilter wirken. Die Polarisation der Oberfläche lässt sich punktuell beeinflussen, indem ein Magnetfeld angelegt wird, das nur an einer (wiederum durch einen Laser) speziell aufgeheizten Region des Speichermediums wirkt. In einem Schreibprozess werden die Regionen der Medienoberfläche gezielt unterschiedlich polarisiert.

Die folgende Tabelle gibt einen Überblick über erhältliche Medienformate und die zugehörigen Standards:

Format	Kapazität	Normierung
3,5 Zoll Format	128 - 256 MB	ISO Norm 10090
5,25 Zoll, RW	1,3 - 9,1 GB	ANSI Norm X3.212
5,25 Zoll, WORM	1,3 - 9,1 GB	ISO/IEC 11560, ANSI Norm X3.220

Tabelle: Medienformate

Auch bei den hier beschriebenen WORM-Medien kann technologisch bedingt ein nachträgliches unbefugtes Überschreiben (Brennen) bislang ungenutzter Bereiche nicht ausgeschlossen werden. Es handelt sich demnach auch hier nicht um "echte" Write-Once-Medien, sondern lediglich um nicht-löschbare Datenträger.

Magneto-optische Systeme weisen eine hohe Langzeitstabilität (nach Herstellerangaben mehr als 30 Jahre) und eine hohe Speicherkapazität von bis zu 9,1 GB je Medium auf. Die folgende Tabelle gibt einen kurzen Überblick über die Eignung magneto-optischer Speichermedien für die elektronische Archivierung:

Medium	Kapazität	Verwendung in Archiven	Revisionssicherheit
3,5 Zoll Format	128 - 256 MB	nicht empfohlen	nein
5,25 Zoll, RW	1,3 - 9,1 GB	mittelgroße Archive	nein
5,25 Zoll, WORM	1,3 - 9,1 GB	mittelgroße Archive	ja*

(* Technologisch bedingt ist ein Überschreiben der Medien prinzipiell nicht vollständig zu verhindern. WORM-Medien werden jedoch im Allgemeinen als revisionssicher angesehen.)

Tabelle: Speichermedien für elektronische Archivierung

Verifikation der gespeicherten Daten

Unabhängig von der Art des gewählten Archivmediums sollte grundsätzlich nach der Speicherung eine Verifikation durchgeführt werden. Zum einen sollte diese durch das System erfolgen, um zu überprüfen, ob ein genaues Abbild der zu speichernden Daten angelegt wurde. Zum anderen sollte aber auch stichprobenartig immer wieder durch den Archivverwalter geprüft werden, ob auch alle für die Archivierung vorgesehen Daten archiviert und nicht durch Fehlkonfigurationen übersehen wurden.

Ergänzende Kontrollfragen:

- Sind die ausgewählten Archivmedien für das zu archivierende Datenaufkommen geeignet?
- Sind die ausgewählten Archivmedien für Langzeitarchivierung geeignet?
- Erfüllen die ausgewählten Archivmedien die Anforderungen an Kompatibilität und Interoperabilität mit anderen IT-Systemen?

M 4.170 Auswahl geeigneter Datenformate für die Archivierung von Dokumenten

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator

Für die Archivierung elektronischer Dokumente müssen geeignete Datenformate gewählt werden. Das Datenformat sollte langfristig eine originalgetreue Reproduktion der Archivdaten sowie ausgewählter Merkmale des ursprünglichen Dokumentmediums (z. B. Papierformat, Farben, Logos, Seitenzahl, Wasserzeichen, Unterschrift) ermöglichen. Die derzeit verwendeten Datenformate sind hierfür unterschiedlich geeignet, ihre Eignung hängt sehr stark vom Einsatzzweck der archivierten Daten und ihren Ursprungsmedien ab. Bei einem Wechsel des Medien- und Datenformats können jedoch in der Regel nicht alle Strukturmerkmale des Ursprungsmediums gleichzeitig abgebildet werden.

in mehreren Formaten gleichzeitig archivieren

Da im Vorfeld meist nicht absehbar ist, welche Merkmale des Originaldokuments bei einer späteren Reproduktion nachgewiesen werden sollen und mit welcher Nachweiskraft dies erfolgen soll, werden Dokumente typischerweise in mehreren elektronischen Datenformaten gleichzeitig archiviert. Dadurch soll eine möglichst hohe Überdeckung der Merkmale des Originaldokuments erreicht werden. Der Konvertierungsvorgang wird häufig als Rendition bezeichnet.

Für die Wahl geeigneter Datenformate sind folgende Kriterien maßgeblich:

- das Datenformat sollte möglichst langfristige Relevanz haben,
- die Dokumentstruktur sollte eindeutig interpretiert werden können,
- der Dokumentinhalt sollte elektronisch weiterverarbeitet werden können,
- Beachtung gesetzlicher Vorschriften,
- die Grammatik und Semantik des Datenformates muss ausführlich dokumentiert sein, so dass eine spätere Migration problemlos möglich ist,
- Merkmale des Originaldokuments (elektronisch oder in Papierform) sollen später eindeutig nachweisbar sein, auch wenn das Originaldokument nicht mehr vorhanden ist.

Struktur und graphische Darstellung

Typischerweise wird neben einer strukturellen Repräsentation (in einer Strukturbeschreibungssprache) bei Papierdokumenten auch eine graphische Repräsentation des Dokuments archiviert. Hinzu kommen unter Umständen elektronische Signaturen zur Beglaubigung der Authentizität.

In den folgenden Abschnitten werden einige typische Datenformate beschrieben und ihre Eignung für die elektronische Archivierung diskutiert.

A. Strukturformate

SGML

SGML (Standard Generalized Markup Language) ist eine Dokumentenbeschreibungssprache, die die logische Struktur und den Inhalt von elektronischen Dokumenten beschreibt. SGML ist als ISO-Norm 8879 standardisiert.

Neben der Struktur (Syntax) von Dokumenten beschreibt SGML insbesondere die Semantik der Strukturelemente des elektronischen Dokuments. SGML bildet jedoch nicht die konkrete Darstellung und Formatierung der Dokumentinhalte bei der Wiedergabe ab.

Wichtige Merkmale von SGML sind:

Document Type Definition

- Die Semantik der SGML-Elemente wird separat in der so genannten DTD (Document Type Definition) definiert. Die DTD dient als Grundlage für den Dokumentenaustausch zwischen Institutionen bzw. Applikationen.
- SGML ist für die unabhängige Darstellung und Speicherung von strukturierten Textdokumenten geeignet, da die Layout-Informationen vom Dokumenteninhalt getrennt behandelt werden.
- SGML kann direkt für die Abbildung von Strukturen in Dokumenten-Management-Systemen verwendet werden.

SGML kann als Format für die Langzeitarchivierung von elektronischen Dokumenten genutzt werden. Bei der Archivierung ist jedoch unbedingt auch die Semantikspezifikation (DTD) zu archivieren. Da SGML keinerlei Layout-Informationen beinhaltet, wird empfohlen, zusätzlich zu SGML-Dokumenten eine graphische Repräsentation des Ursprungsdokuments zu archivieren, z. B. im Format TIFF.

HTML

HTML (Hyper Text Markup Language) ist eine Strukturbeschreibungssprache für elektronische Dokumente. HTML basiert auf einer Untermenge der SGML-Beschreibungselemente und hat sich zum Standard für die Darstellung und den Dokumentenaustausch im World Wide Web entwickelt.

implizite DTD

HTML bietet eine sehr eingeschränkte Zahl möglicher Strukturmerkmale für Dokumente und ist als SGML-Spezialisierung mit impliziter DTD zu verstehen.

Wichtige Merkmale von HTML sind:

- In HTML können Dokumentteile durch "Hyperlinks" zu einer Gesamtdokumentstruktur zusammengefügt werden. Hierdurch können in den laufenden Text Bilder und Textteile eingebunden werden, die physikalisch auf verteilten Servern gelagert sind. Es ist aufgrund der dynamischen Anbindung möglich, dass sich ohne Kenntnis des Dokumentinhabers Teile des Gesamtdokuments ändern, da hinzugelinkte Unterkapitel oder Bilder verändert wurden oder nicht erreichbar sind.

- HTML ist auf die bestehenden Strukturmerkmale festgelegt. Weder die Syntax noch die Semantik der so genannten HTML-Tags kann individuell ergänzt oder erweitert werden.
- Aufgrund der mangelhaften Flexibilität von HTML ist es bei Veränderungen der Anforderungen notwendig, den HTML-Standard zu überarbeiten. Dies erfolgte in den letzten Jahren regelmäßig durch das zuständige Standardisierungsgremium (W3C-Konsortium). Daneben wurden eigenmächtige Erweiterungen durch Hersteller von HTML-Browsern vorgenommen. Auch zukünftig ist mit ständigen Erweiterungen der Sprache zu rechnen.

ständige Erweiterungen

HTML wird als Format für die Langzeitarchivierung nicht empfohlen. Es ist nicht für die Archivierung geeignet, da aufgrund der mangelhaften syntaktischen und semantischen Flexibilität auch künftig in kurzen zeitlichen Abständen Erweiterungen des HTML-Standards zu erwarten sind.

nicht für Archivierung geeignet

Es ist zudem nicht geeignet, da aufgrund der dynamischen Struktur der HTML-Dokumente eine Archivierung des Gesamtdokuments erfolgen muss, d. h. inklusive aller verlinkten Bilder, Subdokumente und Querverweise. Bei der Archivierung von HTML-Dokumenten dürfen keine aktiven Links zu nicht archivierten Dokumentteilen mehr vorhanden sein, da nicht sichergestellt werden kann, dass solche externen Dokumentteile bei späteren Reproduktionen zur Verfügung stehen.

XML

Aufgrund der eingeschränkten Funktion von HTML wurde vom W3C eine Möglichkeit geschaffen, die Vorteile der Sprache SGML zu nutzen, gleichzeitig aber nicht deren volle Komplexität einzubringen. XML wurde als Teilmenge von SGML entwickelt.

Vorteile von SGML, geringere Komplexität

Wichtige Merkmale von XML sind:

- In XML können - im Gegensatz zu HTML - Tags und Attribute neu definiert werden. Hierdurch können Anpassungen an der Syntax und Semantik der Beschreibungselemente vorgenommen werden.
- Analog zu HTML können Links in die Dokumentenstruktur integriert werden. Somit können auf einfache Art und Weise bestehende Dokumente referenziert und z. B. Bilder in Dokumente eingebunden werden.
- XML kann direkt in neueren Web-Browsern angezeigt werden. Zur Darstellung wird eine separate Definition des Layouts in Form der Beschreibungssprache XSL (Extensible Stylesheet Language) benötigt.

XML kann als Format für die Langzeitarchivierung von elektronischen Dokumenten genutzt werden. Bei der Archivierung sind jedoch unbedingt auch die Semantikspezifikation (DTD - Document Type Definition) und ggf. auch die Layout-Informationen, in XSL beschrieben, zu archivieren.

für Archivierung geeignet

PDF

PDF (Portable Document Format) ist ein Dokumentformat, bei dem neben der Strukturinformation von elektronischen Dokumenten auch wesentliche

Layout-Informationen mitgespeichert werden. PDF wurde von der Firma Adobe auf Basis des Datenformats PostScript entwickelt.

Erscheinungsbild ist festgelegt

Das Erscheinungsbild wird dabei durch einen Datenstrom beschrieben, der eine Reihe von graphischen Objekten enthält. Durch diese Beschreibung ist ein Dokument vollkommen festgelegt. Die Entscheidung über das Erscheinungsbild wird dabei zum Zeitpunkt der Erstellung des Dokuments getroffen und ist dann fixiert. Gegenüber einer rein bildlichen Darstellung (Pixeldarstellung) benötigen Dokumente im PDF-Format meist deutlich weniger Speicherplatz.

Zielsetzung beim Einsatz von PDF ist, das Erscheinungsbild eines elektronischen Dokuments unabhängig von der zur Erstellung benutzten Anwendungs-Software, der Hardware-Plattform oder dem Betriebssystem zu bewahren. PDF eignet sich daher primär für die Archivierung von Dokumenten, bei denen eine Abbildung in Papierform vorgesehen ist bzw. die den Charakter von Briefen und Geschäftsdokumenten haben.

PDF ist nicht standardisiert. Wenn es als Datenformat zur elektronischen Archivierung verwendet werden soll, sollte das Datenformat PDF separat dokumentiert werden.

B. Bildformate

TIFF

Das Format TIFF (Tagged Image File Format) wird zur Speicherung gerasterter Bilder verwendet. Eine TIFF-Datei besteht aus einem Datei-Header und der Bildinformation. Der Header enthält so genannte Tags, in denen Eigenschaften des aufgezeichneten Bildes gespeichert sind, z. B. Auflösung oder verwendete Kompressionsverfahren.

Wichtige Merkmale von TIFF sind:

24 Bit Farbtiefe

- Bildinformationen können sowohl in Schwarz/Weiß als auch in Grauabstufungen verlustfrei gespeichert werden, jedoch nur dann, wenn eine Farbtiefe von 24 Bit (Truecolor) gewählt wird. Nur in dieser Stufe können alle Graustufen wiedergegeben werden. Um Farbinformationen originalgetreu aufzunehmen und zu speichern, ist jedoch eine regelmäßige Feineinstellung der optischen Sensoren notwendig, damit die Farbinformation nicht durch Farbverschiebungen verfälscht werden. Dies kann z. B. durch einen Farbabgleich mit Weiß als Referenzfarbe erfolgen.
- Alle gängigen Graphik- und Präsentationsprogramme unterstützen das TIFF Format. Darüber hinaus wird es auch von Archiv- und Workflow-Systemen unterstützt.
- Faxgeräte benutzen TIFF als gängiges Datenformat.
- Die Bilddaten können komprimiert abgespeichert werden. TIFF ist mit den meisten Kompressionsverfahren kompatibel. Zwei der wichtigsten Kompressionsverfahren werden hier kurz angesprochen:
  - ITU/CCITT - Gruppe 4:

    Die ITU-Kompression benutzt TIFF als Eingangsformat. Dabei wird bei normalen Textdokumenten ein Kompressionsfaktor von etwa

1:40 erreicht. Es ist damit ideal geeignet für Schwarz/Weiß-Dokumente. Die Kompression ist verlustfrei.

Die ITU-Kompression ist im Bereich der Archivierung weltweit standardisiert.

- JBIG:

  JBIG ist ein verlustfreies Kompressionsverfahren für Schwarz/Weiß-Bilder im TIFF-Format. Es ist in der ISO/IEC-Norm 11544 standardisiert. Im Vergleich zur ITU-Gruppe-4-Kompression arbeitet es bis zu 70% effektiver.

  JBIG ist derzeit nicht so weit verbreitet wie das ITU-Verfahren und wird nicht von allen Herstellern unterstützt.

verlustfreie Kompression verwenden

TIFF ist in komprimierter Form als Format für die Langzeitarchivierung von Bildern und Bildrepräsentationen von Dokumenten geeignet. Es wird empfohlen, ein verlustfreies Kompressionsverfahren zu verwenden, z. B. ITU/CCITT-Gruppe 4, um den benötigten Speicherbedarf zu minimieren.

GIF

Das Format GIF (Graphics Interchange Format) wird zur Speicherung gerasterter Bilder verwendet.

Wichtige Merkmale von GIF sind:

- Alle gängigen Graphik- und Präsentationsprogramme unterstützen das GIF-Format. Darüber hinaus wird es auch von Archiv- und Workflow-Systemen unterstützt.
- Die Konvertierung in GIF ist verlustbehaftet, es gehen zugunsten einer geringen Dateigröße Bildinformationen verloren.
- Die Verwendung des Formats GIF in Applikationen ist lizenzpflichtig.

nur für kurz- und mittelfristige Archivierung geeignet

Der Einsatz des Formats GIF wird für die Langzeitarchivierung nicht empfohlen, jedoch kann GIF für die kurz- und mittelfristige Archivierung eingesetzt werden.

JPEG

JPEG wurde von der *Joint Photographic Experts Group* entwickelt und eignet sich besonders für Farb- und Grauwertbilder. In diesem Bereich ist die JPEG-Kompression auch effektiver als die ITU-Gruppe-4-Kompression.

JPEG kann anhand einiger Parameter unterschiedlich konfiguriert werden. Je nach Einstellung werden dann unterschiedliche Kompressionsraten erreicht. Allerdings können auch Verluste auftreten.

Wichtige Merkmale von JPEG sind:

- Alle gängigen Graphik- und Präsentationsprogramme unterstützen das Format JPEG.
- Die Konvertierung in JPEG ist in einigen Kompressionsstufen verlustbehaftet, es können dann zugunsten einer geringen Dateigröße wesentliche Bildinformationen verloren gehen.

JPEG ist als Format für die Langzeitarchivierung von Bildern und Bildrepräsentationen von Dokumenten geeignet. Für eine revisionssichere Archivierung wird empfohlen, bei der Auswahl der Kompressionsstufe eine verlustfreie Kompression zu wählen.

verlustfreie Kompressionsstufe verwenden

C. Audio- und Video-Formate

Bei der digitalen Verarbeitung von Audio- und Videodaten entstehen schon bei zeitlich kurzen Aufzeichnungen sehr große Datenmengen. Daher gewinnt eine effektive Kompression an Bedeutung.

Verluste werden oft in Kauf genommen

Verlustfreie Kompressionsverfahren für Audio- und Videodaten erreichen derzeit jedoch nur Kompressionsraten von etwa 2:1. Gebräuchlicher sind Verfahren, die eine Kompressionsrate bis zu 200:1 erreichen, jedoch nicht verlustfrei arbeiten. Der durch die Kompression entstehende, teilweise erhebliche Datenverlust wird typischerweise in Kauf genommen, solange er mit dem menschlichen Auge bzw. Ohr nicht wahrnehmbar ist bzw. nicht als störend empfunden wird.

Die Eignung verlustbehafteter Kompressionsverfahren für die Archivierung von Video- und Tonmaterial ist anwendungsspezifisch zu prüfen.

Im Folgenden werden einige typische Formate vorgestellt:

MPEG

Innerhalb der ISO ist die *Motion Pictures Expert Group* (MPEG) für die Bearbeitung weltweiter Standards zur Kompression digitalisierter Bewegtbilder verantwortlich.

Derzeit sind drei verschiedene Verfahren bekannt:

MPEG1: Dieses Format gibt es in drei verschiedenen Layern. Layer 3 ist in der Kurzform MP3 bekannt und als Kompression für Audiodaten verbreitet.

MPEG2: Dieses Format ist derzeit für die Speicherung von Videodaten auf DVD in Gebrauch und als Standard akzeptiert.

MPEG4: Dieses Format befindet sich noch in der Entwicklung und ist noch nicht abschließend standardisiert.

ITU H.261

Im Jahr 1990 wurde der Standard H.261 von der ITU zur Kodierung von Videosignalen verabschiedet. Die Kodierung nach H.261 ist für die Übertragung auf ISDN-Kanälen optimiert und entwickelt worden.

ITU H.263

Der ITU-Standard H.263 ist eine Weiterentwicklung des Standards H.261 aus dem Jahr 1995/96. Er ist ursprünglich für Datenraten kleiner als 64 kbit/s entwickelt worden. Dieser Beschränkung existiert heute nicht mehr. Die Bildqualität wurde gegenüber dem Standard H.261 bei deutlich verbesserter Kompression erheblich gesteigert.

Ergänzende Kontrollfragen:

- Ist festgelegt, welche Datenformate verwendet werden?

- Sind die Syntax und Semantik der verwendeten Datenformate dokumentiert?
- Ist der Informationsverlust bei der Umwandlung in Standardformate vertretbar?
- Ist das gewählte Datenformat für den Archivierungszeitraum geeignet?
- Wird ein verlustfreies Bild-Kompressionsverfahren für revisionssichere Archivierung verwendet?

M 4.171 Schutz der Integrität der Index-Datenbank von Archivsystemen

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator

Die Index-Datenbank ist besonders wichtig für das korrekte Funktionieren eines Archivsystems. In ihr sind die Verweise auf sämtliche archivierten Dokumente abgelegt. Fehlende oder beschädigte Einträge in der Index-Datenbank können dazu führen, dass archivierte Dokumente nicht oder nur mit sehr hohem Aufwand wiedergefunden und Geschäftsvorgängen zugeordnet werden können.

Daher muss für einen ordnungsgemäßen Archivbetrieb die Integrität der Index-Datenbank sichergestellt werden und überprüfbar sein. Zur Integritätssicherung sind folgende Empfehlungen zu berücksichtigen:

Redundante Ablage der Indexeinträge

In Abhängigkeit von der Archivgröße sind folgende Abstufungen vorzusehen:

tägliche Datensicherung

Bei *kleinen Archiven mit geringem Datenaufkommen* und geringen Anforderungen an die Antwortzeiten ist es ausreichend, eine tägliche Datensicherung der Index-Datenbank vorzunehmen. Die Datensicherung sollte gemäß Baustein B 1.4 *Datensicherungskonzept* vorgenommen werden.

gespiegelte Datenbank

Bei *Archiven mit hohem Datenaufkommen* sowie hohen Anforderungen an die Antwortzeit sollte die Index-Datenbank selbst redundant ausgelegt, d. h. gespiegelt sein. Auch hier ist zusätzlich eine tägliche Datensicherung durchzuführen. Die gespiegelten Teil-Datenbanken sollten in unterschiedlichen Brandabschnitten aufgestellt sein.

Regelmäßige Integritätsprüfung

Die Index-Datenbank sollte regelmäßig (mindestens wöchentlich, bei großen Archiven täglich) geprüft werden, ob sie konsistent und integer ist. Alle in der Index-Datenbank referenzierten Dokumente müssen auf den Archivmedien auffindbar sein. Integritätsverletzungen müssen dokumentiert und zeitnah behoben werden.

Backups auf Wiederherstellbarkeit prüfen

In regelmäßigen Abständen (z. B. monatlich) sollte zudem geprüft werden, ob die Datensicherungen der Index-Datenbank lesbar und wiederverwendbar sind. Bei redundant ausgelegten Datenbanken sollte getestet werden, ob die Funktionsübergabe bei Ausfall eines Teils ordnungsgemäß funktioniert.

Alle Ergebnisse der regelmäßigen Integritätsprüfung sollten ebenfalls archiviert werden, damit Datenänderungen später nachvollzogen werden können.

Ergänzende Kontrollfragen:

- Erfolgt eine regelmäßige Datensicherung der Index-Datenbank des Archivsystems?
- Wird regelmäßig überprüft, ob die Datensicherungen der Index-Datenbank wiederherstellbar sind?

- Ist bei mittleren und großen Archiven die Index-Datenbank redundant ausgelegt, z. B. als Spiegel-Datenbank?
- Befinden sich die gespiegelten Datenbankteile in unterschiedlichen Brandabschnitten?

M 4.172 Protokollierung der Archivzugriffe

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator

Die Zugriffe auf elektronische Archive sind zu protokollieren. Hierdurch soll die Nachvollziehbarkeit der Aktivitäten gewährleistet und eventuelle Fehlerkorrekturen ermöglicht werden. Die folgende Aufzählung gibt einen Überblick darüber, welche Arten von Ereignissen mit Hilfe der Protokollierung erkannt werden können:

- Vertraulichkeits- bzw. Integritätsverlust von Daten durch Fehlverhalten der IT-Benutzer,
- fehlerhafte Administration von Zugangs- und Zugriffsrechten,
- Ausschalten des Servers im laufenden Betrieb,
- Verstoß gegen rechtliche Rahmenbedingungen beim Einsatz von Archivsystemen,
- defekte Datenträger,
- Verlust gespeicherter Daten,
- Datenverlust bei erschöpftem Speichermedium,
- Manipulation an Daten oder Software,
- unberechtigtes Kopieren der Datenträger,
- Manipulation eines Kryptomoduls,
- Kompromittierung kryptographischer Schlüssel und
- unberechtigtes Überschreiben oder Löschen von Archivmedien.

rechtliche und interne Bestimmungen beachten

Der Umfang der Protokollierung richtet sich einerseits nach den Anforderungen an die Nachvollziehbarkeit und Authentizität der in Archiven gespeicherten Dokumente. Andererseits müssen auch die organisationsintern abgestimmten Regelungen, z. B. zum Datenschutz, beachtet werden.

Sofern möglich, sollten mindestens folgende Daten protokolliert werden:

- Datum und Uhrzeit des Zugriffs,
- Clientsystem, von dem aus zugegriffen wurde,
- Archivbenutzer und ausgeübte Benutzerrolle,
- ausgeführte Aktionen sowie
- eventuelle Fehlermeldungen und -codes.

Die Zeitdauer der Aufbewahrung der Protokolldaten ist im Archivierungskonzept festzulegen.

Protokolldaten regelmäßig auswerten

Die Protokolldaten müssen unter Beachtung organisationsinterner Vorgaben regelmäßig ausgewertet werden, um Missbrauch und Systemfehler zu erkennen. Die Auswertung kann manuell oder mit Unterstützung eines Tools erfolgen. Im Vorfeld sollten kritische Ereignisse definiert werden, also solche, bei deren Auftreten ein Administrator zu benachrichtigen ist. Solche Vorfälle

sollten umgehend signalisiert werden, z. B. unter Nutzung vorhandener Systemmanagement-Umgebungen. Außerdem ist es wichtig, dass die Benachrichtigung rollenbezogen, nicht personenbezogen erfolgt. Wird beispielsweise eine E-Mail an eine konkrete Person geschickt, bleibt die Nachricht unter Umständen unbeachtet, wenn diese Person nicht anwesend ist.

kritische Ereignisse signalisieren

Folgende Ereignisse weisen bei der Archivierung typischerweise eine hohe Kritikalität auf und sollten daher permanent protokolliert, überwacht und bei Auftreten umgehend signalisiert werden:

- Kopieren von Archivmedien,
- Kopieren von Archivsystem-Datenträgern,
- Löschen oder Löschmarkierung von Datensätzen,
- Offline-Schaltung von Archivmedien in Archivsystemen,
- Entnahme von Archivmedien aus dem Archivsystem,
- Einlegen von Archivmedien,
- Online-Schalten von Archivmedien,
- Fehler oder Probleme beim Zugriff auf das Archiv,
- Systemfehler und Timeouts,
- Katastrophenszenarien (Brand, unzulässige Temperatur, Wasser etc.), die in der Regel durch externe Sensorik gemeldet werden.

Nach der Signalisierung sollte das Ereignis sofort geprüft und gegebenenfalls weiter eskaliert werden. Typischerweise erfolgt eine erste Eskalation an den Leiter IT. Organisationsspezifisch können jedoch auch andere Eskalationsprozesse vorgesehen sein.

Ergänzende Kontrollfragen:

- Erfolgt eine Protokollierung der Aktivitäten am Archivsystem?
- Werden organisationsinterne und rechtliche Vorgaben bei der Protokollierung eingehalten?
- Wird protokolliert, ob und welche Medien der Jukebox entnommen oder darin eingesetzt wurden?
- Erfolgt eine Signalisierung beim Auftreten von Sicherheitsverletzungen?
- Bestehen Regelungen zur Eskalation beim Auftreten von Sicherheitsverletzungen?

M 4.173 Regelmäßige Funktions- und Recoverytests bei der Archivierung

Verantwortlich für Initiierung: Leiter IT, Archivverwalter

Verantwortlich für Umsetzung: Leiter IT, Administrator, Archivverwalter

Durch verschiedene Ursachen in den Bereichen Datenträger, Hardware und beim Programmablauf kann es bei der Archivierung zu Datenverlusten kommen. Regelmäßige Funktions- und Recoverytests sind daher unumgänglich.

regelmäßige Prüfung der Datenbestände

Datenträger unterliegen ebenso wie alle anderen Archivierungskomponenten Verschleißerscheinungen und sollten daher mindestens einmal jährlich auf Lesbarkeit und Integrität geprüft werden.

Werden Fehler auf einem Archivmedium festgestellt, so ist unverzüglich sicherzustellen, dass die betroffenen Dateien aus dem Backup-Bestand wieder hergestellt werden. Wenn fehlerhafte Archivdatenträger ausgetauscht werden müssen, so sind diese nach der Kopie der darauf enthaltenen Daten sicher zu löschen bzw. zu vernichten (siehe auch M 2.167 *Sicheres Löschen von Datenträgern*). Der gesamte Vorgang ist zu dokumentieren.

Test der Hardware

Alle Hardwarekomponenten, insbesondere die mechanischen Teile des Archivs, müssen regelmäßig auf einwandfreie Funktion geprüft werden. Nur so kann gewährleistet werden, dass archivierte Datenbestände den geforderten Verfügbarkeitsanforderungen entsprechen und beim Schreiben und Lesen der Daten die Datenintegrität gegeben ist.

tägliche Auswertung von Log-Dateien

Der Archivierungsvorgang selbst kann fehlerhaft verlaufen. Mögliche Ursachen können sein: Konfigurationsfehler, Softwarefehlfunktionen (z.B. beim Einsatz neuer Programme), Probleme mit den Speichermedien oder Änderungen und Fehler in der Ablaufsteuerung. Einmal pro Tag ist daher zu überprüfen, ob alle Archivierungsprozesse fehlerfrei abgelaufen sind. Dies kann durch Auswertung von Log-Dateien sowie stichprobenartige Ansicht der erstellten Archivmedien durch den Administrator geschehen.

Die notwendigen Integritätsprüfungen der Index-Datenbank sind in Maßnahme M 4.171 *Schutz der Integrität der Index-Datenbank von Archivsystemen* beschrieben.

Ergänzende Kontrollfragen:

- Werden alle Archivmedien regelmäßig auf Lesbarkeit und Integrität geprüft?
- Werden die mechanischen Teile des Archivs regelmäßig auf einwandfreie Funktion geprüft?
- Werden neue Datenbestände täglich kontrolliert und die Log-Dateien ausgewertet?

M 4.174 Vorbereitung der Installation von Windows NT/2000 für den IIS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Vorbereitungen des Betriebssystems sind die grundlegenden Maßnahmen für die Installation des IIS. Diese Maßnahmen sind als erstes technisch umzusetzen und lassen sich nicht oder nur schwer nachträglich realisieren.

Version des Betriebssystems

Englische Version

Die englische Version von Windows NT/2000 ist weiter verbreitet als die deutsche Version. Dies führt dazu, dass Tools, Service Packs und Hotfixes für die englische Version schneller verfügbar sind. Es gibt auch Tools, die nur mit der englischen Version von Windows NT/2000 einsetzbar sind. Es ist auch möglich, die englische Version von Windows NT/2000 so zu konfigurieren, dass Fehlermeldungen in deutscher Sprache ausgegeben werden. Es sollte demnach die englische Version von Windows NT/2000 eingesetzt werden.

Installation des Servers

Bei der Installation eines Rechners als Internet-Server sollte auch das Betriebssystem neu installiert werden, da die Gefahr bestehender Sicherheitslücken bei einem historisch gewachsenen System sehr groß ist.

Stand-Alone-Server

Die Installation von Windows NT/2000 sollte als Stand-Alone-Server erfolgen. Wenn möglich sollte der Server nicht als Domänen-Controller oder Mitglied einer Domäne konfiguriert werden, da die Gefahr besteht, dass ein Angreifer Informationen über vorhandene Benutzer und Systeme gewinnen kann. Ebenfalls sollte der Server nicht in das Active Directory (Windows 2000) der Organisation eingebunden werden.

Partitionierung

Für die spätere Installation des Web-Servers bietet es sich an, **zwei getrennte** Partitionen zu erstellen. Dadurch besteht die Möglichkeit, das *Webroot*-Verzeichnis, auf das von extern zugegriffen wird, von den Systemverzeichnissen zu trennen.

Dateisystem

Um auf der Verzeichnisebene eine größere Sicherheit zu gewährleisten, ist als Dateisystem NTFS zu wählen. Die Zugriffe und Berechtigungen, z. B. *Lesen, Schreiben, Ausführen*, auf Dateien und Verzeichnisse werden dabei über Access Control Lists (ACLs) festgelegt und können auf bestimmte Benutzer beschränkt werden.

Windows NT mit IIS 2.0

Bei Windows NT bietet der Installations-Wizard während der Installation von Windows NT 4.0 Server die Möglichkeit, den IIS 2.0 mit zu installieren. Dieser Installationsschritt ist zu überspringen, um den IIS 4.0 zu installieren.

Internet Explorer

Voraussetzung für die Installation des IIS ist bei Windows NT der Internet Explorer 4.0.1. Microsoft empfiehlt, die Version 4.01 mit dem Service Pack 2 zu installieren, da auf die erweiterten Möglichkeiten des Internet Explorer 5 verzichtet werden kann.

Der "Active Desktop" sollte auf keinem IIS-System aktiviert sein. Er ist in den Eigenschaften des Desktops zu deaktivieren.

Windows 2000

Bei einer Neuinstallation eines Windows 2000 Servers wird der IIS 5.0 standardmäßig mit installiert. Auch beim Update eines Systems, z. B. Windows NT 4.0 Server, wird ein vorhandener IIS 4.0 automatisch aktualisiert. Bei einem historisch gewachsenen System besteht die Gefahr, dass bestehende Sicherheitslücken auf das neue System übertragen werden. Deshalb ist bei einem Internet-Web-Server so weit wie möglich eine Neuinstallation zu empfehlen. Ansonsten muss der IIS über die Systemsteuerung *Software | Windows-Komponenten hinzufügen/entfernen* hinzugefügt werden.

Updates und Patches

Updates und Patches

Bei der Installation von Windows NT/2000 sind eine Reihe von Updates und Patches zu berücksichtigen. Eine aktuelle Übersicht ist auf den Web-Seiten von Microsoft (*http://www.microsoft.com/ntserver/downloads/default.asp* und *http://www.microsoft.com/windows2000/server/default.asp*) oder auf den Web-Seiten des RUS CERT (*http://cert.uni-stuttgart.de/ms.php*) zu finden. Der Administrator eines Web-Servers sollte das System aktuell halten.

Microsoft stellt ein Tool zur Verfügung (*HFCHECK.WSF*), das den aktuellen Patch-Status für Windows NT und Windows 2000 sowie die aktuellen Hotfixes für den IIS 4.0 und IIS 5.0 untersucht. Das Tool kann unter

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24168

herunter geladen werden. Eine Anleitung ist unter

http://www.aspheute.com/artikel/20000914.htm

erhältlich.

Ergänzende Kontrollfragen:

- Wird die englische Version des Betriebssystems eingesetzt?
- Wurde der Server als Stand-Alone-Server installiert?
- Wurden bei der Installation mindestens zwei Partitionen eingerichtet?
- Wird als Dateisystem NTFS verwendet?

M 4.175 Sichere Konfiguration von Windows NT/2000 für den IIS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der sichere Einsatz des Internet Information Servers (IIS) erfordert, dass das zugrunde liegende Betriebssystem entsprechend konfiguriert ist. Die folgenden Einstellungen sollten an allen IT-Systemen vorgenommen werden, die als Internet- oder Intranet-Server mit der IIS-Software eingesetzt werden.

Abschalten der NTFS 8.3 Namensgeneration

NTFS kann automatisch 8.3-Namen für die Abwärtskompatibilität mit 16-Bit-Anwendungen generieren. Da generell keine 16-Bit-Applikationen auf einem IIS-System verwendet werden sollten, ist diese Funktion abzuschalten. Zusätzlich zur Sicherheit wird die Performance des Systems verbessert.

Um die automatische 8.3-Namensgeneration abzuschalten, sind folgende Einträge in der Registrierung anzupassen:

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	\CurrentControlSet\Control\FileSystem
Name	NtfsDisable8dot3NameCreation
Type	REG_DWORD
Wert	1

Tabelle: Einträge in Registrierung

Systembootzeit auf 0 Sekunden setzen

Um die Systembootzeit auf 0 Sekunden zu setzen, ist in der *Systemsteuerung* | *System* | *Starten/Herunterfahren* | *Liste für X Sekunden anzeigen* der Wert 0 einzutragen.

Entfernen des OS/2 und POSIX Subsystems

Windows NT/2000 bietet die Möglichkeit, DOS, Win16, OS/2 1.x und POSIX Anwendungen zu starten. Nur wenige Anwender nutzen diese Möglichkeit und diese Subsysteme sind nicht so detailliert untersucht wie das Win32 Subsystem. Da jederzeit potentielle Sicherheitslücken in diesen Subsystemen auftreten können, sollten diese Subsysteme entfernt werden, wenn sie nicht benötigt werden.

Das Entfernen des OS/2 und POSIX Subsystems erfolgt durch folgende Änderungen in der Registrierung:

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SOFTWARE
Schlüssel	\Microsoft\OS/2 Subsystem for NT
Aktion	Alle Schlüssel löschen

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	\CurrentControlSet\Control\Session Manager\Environment
Name	Os2LibPath
Aktion	Den Schlüssel Os2LibPath löschen

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	\CurrentControlSet\Control\Session Manager\SubSystems
Aktion	Die Schlüssel Posix und OS/2 löschen

Tabelle: Änderungen in der Registrierung

Anschließend sind die Verzeichnisse *\winnt\system32\os2* und alle Unterverzeichnisse davon zu löschen. Die Änderungen werden nach dem nächsten Neustart wirksam.

Hinweis: Die Schlüssel für das OS/2 Subsystem werden nach einem Systemstart wieder erstellt, aber solange diese leer sind, gilt das OS/2 Subsystem als entfernt.

Entfernen des Buttons *Herunterfahren* in der Anmeldemaske

Trotz einer geeigneten Zutrittskontrolle kann es vorkommen, dass nicht berechtigte Personen an die Konsole eines Windows NT/2000-Servers gelangen. Damit diese Personen nicht die Möglichkeit bekommen, über die Anmeldemaske von Windows den Rechner herunterzufahren, sollte diese Schaltfläche entfernt werden.

Das Entfernen der Schaltfläche *Herunterfahren* in der Anmeldemaske erfolgt durch folgende Änderungen in der Registrierung:

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SOFTWARE
Schlüssel	\Microsoft\Windows NT\Current Version\Winlogon
Name	ShutdownWithoutLogon
Type	REG_SZ
Wert	0

Tabelle: Änderungen in der Registrierung

Ergänzende Kontrollfragen:

- Wurde die automatische Generierung von 8.3-Namen abgeschaltet?
- Wurde die Systembootzeit auf 0 Sekunden gesetzt?
- Wurden die OS/2 und POSIX Subsysteme entfernt?
- Wurde die Schaltfläche *Herunterfahren* in der Anmeldemaske entfernt?

M 4.176 Auswahl einer Authentisierungsmethode für Webangebote

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Für E-Commerce- und E-Government-Anwendungen, personalisierte Webangebote oder nur allgemein zur Realisierung von Zugriffsbeschränkungen auf bestimmte Bereiche eines Webangebots werden Mechanismen zur Identifikation und Authentisierung verschiedener Benutzer benötigt.

In Abhängigkeit von den konkreten Anforderungen an den Schutz der Dokumente vor unbefugtem Zugriff und die Qualität der Authentisierung muss eine geeignete Methode ausgewählt werden. Die Wahl der Authentisierungsmethode und die Gründe, die zu der Wahl geführt haben, sollten dokumentiert werden.

Authentisierungsmethoden bei HTTP

Das Protokoll HTTP/1.1 sieht zwei verschiedene Methoden zur Benutzerauthentisierung vor.

Basic Authentisierung

Die erste Methode ist die so genannte *Basic-Access-Authentisierung*. Dabei sendet der Client den Benutzernamen und das Passwort *Base64*-kodiert im so genannten *Authorization Header* des HTTP-Requests an den Server. *Base64* ist eine Methode zur Kodierung von Binärdaten in 7-Bit ASCII, die hier zur Übertragung von Sonderzeichen über die HTTP-Schnittstelle genutzt wird. Das Passwort ist somit zwar nicht auf den ersten Blick ablesbar, kann aber von einem potentiellen "Lauscher" problemlos ermittelt werden, da es unverschlüsselt ist. Daher ist dieser Authentisierungstyp allenfalls für sehr geringe Vertraulichkeitsanforderungen zu gebrauchen.

Digest-Authentisierung

Die zweite Methode zur HTTP-Authentisierung ist die *Digest-Authentisierung*. Bei dieser Art der Authentisierung muss auf dem Server das Passwort des Benutzers im Klartext vorliegen. Der Client erhält vom Server einen Zufallsstring, die so genannte Challenge. Aus dieser Challenge und dem Passwort des Benutzers errechnet der Client nach einem standardisierten Verfahren einen so genannten *Digest*, der dann zur Authentisierung an den Server gesandt wird. Da der Server sowohl über den von ihm generierten Zufallsstring, als auch über das Passwort des Benutzers verfügt, kann er den Digest ebenfalls berechnen und so die Authentisierung durchführen. Da bei der Digest-Authentisierung das Passwort nicht über das Netz verschickt wird, eignet sich diese Methode für einen etwas höheren Schutzbedarf.

Ein Problem bei der Verwendung der oben genannten Authentisierungsmethoden ist die Sicherheit der Passwortdaten auf dem Server: Bei Verwendung der Digest-Authentisierung müssen die Authentisierungsdaten der Benutzer auf dem Webserver im Klartext vorhanden sein. Bei Verwendung der Basic-Authentisierung wird meist ein Hash-Wert des Passwortes gespeichert. Eine Sicherung der Passwortdateien auf dem Server vor unbefugtem Zugriff ist daher besonders wichtig.

Formularbasierte Authentisierung

Neben der HTTP-Authentisierung existiert ein weiterer Weg, Zugriffskontrolle über das HTTP-Protokoll zu realisieren: die Authentisierung kann nicht

über den Webserver selbst, sondern über eine serverseitige Anwendung durchgeführt werden. Dabei werden Benutzername und Passwort über normale HTML Formulare eingegeben und von der Anwendung überprüft. Dieses Verfahren ist häufig bei Internet-Angeboten realisiert. Es sollte jedoch stets beachtet werden, dass Passwörter oder PINs, die im Klartext über das Internet übertragen werden, leicht mitgelesen werden können. Zudem werden natürlich auch sämtliche Daten, selbst wenn sie auf authentisierte Anfragen hin ausgeliefert werden, unverschlüsselt übermittelt.

Manche Webangebote identifizieren die Benutzer über spezielle Cookies, die im Browser gespeichert werden. Da Cookies bei der Verwendung von HTTP ebenfalls im Klartext übertragen werden, ist diese Methode für die Authentisierung beim Zugriff auf schutzbedürftige Informationen ebenfalls nicht geeignet. Da im Zusammenhang mit Cookies noch weitere Sicherheitsprobleme existieren, sollte diese Methode generell nicht verwendet werden.

Verwendung von SSL

Wenn im Rahmen von E-Government- oder E-Commerce-Angeboten höhere Anforderungen an die Sicherheit der Authentisierung und die Vertraulichkeit der übertragenen Daten bestehen, dann sollte die Übertragung durch die Verwendung von SSL abgesichert werden (siehe auch M 5.66 *Verwendung von SSL*).

Server-Zertifikate

Bei der Verwendung von SSL gibt es zwei verschiedene Betriebsarten: bei der ersten Variante besitzt nur der Server ein Zertifikat. Dies dient dem Benutzer dazu, zu erkennen, dass er wirklich mit dem "richtigen" Server verbunden ist, und ermöglicht nach dem Aufbau einer verschlüsselten Verbindung die sichere Übertragung von Authentisierungsinformationen und Anwendungsdaten.

Ein Server-Zertifikat enthält neben dem Namen der Zertifizierungsstelle auch den Namen des Servers, für den es gültig ist. Es kann von einer Wurzelzertifizierungsstelle (Root-CA) ausgestellt sein oder auch selbst erzeugt werden, beispielsweise mit den im OpenSSL Paket enthaltenen Tools.

Zertifikate, die nicht von einer Wurzelzertifizierungsstelle ausgestellt wurden, die dem Browser bekannt ist, werden vom Browser meist nicht ohne weiteres akzeptiert, sondern der Benutzer muss explizit bestätigen, dass das betreffende Zertifikat akzeptiert werden soll.

Client-Authentisierung über Zertifikate

Bei der zweiten Variante, verfügt auch der Benutzer über ein Zertifikat, das auf dem Client-Rechner vorhanden sein muss, und das der Browser zur Authentisierung an den Server schickt. Voraussetzung dafür ist jedoch, dass die Zertifizierungsstellen, deren Zertifikate verwendet werden, vertrauenswürdig sind. Dass diese Art der Authentisierung in der Praxis nicht häufiger verwendet wird, liegt an dem Aufwand, der zur Umsetzung einer solchen Lösung erforderlich ist. Die serverseitige Konfiguration ist relativ einfach: Neben der Konfiguration des Webservers für SSL muss ein SSL-Server-Zertifikat beschafft und implementiert werden. Der Aufwand, der für jeden einzelnen Benutzer zu betreiben ist, ist jedoch relativ hoch: Jeder Benutzer muss über ein SSL-Client-Zertifikat verfügen, das jeweils im Browser des Benutzers installiert ist. Dies führt zu einer gewissen Einschränkung der Bequemlichkeit, da einer der großen Vorteile der normalen WWW-Nutzung gerade darin besteht,

dass der Zugriff von praktisch jedem beliebigen Rechner aus erfolgen kann. Werden Client-Zertifikate zur Authentisierung benutzt, so ist diese Flexibilität deutlich eingeschränkt, weil das Client-Zertifikat meist nicht überall vorhanden ist. Andererseits kann in bestimmten Situationen, etwa beim Einsatz eines Intranet-Webservers, genau dies erwünscht sein.

Eine häufig verwendete Methode der Benutzerauthentisierung für Webangebote ist die Kombination von formularbasierter Authentisierung und SSL-verschlüsselter Datenübertragung. Diese Methode bietet, wenn die gewählte SSL-Verschlüsselung ausreichend stark gewählt wird, bei vertretbarem Aufwand (Benutzerverwaltung in der Webanwendung und Implementierung eines SSL-geschützten Zugriffs auf den Webserver) ein Sicherheitsniveau, das auch für höhere Sicherheitsanforderungen angemessen ist.

Die folgende Tabelle fasst die verschiedenen Möglichkeiten der Benutzerauthentisierung bei Webservern zusammen:

Methode	**Sicherheitsniveau**	**Aufwand für Implementierung**	**Serveranforderungen**	**Kommentare**
Standard-Authentisierung	Niedrig	Niedrig	Benutzerverwaltung	Authentisierungsinformationen und Daten werden unverschlüsselt übertragen!
Formularbasierte Authentisierung ohne gesicherte Übertragung	Niedrig	Niedrig bis mittel	Implementierung in der jeweiligen Anwendung	Authentisierungsinformationen und Daten werden unverschlüsselt übertragen!
Digest-Authentisierung	Mittel	Niedrig	Benutzerverwaltung	Daten werden unverschlüsselt übertragen.
Formularbasierte Authentisierung über SSL	Hoch	Mittel bis hoch	SSL-Unterstützung im Server, Implementierung in der jeweiligen Anwendung	Authentisierungsinformationen und Daten werden verschlüsselt übertragen!
Zertifikatbasierte Authentisierung über SSL	Hoch bis sehr hoch	Hoch bis sehr hoch	Installation von Server-Zertifikaten. Zertifikatsverwaltung, Public-Key Infrastruktur.	Wird hauptsächlich für sichere Transaktionen über das Internet verwendet.

Tabelle: Benutzerauthentisierung bei Webservern

Der Microsoft Internet Information Server bietet darüber hinaus noch eine weitere Methode, bei der die Windows-Benutzeranmeldung benutzt wird. Diese Methode funktioniert allerdings nur mit dem Microsoft Internet Explorer als Client.

Null-Encryption Modus und schwache Algorithmen abschalten

Beim Aufbau einer SSL-Verbindung wird der zu verwendende Verschlüsselungsmodus zwischen Client und Server ausgehandelt. Unter den zur Verfügung stehenden Algorithmen befinden sich auch solche, die nicht mehr als sicher angesehen werden können. Insbesondere gibt es auch den so genannten Null-Encryption-Modus, bei dem keine Verschlüsselung stattfindet. Bei der Konfiguration des Webservers für die Verwendung von SSL muss darauf geachtet werden, dass der Server keinen der schwachen Algorithmen und insbesondere nicht den Null-Encryption-Modus akzeptiert. Andernfalls könnte es dazu kommen, dass scheinbar eine sichere Verbindung aufgebaut wird (es wird https verwendet), die jedoch in Wirklichkeit zu schwach oder gar nicht verschlüsselt ist. Eine solche Situation könnte von einem Angreifer bewusst herbeigeführt werden, um Authentisierungsinformationen und andere Daten abzuhören. Daher sollte in der SSL-Konfiguration des Webservers die Verwendung des Null-Encryption-Modus und der schwachen Algorithmen abgeschaltet werden.

Ergänzende Kontrollfragen:

- Ist dokumentiert, wie die Entscheidung für die gewählte Authentisierungsmethode gefällt wurde?
- Wurden der Null-Encryption-Modus und die schwachen Algorithmen in der SSL-Konfiguration abgeschaltet?

M 4.177 Sicherstellung der Integrität und Authentizität von Softwarepaketen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Durch unvorsichtiges Ausführen von Programmen, die aus "unsicheren" Quellen stammen, kann beträchtlicher Schaden entstehen. Bösartige Programme (so genannte *Malware*) können beispielsweise Programme zum Ausspähen von Passwörtern, Trojaner oder Backdoors auf einem Computer installieren, oder ganz einfach Daten beschädigen oder löschen.

Beliebte Quellen für solche Schadsoftware sind beispielsweise Programme, die sich als Windows Bildschirmschoner, Virenscanner oder sonstige Hilfsprogramme ausgeben, und per E-Mail unter gefälschten Absenderadressen an sehr viele Empfänger verschickt werden. Oft laden auch unvorsichtige Anwender die Programme aus dem Internet herunter und installieren sie ohne Überprüfung.

Zwei Beispiele, bei denen durch die Überprüfung vorhandener digitaler Signaturen Schaden hätte vermieden werden können, sind ein Vorfall vom März 2002, bei dem die Distribution des Pakets *OpenSSH* auf dem ftp-Server des OpenSSH-Projekts manipuliert wurde, und ein ähnlicher Vorfall vom September 2002, bei dem dies mit der Distribution des Mailservers *sendmail* geschah. In beiden Fällen wurden in die Distributionen Trojaner eingeschleust, die zu einer Kompromittierung des Rechners führen konnten, auf dem die Pakete kompiliert wurden. In beiden Fällen hätte eine Überprüfung der vorhandenen digitalen Signaturen die Manipulation aufdecken können.

Selbst wenn ansonsten keine Verschlüsselungs- oder Signaturtechniken zum Einsatz kommen, sollte die Nutzung in dem Umfang, wie er in dieser Maßnahme beschrieben wird, in Erwägung gezogen werden.

Prüfsummen checken

Software sollte grundsätzlich nur aus bekannten Quellen installiert werden, besonders dann, wenn sie nicht auf Datenträgern geliefert, sondern beispielsweise aus dem Internet heruntergeladen wurde. Dies gilt besonders für Updates oder Patches, die normalerweise nicht mehr auf Datenträgern ausgeliefert werden. Die meisten Hersteller und Distributoren bieten zu diesem Zweck Prüfsummen an, die zumindest eine Prüfung der Integrität eines Paketes erlauben. Die Prüfsummen werden dabei meist auf den Websites der Hersteller veröffentlicht oder auch per E-Mail verschickt. Um die Integrität eines heruntergeladenen Programms oder einer Archivdatei zu verifizieren wird dann die veröffentlichte Prüfsumme mit einer von einem entsprechenden Programm lokal erzeigten Prüfsumme verglichen.

Falls zu einem Softwarepaket Prüfsummen angeboten werden, so sollten diese vor der Installation des Paketes überprüft werden.

Eine Überprüfung der Authentizität kann mit Prüfsummen jedoch nicht erfolgen. Daher werden in vielen Fällen für Programme oder Pakete digitale Signaturen angeboten, die meist mit einem der Programme PGP oder GnuPG erzeugt wurden. Die zur Überprüfung der Signatur benötigten öffentlichen Schlüssel sind wiederum meist auf den Webseiten des Herstellers oder von

Public-Key-Servern verfügbar, und mit den Programmen PGP oder GnuPG können die Signaturen überprüft werden. Ergibt die Prüfung, dass es sich um eine gültige Signatur handelt, die mit einem bekannten Schlüssel erzeugt wurde, so ergibt dies einen deutlich höheren Grad an Vertrauenswürdigkeit für das Paket, als lediglich das Vorhandensein einer Prüfsumme.

Das bei Linux-Distributionen verbreitete Paketverwaltungssystem RPM (Redhat Package Manager) hat ebenso wie das Paketverwaltungssystem der Debian-Distribution bereits eine integrierte Überprüfungsfunktionalität.

Falls zu einem Softwarepaket digitale Signaturen verfügbar sind, sollten diese auf jeden Fall vor der Installation des Pakets überprüft werden.

Ein prinzipielles Problem bei der Verwendung digitaler Signaturen stellt die Verifikation der Authentizität des verwendeten Schlüssels selbst dar. Trägt der Schlüssel keine Signatur einer bekannten vertrauenswürdigen Person oder Organisation (etwa eines Trustcenters), so bieten die mit diesem Schlüssel erzeugten Signaturen keine wirkliche Sicherheit, dass das Softwarepaket tatsächlich vom Entwickler, Hersteller oder Distributor stammt. Daher sollten die öffentlichen Schlüssel, sofern sie nicht zertifiziert sind, möglichst aus einer anderen Quelle als das Softwarepaket selbst bezogen werden, beispielsweise von einer CD-ROM des Herstellers, von einem anderen Spiegelserver, auf dem das Paket ebenfalls heruntergeladen werden kann, oder von einem Public Key Server.

Zur Überprüfung von Prüfsummen und digitalen Signaturen müssen die entsprechenden Programme lokal vorhanden sein. Die Administratoren sollten über die Bedeutung und Aussagekraft von Prüfsummen und digitalen Signaturen informiert sein und die entsprechenden Programme einsetzen können.

Ergänzende Kontrollfragen:

- Ist bekannt, ob für die eingesetzten Softwarepakete Prüfsummen oder digitale Signaturen verfügbar sind?
- Sind die notwendigen Programme zur Überprüfung von Prüfsummen oder digitalen Signaturen verfügbar?
- Werden digitale Signaturen, sofern verfügbar, überprüft?

M 4.178 Absicherung der Administrator- und Benutzerkonten beim IIS-Einsatz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Beim Einsatz eines Internet Information Servers (IIS) sollten die Administrator- und Benutzerkonten durch folgende Konfigurationsänderungen abgesichert werden.

Verschlüsseln der SAM-Datei mit dem SYSKEY-Verfahren

Windows NT/2000 schützt seine Passwortdateien, indem es sie dauernd als vom Betriebssystem geöffnet erklärt. Programme, die auf die SAM-Informationen zugreifen, nutzen die dafür vorgesehenen Windows API Funktionen. Allerdings existieren unter Windows an bestimmten Stellen Kopien der SAM-Datei unter anderen Namen, z. B. *Winnt/repair/-SAM*. Diese Datei ist standardmäßig für jeden angemeldeten Benutzer zugänglich. Zwar kann man Windows dazu auffordern, keine Sicherungskopien der SAM-Datei zu erstellen, allerdings kann ein Systemabsturz dazu führen, dass die SAM-Datenbank beschädigt wird. Es wird daher empfohlen, eine Sicherungskopie der SAM-Datei auf einem externen Speichermedium anzulegen. Dieses Medium sollte so aufbewahrt werden, dass nur der Administrator darauf zugreifen kann.

Sollte ein potentieller Angreifer trotzdem Zugriff auf die Daten der SAM-Datenbank erhalten, könnte er zwar nicht direkt die Passwörter ermitteln, hätte aber die Möglichkeit, mit entsprechenden Kenntnissen eine Brute-Force Attacke gegen diese Datei auszuführen. Um auch dies zu verhindern, verwendet Windows 2000 (und Windows NT 4 ab Service Pack 3) das zusätzliche Sicherheitssystem SYSKEY.

SYSKEY ist ein Verschlüsselungsverfahren für die SAM-Datei. Unabhängig von der Verschlüsselung der Benutzerkennwörter wird die SAM-Datei durch SYSKEY als gesamtes durch einen nicht veröffentlichten Algorithmus verschlüsselt. Brute-Force- oder ähnliche Angriffe werden dadurch erschwert. SYSKEY sollte auf jeden Fall verwendet werden, da der zusätzliche Rechenaufwand nur unwesentlich ist. In der Regel sind praktisch keine Leistungseinbußen am Server festzustellen.

Sichern des Administratorkontos mit *passprop.exe*

Bei wiederholter Eingabe des falschen Namens und des falschen Kennworts, wenn z. B. ein Angreifer versucht, das Kennwort zu erraten, wird das Administratorkonto normalerweise nicht gesperrt. Eine Sperrung des Administratorkontos wird durch den Einsatz des Tools *passprop* aus dem Windows NT-Resource-Kit (NTRK) ermöglicht. Nach Sperren des Administratorkontos kann sich der Administrator ausschließlich lokal am Server anmelden.

Das Programm *passprop* ist mit folgender Option auf dem IIS Server auszuführen: *passprop /adminlockout*

Verwendung von sicheren Passwörtern mittels *passfilt.dll* erzwingen

Um die Verwendung von sicheren Passwörtern zu erzwingen, ist die Datei *passfilt.dll* aus dem NTRK in das Verzeichnis *%SYSTEMROOT%\ SYSTEM32*

zu kopieren. Zum Aktivieren der Filterfunktion für Passwörter ist die Registrierung wie folgt zu ändern:

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	CurrentControlSet\Control\LSA
Name	Notification Packages
Type	REG-MULTI-SZ
Wert	PASSFILT

Tabelle: Aktivieren der Filterfunktion für Passwörter

Dies bedeutet, dass die Zeichenfolge *PASSFILT* an die vorhandenen Daten für den *REG-MULTI-SZ*-Wert angehängt wird. Die vorhandenen Zeichen sind dabei nicht zu ersetzen, sondern nur zu ergänzen. Die Änderungen werden erst nach einem Systemstart wirksam.

Ergänzende Kontrollfragen:

- Wird die SAM-Datei mit dem SYSKEY-Verfahren verschlüsselt?
- Wird das Administratorkonto mit *passprop.exe* gesichert?
- Wird die Verwendung von sicheren Passwörtern erzwungen?

M 4.179 Schutz von sicherheitskritischen Dateien beim IIS-Einsatz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um einen unbefugten Zugriff auf die allgemeinen administrativen Tools zu erschweren, sollten diese in einem Verzeichnis außerhalb des *%systemroot%*-Verzeichnisses gespeichert werden. Anschließend ist die Access Control List (ACL) so anzupassen, dass nur Administratoren uneingeschränkten Zugriff erhalten. Beispielsweise kann ein Verzeichnis *\CommonTools* angelegt werden, in das die folgenden Dateien aus dem *%systemroot%*-Verzeichnis verschoben werden.

arp.exe	at.exe	atsvc.exe	cacls.exe
cmd.exe	cscript.exe	debug.exe	edit.com
edlin.exe	ftp.exe	finger.exe	ipconfig.exe
net.exe	netsh.exe	netstat.exe	nslookup.exe
ping.exe	poledit.exe	posix.exe	qbasic.exe
rcp.exe	rdisk.exe	regedit.exe	regedt32.exe
regini.exe	regsrv3.exe	rexec.exe	route.exe
rsh.exe	runonce.exe	secfixup.exe	syskey.exe
telnet.exe	tftp.exe	tracert.exe	tskill.exe
wscript.exe	xcopy.exe		

Tabelle: Administrative Tools

Die Systemüberwachungsfunktion von Windows ME und 2000 sorgt durch die konsequente Wiederherstellung gelöschter oder geänderter Systemdateien im Allgemeinen für ein stabiler laufendes System. Sie unterbindet damit jedoch alle ändernden Zugriffe auf die Systemdateien. So verhindert sie zum Beispiel auch vom Benutzer gewünschte Eingriffe oder die Installation von Software, die Systemdateien ersetzen muss. Damit die Dateien in Windows 2000 entfernt werden können, muss die kontinuierliche Systemwiederherstellung für die Zeit der Verschiebung deaktiviert werden.

Um die Systemwiederherstellung zu umgehen, ist diese in der Registrierung wie folgt zu deaktivieren:

Um die Systemwiederherstellung zu umgehen, ist diese in der Registrierung wie folgt zu deaktivieren:

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SOFTWARE
Schlüssel	Microsoft \Windows NT\CurrentVersion\WinLogon
Name	SFCDisable
Type	REG_DWORD
Wert	0 (Systemwiederherstellung aktiv) ffffff9d (Systemwiederherstellung inaktiv)

Tabelle: Änderung der Registrierung

Die Änderungen greifen erst nach einem Neustart. Nach Auslagern der administrativen Tools kann die Systemwiederherstellung wieder aktiviert werden.

Da der Web-Server normalerweise keinerlei Programme unter *%windir%* und *%windir%\system32* ausführt, kann die Zugriffsbeschränkung auf alle*.exe*-Dateien in den genannten Verzeichnissen erweitert werden.

Sind auf dem Web-Server das Resource Kit oder andere administrative Programme installiert, so sollten die entsprechenden Bereiche mit folgenden Zugriffsrechten versehen werden: *Administrator Vollzugriff, System Vollzugriff*

Ein weiterer Schwachpunkt bei den Zugriffsrechten von Windows stellt das *%systemdrive%* (C:\) dar. Nach einer Standardinstallation hat dort der Benutzer *Everyone* Vollzugriff. Die Zugriffsrechte auf *%systemdrive%* sollten ebenfalls eingeschränkt werden.

Ergänzende Kontrollfragen:

- Wurden die administrativen Tools in ein eigenes Verzeichnis verschoben?
- Wurde dieses Verzeichnis durch eine geeignete ACL geschützt?

M 4.180 Konfiguration der Authentisierungsmechanismen für den Zugriff auf den IIS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Jede HTTP-Anforderung eines Browsers wird unter dem IIS im Sicherheitskontext eines Benutzerkontos in Windows NT bzw. Windows 2000 ausgeführt. Das Benutzerkonto muss entweder auf dem IIS oder in der Domäne (oftmals bei Intranet-Servern) definiert werden.

Beim Zugriff auf den IIS wird zunächst anhand der IP-Adresse bzw. des Domänennamens geprüft, ob der Client berechtigt ist, auf den IIS zuzugreifen. Anschließend erfolgt die Authentisierung, aus der die Zuordnung des Benutzerkontos mit den entsprechenden Rechten resultiert. Die zugelassenen IP-Adressen bzw. Domänennamen und die Authentisierungsmethode wird in der Microsoft Management Console (MMC) unter der Option *Eigenschaften* des entsprechenden Web-Verzeichnisses definiert.

Der IIS 4.0 unterstützt vier Authentisierungsmethoden für den WWW-Server:

- Anonymer Zugriff
- Standard-Authentisierung
- Windows-Authentisierung
- Authentisierung über Client-Zertifikate

Im IIS 5.0 wurden die Authentisierungsmethoden erweitert. Zusätzlich zu den oben genannten Methoden wurde Kerberos V5 in die Windows-Authentisierung integriert und die Digest-Authentisierung zur Verfügung gestellt.

Für den Zugriff auf den FTP-Server kann zwischen *Anonymer Zugriff* und *Standard-Authentisierung* gewählt werden.

Anonymer Zugriff

Anonyme Authentisierung

Für den anonymen Zugriff auf den Web-Server wird das Benutzerkonto *IUSR_Computername* verwendet. Dieses wird automatisch bei der Installation des IIS erstellt und mit einem zufälligen Passwort versehen. Das Benutzerkonto *IUSR_Computername* gehört der Gruppe *Gast* an und besitzt das Recht, sich lokal am System anzumelden.

Bei einem anonymen Zugriff auf den FTP-Server meldet sich der Nutzer mit dem Benutzernamen *anonymous* an. Als Passwort wird in der Regel die E-Mail-Adresse des Benutzers verwendet. Für den Dateizugriff werden die Berechtigungen des Kontos *IUSR_Computername* herangezogen.

Standard-Authentisierung

Standard-Authentisierung

Die Standard-Authentisierung basiert auf der Verwendung von Benutzernamen und Passwort, wobei der Benutzer über lokale Anmelderechte verfügen muss. Durch Festlegen geeigneter Benutzergruppen kann der Zugriff auf ausgewählte Ressourcen beschränkt werden. Die übertragenen Anmeldeinformationen zum Zugriff auf den WWW-Server werden nicht sicher verschlüsselt

(UUEncoding oder Base64-Kodierung) und können abgefangen und leicht decodiert werden.

Bei der Verwendung der Standard-Authentisierung auf einem FTP-Server werden wie bei der anonymen Anmeldung der Benutzername und das Passwort unverschlüsselt im Klartext übertragen. Aus diesem Grund sollte diese Authentisierungsmethode nicht in unsicheren Netzen verwendet werden.

Windows-Authentisierung

Windows-Authentisierung

Die Authentisierung mittels Windows Challenge/Response eignet sich insbesondere für ein Intranet mit einer Windows-basierten Client-Server-Umgebung. Wenn ein Benutzer sich lokal als Domänenbenutzer angemeldet hat, kann er ohne zusätzliche Authentisierung auf weitere Server dieser Domäne zugreifen.

Windows 2000 verwendet bei der Windows-Authentisierung die Protokolle NTLM und Kerberos V5, die auch zur Authentisierung am Web-Server eingesetzt werden können. Welches Protokoll zum Einsatz kommt, ist abhängig von den Fähigkeiten des beteiligten Clients bzw. Servers. Standardmäßig wird Kerberos V5 verwendet. Unterstützt einer der Kommunikationspartner dieses Protokoll nicht, wird NTLM für die Authentisierung genutzt.

Authentisierung über Client-Zertifikate

Authentisierung über Client-Zertifikate

Eine weitere Option im Bereich *Verzeichnissicherheit* ist die Anwendung der SSL-Sicherheitsfunktionen (Secure Socket Layer) zur Authentisierung eines Benutzers (Server- und Client-Authentisierung) und zur Verschlüsselung der zu übertragenen Daten. Der IIS unterstützt die SSL Version 3.0. Beim Anmeldevorgang wird vom Browser des Benutzers das Client-Zertifikat an den Web-Server übertragen und dort verifiziert. Der IIS ordnet das Zertifikat einem entsprechenden Windows-Benutzerkonto zu, über das die Rechte und Zugriffsrichtlinien des Benutzers definiert werden.

Für die Server-Authentisierung muss dem Client-Browser das Server-Zertifikat bekannt sein. Wird eine Verbindung zum ersten mal zu einem Server aufgebaut, dessen Zertifikat noch nicht bekannt ist und nicht von einer Zertifizierungsinstanz signiert wurde, der der Browser vertraut, kann es unter den Sicherheitseinstellungen des Browsers hinzugefügt werden.

Zur Verwendung von SSL muss zunächst ein Schlüsselpaar erzeugt und ein gültiges Server-Zertifikat von einer vertrauenswürdigen Drittorganisation, einer so genannten Zertifizierungsinstanz, angefordert und installiert werden. Die Verwaltung der Schlüssel auf dem IIS erfolgt mit Hilfe des Schlüsselmanagers, der über die Schaltfläche *Bearbeiten* im Feld *Sichere Kommunikation* auf der Registerkarte *Verzeichnissicherheit* aufgerufen werden kann.

Voraussetzung für die Client-Authentisierung ist, dass der Server über ein gültiges Server-Zertifikat verfügt. Außerdem müssen dem Server die Zertifikate der zugriffsberechtigten Clients bekannt sein. Die Client-Zertifikate werden ebenfalls über die Registerkarte *Verzeichnissicherheit* im Feld *Sichere Kommunikation* konfiguriert. Nachdem ein Server-Zertifikat installiert ist, kann über die Schaltfläche *Bearbeiten* das Dialogfeld *Sichere Kommunikation* geöffnet werden.

Im IIS 5.0 wird die Verwaltung der Zertifikate durch den IIS-Zertifikats-Assistenten und den Assistenten für Zertifikatsvertrauenslisten vereinfacht.

Digest-Authentisierung

Digest-Authentisierung

Die Digest-Authentisierung weist grundsätzlich die selben Merkmale wie die Standard-Authentisierung auf. Allerdings werden die Anmeldeinformationen durch eine stärkere Verschlüsselung geschützt. Vor der Übertragung durchlaufen die Anmeldeinformationen einen nicht umkehrbaren Prozess (Hashing), aus dem ein Hashwert oder Nachrichtendigest resultiert. Der ursprüngliche Inhalt kann nicht aus dem Hashwert ermittelt werden.

Die Digest-Authentisierung ist ein Funktionalität von HTTP 1.1 und ist so strukturiert, dass sie bei Proxy-Servern und anderen Firewall-Anwendungen verwendet werden kann. Die Digest-Authentisierung kann nur bei Domänen-Controllern in einer Windows 2000-Domäne eingesetzt werden. Da der Domänen-Controller über Textkopien von Kennwörtern im Klartext verfügt, muss er unbedingt vor Zugriffen Unbefugter geschützt werden.

Bei Auswahl der Authentisierungsmethode ist sicherzustellen, dass sie den Anforderungen an die Benutzerauthentisierung auf dem IIS entspricht. Die folgende Tabelle zeigt eine Zusammenfassung der möglichen Authentisierungsmethoden:

Methode	**Sicherheitsebene**	**Serveranforderungen**	**Clientanforderungen**	**Kommentare**
Anonyme Authentisierung	Keine	Konto IUSR_Computername	Beliebiger Browser	Wird für öffentliche Bereiche von Internet-Sites verwendet.
Standard-Authentisierung	Niedrig	Gültige Konten	Eingeben von Benutzername und Kennwort	Kennwörter werden unverschlüsselt übertragen.
Digest-Authentisierung	Mittel	Kopie aller Kennwörter als unformatierter Text, gültige Konten	Kompatibilität	Kann bei Proxy-Servern und anderen Firewalls verwendet werden.
Integrierte Windows-Authentisierung	Hoch	Gültige Konten	Browser-Unterstützung	Wird für private Bereiche von Intranets verwendet.

Tabelle: Authentisierungsmethoden

Methode	Sicherheitsebene	Serveranforderungen	Clientanforderungen	Kommentare
Zertifikat-Authentisierung	Hoch	Installation von Server-Zertifikaten. Konfigurieren von Zertifikatsvertrauenslisten (nur für die erste Verwendung).	Browser-Unterstützung	Wird hauptsächlich für sichere Transaktionen über das Internet verwendet.
Anonyme FTP-Authentisierung	Keine	Konto IUSR_Computer-name	Keine	Wird für öffentliche Bereiche von FTP-Sites verwendet.
FTP-Standard-Authentisierung	Niedrig	Gültige Konten	Eingeben von Benutzername und Kennwort	Kennwörter werden unverschlüsselt übertragen.

Tabelle: Zusammenfassung der Authentisierungsmethoden

Ergänzende Kontrollfragen:

- Wird der Zugriff auf den IIS entsprechend den Anforderungen an die Benutzerauthentisierung durch eine geeignete Authentisierungsmethode geschützt?

M 4.181 Ausführen des IIS in einem separaten Prozess

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der IIS 4.0 bietet die Möglichkeit, Server-seitige Anwendungen, z. B. ASP, CGI, ISAPI, IDC, SSI, im gleichen Prozess (*Inetinfo.exe*) wie der IIS auszuführen. Alternativ können die Anwendungen in einem separaten Prozess (*DLLhost.exe*) ausgeführt werden.

Der IIS 5.0 ergänzt beide oben genannten Methoden durch eine weitere Möglichkeit, die zusammengefasste Methode. Bei dieser Methode können zwei oder mehrere Anwendungen in einem Prozess (*DLLhost.exe*) zusammengefasst und unabhängig vom Hauptprozess (*Inetinfo.exe*) ausgeführt werden.

Durch die Trennung von Prozessen kann die Sicherheit und Verfügbarkeit des IIS erhöht werden, da ein Anwendungsfehler nicht zum Absturz der gesamten Site führt. Allerdings ist hiermit meist eine Verminderung der Performance verbunden.

Die Einstellungen zur Prozessisolierung werden im Fenster *Eigenschaften* des virtuellen Verzeichnisses definiert. Beim IIS 4.0 erfolgt eine Prozessisolation durch Auswahl des Kästchens *Getrennter Speicherbereich (isolierter Prozess)*. Im IIS 5.0 können die Methoden im Feld *Anwendungsschutz* eingestellt werden. Dieser umfasst drei Ebenen:

- **Niedrig (IIS-Prozess)** - Die Anwendung wird (unter Verwendung der Datei *Inetinfo.exe*) im selben Prozess ausgeführt wie die Web-Dienste.
- **Mittel (zusammengefasst)** - Die Anwendung wird in einem zusammengefassten Prozess ausgeführt. Das bedeutet, dass üblicherweise alle Anwendungen zusammen außerhalb jedes Web-Dienstes (unter Verwendung der Datei *DLLhost.exe*) ausgeführt werden.
- **Hoch (isoliert)** - Die Anwendung wird in ihrem eigenen, isolierten Kontext abseits der Web-Dienste und anderer Anwendungen ausgeführt (unter Verwendung einer anderen Instanz der Datei *DLLhost.exe*).

Entsteht ein Fehler bei einer Anwendung, die im *niedrigen Modus* ausgeführt wird, können die Dienste des Web-Servers ebenfalls teilweise oder ganz mit abstürzen. Dieser Modus sollte daher nicht verwendet werden. Wenn alle Anwendungen im *zusammengefassten Modus* ausgeführt werden, so sind bei einem Programmabsturz nur diese betroffen. Werden alle Anwendungen im *isolierten Modus* ausgeführt, ist unter Umständen mit deutlichen Leistungseinbrüchen des IIS zu rechnen. Aus diesem Grund wird empfohlen, dass nicht mehr als zehn Anwendungen im *isolierten Modus* ausgeführt werden.

Ergänzende Kontrollfragen:

- Wird der IIS in einem separaten Prozess ausgeführt?

M 4.182 Überwachen des IIS-Systems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Überwachung aller IIS-Systeme ist wichtig, um Zugriffe auf den Server zu dokumentieren und Angriffe erkennen zu können. Hierzu stellt der IIS mehrere Protokollformate und eine Vielzahl von Protokollierungsoptionen zur Verfügung. Diese Optionen sind im Eigenschaftsfenster einer Web-Seite zu konfigurieren.

Für die Protokollierung stehen vier Protokollformate zur Verfügung:

- **Microsoft IIS** ist ein festes ASCII-Format, dass das Standardformat für den IIS ist. Es steht seit der ersten Version des IIS zur Verfügung. In diesem Format werden mehr Informationen aufgezeichnet als im NCSA-Format (National Center for Supercomputing Applications), es kann jedoch bezüglich des Layouts nicht angepasst werden.
- **NCSA allgemein** ist ebenfalls, wie das Protokollformat Microsoft IIS, ein festes ASCII-Format, welches nicht angepasst werden kann. Es werden nur die elementaren Informationen in Bezug auf die Aktivitäten um den IIS-Dienst gespeichert. Dieses Dateiformat kann nicht für FTP-Sites verwendet werden.
- **ODBC** ist eine Option, mit der die Protokolle direkt über eine ODBC-Datenquelle in einer Datenbank gespeichert werden können.
- **W3C-erweitert** ist ein Protokollformat, das dem Standard des W3C (World Wide Web Consortium) entspricht. Die Protokolldateien werden im ASCII-Format gespeichert und der Inhalt kann angepasst werden. Alle Zeiteinträge werden in UTC-Zeit aufgezeichnet.

W3C-erweitertes Protokollformat

Für die Protokollierung des IIS sollte das *W3C-erweiterte* Format gewählt werden, da es die umfangreichsten Konfigurationsmöglichkeiten aufweist. Die folgende Tabelle zeigt einen Überblick über mögliche Protokolloptionen (Feld) und deren Kennzeichnung in der Protokolldatei.

Das W3C-erweiterte Protokollformat:

Feld	Kennzeichnung	Beschreibung
Datum	date	Das Datum, an dem die Aktivität aufgetreten ist.
Zeit	time	Die Zeit, zu der die Aktivität aufgetreten ist.
Client-IP-Adresse	c-ip	Die IP-Adresse des Clients, der auf den Server zugegriffen hat.
Benutzername	c-username	Der Name des Benutzers, der auf den Server zugegriffen hat.
Dienstname	s-sitename	Der Name des Internet-Dienstes, der vom Client-Computer angesprochen wurde.

Tabelle: Das W3C-erweiterte Protokollformat

Feld	Kennzeichnung	Beschreibung
Server-Name	s-computername	Der Name des Servers, auf dem der Protokolleintrag generiert wurde.
Server-IP	s-ip	Die IP-Adresse des Servers, auf dem der Protokolleintrag generiert wurde.
Server-Anschluss	s-port	Die Anschlussnummer, mit der der Client verbunden ist.
Methode	cs-method	Die Aktion, die der Client auszuführen versucht hat (zum Beispiel ein *GET*-Befehl).
Stamm-URI	cs-uri-stem	Die Ressource, auf die zugegriffen wurde, zum Beispiel eine HTML-Seite, ein CGI-Programm oder ein Script.
URI-Abfrage	cs-uri-query	Die Abfrage, die der Client gegebenenfalls auszuführen versuchte, d. h. eine oder mehrere Suchzeichenfolgen, für die der Client nach einer Übereinstimmung gesucht hat.
HTTP-Status	sc-status	Der Status der Aktion in HTTP-Terminologie.
Win32-Status	sc-win32-status	Der Status der Aktion in der von Windows NT/2000 verwendeten Terminologie
Bytes gesendet	cs-bytes	Die Anzahl der vom Server gesendeten Bytes.
Bytes empfangen	sc-bytes	Die Anzahl der vom Server empfangenen Bytes.
Zeitdauer	time-taken	Die Zeitspanne, die für die Aktion benötigt wurde.
Protokollversion	cs-protocol	Die Protokollversion (HTTP, FTP), die vom Client verwendet wird. Für HTTP ist dies entweder HTTP 1.0 oder HTTP 1.1.
Benutzeragent	cs(User-Agent)	Der auf dem Client verwendete Browser.
Cookie	cs(Cookie)	Der Inhalt des gesendeten oder empfangenen Cookie, falls vorhanden.
Referenz-URI	cs(Referer)	Die Site, in der ein Benutzer auf einen Hyperlink geklickt hat, der ihn zu dieser Site geführt hat.

Tabelle: Das W3C-erweiterte Protokollformat (Fortsetzung)

Minimale Protokollierung

Eine minimale Protokollierung sollte folgende Informationen beinhalten:

- Datum,
- Zeit,
- Client IP-Addresse,
- Benutzername,
- Methode,
- Stamm-URI,
- WIN32-Status,
- HTTP-Status,
- Benutzeragent,
- Server IP-Adresse und
- Server-Anschluss.

Dienstspezifische Protokollierung

Zu beachten ist, dass der IIS in der Standardkonfiguration auch Standardnamen für die Protokolldateien in Abhängigkeit vom gewählten Format (z. B. *W3C-erweitert*) verwendet. Das bedeutet, dass die Protokolldaten für alle Dienste in einer einzigen Protokolldatei abgelegt werden. Es besteht jedoch die Möglichkeit, für jede Web-Seite und FTP-Site ein eigenes Verzeichnis für die Protokollierung auszuwählen, um die Protokolle besser auswerten zu können und von einander zu trennen. Diese Vorgehensweise wird empfohlen. Außerdem können die Protokolldateien so auf ein gesondertes Laufwerk ausgelagert und zentral verwaltet werden.

Im IIS 5.0 wurden die Protokollierungsmöglichkeiten erweitert. Er enthält eine Funktion, mit der die CPU-Auslastung des Servers in Zusammenhang mit der Web-Seite überwacht werden kann. Diese Funktion ist nur bei Verwendung des Protokollformats *W3C-erweitert* verfügbar. Dabei wird die Prozessorauslastung pro Web-Seite protokolliert, Daten auf Script- und Anwendungsebene werden nicht dokumentiert.

Schützen der Protokolldaten

Die Protokolldateien sind durch geeignete ACLs (Access Control Lists) vor unberechtigten Zugriffen zu schützen. Dadurch wird böswilligen Benutzern die Möglichkeit genommen, durch Löschen von Protokolldateien Spuren zu beseitigen. Die Zugriffsrechte auf die vom IIS erzeugten Protokolldateien sollten höchstens wie folgt eingestellt werden:

- Administrator (Vollzugriff) und
- System (Vollzugriff).

Die Sicherung und Auswertung der Protokolldateien sollte regelmäßig erfolgen. Für die Sicherung der Dateien bietet Microsoft verschiedene Speicheroptionen an. Beispielsweise können Dateien stündlich, täglich, wöchentlich, monatlich oder in Abhängigkeit von ihrer Dateigröße gesichert werden. Die Auswahl dieser Optionen sollte unter Berücksichtigung des zu erwartenden Verkehrs und somit der zu erwartenden Protokolldaten erfolgen.

Regelungen zur Auswertung der Dateien sind in einer geeigneten, allgemein verbindlichen Vorgabe zu dokumentieren (siehe M 2.64 *Kontrolle der Protokolldateien.*

M 4.183 Sicherstellen der Verfügbarkeit und Performance des IIS

Verantwortlich für Initiierung: Leiter IT IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Verfügbarkeit und Performance sind für den Erfolg eines Internet-Angebots von entscheidender Bedeutung. Lange Wartezeiten werden von keinem Anwender auf Dauer akzeptiert, deshalb muss ein Internet-Server ständig verfügbar und seine Reaktionszeit möglichst kurz sein. Insbesondere durch den Einsatz von SSL zur Verschlüsselung einer Kommunikationsverbindung wird die Performance eines Web-Servers stark beeinflusst.

In dieser Maßnahme werden Möglichkeiten vorgestellt, die Verfügbarkeit und die Performance von Server-Diensten zu erhöhen. Dabei werden sowohl einfache Standby-Lösungen für den Ausfall eines Systems als auch komplexe Verfahren für eine optimale Lastverteilung auf mehrere Server beschrieben.

Zu Beginn sind die bestehenden Server-Systeme und deren Netzanbindung zu betrachten. In der Regel befindet sich ein Web-Server hinter einer Firewall in einer so genannten demilitarisierten Zone (DMZ). Das bedeutet für die Firewall, dass sie ebenfalls hochverfügbar und performant auszulegen ist, wenn entsprechende Anforderungen an den Web-Server bestehen. Die beste Performance eines Web-Servers nützt nichts, wenn die Zugriffe durch mangelhafte Performance oder Ausfälle der Firewall beschränkt oder verhindert werden.

Cold-Standby-Lösung

Cold-Standby

Um die Verfügbarkeit eines Systems zu gewährleisten, wurden in der Vergangenheit so genannte Cold-Standby-Lösung eingesetzt. Ein zweiter, vorkonfigurierter Server wurde bereitgestellt, der nur beim Ausfall des laufenden Systems zum Einsatz kam. Eine solche Lösung trägt in der Regel nur wenig zum unterbrechungsfreien Betrieb und zur Skalierbarkeit des Gesamtsystems bei, da der zweite Server nicht im Regelbetrieb genutzt wird und die Umschaltung im Fehlerfall eine gewisse Zeit in Anspruch nimmt.

In modernen Systemen werden für diese Zwecke Server-Farmen, lastverteilende Systeme und Cluster eingesetzt.

Server-Farm

Server-Farm

Eine Server-Farm besteht aus zwei oder mehreren Servern. Diese Server stellen die gleichen Dienste zur Verfügung und arbeiten mit gespiegelten Datenbeständen. Hierdurch wird die Verfügbarkeit und Performance skalierbar erweitert. Beim Ausfall eines Servers werden die Aufgaben von einem oder mehreren Servern der Farm übernommen. Werden die Server einer Farm an unterschiedlichen Orten (Räumen/Gebäuden) aufgestellt, kann der Betrieb sogar bei Brand, Wassereinbruch und Leitungsausfall der Netzanbindung usw. aufrecht erhalten werden.

Wie die einzelnen Anfragen an die Server einer Server-Farm verteilt werden, ist in den folgenden Abschnitten erörtert.

Round Robin

Round Robin

Zur Verteilung der Benutzeranfragen auf die einzelnen Server, z. B. in einer Server-Farm, bietet das Round-Robin-DNS-Verfahren eine einfache Möglichkeit. Beim Round-Robin-DNS werden im Domain Name Service (DNS) einem Hostnamen die IP-Adressen aller Server der Server-Farm zugeordnet. Anschließend meldet der DNS der Reihe nach diese IP-Adressen zurück, wenn Clients die IP-Adresse dieses Hostnamens dort erfragen. Auf diese Weise wird eine Aufteilung der Client-Anfragen auf die jeweiligen Server erreicht.

Ein Nachteil des Round-Robin-Verfahrens ist, dass weder der Ausfall noch die Auslastung der einzelnen Server berücksichtigt wird. Es ist also nicht ausgeschlossen, dass ein Benutzer auf einen Server gelenkt wird, der nicht mehr verfügbar oder stark ausgelastet ist.

Lastverteilung durch Load-Balancer

Load Balancing

Besser als der Einsatz von Systemen mit einer statischen Lastverteilung ist der Einsatz eines Load-Balancer, der sowohl die Verfügbarkeit als auch die Auslastung eines Servers oder Dienstes berücksichtigt. Ist ein Server nicht verfügbar, so werden die Anfragen eines Benutzers auf einen anderen Server der Farm weitergeleitet. Idealerweise wird für jede Anfrage der Server mit der geringsten Auslastung gewählt.

Technisch ist für die gesamte Server-Farm nur eine Adresse für den Benutzer sichtbar. Diese ist auf dem Load-Balancer als virtuelle Adresse eingerichtet. Eine Anfrage auf diese Adresse leitet der Load-Balancer an einen realen Server der Farm weiter, wobei der Zugriff für den Benutzer völlig transparent erfolgt. Voraussetzung für eine solche Lösung sind identische, gespiegelte Inhalte auf allen beteiligten Web-Servern.

Lastverteiler stehen als Hard- und Software-Lösungen zur Verfügung. Hardware-Lösungen können aus dedizierten Geräten (Router, Bridges) bestehen, aber auch in bestehende Netzkomponenten, wie Switches, integriert sein. Mit Hilfe von Software-Lösungen können herkömmliche Unix/Linux-Rechner zum Load-Balancer aufgerüstet werde, andere Sofware-Lösungen werden direkt auf den betroffenen Servern installiert. Microsoft hat mit *Windows Load Balancing Service* (WLBS) für Windows NT Server diesen Weg gewählt. Bei Windows 2000 Advanced Server heißt der Load-Balancer *Network Load Balancing* (NLB). Bei WLBS/NLB kommen alle Client-Anfragen bei allen Servern der Farm an. Der für die Bearbeitung der Anfrage gewählte Server wird dann nach einem festen Schema bestimmt. Fällt einer der Server aus, werden die verbleibenden Server automatisch neu konfiguriert.

Wie die Anfragen an die einzelnen Server einer Farm verteilt werden, kann durch unterschiedliche Kriterien festgelegt werden. In der Regel wird nach der geringsten Anzahl bestehender Verbindungen (*Least Connections*), einer frei definierbaren Gewichtung (*Weighting*), der Systemauslastung (*System Load*) und der Antwortzeit (*Round Trip Time*) entschieden. Auch die bereits erörterte Methode *Round Robin* kann hier zum Einsatz kommen.

Um die Verfügbarkeit weiter zu erhöhen, sind Load-Balancer redundant auszulegen. In einer solchen Konstellation sollten die Load-Balancer mittels

Failover verbunden sein. Über dieses Failover wird ständig der Status und die Konfiguration des Partners ermittelt. Fällt ein Load-Balancer aus, so übernimmt der Failover-Partner die bestehenden Verbindungen. Ausgenommen sind verbindungsorientierte, statusgebundene Verbindungen, wie z. B. *telnet*.

Durch Server-Farmen und Load-Balancer kann die Ausfallsicherheit und Lastverteilung von einfachen Server-Diensten erheblich erhöht werden. Für ein Web-Angebot mit einem ständig wechselnden größeren Datenbestand eignen sich diese Verfahren allerdings weniger, da die Replizierung oder Spiegelung der Daten sehr aufwendig sein kann. Sind komplexe Anwendungen abzusichern, so ist ein mehrstufiges System zu wählen, bei dem der Web-Server beispielsweise Transaktionen an separate Applikations- und Datenbank-Server weiterleitet.

Cluster

Cluster

Clustering wird bei Servern eingesetzt, bei denen sich der Datenbestand häufig ändert und somit die Installation einer Server-Farm nicht geeignet ist. Beim Clustering arbeiten alle Systeme mit einem gemeinsamen, externen Datenbestand. Dieser gemeinsame Datenbestand befindet sich in der Regel auf einem externen RAID-Plattensystem. Der Systemstatus der beteiligten Rechner wird regelmäßig gesichert, so dass bei Ausfall eines Servers ein anderer die Funktion des ausgefallenen Servers übernehmen kann.

Auch bei den Cluster-Lösungen werden sowohl Cold-Standby- als auch Hot-Standby-Lösungen angeboten. Die Hot-Standby-Lösungen stellen den angebotenen Dienst innerhalb weniger Sekunden wieder zur Verfügung. Beispiele solcher Cluster-Systeme sind *Microsoft Cluster Service* (MSCS) der Windows NT 4.0 Enterprise Edition beziehungsweise des Windows 2000 Advanced Server, Hewlett-Packards Unix Cluster (*mc/Service Guard*), Suns *Enterprise Cluster*, Siemens *ServerShield* und Compaqs *Online Storage Recovery System*.

Die genannten Lösungen können aber nur dann greifen, wenn auch das Netzdesign für eine entsprechende Verfügbarkeit ausgelegt ist.

Ergänzende Kontrollfragen:

- Ist die Einsatzumgebung für die gewünschte Verfügbarkeit und Performance ausgelegt?
- Erfüllt die Lastverteilung die Anforderungen aufgrund von Art und Umfang des Datenbestandes?

M 4.184 Deaktivieren nicht benötigter Dienste beim IIS-Einsatz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Als Grundsatz für die Konfiguration eines Web-Servers sollte, wie auch bei allen anderen von extern erreichbaren Servern, eine Konfiguration mit minimalen Diensten und Berechtigungen stehen. Je mehr Dienste und Services ein Server anbietet, desto größer sind die Angriffsmöglichkeiten, einerseits durch die steigende Zahl von Angriffspunkten, andererseits durch mögliche dienstspezifische Schwachstellen. Beispielweise liefert SNMP (Simple Network Management Protocol) einem Angreifer viele Informationen über das Zielsystem. Dieser Dienst läuft über UDP. Viele Scanner arbeiten standardmäßig nur mit dem TCP-Protokoll, so dass UDP-Dienste oft nicht genügend geprüft oder übersehen werden. Auch werden Dienste, die nur zur Erstinstallation benötigt wurden, oft vergessen und bleiben für den Wirkbetrieb aktiv.

Im Folgenden werden die Dienste aufgeteilt in:

- notwendige Dienste,
- bei Bedarf benötigte Dienste und
- in der Regel nicht benötigte Dienste.

Notwendige Dienste

Notwendige Dienste sind für das korrekte Funktionieren des IIS in der Regel unverzichtbar. Sie sollten normalerweise installiert und aktiviert sein.

- Ereignisprotokoll,
- Lizenzprotokollierdienst,
- Windows NTLM Security Support Provider,
- Remote Procedure Call (RPC) Dienst,
- Windows NT Server oder Windows NT Workstation,
- IIS Admin-Dienst,
- MSDTC (Distributed Transaction Coordinator),
- WWW-Publishing-Dienst und
- Geschützter Speicher.

Bei Bedarf benötigte Dienste

Diese Dienste sollten nur dann installiert und aktiviert werden, wenn sie für die jeweilige Anwendung benötigt werden. Anderenfalls sollten sie deaktiviert werden.

- FTP-Publishing-Dienst,
- NNTP-Dienst (nur wenn NNTP verwendet wird),
- SMTP-Dienst (nur wenn SMTP verwendet wird),

- Indexdienst (erforderlich, wenn Index Server eingesetzt wird),
- Zertifizierungsinstanz (erforderlich, wenn Zertifikate ausgestellt werden sollen),
- Plug & Play (nicht erforderlich aber empfohlen, kann nach Installation der gesamten Hardware deaktiviert werden),
- Server-Dienst (wird nur benötigt, wenn der Benutzermanager ausgeführt werden soll),
- Telefondienst (erforderlich bei Zugriffen über DFÜ) und
- Workstation (wichtig, wenn UNC-Verzeichnisse genutzt werden). Das Kürzel UNC steht für *Uniform Naming Convention*, es bezieht sich auf eine Vereinbarung von verschiedenen Software-Herstellern für universelle Namensgebungen in einem Netz. Ein Ordner kann physikalisch an einem anderen Ort gespeichert sein, durch die Freigabe kann er über den UNC-Pfad mit dem Freigabenamen direkt angesprochen werden. Dieser Dienst sollte erst am Ende der Installation deaktiviert werden.
- USV (Unterbrechungsfreie Stromversorgung).

In der Regel nicht benötigte Dienste

Diese Dienste sollten in der Regel nicht auf einem IIS aktiv sein.

- Warndienst,
- Ablagemappen-Server,
- Computerbrowser,
- DHCP-Client,
- Windows Nachrichtendienst,
- Anmeldedienst,
- Taskplaner,
- RAS (Remote Access Service),
- Netzwerk-DDE und Netzwerk-DDE-Server-Dienst,
- Netzwerkmonitoragent,
- Einfache TCP/IP-Dienste (echo, daytime, quotes, discard),
- Spooler-Dienste,
- NetBIOS-Schnittstelle,
- TCP/IP NetBIOS-Hilfsanwendung,
- WINS-Client,
- NWLink NetBIOS und
- NWLink IPX/SPX-kompatibles Übertragungsprotokoll.

Ergänzende Kontrollfragen:

- Sind auf dem IIS nur die minimal notwendigen Dienste aktiviert?

M 4.185 Absichern von virtuellen Verzeichnissen und Web-Anwendungen beim IIS-Einsatz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um einen unberechtigten Zugriff auf das Dateisystem des Web-Servers zu verhindern, sind entsprechende ACLs (Access Control Lists) einzurichten, in denen die Zugriffsrechte restriktiv vergeben werden (siehe auch M 4.53 *Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse unter Windows NT*). Der Umgang mit Scripts und CGI-Anwendungen erfordert besondere Aufmerksamkeit, da hier Ausführungsrechte benötigt werden.

Wird für das Konto *IUSR_Computername* für eine Ressource die Berechtigung *Kein Zugriff* festgelegt, wird anonymen Benutzern der Zugriff auf diese Ressource verweigert.

Im Allgemeinen sollten folgende Dateiberechtigungen auf dem IIS vergeben werden:

Dateitypen	**Beispiele**	**Nutzer (ACL)**	**Zugriffsrechte (ACL)**
Scripts, ausführbare Dateien	*.exe, *.dll, *.cmd, *.pl, *.asp, *.cgi	Jeder	Beschränkter Zugriff (X)
		Administratoren	Vollzugriff
		System	Vollzugriff
Eingebundene Dateien	*.inc, *.shtml, *.shtm	Jeder	Beschränkter Zugriff (X)
		Administratoren	Vollzugriff
		System	Vollzugriff
Statische Dateien	*.html, *.gif, *.jpeg	Jeder	Beschränkter Zugriff (R)
		Administratoren	Vollzugriff
		System	Vollzugriff
Kombination statische/ ausführbare Dateien	*.html, *.gif, *.jpeg, *.exe, *.dll, *.cmd, *.pl, *.asp, *.cgi	Jeder	Lesen (RX)
		Administratoren	Vollzugriff
		System	Vollzugriff
Datenbanken	*.mdb	Jeder	Beschränkter Zugriff (RW)
		Administratoren	Vollzugriff
		System	Vollzugriff

Tabelle: Zugriffsrechte auf Dateitypen

Besser als für jede Datei die ACL zu setzen, ist es, für jeden Dateityp ein Verzeichnis anzulegen und die ACL für dieses Verzeichnisse festzulegen. Zum Beispiel wäre eine Verzeichnisstruktur wie diese denkbar:

Verzeichnis	**Dateitypen**	**Nutzer (ACL)**	**Zugriffsrechte (ACL)**
\inetpub\wwwroot\ myserver\script	Scripts	Jeder	Beschränkter Zugriff (X)
		Administratoren	Vollzugriff
		System	Vollzugriff
\inetpub\wwwroot\ myserver\executable	Ausführbare Dateien	Jeder	Beschränkter Zugriff (X)
		Administratoren	Vollzugriff
		System	Vollzugriff
\inetpub\wwwroot\ myserver\include	Eingebundene Dateien	Jeder	Beschränkter Zugriff (X)
		Administratoren	Vollzugriff
		System	Vollzugriff
\inetpub\wwwroot\ myserver\static	Statische Dateien	Jeder	Beschränkter Zugriff (R)
		Administratoren	Vollzugriff
		System	Vollzugriff
\inetpub\wwwroot\ myserver\images	Bilddateien	Jeder	Beschränkter Zugriff (R)
		Administratoren	Vollzugriff
		System	Vollzugriff
\inetpub\wwwroot\ myserver\database	Datenbank-dateien	Jeder	Beschränkter Zugriff (RW)
		Administratoren	Vollzugriff
		System	Vollzugriff

Tabelle: Zugriffsrechte auf Verzeichnisse

Beim Einsatz des IIS als FTP- bzw. als SMTP-Server sollten auch folgende Verzeichnisse durch eine spezielle ACL geschützt werden:

c:\inetpub\ftproot (FTP-Server)

c:\inetpub\mailroot (SMTP-Server)

Jeder Benutzer hat standardmäßig auf diese beiden Verzeichnisse Vollzugriff. Dieser Zugriff sollte abhängig von der notwendigen Funktionalität herabgesetzt werden. Wenn jeder Benutzer Schreibrecht erhalten soll, ist es empfehlenswert, das Verzeichnis auf eine andere Festplatte auszulagern. Um von einem FTP-Server Dateien herunterzuladen, ist ein Leserecht im

Verzeichnis *ftproot* ausreichend. Hierdurch wird verhindert, dass vorhandene Informationen verändert oder ersetzt werden. Auf das *mailroot*-Verzeichnis sollten nur die Benutzer zugreifen können, die den SMTP-Dienst nutzen sollen. Über die MMC (Microsoft Management Console) können weitere Einstellungen, z. B. zur Authentisierung, vorgenommen werden.

Die Zugriffsrechte auf Dateien und Verzeichnisse (NTFS-Berechtigungen) werden mit Hilfe des Windows Explorers im Menü *Eigenschaft* | *Sicherheit* festgelegt. Darüber hinaus besteht die Möglichkeit, über die MMC des IIS weitere Berechtigungen für virtuelle Web-Verzeichnisse zu vergeben. Folgende Optionen können ausgewählt werden:

- Lesen: (standardmäßig aktiviert) Benutzer können den Inhalt und die Eigenschaften von Dateien anzeigen.
- Schreiben: Benutzer können den Inhalt und die Eigenschaften von Dateien ändern.
- Zugriff protokollieren (Besuche protokollieren): Für jeden Besuch einer Web-Seite wird ein Protokolleintrag erstellt.
- Verzeichnis durchsuchen (erlaubt): Benutzer können Dateilisten und Auflistungen anzeigen.
- Indizieren des Verzeichnisses (Ressource indizieren): Ermöglicht dem Indexdienst die Indizierung der jeweiligen Ressource.
- Scriptzugriff (nur IIS 5.0): Benutzer haben Zugriff auf Quelldateien. Ist *Lesen* aktiviert, kann der Quellcode gelesen werden. Ist *Schreiben* aktiviert, ist der Schreibzugriff auf den Quellcode möglich. *Scriptzugriff* ermöglicht den Zugriff auf den Quellcode für Dateien, z. B. auf die Scripts in einer ASP-Anwendung. Diese Option ist nur verfügbar, wenn *Lesen* oder *Schreiben* aktiviert ist.
- FrontPage-Web (nur bei Web-Seite).

Die Standardeinstellungen sind Lesen, Zugriff protokollieren und Indizieren des Verzeichnisses.

Stimmen diese Berechtigungen nicht mit den NTFS-Berechtigungen überein, werden die Einstellungen mit den geringsten Rechten wirksam. Das bedeutet, es wird die Schnittmenge gebildet.

Ergänzende Kontrollfragen:

- Wurden die Dateien im *webroot*-Verzeichnis, insbesondere Scripts und ausführbare Dateien, durch geeignete ACLs geschützt?
- Wurde beim Einsatz des IIS als FTP-Server das Verzeichnis *\Inetpub\ftproot* mit einer speziellen ACL versehen?
- Wurde beim Einsatz des IIS als SMTP-Server das Verzeichnis *\Inetpub\mailroot* mit einer speziellen ACL versehen?

M 4.186 Entfernen von Beispieldateien und Administrations-Scripts des IIS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Bei der Standardinstallation des IIS werden eine Reihe von Beispieldateien sowie einige Administrations-Scripts installiert, die den Administrator bei der Verwaltung des IIS unterstützen sollen.

Insbesondere Script-Dateien können von Unbefugten ausgenutzt werden, um Informationen über den Web-Server zu erhalten. Ein Beispiel für einen solchen Angriff ist das Ausnutzen von *showcode.asp*, um Dateien auch außerhalb des *Webroot*-Verzeichnis anzuzeigen.

Beispielanwendungen sollten niemals auf einem produktiven Server installiert sein. Das betrifft ebenfalls die SDK Dokumentation (Software Development Kit). Alle Beispiele sind zu entfernen. Die nachfolgende Tabelle zeigt eine Übersicht über einige Beispielverzeichnisse.

Technologie	**Ort**
IIS	c:\inetpub\iissamples
IIS SDK	c:\inetpub\iissamples\sdk
Admin Scripts	c:\inetpub\AdminScripts
Data access	c:\Program Files\Common Files\System\msadc\Samples

Tabelle: Beispielanwendungen

Neben nicht benötigten Dateien sollten auch nicht benötigte Verzeichnisse, insbesondere virtuelle Verzeichnisse, entfernt werden.

Das virtuelle Web-Verzeichnis */IISADMPWD* enthält **.htr*-Dateien, die zur Passwortänderung verwendet werden. Der Zugriff von *Anonymous* auf dieses Verzeichnis ist erlaubt. Physikalisch befindet sich das Verzeichnis im Pfad *%systemroot%\system32\inetsrv\iisadmpwd*. Dieses virtuelle Verzeichnis ist nicht Bestandteil des IIS 5.0, wird aber bei einem Update von IIS 4.0 nicht entfernt. Die Passwortänderung über die HTTP-Schnittstelle wurde primär für den Gebrauch im Intranet entwickelt. Wenn dieses Feature nicht benötigt wird, sollte das Verzeichnis (virtuell und physikalisch) entfernt werden.

Ergänzende Kontrollfragen:

- Wurden alle Beispielanwendungen entfernt?
- Wurde das Verzeichnis *IISADMPWD* entfernt bzw. der Zugriff eingeschränkt?

M 4.187 Entfernen der FrontPage Server-Erweiterung des IIS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Microsoft FrontPage Server-Erweiterungen stellen mehrere Programme bereit, die das Verwalten und Erstellen von Dokumenten sowie das Durchsuchen einer Web-Site ermöglichen.

Beispielsweise können mit Hilfe der FrontPage Server-Erweiterungen folgende Aufgaben durchgeführt werden:

- Verwalten von Web-Seiten mit FrontPage Server-Erweiterungen. Dies umfasst das Festlegen von Berechtigungen für Autoren, Administratoren und Besucher der Web-Site.
- Erstellen von Dokumenten auf Web-Seiten mit FrontPage Server-Erweiterungen. Dies umfasst die automatische Verwaltung von Hyperlinks, das Erstellen und Verwalten von Navigationsleisten auf allen Seiten sowie das automatische Formatieren von Seiten für ein verfeinertes Erscheinungsbild.
- Erweitern der Funktionalität der Web-Site. Dies umfasst interaktive Diskussionsgruppen, Zugriffszähler und Suchformulare.

Im Internet gibt es viele Web-Seiten, die die FrontPage Server-Erweiterung zur Verfügung stellen, diese aber nicht verwenden. Die FrontPage Server-Erweiterungen sollten vollständig entfernt werden, sofern sie nicht benötigt werden. Falls nur einige dieser FrontPage Server-Erweiterung zum Einsatz kommen, sollten nur die notwendigen Erweiterungen installiert sein.

Ergänzende Kontrollfragen:

- Wurden alle nicht benötigten FrontPage Server-Erweiterungen entfernt?

M 4.188 Prüfen der Benutzereingaben beim IIS-Einsatz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Viele Web-Seiten beinhalten Formularfelder zur Eingabe von benutzerspezifischen Informationen, z. B. für Bestellungen, Gästebucheinträge etc. In einigen Fällen werden die Benutzereingaben zum Aufruf weiterer ASP-Seiten verwendet oder direkte SQL-Abfragen erstellt. Dabei besteht die Gefahr, dass Eingaben, die vom System nicht erwartet werden, z. B. Sonderzeichen, Buchstaben anstelle von Zahlen, zu unnötigen Ressourcenbelastungen und Pufferüberläufen führen können. Als Folge können dadurch unter Umständen Sicherheitsfunktionen umgangen werden.

Um Schäden zu vermeiden, sind Benutzereingaben und URL-Erweiterungen immer zu prüfen, bevor diese an einen neuen Prozess übergeben werden, der ggf. auf externe Ressourcen, wie das Dateisystem oder eine Datenbank, zugreift. Eine Benutzereingabe kann z. B. auf Basis des verwendeten Zeichensatzes überprüft werden. Dabei sollten nur Eingaben zugelassen werden, die einem erlaubten Schema entsprechen und beispielsweise nur Zahlen und Zeichen aus den Bereichen 0-9, a-z, A-Z und _ enthalten.

Die Überprüfung einer Benutzereingabe kann durch spezielle Scripts erfolgen, beispielsweise durch ein VBScript, das die Klasse *RegExp* und die Funktion *Replace* dafür verwendet. Weitere Details hierzu werden auf dem Internet-Angebot von Microsoft erörtert:

http://www.microsoft.com/jscript

http://msdn.microsoft.com/workshop/languages/clinic/ scripting051099.asp

Ergänzende Kontrollfragen:

- Werden Benutzereingaben in Formularfeldern und URLs geprüft?

M 4.189 Schutz vor unzulässigen Programmaufrufen beim IIS-Einsatz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

In dieser Maßnahme werden Einstellungen für die IIS-Konfiguration beschrieben, um ein unzulässiges Aufrufen von Programmen zu verhindern.

Unterbinden des *exec* Aufrufes beim IIS-Einsatz

Der *exec* Aufruf kann dazu verwendet werden, beliebige Kommandos auf dem Web-Server von einer HTML-Webseite aufzurufen. Der IIS 5.0 unterdrückt diese Option in der Standardinstallation. Dies sollte aber anhand des entsprechenden Eintrages in der Registrierung überprüft werden. Der Eintrag sollte wie folgt eingerichtet sein:

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	CurrentControlSet\Services\W3SVC\Parameters
Name	SSIEnableCmdDirective
Type	REG_DWORD
Wert	0

Tabelle: Änderung der Registrierung

Deaktivieren der übergeordneten Pfade beim IIS-Einsatz

Die Option *Übergeordnete Pfade* ermöglicht (ASP-Skripten) die Verwendung relativer Pfade zum übergeordneten Verzeichnis, d. h. Pfade, die ".." enthalten. Wenn diese Option aktiviert ist, sollte für das übergeordnete Verzeichnis kein Ausführungsrecht bestehen, da anderenfalls ein Skript versuchen könnte, ein unzulässiges Programm in diesem Verzeichnis auszuführen.

Standardmäßig werden im IIS die übergeordneten Pfade zugelassen. Diese Option sollte deaktiviert werden. Um die übergeordneten Pfade zu deaktivieren, sind in der Microsoft Management Console mit einem Rechtsklick die Eigenschaften einer Web-Seite zu öffnen. Anschließend ist unter dem Reiter *Basisverzeichnis* die Konfiguration zu wählen. Dort sind unter dem Reiter *Anwendungsoptionen* die *Übergeordneten Pfade* zu deaktivieren.

Entfernen von nicht benötigten Anwendungsverknüpfungen beim IIS-Einsatz

Der IIS ist so vorkonfiguriert, dass allgemeingültige Dateierweiterungen unterstützt werden (beispielsweise . *asp*). Wenn der IIS 5.0 eine Anfrage für eine solchen Erweiterung erhält, wird diese Anfrage an eine entsprechende DLL weitergegeben. Die Verknüpfungen können wie folgt editiert werden:

Microsoft Management Console | Rechtsklick auf IIS-Server | Haupteigenschaften: WWW-Dienst | Bearbeiten | Basisverzeichnis | Konfiguration

Die folgende Tabelle zeigt eine Übersicht über Anwendungen und Dateierweiterungen. Nicht benötigte Verknüpfungen sollten entfernt werden:

Anwendung	**Erweiterung**
Web-based Password Reset	.htr
Internet Database Connector	.idc
Server-side includes	.shtm, .stm, .shtml
Index Server	.htw, .htx, .ida
Index Server query	.idq
Internet Printing	.printer

Tabelle: Anwendungsverknüpfungen

Ergänzende Kontrollfragen:

- Wurde der Aufruf des Kommandos *#exec* unterbunden?
- Wurde die Option *Übergeordnete Pfade* deaktiviert?
- Wurden alle nicht benötigten Anwendungsverknüpfungen entfernt?

M 4.190 Entfernen der RDS-Unterstützung des IIS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Remote Data Service (RDS) ist eine Komponente der *Microsoft Data Access Components* (MDAC). Diese Komponente ermöglicht den Fernzugriff auf Datenbanken, wie z. B. SQL-Server oder Microsoft Access, über den IIS. RDS beinhaltet die Teilkomponente *DataFactory*. Dieses Objekt erlaubt standardmäßig eine implizite Fernausführung von Datenzugriffsanfragen.

Dadurch besteht die Gefahr, dass unter bestimmten Umständen unbefugte Internet-Clients auf beliebige Daten innerhalb der durch den *Remote Data Service* zugänglichen Datenbank zugreifen bzw. beliebige Kommandos mit erhöhten Rechten auf dem Server ausführen können.

Um einen Missbrauch der RDS-Funktionalitäten zu verhindern, sind diese zu deaktivieren, sofern sie nicht unbedingt erforderlich sind. Um die RDS-Funktionalität zu deaktivieren, müssen auf dem IIS folgende Registrierungseinträge (und etwaige Teilschlüssel) entfernt werden:

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	CurrentControlSet\Services\W3SVC\ Parameters\ADCLaunch\ RDSServer.DataFactory

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	CurrentControlSet\Services\W3SVC\ Parameters\ADCLaunch\ AdvancedDataFactory

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	CurrentControlSet\Services\W3SVC\ Parameters\ADCLaunch\ VbBusObj.VbBusObjCls

Tabelle: IIS Registrierungseinträge

Die o. g. Änderungen können zu Einschränkungen einiger Beispiel-Websites des IIS 4.0 führen. Weitere Standardfunktionen von IIS werden jedoch nicht beeinträchtigt. Eine Datenbankabfrage über *Active Server Pages* (ASPs), die in Bezug auf die Datenbankkonnektivität nur von ADO (ActiveX Data Objects) abhängig sind, ist weiterhin möglich.

Folgende Empfehlungen sollten generell beim Datenbankzugriff mit Hilfe von ASP-Seiten beachtet werden:

- Alle nicht unbedingt benötigten ODBC-Treiber sind zu entfernen, insbesondere der Microsoft Text-Treiber.
- Bei der Vergabe von NTFS-Berechtigungen (ACLs) ist restriktiv vorzugehen und der Zugang auf die Personen zu beschränken, denen vertraut wird.
- Beim Arbeiten mit SQL-Server sollte dieser mit einem Benutzerkonto auf niedriger Privilegebene ausgeführt werden. Außerdem sollten erweiterte gespeicherte Prozeduren nicht zugelassen werden.

Ergänzende Kontrollfragen:

- Wurde die RDS-Unterstützung deaktiviert?
- Wurde eine angemessene Sicherheitsrichtlinie durchgesetzt?

M 4.191 Überprüfung der Integrität und Authentizität der Apache-Pakete

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Ist bei der Planung für den Einsatz des Apache-Webservers entschieden worden, den Apache-Webserver entweder aus dem Quelltext zu kompilieren oder eine der Binärversionen von der der Apache Foundation zu verwenden, so muss die Integrität des Quellcode- oder Installationspaketes, das aus dem Internet heruntergeladen wurde, überprüft werden (siehe auch M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*).

Apache Pakete sind mit PGP signiert

Die Entwickler des Apache-Projektes verwenden schon seit längerer Zeit digitale Signaturen mit der Software PGP zur Absicherung der Quellcode-Pakete (siehe auch M 5.63 *Einsatz von GnuPG oder PGP*). Die Signatur der Apache-Quelltexte befindet sich stets in einer gesonderten Datei, die den gleichen Namen trägt, wie das Quelltext-Paket selbst, jedoch ergänzt durch das Suffix *.asc*. Die öffentlichen Schlüssel der Apache Entwickler finden sich in der Datei *http://www.apache.org/dist/httpd/KEYS*. Diese Datei KEYS ist auch als Bestandteil des jeweiligen Apache-Paketes im Lieferumfang vieler (Unix-) Betriebssysteme enthalten.

Vor der Installation des Apache-Webservers aus einem Paket, das aus dem Internet geladen wurde, sollte stets die Integrität und Authentizität der Software durch Kontrolle der entsprechenden Signatur überprüft werden.

Public Keys überprüfen

Um zu vermeiden, dass zur Kontrolle der Signatur manipulierte öffentliche Schlüssel zum Einsatz kommen, sollte die Datei KEYS oder die darin enthaltenen Schlüssel unabhängig vom eigentlichen Softwarepakte bezogen werden. Es bieten sich eine oder mehrere der folgenden Methoden an:

- Verwendung einer KEYS Datei, die bereits vor längerer Zeit vom zentralen Webserver des Apache-Projektes (und nicht von einem Spiegelserver) heruntergeladen wurde.
- Verwendung von KEYS Dateien von mehreren Spiegelservern.
- Verwendung einer KEYS Datei aus einer bereits auf CD-ROM vorhandenen Version des Apache-Webservers.

Prinzipiell genügt es schon, nur den Fingerabdruck (englisch: Fingerprint) des jeweiligen benutzten öffentlichen GPG-Schlüssels zu vergleichen.

Prüfung dokumentieren

Die Herkunft der zu installierenden Software sollte ebenso wie der Prozess der Integritätsprüfung der Software dokumentiert werden.

Ergänzende Kontrollfragen:

- Wurde eine Integritätsprüfung der Software vorgenommen?
- Sind die Herkunft der Software und die vorgenommene Integritätsprüfung dokumentiert?

M 4.192 Konfiguration des Betriebssystems für einen Apache-Webserver

Verantwortlich für Initiierung: Administrator, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Das Betriebssystem des Rechners, auf dem ein Apache-Webserver installiert werden soll, muss vor der Installation sicher und möglichst "schlank" konfiguriert werden. Der Rechner sollte keine anderen als die zum Betrieb des Webservers nötigen Dienste nach außen anbieten. Alle anderen nicht benötigten Systemdienste und Programme sollten so weit wie möglich entfernt werden. Allgemeine Hinweise zur Konfiguration finden sich beispielsweise in den Bausteinen B 3.102 *Unix-Server* und B 3.106 *Windows 2000 Server*.

Diese Maßnahme beschreibt einige zusätzliche Schritte, die unternommen werden sollten, wenn ein Rechner für die Installation eines Apache-Webservers vorbereitet wird.

Kein Compiler und Skripting-Engines

Auf dem Webserver-Rechner sollte kein Compiler installiert sein. Soll der Apache-Webserver aus den Quelltexten kompiliert werden, so sollte dies nicht auf dem Produktionsrechner geschehen, sondern auf einem entsprechend ausgestatteten und konfigurierten Entwicklungsrechner. Außer den Skriptsprachen-Interpretern oder Laufzeitumgebungen (beispielsweise Perl, PHP oder die Java-Runtime), die für die Systemadministration oder die Realisierung dynamischer Webseiten benötigt werden, sollten keine weiteren Laufzeitumgebungen installiert sein.

Kein Webbrowser, ftp-Client oder wget, keine Kommunikationsprogramme

Client-Programme zum Einloggen auf andere Rechner oder zum Herunterladen von Dateien aus dem Internet (beispielsweise ssh- oder Telnet-Clients, Webbrowser, ftp-Clients oder *wget*) sollten möglichst nicht auf dem Webserver installiert sein, sofern sie nicht für den Betrieb des Webservers unbedingt benötigt werden.

Sind keine derartigen Programme installiert, so kann dies weniger versierte Angreifer daran hindern, nach dem erfolgreichen Ausnutzen einer Sicherheitslücke den Webserver dauerhaft zu kompromittieren, da sie dazu oft Dateien (etwa rootkits oder Backdoor-Programme) von anderen Rechnern unter ihrer Kontrolle herunterladen müssen.

Soll der Apache-Webserver unter Windows installiert werden, so kann zusätzlich M 4.174 *Vorbereitung der Installation von Windows NT/2000 für den IIS* berücksichtigt werden.

Eigene Partition für WWW-Dateien

Das Verzeichnis, das die WWW-Dateien enthalten soll wird im Apache-Webserver mit der Konfigurationsdirektive *DocumentRoot* festgelegt. Das dafür vorgesehene Verzeichnis sollte in einem eigenen Filesystem (unter Unix) bzw. auf einer eigenen Partition (unter Windows) angelegt werden.

Eigene Partition für Logdateien

Das Verzeichnis, das für die Logdateien des Apache-Webservers vorgesehen ist, sollte ebenfalls in einem eigenen Filesystem bzw. auf einer eigenen Partition angelegt werden. Je nach Auslastung des Webservers und dem gewählten Logformat können die Logdateien schnell eine beträchtliche Größe annehmen. Daher sollte das entsprechende Filesystem von vorne herein genügend groß angelegt werden.

Unter Windows sollte auf jeden Fall NTFS als Dateisystem gewählt werden, da FAT keine sinnvolle Benutzertrennung und Rechtevergabe erlaubt. Sofern das Betriebssystem verschiedene Filesystem-Typen unterstützt, sollte ein Filesystem gewählt werden, das eine möglichst gute Performance beim Lesen von Dateien bietet.

Sichere Protokolle zur Remote-Administration und zum Datentransfer verwenden

Erfolgt die Administration des Serverrechners nicht lokal, so sollten zur Administration des Server-Betriebssystems nur entsprechend sichere Produkte bzw. Protokolle verwendet werden. Gleiches gilt, falls die WWW-Dateien nicht über Wechseldatenträger, sondern über das Netz auf den Webserver übertragen werden. Telnet und ftp sollten nicht eingesetzt werden, stattdessen sollte ssh bzw. sftp benutzt werden.

Apache-Account anlegen

Bei der Standardinstallation eines Betriebssystems werden oft Accounts (Benutzerkonten) angelegt, die in der Minimalkonfiguration, wie sie für einen Webserver hergestellt werden sollte, nicht benötigt werden. Diese Accounts sollten gelöscht oder zumindest deaktiviert werden. Stattdessen sollte für den Apache-Webserver ein eigener Account (etwa *apache*) und eine eigene Gruppe eingerichtet werden, der über möglichst wenig Rechte verfügt. Unter diesem Account sollte insbesondere keine interaktive Anmeldung am System möglich sein. Dazu kann dem Apache-Account beispielsweise auf den meisten Unix-Systemen die Login-Shell */bin/false* zugeordnet werden.

Soll der Rechner als öffentlicher Webserver dienen und in einer Firewall-Umgebung aufgestellt werden, so sollte in Erwägung gezogen werden, die Logdateien des Systems und gegebenenfalls auch des Apache-Webservers nicht nur auf dem Rechner selbst zu speichern, sondern auf einen zweiten Rechner zu kopieren. Wie dies konkret implementiert wird, hängt stark von der jeweiligen Einsatzumgebung ab, so dass an dieser Stelle keine detaillierten Empfehlungen gegeben werden können. Prinzipiell sollte jedoch die Übertragung der Logdaten auf den anderen Rechner so gelöst werden, dass keine Verbindung aus der Firewall-Umgebung in das interne Netz geschaffen wird, die eventuell von einem Angreifer ausgenutzt werden könnte.

Ergänzende Kontrollfragen:

- Wurden unnötige Accounts gelöscht?
- Welche Skript-Interpreter und Compiler sind auf dem Webserver-Rechner installiert? Wozu werden diese gegebenenfalls benötigt?
- Auf welche Art erfolgt die Administration des Systems?
- Wie sieht das Partitions- bzw. Filesystem-Layout des Systems aus?
- Werden Logdaten auf einen weiteren Rechner übertragen?

M 4.193 Sichere Installation eines Apache-Webservers

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Bei der Installation eines Apache-Webservers sind verschiedene Aspekte zu berücksichtigen, die direkten Einfluss auf die Sicherheit haben.

Das Betriebssystem des Webserver-Rechners muss sicher installiert und konfiguriert sein. Dazu müssen die entsprechenden IT-Grundschutz-Bausteine umgesetzt werden. Darüber hinaus gibt M 4.192 *Konfiguration des Betriebssystems für einen Apache-Webserver* Hinweise, welche zusätzlichen Schritte auf dem Rechner durchgeführt werden sollten, der den Apache-Webserver beherbergen soll.

Ein wichtiger Aspekt, der bei der Installation des Apache-Webservers beachtet werden muss, ist die Integrität der zu installierenden Software (siehe M 4.191 *Überprüfung der Integrität und Authentizität der Apache-Pakete*).

Apache-Dokumentation nutzen!

Die mit dem Apache-Webserver mitgelieferte Dokumentation ist sehr detailliert und beschreibt die notwendigen Schritte recht ausführlich. Diese Grundschutz-Maßnahme kann die mitgelieferte Dokumentation nicht ersetzen, sondern lediglich Hinweise auf Punkte geben, die besonders zu beachten sind. Sie bezieht sich auf die Installation einer Binärversion von der Apache-Foundation oder eines aus dem Quellcode kompilierten Apache-Webservers. Apache-Versionen von Betriebssystemherstellern oder Distributoren können davon abweichen.

Multiprocessing-Module

Seit der Version 2 bietet der Apache-Webserver die Auswahl zwischen verschiedenen sogenannten Multiprocessing-Modulen (MPMs). Die Wahl eines bestimmten MPMs kann die Performance des Apache-Webservers bei verschiedenen Einsatzbedingungen beeinflussen. Das benutzte MPM muss beim Kompilieren des Webservers festgelegt werden. Normalerweise kann das "Standard-MPM" für das jeweilige Betriebssystem übernommen werden, nur bei speziellen Anforderungen sollte davon abgewichen werden. In diesem Fall bietet die Apache-Dokumentation Informationen zur Auswahl eines MPMs. Wie die gesamte Konfiguration sollte die Auswahl des MPMs dokumentiert werden.

"configure, make, make install" nicht als root bzw. Administrator

Das Kompilieren des Apache-Webservers aus dem Quellcode sollte nicht als *root* oder Systenadministrator erfolgen. Nachdem die Integrität und Authentizität des Quellcodepackets anhand der digitalen Signaturen überprüft wurde, sollten das Entpacken, die Konfiguration (*configure*, Festlegung des Installationsverzeichnisses sowie von Vorgabewerten, die fest einkompiliert werden, sowie der zu kompilierenden Module) und der eigentliche Übersetzungsvorgang (*make*) unter einem unprivilegierten Benutzeraccount durchgeführt werden. Erst der letzte Schritt, die eigentliche Installation des übersetzten Programms (*make install*) muss gegebenenfalls mit höheren Privilegien erfolgen. Wird das Zielverzeichnis der Installation vorab manuell angelegt und erhält der unprivilegierte Benutzeraccount Schreibberechtigung für dieses Verzeichnis, so kann selbst dieser letzte Schritt unter diesem Account durchgeführt werden.

Wird der Apache-Webserver aus dem Quellcode übersetzt, so muss genau dokumentiert werden, welche Konfigurationsoptionen dabei gewählt wurden. Die Konfiguration muss sich anhand dieser Dokumentation jederzeit nachvollziehen und reproduzieren lassen. Es empfiehlt sich auch, ein Protokoll der Ausgaben des Konfigurations- und Übersetzungslaufs (beispielsweise durch Umleiten der Ausgaben in eine Datei) anzufertigen und aufzubewahren.

Bei der Installation des Apache-Webservers werden im Zielverzeichnis der Installation mehrere Unterverzeichnisse erstellt. Als Zielverzeichnis unter Unix wird im Rahmen dieser Maßnahme das Verzeichnis */usr/local/apache* angenommen, unter Windows *d:\programme\apache*. Das Unterverzeichnis *conf* enthält die Konfigurationsdateien. Die Unterverzeichnisse *logs* und *htdocs* sind in der Standardinstallation für Logdateien bzw. WWW-Dokumente vorgesehen. Diese sollten jedoch nicht benutzt werden, sondern es sollten Verzeichnisse auf eigenen Partitionen benutzt werden (siehe auch M 4.192 *Konfiguration des Betriebssystems für einen Apache-Webserver*). Im Rahmen dieser Maßnahme werden dafür

- *W:\htdocs* unter Windows und
- */var/www/htdocs* unter Unix (wobei */var/www* der Mountpoint eines eigenen Filesystems ist)

für die WWW-Dateien sowie für die Logfiles

- *L:\logs* unter Windows und
- /var/wwwlogs unter Unix

angenommen.

httpd.conf

Die zentrale Konfigurationsdatei für den Apache-Webserver ist die Datei *httpd.conf* im Unterverzeichnis *conf*. Dabei handelt es sich um eine reine Textdatei, die je nach Installationsart bereits mit sinnvollen Konfigurationseinstellungen vorbelegt ist. Die Datei ist außerdem mit ausführlichen Kommentaren zur Dokumentation versehen, die sie weitgehend selbsterklärend machen. Die Konfiguration erfolgt durch sogenannte Direktiven. Dabei handelt es sich entweder um "Name-Wert-Paare" oder um Abschnitte in der Datei, die durch "Tags" der Form *<Direktive> </Direktive>* abgegrenzt werden.

Dokumentation

Alle Schritte, die bei der Installation gemacht werden, sollten so dokumentiert werden, dass sich die Konfiguration im Notfall schnell verstehen und reproduzieren läßt. Dies betrifft neben den Einstellungen beim Kompilieren auch Installationspfade, Berechtigungen, Änderungen an der Datei *httpd.conf* und ähnliche Informationen.

Sichere Installation des Apache-Webserver unter Unix

Der Start des Apache-Webservers sollte im Allgemeinen aus den Startupskripts des Betriebssystems erfolgen. So steht der Webserver auch nach einem Reboot des Server-Rechners direkt zur Verfügung. Ausnahmen bestehen hier unter Umständen beim Einsatz von SSL (siehe auch M 5.107 *Verwendung von SSL im Apache-Webserver*).

Festlegung von Benutzer und Gruppe

Normalerweise muss der Start des Apache-Webservers unter dem Benutzerkonto *root* erfolgen, damit der Apache-Webserver den "WWW-Port" 80/tcp

benutzen kann. Der Apache-Webserver darf jedoch nicht ständig mit Root-Rechten ausgeführt werden. Zu diesem Zweck muss ein eigenes Benutzerkonto und eine eigene Gruppe, z. B. *apache*, angelegt werden. Mittels der Direktiven *user* und *group* in der Konfiguration *httpd.conf* wird festgelegt, unter welchem Benutzerkonto der Apache-Webserver ausgeführt werden soll. In der Datei *httpd.conf* wird durch die Direktiven

```
user apache
group apache
```

festgelegt, dass der Webserver nach dem Start die Benutzer- und Gruppen-Kennung *apache* annehmen soll.

Nach der Installation sollte die Konfiguration der Dateizugriffsrechte kontrolliert werden. Das Apache-Verzeichnis und alle darüber liegenden Verzeichnisse müssen dem Benutzer *root* (oder einem sonstigen Systemkonto) und einer entsprechenden Systemgruppe gehören. Nur die Eigentümer dürfen Schreibzugriff auf diese Verzeichnisse haben. Gleiches gilt für die Unterverzeichnisse des Apache-Verzeichnisses, die Binärdateien, Konfigurations- oder Logdateien enthalten. In der Installation einer Quellcode-Distribution des Apache-Webservers sind dies die Verzeichnisse *bin*, *conf* und *logs*. Auch die Binärdateien selbst sollten nur von root geschrieben werden können.

Sichere Installation unter Windows

Eine sichere Installation des Apache-Webservers unter Windows erfordert einige zusätzliche Maßnahmen, da die Standardkonfiguration, wie sie direkt aus der Kompilierung der Quelltextdistribution entsteht, genauso wie die Standardinstallation des Apache 2.0 mit dem mitgelieferten Microsoft Installer Plugin einige wichtige Regeln zur Absicherung des Apache-Webservers nicht umsetzen. Beispielsweise wird der Apache-Webserver damit unter dem Konto *LocalSystem* ausgeführt.

Im Rahmen der Installation sollten daher die folgenden Änderungen an der Konfiguration vorgenommen werden:

Für den Apache-Webserver sollte ein spezielles Benutzerkonto (bspw. *apache*) eingerichtet werden, das nur über die minimal notwendigen Rechte verfügt. Dieses Benutzerkonto muss ein Mitglied der Gruppe *Benutzer* sein. Zusätzlich müssen dem Benutzerkonto im User Manager spezielle Benutzerrechte eingeräumt werden, damit der Webserver als Dienst ablauffähig ist. Erforderlich sind die Benutzerrechte

- Anmelden als Dienst,
- Sichern von Dateien und Verzeichnissen und
- Wiederherstellen von Dateien und Verzeichnissen.

Laut Dokumentation benötigt der Apache-Webservers zusätzlich das Benutzerrecht *Als Teil des Betriebssystems handeln*, obwohl der Apache-Webserver auch ohne dieses Privileg arbeitet. Dieses spezifische Benutzerrecht räumt dem jeweiligen Benutzer sehr viele Privilegien auf dem lokalen Rechner ein. Bei Verwendung des Apache-Webservers unter Windows NT sollte daher im Einzelfall geprüft werden, ob die Vergabe dieses Benutzerrechtes wirklich notwendig ist.

Außerdem sollten die Zugriffsrechte im Dateisystem modifiziert werden, da in der Voreinstellung alle Benutzer Vollzugriff auf alle Dateien des Apache-Webservers haben. Bei der Beschränkung des Zugriffs auf diese Verzeichnisse muss jedoch sichergestellt werden, dass der Apache-Webserver über die für den ordnungsgemäßen Ablauf notwendigen Zugriffsrechte verfügt.

Die folgende Tabelle gibt die notwendigen Zugriffsrechte für die im Verzeichnis *d:\programme\apache* enthaltenen Dateien und Ordner an.

Datei bzw. Verzeichnis	**Zugriffsrechte**
Apache	Administrator: F System: F apache: R
Apache/Apache.exe	apache: RX
Apache/ApacheCore.dll	apache: RX
Apache/Win9xConHook.dll	apache: RX
Apache/logs	apache: RWXD
Apache/logs/*	apache: RWD
htdocs	WWW-Redakteure: F apache: RX
proxy	apache: RWD

Tabelle: Zugriffsrechte

Der Zugriff auf das *htdocs* Verzeichnis, das den WWW-Dateibaum enthält (hier *W:\htdocs*), sowie seine Unterverzeichnisse, sollte so eingeschränkt werden, dass nur Benutzer (im obigen Beispiel WWW-Redakteure genannt), die Daten in den Webserver einstellen dürfen, Zugriff auf die jeweiligen Verzeichnisse haben.

Ergänzende Kontrollfragen:

- Wurde die Integrität der Software vor der Installation überprüft?
- Wie ist die Konfiguration dokumentiert?
- Welche Zugriffsrechte bestehen auf das WWW-Verzeichnis (DocumentRoot)?

M 4.194 Sichere Grundkonfiguration eines Apache-Webservers

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Nachdem der Apache-Webserver installiert wurde, muss eine sichere Grundkonfiguration vorgenommen werden. Dies betrifft beispielsweise die Einstellungen für Erweiterungsmodule und für Zugriffe auf Verzeichnisse innerhalb und außerhalb des WWW-Bereichs, aber auch Einstellungen, die auf den Performance des Servers Einfluss haben.

Generell sollte mittels der Direktive HostnameLookups Off explizit festgelgt werden, dass der Server keine Namensauflösung für IP-Adressen vornimmt, von denen HTTP-Anfragen gesendet werden. In den Logdateien werden dann die Zugriffe mit der betreffenden IP-Adresse gespeichert und diese kann später, falls nötig, bei der Auswertung der Logdateien aufgelöst werden.

Server-Wurzelverzeichnis und Logdateien

In der Datei *httpd.conf* wird mit der Direktive

```
ServerRoot /usr/local/apache
```

das Verzeichnis angegeben, in dem der Apache-Webserver installiert wurde. Relativ zu diesem Verzeichnis werden beispielsweise die Konfigurationsdateien gesucht.

Mit der Direktive

```
ErrorLog /var/wwwlogs/error.log
```

wird die Fehlerprotokolldatei für den Server festgelegt. Die Direktive *LogLevel* gibt an, welche Art von Fehlern protokolliert werden soll. Je nach *LogLevel* kann die Fehlerprotokolldatei recht schnell anwachsen. Normalerweise ist die Default-Einstellung *warn* für den *LogLevel* angemessen.

Für die Erzeugung von Zugriffsprotokollen ist das Modul *mod_log_config* zuständig. Ist dieses Modul geladen, so können mit der Direktive *LogFormat* die zu protokollierenden Informationen festgelegt werden. Mit der Direktive *AccessLog* wird anschliessend eine Datei für die Zugriffsprotokolldatei angegeben. Informationen zur Festlegung eines geeigneten Formats für Logdateien finden sich in der *httpd.conf* Beispieldatei sowie in der Apache-Dokumentation.

Da Zugriffsprotokolldateien noch mehr als Fehlerprotokolldateien sehr schnell anwachsen können, sollten sie regelmäßig gesichert werden. Anschliessend sollte der Server mit einer neuen Zugriffsprotokolldatei neu gestartet werden.

Informationen über den Server

Aus den HTTP-Header-Zeilen von Antworten auf Anfragen oder in Fehlermeldungen können Angreifer oft Informationen über die Version der Server-Software und andere Details gewinnen. Diese Informationen können dann eventuell dazu genutzt werden, um bestimmte Angriffsmethoden auszuwählen

und so schneller den Server zu kompromittieren. Daher sollte auf diesen "Seitenkanälen" so wenig Informationen wie möglich geliefert werden.

ServerTokens und ServerSignature

Mit der Direktive *ServerTokens* wird gesteuert, welche Informationen der Server in den HTTP-Header-Zeilen der Antwort auf Anfragen über sich selbst liefert. Dies sollte mittels

ServerTokens Prod

auf das Mindestmaß beschränkt werden. Mittels

ServerSignature Off oder ServerSignature EMail

sollte außerdem die Information beschränkt werden, die der Server bei servergenerierten Dokumenten übermittelt.

ServerAdmin

In bestimmten Fehlermeldungen wird vom Server die E-Mail-Adresse des Administrators als Kontakt genannt. Daher sollte eine Funktions-E-Mail-Adresse (beispielsweise *admin@servername*) eingerichtet und mittels

ServerAdmin admin@servername

im Server eingestellt werden. E-Mails an diese Adresse müssen vom Server-Administrator regelmäßig ausgewertet werden.

Einstellungen für Verzeichnisse und Dateien

DocumentRoot

Die Wurzel des WWW-Dateibaums wird durch die *DocumentRoot*-Direktive festgelegt:

DocumentRoot /var/www/htdocs

Dies bedeutet jedoch nicht, dass keine Dokumente ausserhalb des hier angegebenen Verzeichnisses ausgeliefert würden. Durch Direktiven wie *Alias* (Modul *mod_alias*) oder durch symbolische Links können auch Dokumente ausserhalb der *DocumentRoot* ausgeliefert werden. Der Zugriff auf die Dateien des Webserver-Rechners außerhalb des WWW-Verzeichnisses sollte in der Apache Konfigurationsdatei über einen Limit-Abschnitt für das Wurzelverzeichnis / verhindert werden:

```
<Directory / >
 Options None
 AllowOverride None
 Order Deny,Allow
 Deny from All
</Directory>
```

Lediglich der Zugriff auf das mittels *DocumentRoot* festgelegte WWW-Verzeichnis sollte wieder mittels eines entsprechenden *Limit*-Abschnittes für Anfragen geöffnet werden.

```
<Directory /var/www/htdocs >
 Order Deny,Allow
 Allow from All
</Directory>
```

Werden Verzeichnisse von ausserhalb der *DocumentRoot* mittels *Alias* in den WWW-Dokumentenbaum eingebunden, so muss auch für diese mit einer entsprechenden *Directory*-Direktive der Zugriff erlaubt werden.

Ist kein Datentransfer von Clients zum Webserver vorgesehen, so sollten PUT-Requests mittels einer entsprechenden *Limit*-Direktive verboten werden.

Optionen für Verzeichniszugriff

Für den Zugriff auf die Verzeichnisse im WWW-Dateibaum existieren eine Reihe von Optionen, die mit der Direktive *Options* innerhalb eines <*Directory*> Abschnitts festgelegt werden können. Wie oben beschrieben sollten per Default alle Optionen mittels *Options None* ausgeschaltet werden und nur in solchen Bereichen, in denen bestimmte Funktionalitäten benötigt werden, sollten diese aktiviert werden. Beispiele:

- Die Erstellung automatischer Listings durch den Webserver, falls kein Verzeichnisindex als HTML-Datei verfügbar ist, wird durch die Option *Indexes* gesteuert. Sie sollte generell abgeschaltet werden (siehe oben: *Options none*) und nur in den Teilbereichen aktiviert werden, wo diese Funktionalität explizit benötigt wird.
- Mit der Option *FollowSymLinks* wird festgelegt, ob der Server symbolische Links im Filesystem verfolgt. Diese Option sollte ebenfalls normalerweise deaktiviert bleiben und nur in den Teilbereichen aktiviert werden, wo diese Funktionalität explizit benötigt wird.
- Mit der Option *Includes* kann festgelegt werden, dass der Server im betreffenden Verzeichnis *Server-Side Includes* auswertet. *Server-Side Includes* sind eine Möglichkeit zur "Modularisierung" von Webseiten, die damit vom Server dynamisch zusammengesetzt werden können. Da *Server-Side-Includes* bei unsachgemäßer Anwendung Sicherheitsprobleme aufweisen sollte diese Option normalerweise deaktiviert bleiben. Eine etwas sicherere Alternative ist die Option *IncludesNOEXEC*, bei der keine Programme ausgeführt werden, die eventuell in Include-Dateien enthalten sind.

.htaccess-Dateien

.htaccess-Dateien bieten die Möglichkeit, innerhalb eines Verzeichnisses im WWW-Dateibaum Einstellungen für dieses Verzeichnis festzulegen. Diese Einstellungen überschreiben gegebenenfalls solche, die in der Datei *httpd.conf* getroffen wurden.

Das Überschreiben der Konfigurationseinstellungen durch Einträge in den *.htaccess*-Dateien sollte per Default abgeschaltet sein und nur bei Bedarf für einzelne Bereiche freigeschaltet werden. Welche Einstellungen in *.htaccess*-Dateien verändert werden dürfen, wird mit der Option *AllowOverride* festgelegt (siehe oben: *AllowOverride None*). Da *.htaccess*-Dateien im WWW-Bereich stehen und eventuell sensitive Informationen enthalten, sollte außerdem mit der Einstellung

```
<Files ~ "^\.ht">
Order allow,deny
Deny from all
<Files>
```

festgelegt werden, dass Files, deren Name mit "*.ht*" beginnt, nicht ausgeliefert werden dürfen.

Einstellungen für URL-Bereiche

Neben der Zugriffssteuerung auf Verzeichnisse kann dies mit der <*Location*> -Direktive auch für bestimmte "URL-Bereiche" auf dem Webserver geschehen. Dies ist beispielsweise relevant, wenn ein Verzeichnis von außerhalb des *DocumentRoot*-Directories mit einer *Alias*-Direktive in den WWW-Dokumentenbaum eingebunden wurde oder wenn bestimmte URL-Bereiche nicht direkt einem Verzeichnis im Dateisystem entsprechen. Dies kann beispielsweise bei dynamisch erzeugten Webseiten der Fall sein.

Module

Bei der Installation einer Binärversion des Apache-Webservers werden eine Anzahl von Erweiterungsmodulen standardmäßig mit installiert. Das Laden eines Moduls erfolgt durch die Direktive *LoadModule*. So würde beispielsweise die Zeile

LoadModule access_module modules/mod_access.so

das Modul *mod_access* laden. Prinzipiell sollten nur diejenigen Module im Server aktiviert werden, die für den Betrieb des Webservers benötigt werden. Der Grund hierfür ist der gleiche wie bei der Absicherung des Betriebssystems: Systeme sollten stets möglichst minimal konfiguriert werden, um so das Risiko des Vorhandenseins einer Sicherheitslücke zu minimieren.

Die Module *mod_status* und *mod_info* sollten nach Möglichkeit nicht geladen werden, da bei Verwendung dieser Module der Apache-Webserver eine Reihe von Statusinformationen über den Webserver über die HTTP-Schnittstelle bereitstellt. Wird der Zugriff auf die Statusinformationen aus wichtigen Gründen benötigt, so sollte zumindest eine sehr restriktive Zugangsbeschränkung über entsprechende <*Location*> Direktiven vorgenommen werden.

Die Auswahl der Module sollte dokumentiert werden, damit zu jeder Zeit nachvollzogen werden kann, welche Module zu welchem Zweck gebraucht werden.

Performance-Einstellungen

Der Apache-Webserver erlaubt verschiedene Einstellungen, mit denen die Performance des Webservers beeinflusst werden kann. Diese Einstellungen hängen teilweise vom gewählten MPM und Betriebssystem ab.

Für diese Einstellungen enthält die Standardkonfiguration Vorgabewerte, die in vielen Fällen ausreichend sind. In der Dokumentation werden die einzelnen Direktiven erläutert. Von den Vorgabewerten sollte nur dann abgewichen werden, wenn die Auswirkungen absehbar sind, idealerweise sollten Änderungen auf einem Testsystem überprüft werden, bevor sie auf einem Produktivsystem übernommen werden.

Generell sollte bei Änderungen an systemnahen Einstellungen, die auf das Zusammenspiel zwischen dem Apache-Webserver und dem unterliegenden Betriebssystem Einfluss haben, eher konservativ vorgegangen werden.

Ergänzende Kontrollfragen:

- Welche Information wird als ServerToken zurückgeliefert?

- Welche Adresse wird als ServerAdmin zurückgeliefert? Ist dafür eine entsprechend Funktions-E-Mail-Adresse angelegt und werden Mails an diese Adresse regelmäßig ausgewertet?
- Welche Module werden geladen? Ist dokumentiert, zu welchem Zweck?
- Wie sind die Optionen für das WWW-Verzeichnis gesetzt?
- In welchen Abständen werden die Logfiles archiviert?

M 4.195 Konfiguration der Zugriffssteuerung beim Apache-Webserver

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Für die Einrichtung von Zugriffsbeschränkungen auf den Apache-Webserver oder einzelne Bereiche des Webangebots gibt es beim Apache-Webserver verschiedene Möglichkeiten, die teilweise bereits im Webserver-Programm selbst implementiert sind, teilweise über Erweiterungsmodule eingebunden werden können. Zwei verbreitete Arten der Zugriffssteuerung sind die Beschränkung des Zugriffs auf bestimmte IP-Adressbereiche oder Domains (beispielsweise im Intranet) und die Abfrage eines Benutzernamens und eines Passworts beim Zugriff auf bestimmte Ressourcen (siehe auch M 4.176 *Auswahl einer Authentisierungsmethode für Webangebote*).

Beschränkungen auf IP-Adressen und Domains

Das Modul *mod_access* bietet die Möglichkeit, den Zugriff auf den Webserver oder auf Teilbereiche des Webangebots auf bestimmte IP-Adressen oder Domains zu beschränken. Beispielsweise würde durch

```
<Directory /var/www/htdocs/Abteilung1 >
Order Deny,Allow
Deny from all
Allow from 10.0.0.0/24
</Directory>
```

der Zugriff auf das Verzeichnis *Abteilung1* nur solchen Clients erlaubt, die eine IP-Adresse der Form 10.0.0.x haben. Analog kann der Zugriff mittels

```
Allow from bund.de
```

für alle Anfragen aus der Domain *bund.de* erlaubt werden. Diese Art von Zugriffsbeschränkungen bieten allerdings nur einen schwachen Schutz vor unbefugtem Zugriff, da sie durch *IP-Spoofing* oder *DNS-Spoofing* relativ leicht umgangen werden können.

Zusätzlich bietet *mod_access* weitere Möglichkeiten für Zugriffsbeschränkungen, etwa basierend auf bestimmten HTTP-Header-Zeilen. Da HTTP-Header aber sehr leicht mitgelesen oder gefälscht werden können, eignet sich dies nur sehr beschränkt für Zugriffssteuerung.

Benutzernamen und Passwörter

Die HTTP-Basic-Authentisierung ist beim Apache-Webserver direkt im "Kern" des Webserver-Programms implementiert. Dabei wird beispielsweise der Zugriff auf ein Verzeichnis folgendermaßen passwortgeschützt:

```
<Directory /var/www/htdocs/vertraulich >
 AuthType Basic
 AuthName "Interne Dokumente"
 AuthUserFile /var/auth/wwwusers
 Require valid-user
</Directory>
```

In diesem Fall muss ein Benutzer, der auf dieses Verzeichnis zugreifen will, einen Benutzernamen und ein Passwort angeben, die dann mit den Benutzername-Passwort-Kombinationen in der Datei */var/auth/wwwusers* verglichen werden. Der Zugriff wird für alle gültigen Kombinationen gestattet. Alternativ kann der Zugriff mit der Direktive

Require user Mitarbeiter

der Zugriff nur für den Benutzer "Mitarbeiter" gestattet werden.

htpasswd-Dateien außerhalb des WWW-Dateibaums speichern

Dabei ist die Datei */var/auth/wwwusers* eine Datei im *.htpasswd*-Format, die ähnlich einer normalen passwd-Datei unter Unix aufgebaut ist. *htpasswd*-Dateien können mit dem Programm *htpasswd* erzeugt und gepflegt werden, das zum Apache-Paket gehört. Sie enthalten Usernamen und die Hashwerte der Passwörter. Aus diesem Grund dürfen *.htpasswd*-Dateien niemals innerhalb des WWW-Dateibaums gespeichert werden, da sie sonst von Angreifern heruntergeladen werden könnten. Offline ist es dann leicht, die Passwörter zu knacken, da die Passwörter nur mit dem normalen, veralteten Unix *crypt*-Verfahren gehasht werden.

Neben der Zugriffskontrolle auf Verzeichnisse können analog auch URL-Bereiche mit der <*Location*> Direktive geschützt werden.

Weitere Authentisierungsmechanismen sind beim Apache-Webserver über Erweiterungsmodule realisiert. Dies sind unter anderem:

- *mod_auth_ldap* und *mod_auth_dbm*: Diese Module erlauben die Speicherung von Benutzernamen und Passwörtern für die HTTP-Basic-Authentisierung auf einem LDAP-Server bzw. in einer DBM-Datei.
- *mod_auth_digest:* Dieses Modul implementiert das Digest-Authentisierungsverfahren.
- *mod_access*: Dieses Modul realisiert die Zugriffssteuerung auf der Basis von IP-Adressen, Client-Hostnamen und anhand einiger anderer Kriterien.
- *mod_auth_anon*: Dieses Modul erlaubt eine Zugriffsbeschränkung analog zum anonymen Zugriff auf ftp-Server via HTTP-Basic. Dabei wird ein fest vorgegebener Benutzername abgefragt (etwa "*anonymous*") und der Besucher muss eine E-Mailadresse als Passwort angeben.

Nur schwacher Schutz!

Da HTTP ein Klartext-Protokoll ist, bietet die Benutzerauthentisierung über HTTP-Basic nur sehr schwachen Schutz vor unbefugtem Zugriff. Daher dürfen beispielsweise keinesfalls solche Benutzernamen und Passwörter zur Authentisierung über HTTP-Basic verwendet werden, die auch für die Anmeldung an internen Systemen benutzt werden.

Sollen (etwa zur Realisierung einer Art "Single-Sign-On") Benutzernamen und Passwörter anderer Systeme für die Benutzerauthentisierung beim Apache-Webserver verwendet werden, so muss die Übertragung durch die Verwendung von SSL (siehe auch M 5.107 *Verwendung von SSL im Apache-Webserver*) gesichert werden.

Einsatz von SSL

Mit dem Modul *mod_ssl* kann SSL beim Apache-Webserver eingesetzt werden. Neben der Verschlüsselung der Verbindung und der Authentisierung des Servers gegenüber dem Client mittels Server-Zertifikat bietet *mod_ssl* auch die Möglichkeit, mittels Client-Zertifikaten Zugriffsbeschränkungen zu implementieren. Die Apache-Dokumentation enthält eine größere Zahl gut dokumentierter Beispiele für solche Konfigurationen.

Ergänzende Kontrollfragen:

- Sind die Möglichkeiten und Einschränkungen der verschiedenen Methoden zur Zugriffssteuerung bekannt?

M 4.196 Sicherer Betrieb eines Apache-Webservers

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um die Sicherheit eines Apache-Webservers auch im Betrieb aufrecht zu erhalten, genügt es nicht, eine sichere Anfangskonfiguration zu erzeugen. Vielmehr muss regelmäßig eine Reihe von Maßnahmen durchgeführt werden, um eventuelle Probleme rechtzeitig zu entdecken. Beim Betrieb eines Apache-Webservers sollten insbesondere folgende Aspekte berücksichtigt werden:

Konfigurationsänderungen dokumentieren

Änderungen an der Konfiguration müssen sorgfältig dokumentiert werden, so dass zu jeder Zeit nachvollzogen werden kann, wer aus welchem Grund was geändert hat. Für die Änderungen an den Konfigurationsdateien sollte ein Revisionskontrollprogramm (unter Unix genügt dazu beispielsweise *RCS*) eingesetzt werden, das es erlaubt, jederzeit auch einen früheren Stand der Konfiguration wieder herzustellen.

Syntax prüfen

Nach jeder Änderung an der Datei httpd.conf muss zunächst mit dem Befehl apachectl configtest geprüft werden, ob die Syntax der Konfigurationsdatei korrekt ist. Syntaxfehler in der Konfigurationsdatei können sonst dazu führen, dass der Server nicht neu startet.

Zugriffsberechtigungen und Integrität von Programmen und Skripten überwachen

Die Zugriffsberechtigungen im Dateisystem des Webservers und die vergebenen Zugriffsberechtigungen für Inhalte des Webservers sollten regelmäßig überprüft werden. Insbesondere sollte dies nach Software-Updates oder Konfigurationsänderungen geschehen. Für die Dateien des Servers selbst (beispielsweise das Serverprogramm *httpd,* das Kontrollskript *apachectl* und die Erweiterungsmodule) sollten Prüfsummen angelegt und regelmäßig überprüft werden.

Falls auf dem Webserver Server-Side-Includes, cgi-Skripte oder andere Server-Erweiterungen eingesetzt werden, sollten für alle Dateien, die ausführbaren Code enthalten, ebenfalls Prüfsummen angelegt und regelmäßig überprüft werden. Bei Server-Erweiterungen wie PHP oder Java-Server-Pages, bei denen ausführbare Bestandteile und normale Inhalte vermischt auftreten, kann dies einen erheblichen Aufwand verursachen.

Die Maßnahmen zum Schutz von Authentisierungsdaten sollten regelmäßig überprüft werden. Dies betrifft beispielsweise Zugriffsrechte auf *.htaccess*-Dateien und Passwortdateien sowie gegebenenfalls auf Client-Zertifikate.

SSL-Zertifikate und CRLs

Sofern SSL genutzt wird, müssen regelmäßig die Sicherheitsvorkehrungen zum Schutz der privaten Schlüssel des Webservers überprüft werden (siehe M 5.107 *Verwendung von SSL im Apache-Webserver*). Ebenso muss darauf geachtet werden, dass rechtzeitig vor Ablauf der Gültigkeitsdauer des Server-Zertifikats ein neues Zertifikat beschafft wird.

Sofern CRLs (Certificate Revocation Lists) genutzt werden, müssen diese in regelmäßigen Abständen aktualisiert werden.

Auf dem Laufenden bleiben!

Die Administratoren müssen sich über aktuelle Sicherheitslücken in der eingesetzten Software frühzeitig informieren (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*). Informationen zum Apache-Webserver finden sich in der Mailingliste zum Apache-Webserver und auf den

Webseiten der Apache Software Foundation (*www.apache.org*).

Protokolldateien auswerten

Die Protokolldateien des Apache-Webservers sowie des unterliegenden Betriebssystems sollten regelmäßig ausgewertet werden. Unregelmäßigkeiten in den Webserver-Logdateien, die Hinweise auf mögliche Probleme mit dem Webserver sein können, sind beispielsweise:

- Eine Häufung von Anfragen, die einen HTTP-Fehler erzeugen, beispielsweise "404 - Datei nicht gefunden" oder "403 - Zugriff verweigert".
- Eine Häufung von Anfragen von einer bestimmten IP-Adresse.
- Eine Häufung von Anfragen nach einer bestimmten Datei.

Meist sind solche Unregelmäßigkeiten nicht unbedingt Hinweise auf eine Kompromittierung des Servers, sondern eher auf fehlerhafte Einstellungen.

Zum sicheren Betrieb gehören weiter auch regelmäßig durchzuführende Maßnahmen der Datensicherung und der Notfallvorsorge (siehe auch M 6.89 *Notfallvorsorge für einen Apache-Webserver*).

Ergänzende Kontrollfragen:

- Werden die Zugriffsberechtigungen auf Bereiche des Webservers regelmäßig überprüft?
- Werden die Protokolldateien des Apache-Webservers regelmäßig überprüft?

M 4.197 Servererweiterungen für dynamische Webseiten beim Apache-Webserver

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der Apache-Webserver bietet viele Möglichkeiten für die Realisierung dynamischer Webseiten. Diese sind über Erweiterungsmodule realisiert. In der Quelltext-Distribution des Apache-Webservers sind beispielsweise folgende Module enthalten:

- *mod_cgi* für die Ausführung von cgi-Programmen,
- *mod_include* für die Realisierung von Server-Side-Includes (SSI), sowie
- *mod_isapi* für die Ausführung von ISAPI-Erweiterungen unter Windows.

Bei der Ausführung von Programmen über die Schnittstellen CGI, SSI und ISAPI werden diese prinzipiell mit den Berechtigungen des Apache-Webservers ausgeführt. Dies führt zu einer Reihe von Problemen, da der Apache-Webserver mit möglichst wenig Berechtigungen ausgestattet sein sollte. Um diese grundsätzliche Einschränkung zu umgehen, existiert das Modul *mod_suexec*, das die Ausführung von Programmen unter einer anderen Benutzerkennung als der des Apache-Webservers erlaubt.

Neben den Modulen aus der Apache-Distribution selbst existiert eine große Zahl weiterer Module, mit denen sich dynamische Webseiten realisieren lassen. Teilweise werden diese Module von Projekten entwickelt, die ebenfalls unter dem Dach der Apache Software Foundation (ASF) arbeiten, teilweise von unabhängigen Projekten oder kommerziellen Anbietern. Einige verbreitete Beispiele sind

- *mod_perl* für dynamische Webseiten mit Perl (von der ASF),
- *mod_jk* für Java Servlets und Java-Server-Pages (vom Jakarta-Projekt der ASF) und
- *mod_php* für dynamische Webseiten mit PHP.

Da sich Arbeitsweise, Möglichkeiten und Probleme der einzelnen Module stark unterscheiden, kann im Rahmen dieser Maßnahme nicht auf alle Aspekte eingegangen werden, sondern es werden lediglich einige grundlegende Hinweise gegeben. Administratoren und Entwickler dynamischer Webseiten müssen sich daher in jedem Fall gründlich mit den Sicherheitsaspekten des jeweils gewählten Erweiterungsmoduls beschäftigen.

Prinzipiell müssen die Dateien des jeweiligen Erweiterungsmoduls genau so vor unbefugtem Zugriff geschützt werden, wie die Dateien des Apache-Webservers selbst. Dies gilt sowohl für die ausführbaren Dateien, die meist im Bibliotheksverzeichnis des Apache-Webservers abgelegt sind, als auch für etwa vorhandene Konfigurationsdateien wie beispielsweise die Datei *php.ini* bei der Verwendung von *mod_php*.

Für Programme, die über den cgi-Mechanismus ausgeführt werden, kann in der Datei *httpd.conf* mit der Direktive *ScriptAlias* ein Verzeichnis angegeben werden, in dem die Programme vom Webserver gesucht werden. Dieses Ver-

zeichnis sollte in jedem Fall außerhalb des normalen WWW-Dokumentenbaums gewählt werden. Beispiel:

Script-Alias /cgi-bin /usr/local/apache/cgi.

Dateien innerhalb des WWW-Dokumentenbaums sollten grundsätzlich (zumindest für den Apache-Webserver) nicht ausführbar sein, das heisst mit den Mitteln des jeweiligen Betriebssystems sollte für den Benutzeraccount des Apache-Webserver das Ausführungsrecht für diese Dateien entfernt werden.

Grundregel: Never trust the user!

Die Grundregel für die Entwicklung dynamischer Webseiten, bei denen Informationen verarbeitet werden, die von außen über den Webserver an das jeweilige Programm übergeben wurden, ist, dass diese Eingaben niemals ungefiltert im Programm verwendet werden dürfen, sondern stets vor ihrer Verwendung mit einer geeigneten Funktion "bereinigt" werden sollten. Dies muss bei der Programmierung stets berücksichtigt werden.

Die Skriptsprache *Perl* bietet darüber hinaus den sogenannten *taint*-Modus, in dem Daten, die von außen kommen, für bestimmte Funktionsaufrufe nicht zugelassen sind. Werden cgi-Skripte in Perl geschrieben, so sollten sie stets im *taint*-Modus ausgeführt werden.

Diese Regel gilt selbst dann, wenn es sich nicht um Eingaben handelt, die Benutzer direkt in ein Eingabeformular eingeben, sondern nur um solche Informationen, die über Auswahllisten übergeben wurden. Nicht einmal Eingaben, die bei der Erzeugung der "absendenden" Webseite vom Programm selbst als "versteckte Parameter" in die Webseite eingebettet wurden, dürfen direkt übernommen werden. Da HTML-Seiten auf der Client-Seite im Klartext vorliegen und über das Klartext-Protokoll HTTP übertragen werden, können alle Daten und Eingaben entweder auf dem Client-Rechner oder bei der Übertragung beliebig manipuliert werden.

Dynamische Webseiten werden meist so realisiert, dass in einer Datei HTML-Code und Anweisungen der jeweils verwendeten Programmiersprache vermischt sind. Bei der Verarbeitung einer Anfrage werden dann die Anweisungen vom jeweiligen Modul ausgeführt und die Ausgaben der betreffenden Programmfunktionen in die HTML-Seite eingebettet, die an den Client geschickt wird. Eine andere Möglichkeit ist es, dass ein weiteres Programm ausgeführt wird, welches als Ausgabe eine vollständige HTML-Seite erzeugt.

Beim Design dynamischer Webseiten sollte darauf geachtet werden, dass Programmcode und HTML-Code möglichst gut voneinander getrennt werden. Sofern das verwendete Modul diese Möglichkeit bietet sollte Programmcode am besten gar nicht direkt in der HTML-Seite enthalten sein, sondern nur über einen Verweis auf eine entsprechende Datei eingebettet werden. Dies erlaubt eine bessere Rollentrennung zwischen dem graphischen Design der Webseiten und der Programmierung.

Keine Zugangsdaten im WWW-Bereich

In keiner Datei, die sich im "öffentlich zugänglichen" Bereich des Webservers befindet, dürfen in "Skript-Komponenten" Zugangsdaten für den Zugriff auf Datenbanken oder ähnliches stehen. Wird für die Realisierung von dynamischen Seiten der Zugriff auf Datenbanken benötigt, so muss dies so implementiert werden, dass Zugangsdaten außerhalb des WWW-Dokumentenbaums vorgehalten werden.

Als zusätzlicher Schutz sollte mit entsprechenden Apache-Direktiven dafür gesorgt werden, dass Dateien, die typischerweise Konfigurationsdateien sind, nicht ausgeliefert werden. Beispielsweise kann mit

```
<FilesMatch "*\.(conf|cnf)$">
 Order Deny,Allow
 Deny from all
</FilesMatch>
```

die Auslieferung von Dateien mit den Endungen *.conf* und *.cnf* verboten werden. Die Liste der so verbotenen Dateitypen sollte jeweils an die konkreten Gegebenheiten angepasst werden.

Ergänzende Kontrollfragen:

- Sind die Administratoren und Anwendungsentwickler mit den Sicherheitsaspekten der eingesetzten Programmiersprache vertraut?
- In welchem Verzeichnis liegen cgi-Skripte?

M 4.198 Installation eines Apache-Webservers in einem chroot-Käfig

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Zur Erhöhung der Systemsicherheit kann der Apache-Webserver in einem sogenannten chroot-Käfig installiert werden. Dieser Schritt sollte insbesondere dann in Betracht gezogen werden, wenn der Apache-Webserver ein öffentlich zugängliches Webangebot beherbergt. Durch den Systemaufruf *chroot()* wird unter Unix der Zugriff eines bestimmten Programms auf einen Teil des Dateibaums beschränkt. Dies geschieht dadurch, dass alle Zugriffe, die dieses Programm (und die von ihm aufgerufenen Programme) auf das Dateisystem durchführt, relativ zu dem Verzeichnis erfolgen, das beim Aufruf der Funktion *chroot()* angegeben wurde. Dieses Verzeichnis wird so zur Wurzel eines virtuellen Dateibaums, der als *chroot-Käfig* oder *chroot jail* bezeichnet wird.

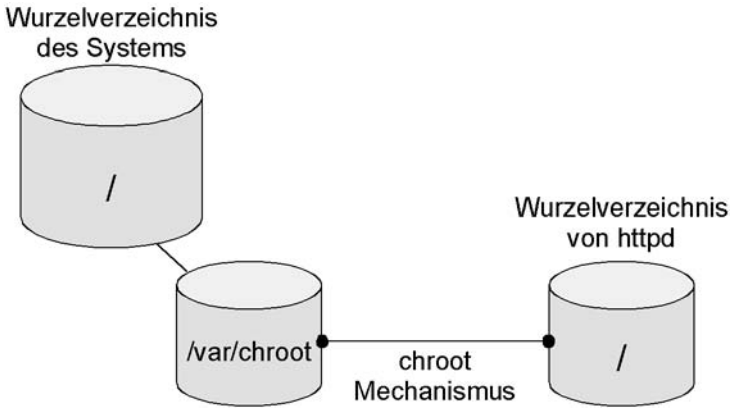


Abbildung: Wurzelverzeichnis

Neben dem Systemaufruf *chroot()* steht auch ein ausführbares Programm gleichen Namens zur Verfügung, das zum Start beliebiger Programme (und damit auch des Apache-Webservers) in einem solchen chroot-Käfig genutzt werden kann. Wenn es beispielsweise einem Angreifer gelingen würde, eigenen Programmcode im Prozessraum des Webservers auszuführen, so würde in diesem Fall der unmittelbare Schaden zunächst dadurch begrenzt werden, dass der Angreifer keinen direkten Zugriff auf das eigentliche Betriebssystem erhält. Zwar existieren Möglichkeiten, aus einem chroot-Käfig auszubrechen, aber da ein Angreifer erst einmal erkennen muss, dass er sich in einem chroot-Käfig befindet und dann auch noch aus diesem ausbrechen muss, wird auf jeden Fall ein Angriff verzögert. Während dieser Zeit kann eventuell der Angriff erkannt und Gegenmaßnahmen eingeleitet werden.

Der chroot-Käfig muss Kopien aller Dateien enthalten, die zur Ausführung des Apache-Webservers (sowie etwaiger Zusatzprogramme, CGI-Skripte und ähnlichem) notwendig sind. Welche Dateien dies sind, hängt von einer Vielzahl von Faktoren ab (z. B. Release-Stand des Betriebssystems oder ver

wendeter Hardware-Plattform). Daher kann an dieser Stelle keine Mindestkonfiguration angegeben werden, sondern diese muss anhand der vorhandenen Dokumentation und der konkreten Anforderungen im Einzelfall zusammengestellt werden.

Wird in Betracht gezogen, den Apache-Webserver in einem chroot-Käfig zu installieren, so muss auf jeden Fall ausreichend Zeit für Planung und Tests vorgesehen werden. Bei der Installation muss dokumentiert werden,

- welches das Wurzelverzeichnis des chroot-Käfigs ist und
- welche Betriebssystemkomponenten im chroot-Käfig zur Verfügung gestellt werden.

Insbesondere müssen einige *Device Files* im chroot-Käfig angelegt werden, außerdem werden entsprechend "abgespeckte" Versionen der Dateien */etc/passwd* und */etc/group* benötigt. Aus diesen Dateien sollten alle nicht benötigten Einträge bis auf den Benutzer bzw. die Gruppe entfernt werden, unter denen der Apache-Webserver laufen soll. Je nach Betriebssystem können noch andere Einträge erforderlich sein.

Die Zugriffsberechtigungen für das Wurzelverzeichnis für den chroot-Käfig sollten so restriktiv wie möglich eingestellt werden.

Die Einrichtung eines chroot-Käfigs ist relativ aufwendig. Für öffentlich zugängliche Webangebote kann sie jedoch die Sicherheit erhöhen.

M 4.199 Vermeidung gefährlicher Dateiformate

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Benutzer, Administrator

E-Mail ist mittlerweile der wichtigste Übertragungsweg für Computer-Viren und Würmer. Eine rein textbasierte E-Mail ohne Anhänge ist dabei ungefährlich. Gefährlich wird es erst, wenn E-Mail-Anhänge ausgeführt werden oder die E-Mail HTML-basiert ist (siehe unten). Prinzipiell können E-Mails Anhänge in beliebiger Art und Menge beigefügt werden. Durch ein Zuviel an Anhängen kann die Verfügbarkeit eines E-Mail-Clients oder des E-Mail-Servers beeinträchtigt werden (siehe G 5.75 *Überlastung durch eingehende E-Mails* bzw. G 5.76 *Mailbomben*). Die größere Gefahr sind aber Anhänge, die ausführbaren Code enthalten und damit ungeahnte Nebeneffekte auslösen können.

Attachments nicht automatisch öffnen

Der E-Mail-Client sollte so eingestellt sein, dass Anhänge nicht versehentlich gestartet werden können, sondern das Programm vor der Ausführung warnt bzw. zumindest nachfragt, ob die Datei geöffnet werden soll. Das Betriebssystem bzw. der E-Mail-Client sollte außerdem so eingerichtet sein, dass Dateien zunächst nur in Viewern oder anderen Darstellungsprogrammen angezeigt werden, die eventuell in den Dateien enthaltenen Programmcode, wie Makros oder Skripte, nicht ausführen.

Dateien in möglichst "ungefährlichen" Formaten weitergeben

Vor dem Absenden einer E-Mail sollte sich jeder überlegen, ob es wirklich nötig ist, ein Attachment anzuhängen, oder ob die Informationen nicht genauso gut als Text in die E-Mail direkt eingefügt werden kann. Ansonsten sollten Dateien in möglichst "ungefährlichen" Formaten weitergegeben werden, also z. B. sollten Textdokumente statt als DOC- oder SDW-Datei möglichst nur im RTF-Format nach außen gegeben werden (siehe auch M 4.134 *Wahl geeigneter Datenformate*). Wenn sich die Versendung von Dateien in "gefährlichen" Formaten nicht vermeiden lässt, sollte überlegt werden, den Empfänger mit einer kurzen E-Mail darauf hinzuweisen, dass als nächstes eine E-Mail mit solchen Attachments zu erwarten ist.

Empfehlungen

Für den Umgang mit Dateiformaten, die als potentiell problematisch eingeschätzt werden, können verschiedene Regelungen getroffen werden. Wichtig ist aber auf jeden Fall, dass alle Betroffenen sich der Problematik bewusst sind und entsprechend vorsichtig mit diesen Dateiformaten umgehen.

Die restriktivste Form ist es, das Öffnen aller als problematisch eingestuften Dateiformate zu verbieten bzw. diese am E-Mail-Gateway herauszufiltern. Dies führt allerdings erfahrungsgemäß zu großen Akzeptanzproblemen seitens der Kunden und der Mitarbeiter. Besser ist es im allgemeinen, einerseits die Mitarbeiter für die Problematik zu sensibilisieren und zum Mitdenken anzuregen und sie andererseits technisch zu unterstützen, indem die Gefährdungspotentiale durch entsprechende Konfiguration und Sicherheitswerkzeuge minimiert werden (siehe auch M 2.224 *Vorbeugung gegen Trojanische Pferde*, M 5.69 *Schutz vor aktiven Inhalten*).

Im folgenden werden einige Einschätzungen verschiedener Dateiformate gegeben. Diese können sich allerdings jederzeit ändern, wenn z. B. ein Hersteller

seinem Produkt neue Features hinzufügt, die ungeplante Nebenwirkungen haben, bzw. ein Tüftler solche Nebenwirkungen herausfindet.

- Als weitgehend harmlos gelten bisher ASCII-, GIF-, JPEG-formatierte Dateien.

weitgehend harmlos

- Als möglicherweise gefährlich sollten die folgenden Dateiformate behandelt werden: alle Dateiformate von Office-Paketen wie Microsoft Office, Star Office oder Open Office mit integrierter Makrosprache, z. B. Word, Excel, Powerpoint (.DOC, .XLS, .PPT, SDW, SXW usw.). Besonders kritisch sind alle ausführbaren Programme (wie .COM, .EXE, .PIF) oder Skript-Sprachen (.VBS, .JS, .BAT unter Windows, ebenso wie Perl- oder Shellskripte unter Unix), Registrierungsdateien (.REG) sowie Bildschirmschoner (.SCR).

  Vorsichtshalber sollte für alle diese Dateitypen eine "ungefährliche" Standardapplikation festgelegt werden, mit der diese zwar geöffnet werden, innerhalb deren aber eventuelle Computer-Viren keinen Schaden auslösen können. Beispielsweise sollten Dateitypen wie *.VBS, *.JS oder *.BAT grundsätzlich mit einem einfachen, nicht makrofähigen Texteditor geöffnet werden.

  Windows-Betriebssysteme sollten außerdem so konfiguriert sein, dass bei Registrierungsdateien (.REG) als Standardvorgang *Bearbeiten* statt *Zusammenführen* eingestellt ist. Dadurch wird die Datei zunächst in einem Editor dargestellt und nicht der Registrierungsdatenbank hinzugefügt, wenn sie aktiviert wird.

möglicherweise gefährlich

- Mit Zusatzmaßnahmen als vertretbar angesehen werden können: HTML, wenn ein JavaScript-Filter oder andere Sicherheitsvorkehrungen eingesetzt werden, RTF (mit COM-Object-Filter), ZIP (hier sollten die Benutzer allerdings gewarnt werden, dass die enthaltenen Dateien problematisch sein können), PDF (dabei ist darauf zu achten, dass der PDF-Reader auf dem Endgerät als Standard installiert ist und nicht Adobe Acrobat).

Zusatzmaßnahmen empfohlen

Bunt, aber gefährlich!

Immer mehr E-Mails sind heutzutage auch HTML-formatiert. Dies ist einerseits oft lästig, weil nicht alle E-Mail-Clients dieses Format anzeigen können. Andererseits kann dies aber auch dazu führen, dass bereits bei der Anzeige solcher E-Mails auf dem Client ungewollte Aktionen ausgelöst werden, da HTML-Mails eingebetteten JavaScript- oder VisualBasic-Skript-Code enthalten können.

Durch Kombination verschiedener Sicherheitslücken in E-Mail-Clients und Browsern ist es in der Vergangenheit immer wieder zu Sicherheitsproblemen mit HTML-formatierten E-Mails gekommen (siehe auch G 5.110 *Web Bugs*). Ein Beispiel hierfür findet sich unter anderem im CERT-Advisory CA-2001-06 (unter *http://www.cert.org/advisories/CA-2001-06.html*).

HTML-formatierte E-Mails

Generell sollten möglichst keine HTML-formatierten E-Mails oder solche mit aktiven Inhalten zu versenden. Außerdem sollte die Möglichkeit überprüft werden, in eingehenden E-Mails enthaltene aktive Inhalte herauszufiltern, beispielsweise an der Firewall. Weiterhin sollten E-Mail-Clients gewählt werden, bei denen HTML-formatierte E-Mails als solche zu erkennen sind, damit der Benutzer diese nicht unbewusst öffnet.

Generell sollte eine Vorgabe innerhalb einer Organisation zum Umgang mit HTML-formatierten E-Mails erstellt werden. Beim Empfang von HTML-formatierten E-Mails sollte festgelegt werden, ob diese

- unverändert an die Benutzer weitergeleitet und die Benutzer für den verantwortungsvollen und vorsichtigen Umgang mit solchen E-Mails geschult und sensibilisiert werden,
- mit Hilfe von serverseitigen Tools in ein reines Textformat umgewandelt und danach mit einem entsprechenden Hinweis an die Benutzer weitergeleitet werden (dabei können allerdings Informationen verloren gehen),
- nicht direkt an die Benutzer weitergeleitet werden, sondern an einen besonderen Arbeitsplatz, wo sie mit besonderen Sicherheitsvorkehrungen vom Empfänger eingesehen werden können (je nach E-Mail-Aufkommen kann dies allerdings einen nicht akzeptablen Aufwand mit sich bringen).

Grundsätzlich sollten alle Benutzer für diese Problematik sensibilisiert sein.

Ergänzende Kontrollfragen:

- Ist der Umgang mit Dateiformaten, die als problematisch eingeschätzt werden, geregelt?
- Wissen alle Benutzer, wie mit problematischen Attachments umzugehen ist?

M 4.200 Umgang mit USB-Speichermedien

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Über die USB-Schnittstelle lassen sich eine Vielzahl von Zusatzgeräten an PCs anschließen. Beispiele sind Festplatten, CD/DVD-Brenner und Memory-Sticks. USB-Memory-Sticks bestehen aus einem USB-Stecker und einem Speicherchip. Trotz großer Speicherkapazität sind sie so handlich, dass sie beispielsweise in Form von Schlüsselanhängern hergestellt werden und in jede Hosentasche passen. Die Preise sind so stark gefallen, dass USB-Sticks auch im Privatbereich Disketten überflüssig machen können. In modernen Betriebssystemen sind die Treiber für USB-Massenspeichergeräte bereits integriert, so dass zum Betrieb keine Softwareinstallation mehr notwendig ist. Im Allgemeinen bezieht sich diese Maßnahme nicht ausschließlich auf USB-Speichermedien, sondern generell auf alle USB-Geräte, die Daten speichern können. Unter anderem können auch USB-Drucker und USB-Kameras zum Speichern der Daten "missbraucht" werden. Dies gilt insbesondere für "intelligente" USB-Geräte wie PDAs, die jede beliebige USB-Identität annehmen können, wenn sie mit spezieller Software ausgestattet sind.

Ähnlich wie über Disketten können über USB-Speichermedien unkontrolliert Informationen und Programme ein- oder ausgelesen werden. Daher ist mit USB-Speichermedien generell genauso wie mit herkömmlichen Speichermedien umzugehen. Der Zugriff auf Diskettenlaufwerke kann relativ einfach verhindert werden (siehe M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*). Der Betrieb von USB-Speichermedien lässt sich dagegen nur sehr schwer verhindern, wenn die USB-Schnittstelle für andere Geräte genutzt wird. So werden beispielsweise Notebooks ausgeliefert, die zum Anschluss einer Maus nur die USB-Schnittstelle zur Verfügung stellen. Deswegen ist es meist nicht sinnvoll, ein "USB-Schloss" zu verwenden oder die Schnittstelle durch andere mechanische Maßnahmen zu deaktivieren. Die Nutzung von Schnittstellen sollte daher durch entsprechende Rechtevergabe auf Ebene des Betriebssystems oder mit Hilfe von Zusatzprogrammen geregelt werden. Alternativ kann das Hinzufügen von Geräten überwacht werden. Beim Anschluss von Datenspeichern an externen Schnittstellen werden oftmals vom Betriebssystem Treiber bzw. Kernelmodule geladen oder Einträge in Konfigurationsdateien (wie der Windows-Registry) erzeugt, die detektiert werden können. Nachdem die Veränderungen festgestellt wurden, kann dann beispielsweise eine Protokolldatei erstellt oder ein Administrator benachrichtigt werden. Dies alles kann jedoch nur mit Hilfe von Zusatzsoftware realisiert werden. Hierfür ist entweder eine Eigenentwicklung oder ein Drittprodukt notwendig.

Im Folgenden werden die technischen Details für Windows 2000 und XP beschrieben.

Gerätetreiber deaktivieren

- Windows 2000

  Unter Windows 2000 kann das Starten des Gerätetreibers für USB-Speichermedien deaktiviert werden. Mit dieser Möglichkeit wird dem Standard-Benutzer die Möglichkeit, USB-Massenspeichergeräte hinzuzufügen, komplett entzogen, da er die Startart des Gerätetreibers nicht verändern kann. Auch einem Standard-Benutzer mit erschlichenem Administratorkennwort wird der Datendiebstahl zumindest schwerer gemacht.

  USB-Sticks werden unter Windows 2000 als USB-Massenspeichergeräte registriert. Zum Ausführen wird der Gerätetreiber als Dienst gestartet.

  In der Registrierung kann hinterlegt werden, wie der Dienst gestartet wird (Manuell, Automatisch oder Deaktiviert). So wird unter *HKLM/System/CurrentControlSet/Services* der Dienst *USBStor* als Gerätetreiber für die USB-Massenspeichergeräte bereitgestellt. Die unterschiedlichen Startarten können unter dem Unterschlüssel Start eingestellt werden. Die Festlegung, dass das Starten des Gerätertreibers USBStor deaktiviert (0x00000004) ist, verhindert, dass Massenspeichergeräte installiert oder hinzugefügt werden können.

- Windows XP

  Windows XP verhält sich anders als Windows 2000. Wird ein dem Rechner bekanntes Massenspeichergerät hinzugefügt, wird der Treiber geladen, und wenn in der Registrierung die Startart auf deaktiviert steht, wird der Einsatz des Massenspeichergeräts verhindert. Sobald jedoch ein dem Rechner unbekanntes USB-Massenspeichergerät hinzugefügt wird, werden neue Treiber installiert und die Einstellungen des Dienstes USBStor in der Registrierung überschrieben. Die Startart wird dabei auch wieder zurückgesetzt, so dass unter Windows XP der Einsatz von USB-Massenspeichergeräten nicht global verhindert werden kann.

  Ab Service Pack 2 bietet Windows XP die Möglichkeit, zumindest den Schreibzugriff auf USB-Blockspeichergeräte zu unterbinden. Damit wird die USB-Schnittstelle einem CD-ROM-Laufwerk gleichgesetzt, das nur das Lesen eines Mediums erlaubt. Die Deaktivierung des Schreibzugriffs erfolgt durch das Erstellen des Registrierungs-Schlüssels *HKLM\System\CurrentControlSet\Control\StorageDevicePolicies\WriteProtect*, der auf den Wert 1 gesetzt wird.

Überwachen des Rechners

- Windows 2000/XP

  Sehr vielversprechend ist unter beiden Betriebssystemen die Möglichkeit, die Registrierung zu überwachen und damit nur auf das Hinzufügen zu reagieren. Ein Missbrauch würde sofort auffallen.

Wenn das Hinzufügen von neuen Geräten beobachtet wird, können Aktionen initiiert werden. Jedes neue USB-Gerät wird in der Registrierung unter *HKLM\System\CurrentControlSet\Enum\USB* aufgeführt. Mit Hilfe eines Skriptes oder Programms könnte dieser Schlüssel daraufhin überwacht werden, ob ein Gerät unerlaubt hinzugefügt wird. Es kann eine Positivliste für erlaubte Geräte in dem Programm abgearbeitet werden, so dass auf möglicherweise benötigte Geräte nicht reagiert wird. Wird das unerlaubte Hinzufügen eines Geräts erkannt, kann eine Aktion (Herunterfahren des Systems, Benachrichtigen des Administrators per net send oder E-Mail) ausgeführt werden. Für eine solche Überwachung der Registrierung ist spezielle Software notwendig, die ein Drittprodukt sein oder aus Eigenentwicklung stammen kann.

Ergänzende Kontrollfragen:

- Ist der Umgang mit USB-Speichermedien geregelt?

M 4.201 Sichere lokale Grundkonfiguration von Routern und Switches

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Sämtliche Konfigurationsarbeiten an Routern und Switches müssen entsprechend der erstellten Sicherheitsrichtlinie (siehe M 2.279 *Erstellung einer Sicherheitsrichtlinie für Router und Switches*) durchgeführt werden und wie in M 2.281 *Dokumentation der Systemkonfiguration von Routern und Switches* beschrieben dokumentiert und kommentiert werden.

Betriebssystem

Da Router und Switches durch ihren Einsatz im Netz eine besonders große Anzahl von Kommunikationspartnern und damit potentiellen Angreifern haben, ist bei der Auswahl, Einrichtung und Pflege des Betriebssystems besondere Sorgfalt notwendig.

Zunächst ist es wichtig, sich einen Überblick über die benötigten und angebotenen Funktionen zu verschaffen. Das Ziel bei der Auswahl sollte sein, eine möglichst stabile Version zu betreiben. Hierbei ist zu beachten, dass mit dem Alter eines Releases in der Regel auch die Zahl der Angriffsmöglichkeiten (Exploits) zunimmt. Andererseits kann ein sehr neues Release (insbesondere mit völlig neuen Funktionen) noch Unzulänglichkeiten oder neue Fehler enthalten.

Im Zweifelsfall ist es meist besser, eine ältere Version einzusetzen, falls diese den funktionalen Anforderungen noch genügt. Allerdings müssen für diese unbedingt die aktuellen Sicherheitspatches eingespielt werden (siehe auch M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*). Versionen, für die vom Hersteller keine Sicherheitspatches mehr zur Verfügung gestellt werden, sollten nicht mehr eingesetzt werden.

Offline-Grundkonfiguration

Vorsicht bei Default-Einstellungen

Bevor ein Router oder Switch an das Produktions-Netz angeschlossen wird, muss eine sichere Grundkonfiguration hergestellt werden. Viele Geräte werden vom Hersteller mit einer Default-Konfiguration ausgeliefert, die vor allem auf eine schnelle Inbetriebnahme mit möglichst umfassender Funktionalität ausgerichtet ist und in der so gut wie keine Sicherheitsmechanismen aktiv sind. Daher muss die Überprüfung der Default-Einstellungen und die Grundkonfiguration offline oder nur in einem eigens dafür eingerichteten und besonders gesicherten Testnetz erfolgen.

Oft ist es möglich, die Konfiguration mit entsprechenden Programmen auf einem Management-Rechner zu erstellen und beispielsweise mit einer Speicherkarte auf das neue Gerät zu übertragen. Ist nur eine Übertragung über das Netz möglich, so darf dies nur im Testnetz oder im Administrationsnetz geschehen.

Bei der Konfiguration muss beachtet werden, dass unter Umständen nicht jedes Administrations- oder Konfigurationswerkzeug (Konsole, Webschnittstelle, externes Konfigurationsprogramm) alle relevanten Informationen anzeigt. So kann es beispielsweise vorkommen, dass die

Systembefehle zur Anzeige einer Konfiguration auf Routern und Switches nicht alle Parameter anzeigen. Daher ist es wichtig, anhand der vorhandenen Dokumentation nachzuvollziehen, dass auch alle relevanten Einstellungen vorgenommen wurden.

Es bietet sich an, die Grundkonfiguration in zwei Schritte zu unterteilen:

- Lokale Konfiguration: Überprüfung und Anpassung der Konfigurationsparameter, die sich auf das Gerät selbst beziehen (beispielsweise Benutzerkonten oder -rollen, Passwörter, Protokolldateien, Einstellungen für Konsolenzugang und serielle Schnittstelle, etc.). Die entsprechenden Schritte sind im Anschluss beschrieben.
- Netzkonfiguration: Überprüfung und Anpassung der Konfigurationsparameter, die sich auf die Funktion des Gerätes im Netz beziehen (beispielsweise Dienste und Protokolle, Einrichtung von Access-Control-Listen (ACLs), VLANs etc.). Die entsprechenden Schritte sind in M 4.202 *Sichere Netz-Grundkonfiguration von Routern und Switches* beschrieben.

Benutzerkonten und Passworte

Die Möglichkeiten für die Einrichtung von Benutzern und Rollen und das Zuweisen von Berechtigungen unterscheiden sich von Hersteller zu Hersteller (gelegentlich auch zwischen einzelnen Geräten oder Software-Releases) teilweise erheblich. Daher ist es empfehlenswert, entsprechend dem vorgegebenen Rechte- und Rollenkonzept für die Administration der aktiven Netzkomponenten ein detailliertes Konzept für die jeweiligen Geräte zu erstellen.

Auf Routern und Switches einiger Hersteller (z. B. Cisco) sind werksmäßig mehrere Benutzerkonten (Accounts) mit abgestuften Berechtigungen für die Administration vorhanden. Andere Geräte sind werksmäßig nur mit einem Benutzerkonto für Administrationszwecke voreingestellt. Voreingestellte Benutzerkonten haben allgemein bekannte Standardnamen und Passwörter, gelegentlich sind Administrations-Accounts sogar ganz ohne Passwort vorkonfiguriert. Auf einschlägigen Internet-Seiten können Listen mit herstellerspezifischen Standard-Accounts und Passwörtern heruntergeladen werden.

Standardnamen ändern

Bei der Inbetriebnahme des Geräts müssen diese Standard-Benutzerkonten, falls möglich, geändert werden. In jedem Fall müssen aber die Passwörter der Standard-Accounts geändert werden. Nicht benutzte Benutzerkonten müssen deaktiviert werden.

Entsprechend dem Rechte- und Rollenkonzept müssen anschließend die vorgesehenen Benutzerkonten und -rollen eingerichtet werden.

Verschlüsselte Speicherung, wenn möglich

Leider werden bei vielen aktiven Netzkomponenten Passwörter im Klartext in den Konfigurationsdateien gespeichert. Insbesondere falls dies der Fall ist, müssen Konfigurationsdateien vor unbefugtem Zugriff besonders geschützt werden. Wo immer es möglich ist, eine verschlüsselte Speicherung von Passwörtern zu konfigurieren, sollte von dieser Möglichkeit Gebrauch gemacht werden. Weitergehende Aspekte sind in M 1.43 *Gesicherte Aufstellung aktiver Netzkomponenten*, M 4.204 *Sichere Administration von Routern und Switches*

und M 6.91 *Datensicherung und Recovery bei Routern und Switches* beschrieben.

Login-Banner

Beim Login wird auf den Geräten meist eine relativ ausführliche Login-Nachricht angezeigt. In dieser Login-Nachricht sind oft Informationen (beispielsweise Modell- oder Versionsnummer, Software-Release-Stand oder Patchlevel) enthalten, die einem potentiellen Angreifer von Nutzen sein können.

Login-Banner ändern

Sofern das Gerät es zulässt, sollte die Standard-Loginnachricht durch eine angepasste Version ersetzt werden, die diese Informationen nicht mehr enthält. Die Modell- und Versionsnummer des Geräts und die Version des Betriebssystems darf unter keinen Umständen vom Login-Banner verraten werden. Stattdessen sollten folgende Informationen bei einer Anmeldung am Gerät angezeigt werden:

- Jeglicher Zugriff darf nur durch autorisiertes Personal erfolgen.
- Alle Arbeiten sind entsprechend der Sicherheitsrichtlinie durchzuführen.
- Das Gerät ist in zentrale Kontrollmechanismen, wie beispielsweise in ein Netzmanagementsystem (NMS) zur Protokollierung und Erkennung von Verstößen gegen die Sicherheitsrichtlinie eingebunden.
- Verstöße gegen die Sicherheitsrichtlinie werden disziplinarisch / strafrechtlich verfolgt.

Protokollierung

Sicherheitsmaßnahmen in bezug auf die Protokollierung auf Netzkomponenten und der Einbindung von Zeitinformationen mit Hilfe von NTP sind in M 4.205 *Protokollierung bei Routern und Switches* beschrieben.

Schnittstellen

Nicht genutzte Schnittstellen auf Routern sind zu deaktivieren. Bei Switches sollten alle nicht genutzten Ports entweder deaktiviert oder einem eigens dafür eingerichteten "Unassigned-VLAN" zugeordnet werden.

Backup der Konfiguration

Die Konfigurationsdateien der Grundkonfiguration bilden die Basis für die weitere Konfiguration. Es wird empfohlen, sowohl von den mit dem Gerät ausgelieferten Default-Konfigurationsdateien als auch von den Dateien, die das Ergebnis der Grundkonfiguration darstellen, Sicherungskopien zu erstellen.

In M 6.91 *Datensicherung und Recovery bei Routern und Switches* werden weitere Aspekte zur Sicherung von Konfigurationsdateien beschrieben.

Ergänzende Kontrollfragen:

- Wurde die Einrichtung anhand der Sicherheitsrichtlinie durchgeführt?
- Wie ist die Abbildung der im allgemeinen Nutzer- und Rollenkonzept definierten Konten auf die Benutzerkonten der Router und Switches?

- Wie sieht das Login-Banner der Geräte aus?

M 4.202 Sichere Netz-Grundkonfiguration von Routern und Switches

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator

Remote-Zugriff

Für die Administration aktiver Netzkomponenten über das Netz wird oft noch Telnet als Standardmöglichkeit angeboten. Oft gibt es auch eine Administrationsmöglichkeit über SNMP oder den Zugriff über eine HTTP-Schnittstelle. Alle diese Protokolle haben den Nachteil, dass sowohl Benutzername und Passwort als auch die Nutzdaten im Klartext über das Netz übertragen werden (siehe auch G 2.87 *Verwendung unsicherer Protokolle in öffentlichen Netzen*).

Daher ist für die Administration entweder ein eigenes Administrationsnetz (Out-of-Band-Management) einzurichten, oder es dürfen nur Protokolle benutzt werden (beispielsweise ssh2), die eine gesicherte Authentisierung und verschlüsselte Übertragung unterstützen.

Soll SNMP außerhalb eines eigenen Administrationsnetzes eingesetzt werden, so darf nur SNMPv3 benutzt werden.

Authentisierungsserver

In großen Netzen sollten Router und Switches möglichst für die Nutzung von Authentisierungsservern unter Verwendung von Einmal-Passwörtern konfiguriert werden. Beispiele hierfür sind RADIUS oder TACACS+. Weitergehende Aspekte sind in M 4.204 *Sichere Administration von Routern und Switches* beschrieben.

Management-Interface und Administrationsnetz

Einige Geräte bieten die Möglichkeit, ein eigenes logisches Interface zur Administration (Management-Interface) zu konfigurieren. Bei Switches sollte dieses Interface einem eigenen VLAN zugeordnet werden, das ausschließlich für administrative Zwecke verwendet wird (Out-of-Band Management) und dem ausschließlich Management-Interfaces angehören. Bei Routern sollten ACLs so konfiguriert werden, dass der Zugriff auf das Management-Interface von der Management-Station aus mit definierten Protokollen erlaubt ist. Alle nicht benötigten Dienste sind für das Management-Interface zu deaktivieren.

Weitere Schritte zur Einrichtung eines Administrationsnetzes (Out-of-Band-Management) sind in M 4.204 *Sichere Administration von Routern und Switches* beschrieben.

Deaktivierung unnötiger Netzdienste

Hersteller aktiver Netzkomponenten legen oft in erster Linie Wert auf eine möglichst einfache Inbetriebnahme und Konfiguration der Komponenten. Daher sind in der Default-Konfiguration meist eine Vielzahl von Diensten aktiviert. Es sollten nur Dienste aktiviert sein, die für den Betrieb notwendig sind. Nicht benötigte Dienste auf den Routern und Switches müssen deaktiviert werden, weil sie ein erhöhtes Risiko darstellen. Die Einstellungen zu den in der nachfolgenden Tabelle genannten Diensten gelten oft für das

gesamte System und nicht explizit für einzelne Schnittstellen/Ports der Geräte. Generell dürfen diese Dienste nicht aus unsicheren Netzen erreichbar sein. Dies ist durch entsprechende Access-Control-Lists sicherzustellen.

In der folgenden Tabelle ist eine Anzahl von Diensten aufgeführt, die oft auf aktiven Netzkomponenten vorhanden sind. Für jeden Dienst ist eine Empfehlung angegeben, wie mit dem Dienst normalerweise verfahren werden sollte.

Dienst	Beschreibung
FINGER	Der Finger-Dienst zeigt die augenblicklich auf einem Gerät angemeldeten Benutzer an. Er hat keinen praktischen Nutzen und sollte deaktiviert werden.
BOOTP	Einige Router und Switches unterstützen BOOTP (Bootstrap-Protocol), sowohl als Server als auch als Client. Damit ist es anderen Komponenten möglich, von diesen Geräten zu booten. BOOTP besitzt keine Funktionen zur Authentisierung oder Verschlüsselung und sollte deaktiviert werden.
HTTP	Eine große Anzahl von Routern und Switches können mit Hilfe von HTTP administriert werden. Dieser Dienst sollte in öffentlichen Netzen auf jeden Fall deaktiviert und allenfalls in einem isolierten Administrationsnetz verwendet werden.
SNMP	SNMP ist ein Administrations- und Netzmanagement-Protokoll. Bis einschließlich der Version SNMPv2 sind die Sicherheitsfunktionen nicht ausreichend. Die Variante SNMPv3 besitzt stärkere Authentisierungs- und Verschlüsselungsoptionen. Dieser Dienst sollte möglichst nur in einem isolierten Administrationsnetz genutzt werden. SNMPv1 und SNMPv2 dürfen keinesfalls außerhalb isolierter Administrationsnetze verwendet werden.
TELNET	Telnet wird oft als Standard-Administrationsschnittstelle für Router und Switches verwendet. Dieser Dienst sollte durch SSH (siehe unten) ersetzt werden. In öffentlichen Netzen darf Telnet nicht zur Administration aktiver Netzkomponenten verwendet werden.

NTP	Das Network Time Protocol NTP dient zur Synchronisation der Systemzeit. Einige Router oder Switches können als Zeitserver für andere Geräte fungieren. NTP besitzt keine Sicherungsfunktionen und sollte daher nicht in öffentlichen Netzen verwendet werden. Es sollte ein interner NTP-Server installiert sein, der über ein Administrationsnetz angesprochen wird.
DNS	Einige Router oder Switches unterstützen die Funktion eines DNS-Clients zur Namensauflösung, beispielsweise im Zusammenhang mit der Protokollierung. Eine Namensauflösung ist bei aktiven Netzkomponenten normalerweise nicht notwendig und bietet keinen echten Nutzen. Daher sollte DNS deaktiviert werden.
CDP	CDP ist ein proprietäres Layer 2 Protokoll zwischen Cisco Routern und Switches. Es sollte zumindest auf Endgeräte-Ports deaktiviert werden.
TFTP	Einige Router und Switches unterstützen das Booten von einem TFTP-Server. TFTP bietet keine Sicherheitsmechanismen. Diese Funktion sollte nur genutzt werden, wenn ein interner TFTP-Server in einem isolierten Administrationsnetz installiert ist.
SSH1	SSH1 ist eine alte Variante des Secure Shell Protokolls, die Sicherheitslücken aufweist. Sie sollte daher nicht verwendet werden. Falls ein Gerät nur SSH1 anbietet, so sollte der Zugriff nur über ein isoliertes Administrationsnetz erfolgen.
SSH2	SSH2 ein sicherer Ersatz für Telnet über öffentliche Netze zur Administration von Routern und Switches eingesetzt werden kann. Trotzdem ist es empfehlenswert, auch den SSH-Zugang durch entsprechende ACLs zusätzlich abzusichern.

Tabelle: Dienste von aktiven Netzkomponenten

Auf Schnittstellen von Switches, aber in erster Linie auf Interfaces von Routern in öffentlichen Netzen sollten außerdem die folgenden Einstellungen zusätzlich berücksichtigt werden.

Dabei kann jedoch keine allgemeine Vorgehensweise vorgegeben werden, sondern es werden nur Empfehlungen für verschiedene Aspekte gegeben. Wenn in bestimmten Fällen von diesen Empfehlungen abgewichen wird, so sollte aber stets klar sein, wieso.

Dienst	Beschreibung, Einstellung
IP source routing	Diese Funktion erlaubt es einem IP-Paket, die Route zum Ziel vorzugeben. Diese Funktion wird für eine Vielzahl von Angriffen verwendet. Deshalb sollte diese Funktion deaktiviert werden.
IP directed broadcast	Dieser Dienst kann für DOS-Attacken ausgenutzt werden. Deshalb sollte diese Funktion deaktiviert werden.
ICMP redirects	Diese ICMP-Funktion kann verwendet werden, um Informationen über Netze herauszufinden. Deshalb muss diese Funktion zumindest an externen Interfaces von Routern deaktiviert werden.
ICMP unreachable notifications	Diese ICMP-Funktion kann verwendet werden, um Informationen über Netze herauszufinden. Deshalb muss diese Funktion zumindest an externen Interfaces von Routern deaktiviert werden.
ICMP mask reply	Diese ICMP-Funktion kann verwendet werden, um Informationen über Netze herauszufinden. Deshalb muss diese Funktion zumindest an externen Interfaces von Routern deaktiviert werden.

Tabelle: Einstellung der Dienste

Anti-Spoofing

Border-Router stellen den Übergang von internen Netzen zu externen Netzen dar. Auf Border-Routern sollten Sicherheitsmaßnahmen ergriffen werden, die IP-Spoofing (siehe auch G 5.48) verhindern. Dies kann beispielsweise durch die Einrichtung entsprechender ACLs erreicht werden. Eine mögliche Variante ist folgender Ansatz:

- An den externen Schnittstellen werden solche Pakete blockiert, deren Absender-IP-Adresse im internen Netz liegt.
- An den internen Schnittstellen werden solche Pakete blockiert, deren Absender-IP-Adresse nicht im internen Netz liegt.

Zumindest bei Paketen, die auf Grund der zweiten Regel blockiert werden, ist eine entsprechende Protokollierung und gegebenenfalls eine Alarmierung der zuständigen Administratoren empfehlenswert. Die Tatsache, dass eine Station innerhalb des eigenen Netzes offensichtlich gefälschte Pakete verschickt, ist nämlich ein klares Indiz dafür, dass entweder eine falsche Konfiguration oder gar ein Sicherheitsproblem vorliegt.

Loopback-Interface

Einige Router-Modelle (beispielsweise von Cisco) bieten die Möglichkeit, ein Loopback-Interface einzurichten. Die dem Loopback-Interface zugewiesene

IP-Adresse kann vom Router als Quelladresse für Protokolle wie Syslog, NTP oder wichtiger Dienste zur Administration benutzt werden. Dadurch kann einebessere Absicherung des Routers erreicht werden, weil die Quell-Adresse im IP-Paket immer die IP-Adresse des Loopback-Interfaces ist.

Routing-Protokolle

Es sollten nur Routing-Protokolle verwendet werden, die eine verschlüsselte Authentisierung unterstützen. In demilitarisierten Zonen dürfen keine dynamischen Routing-Protokolle eingesetzt werden, stattdessen müssen statische Routen eingetragen werden. Die Verwendung von Routing-Protokollen sollte zusätzlich durch die Einrichtung von ACLs abgesichert sein. Mehr Informationen finden sich in M 5.112 *Sicherheitsaspekte von Routing-Protokollen*.

Access Control Lists

Die Verwendung von Access Control Lists (ACLs) zur Einschränkung des Zugriffes auf Routern und zur netzübergreifenden Paketfilterung ist in M 5.112 *Sicherheitsaspekte von Routing-Protokollen* beschrieben.

Spanning Tree

Das Spanning Tree Protocol (STP, IEEE 802.1d) wird von Switches und Bridges verwendet, um Schleifenbildungen innerhalb des Netzes auf der OSI-Schicht 2 zu vermeiden. Es werden BPDUs (Bridge Protocol Data Units) ausgesendet, um die Root-Bridge (basierend auf MAC-Adresse und Priorität) zum Systemstart und bei Topographie-Änderungen zu bestimmen. Dieses Protokoll bietet keine Authentisierung. Deshalb sollte STP zumindest auf allen Endgeräte-Ports deaktiviert werden. In der Konfiguration muss eine eindeutige Root-Bridge festgelegt werden.

VLANs und Trunking

Trunking ermöglicht es, VLANs über mehrere Switches auszudehnen. Die Steuerung von Trunking wird durch den Standard IEEE 802.1q oder durch unterschiedliche proprietäre Trunking-Protokolle realisiert. Dabei wird pro Switch ein physischer Port (Trunk-Port) für die Inter-Switch-Kommunikation reserviert. Diese logische Verbindung zwischen den Switches wird als Trunk bezeichnet.

Trunk-Ports können auf alle VLANs zugreifen. Das heißt, dass der Zugang zu einem Trunk-Port den Zugriff auf alle VLANs dieses Trunks ermöglicht. Manche Geräte bieten allerdings auch die Möglichkeit, den Zugriff eines Trunk-Ports auf bestimmte VLANs zu beschränken ("VLAN Pruning"). Sofern ein Switch eine solche Möglichkeit bietet, ist es empfehlenswert, dies zu nutzen. Auf Endgeräte-Ports sollte Trunking möglichst deaktiviert werden.

Das Default-VLAN darf nicht für ein produktives VLAN verwendet werden.

Wird das proprietäre Protokoll VTP (VLAN Trunking Protocol) des Herstellers Cisco verwendet, so sollte unbedingt die von VTP unterstützte Authentisierung verwendet werden.

Freie Ports

Für nicht benutzte Ports sollte ein eigenes VLAN ("Unassigned-VLAN") eingerichtet werden. Nach Möglichkeit sollten nicht genutzte Ports allerdings ganz deaktiviert werden, da die VLAN-Port-Zuweisung nur wenig zusätzliche Sicherheit bietet.

Ist es gewünscht, bestimmte Ports für den freien Anschluss verschiedener Geräte vorzusehen, so ist es empfehlenswert, für diese Ports eine Sicherung zu implementieren, die erst nach einer Anmeldung den Zugang zum Netz gewährt.

Ein solcher Zugangsschutz kann beispielsweise über den Standard IEEE 802.1x implementiert werden. Der Standard 802.1x wird inzwischen von vielen Switches und den meisten Rechner-Betriebssystemen unterstützt. Darüber hinaus existiert eine Reihe weiterer, teils proprietärer Lösungen, bei denen die Endgeräte auf der Basis ihrer MAC-Adresse oder über andere Mechanismen gegenüber der aktiven Netzkomponente authentisiert werden können, bevor der Zugang zum Netz freigeschaltet wird.

Ergänzende Kontrollfragen:

- Welche Dienste und Protokolle werden zur Administration verwendet?
- Sind nicht genutzte Dienste und Protokolle deaktiviert?
- Wurde ein isoliertes Administrationsnetz eingerichtet?

M 4.203 Konfigurations-Checkliste für Router und Switches

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Zusammenfassend können anhand der folgenden Konfigurations-Checkliste die wichtigsten sicherheitsrelevanten Einstellungen auf Routern und Switches geprüft werden. Es muss jedoch festgehalten werden, dass die sichere Konfiguration von Routern und Switches stark vom Einsatzzweck abhängt. Beispielsweise muss auf Border-Routern die Einrichtung von ACLs, Anti-Spoofing-Konfiguration, etc. berücksichtigt werden. Deshalb sollte die folgende Tabelle lediglich als allgemeine Anleitung verwendet werden. Sicherheitsmaßnahmen, die auf Router anzuwenden sind, gelten auch für Switches, sofern diese Routing-Funktionen unterstützen und soweit diese Funktionen genutzt werden.

Konfigurations-Checkliste für Router und Switches

Erstellung einer Sicherheitsrichtlinie für Router und Switches	
Prüfung und gegebenenfalls Update des Betriebssystems	
Die Router- und Switchkonfiguration offline speichern, sichern und gegen unbefugten Zugang schützen (Nutzung eines TFTP-Servers nur in Verbindung mit Out-of-Band-Management (eigenes Administrationsnetz))	
Dokumentation und Kommentierung der Konfiguration	
Konfiguration von Passwortschutz für alle Zugänge (Konsole, VTY, etc.)	
Einrichtung eines Session-Timeouts	
Keine Trivial-Passworte verwenden	
Verschlüsselte Speicherung der Passworte	
Einrichtung eines physischen Zugangsschutzes für den Konsolenanschluss	
Für Administrationszwecke soweit möglich TELNET durch SSH ersetzen	
Möglichst RADIUS oder TACACS+ zur Authentisierung verwenden	
Einschränkung der Administrationszugänge (z. B. SSH, SNMP, TELNET) durch ACLs, Nutzung von SNMP und TELNET nur in Verbindung mit Out-of-Band-Management (eigenes Administrationsnetz), bei SNMP Änderung der Community-Strings	
Deaktivieren unnötiger Netzdienste	

Bei Routern nicht benötigte Schnittstellen abschalten, bei Switches nicht benötigte Ports in "Unassigned VLAN" oder ebenfalls deaktivieren	
Kritische Schnittstellendienste und Protokolle sperren	
Protokollierung einschalten	
Genaue Uhrzeit auf den Geräten einstellen (interner NTP-Server)	
Einbinden der Zeitinformation bei der Protokollierung	
Auswerten, Überprüfen und Archivieren der Protokolldateien entsprechend der Sicherheitsrichtlinie	
SNMP möglichst deaktivieren, Nutzung nur in Verbindung mit Out-of-Band-Management (Administrationsnetz) oder Verwendung von SNMPv3	
Überprüfung der Default-Einstellungen	
Einrichtung eines Login-Banners	
Deaktivierung von CDP auf Endgeräte Ports	
Speziell für Switches:	
Bei Nutzung von VTP: Authentisierung verwenden	
Deaktivierung von Trunk-Negotiation auf Endgeräte-Ports	
Das Default-VLAN darf nicht genutzt werden	
Einrichtung eines eigenen VLANs für alle Trunk-Ports	
Einrichtung eines Unassigned-VLANs für alle unbenutzten Ports	
Deaktivierung von STP (Spanning Tree) auf Engeräte-Ports	
Festlegung einer Root-Bridge	
Speziell für Router:	
Erstellung einer Kommunikationsmatrix des netzübergreifenden Datenverkehrs	
Begrenzen des netzübergreifenden Datenverkehrs in Abgleich mit Kommunikationsmatrix durch Zugriffslisten	
Blockieren von unbekannten Adressen durch Zugriffslisten (ACLs)	
Falls erforderlich (insbesondere in der DMZ): Konfiguration statischer Routen	
Konfiguration von Integritätsmechanismen der verwendeten Routing Protokolle	

Ergänzende Kontrollfragen:

- Wurde nach Einrichtung der Komponenten eine Überprüfung der Einstellungen anhand der Checkliste durchgeführt?

M 4.204 Sichere Administration von Routern und Switches

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Es gibt unterschiedliche Zugriffsmöglichkeiten, um Router und Switches zu administrieren. Abhängig von der genutzten Zugriffsart müssen eine Reihe von Sicherheitsvorkehrungen getroffen werden. Bei größeren Netzen ist es empfehlenswert, Router und Switches in ein zentrales Netzmanagement-System einzubinden, da sonst eine sichere und effiziente Administration praktisch nicht gewährleistet werden kann.

Die zur Administration verwendeten Methoden sollten in der Sicherheitsrichtlinie festgelegt werden, und die Administration darf nur entsprechend der Sicherheitsrichtlinie durchgeführt werden. Alle nicht verwendeten Administrationsschnittstellen sollten deaktiviert werden. Im folgenden werden einige Punkte beschrieben, die bei der Administration beachtet werden sollten.

Zusätzlich sollte wenn möglich der Administrationszugriff durch die Einrichtung von Access Control Lists (ACLs) eingeschränkt werden (siehe auch M 5.111 *Einrichtung von Access Control Lists auf Routern*).

Remote-Administration

Eine Vielzahl von aktiven Netzkomponenten bietet die Möglichkeit der Remote-Administration mit Hilfe des Dienstes Telnet. Die Nutzung von Telnet birgt allerdings die Gefahr des Ausspähens von Authentisierungsdaten, da sämtliche Daten im Klartext übertragen werden und somit der Datenverkehr inklusive des Benutzernamens und Passwortes mitgelesen werden kann (siehe auch G 2.87 *Verwendung unsicherer Protokolle in öffentlichen Netzen*). Oft wird zur Remote-Administration auch SNMP verwendet. Die Varianten SNMPv1 und SNMPv2 bieten ebenfalls keine ausreichenden Möglichkeiten zur Absicherung der Kommunikation. Erst SNMPv3 bietet Sicherheitsmechanismen, die einen Einsatz auch außerhalb abgeschotteter Administrationsnetze erlauben.

Remote-Administration nur über gesicherte Verbindungen

Bei Remote-Zugriff auf Routern und Switches muss in jedem Fall eine Absicherung der Kommunikation erfolgen. Dies kann beispielsweise durch die Nutzung des Dienstes SSH anstatt Telnet (siehe M 5.64 *Secure Shell*, M 5.64 *Nutzung von SSH*) oder durch die Schaffung eigener LAN-Segmente, die ausschließlich für Administrationszwecke genutzt werden, erreicht werden (siehe Abschnitt Administrationsnetz).

Eine ungesicherte Remote-Administration über externe (unsichere) Netze hinweg darf in keinem Fall erfolgen. Dies muss bereits bei der Festlegung der Sicherheitsrichtlinie berücksichtigt werden. Auch im internen Netz sollten soweit möglich keine unsicheren Protokolle verwendet werden.

Webserver

Viele Geräte bieten die Möglichkeit, Administrationsarbeiten mit Hilfe des Dienstes HTTP über ein Browser-Interface durchzuführen. Auf dem Router

bzw. dem Switch ist in diesem Fall ein HTTP-Server gestartet, der Zugriff erfolgt von beliebigen Clients über Web-Browser.

Die Standardeinstellungen für den Zugriff auf das Web-Interface sind nicht bei allen Herstellern einheitlich. Idealerweise sollte der Zugriff in der Grundeinstellung deaktiviert sein, es ist aber auch möglich, dass dieser Dienst ungeschützt ohne Eingabe von Benutzerinformationen verwendet werden kann. Dies ist bei der Inbetriebnahme der Geräte zu prüfen, gegebenenfalls muss die Konfiguration entsprechend geändert werden.

Wie bei der Nutzung des Dienstes TELNET wird auch beim HTTP der Benutzername und das Passwort im Klartext übertragen. Zudem sind eine Reihe von Exploits bekannt, die Schwachstellen der HTTP-Server der unterschiedlichen Hersteller ausnutzen. Daher wird von der Nutzung des HTTP-Dienstes für Administrationszwecke dringend abgeraten. Der HTTP-Server sollte nach Möglichkeit bei der Erstkonfiguration des Systems deaktiviert werden, sofern der Zugriff nicht über ein gesondertes Management-Netz erfolgt.

Manche Geräte bieten zusätzlich zum Zugriff über HTTP auch die Möglichkeit, über HTTPS auf das Web-Interface zuzugreifen. Sofern diese Möglichkeit besteht, sollte HTTPS in jedem Fall der Vorzug vor HTTP gegeben werden.

Bei der Nutzung des Web-Interfaces muss außerdem beachtet werden, dass oft nicht alle Konfigurationseinstellungen auf diesem Weg zugänglich sind.

Administrationsnetz (Out-of-Band-Management)

Um den Risiken bei der Remote-Administration entgegen zu wirken, bieten einige Geräte die Möglichkeit, einen eigenen logischen Port (Management-Interface) zur Administration zu konfigurieren. Bei Switches sollte dieser Port einem VLAN zugeordnet werden, welches ausschließlich für administrative Zwecke verwendet wird (Out-of-Band-Management) und dem ausschließlich Management-Interfaces angehören. Das Management-Netz sollte komplett von anderen Teilen des Netzes getrennt werden. Dadurch werden Schwachstellen wie unverschlüsselt übertragene Anmeldeinformationen bei den für administrative Aufgaben zur Anwendung kommenden Protokollen wie TELNET oder die veralteten SNMP-Varianten kompensiert.

Access Control Lists (ACLs) sind so zu konfigurieren, dass der Zugriff auf das Management-Interface nur der Management-Station erlaubt ist. Alle nicht benötigten Dienste sind für das Management-Interface zu deaktivieren.

Netzmanagement-Systeme

Aktive Netzkomponenten werden normalerweise in ein zentrales Netzmanagement-System eingebunden. Zusätzlich zum vorigen Abschnitt müssen in diesem Fall die Sicherheitsmaßnahmen, die im Baustein B 4.2 *Netz- und Systemmanagement* beschrieben sind, beachtet werden.

Zentraler Authentisierungsserver

An Stelle lokal auf dem Gerät zu konfigurierender Zugriffs- und Rechtekontrolle kann dies auch über einen zentralen Server erfolgen. Bei großen Umgebungen mit einer hohen Anzahl von aktiven Netzkomponenten

ist die lokale Konfiguration nur bedingt praktikabel. Der Aufwand für die Administration und für viele parallel zu pflegende Berechtigungen ist dann sehr hoch.

Auf dem zentralen Server werden dabei einheitlich alle Zugriffe und Berechtigungen verwaltet. Die sensitiven Daten sind nicht mehr auf den Geräten selbst gespeichert und müssen nicht einzeln gepflegt werden. Stattdessen sind alle Informationen verschlüsselt in einer Datenbank abgelegt und lassen sich übersichtlich verwalten. Ein solcher Server bietet zudem erweiterte Möglichkeiten zur Protokollierung, beispielsweise können Anzahl und Zeitpunkt von Einwahl- oder Zugriffsvorgängen und übertragene Datenmengen dokumentiert werden. Beispiele hierfür sind RADIUS und TACACS+ (Terminal Access Controller Access Control System). Die Authentisierung sollte in komplexen Netzen mit einer Vielzahl von aktiven Netzkomponenten durch einen zentralen Authentisierungsserver abgesichert werden.

Für den Fall, dass kein Authentisierungsserver genutzt werden kann (beispielsweise beim Ausfall des Servers oder bei Netzproblemen), sollte trotzdem ein lokaler Zugriff konfiguriert sein. Dieser ist durch ein nur für diesen Zweck zu nutzendes Passwort abzusichern.

Für lokale Zugänge, die nicht eigens für den Fall eingerichtet wurden, dass der Authentisierungsserver nicht zur Verfügung steht, sollten der Authentisierungsserver nach Möglichkeit genutzt werden, da ansonsten die Benutzer, die sich lokal anmelden, die zentrale Autorisierung und Überwachung umgehen.

Berechtigungsverwaltung für Benutzerkonten und Systemkommandos

Die Berechtigungsverwaltung kann je nach Hersteller auf unterschiedlichen Ebenen und mit unterschiedlichen Graden der Granularität erfolgen. Bei der Berechtigungsverwaltung von Systemkommandos können Kommandos, die nur bestimmten Nutzern oder Gruppen zugänglich sein sollen, in einer Berechtigungsstufe zusammengefasst bzw. dieser zugeordnet werden. Dies ist beispielsweise vom Hersteller Cisco bereits für zwei Stufen vorkonfiguriert:

1. Die Zuordnung von Systemkommandos zu Berechtigungsstufen.
2. Die Zuordnung von Benutzerkonten zu Berechtigungsstufen.

Der Zugriff auf eine Berechtigungsstufe wird durch ein Passwort abgesichert. Ein Nutzer muss für den Zugriff auf ein entsprechend abgesichertes Systemkommando zunächst in die Berechtigungsstufe wechseln und das zugehörige Passwort eingeben. Dann ist er in der Lage, alle dieser Stufe zugeordneten Kommandos auszuführen. Die Berechtigungsvergabe für Benutzerkonten erfolgt, indem der Nutzer einer Berechtigungsstufe zugeordnet wird. Generell sollte gelten, dass jedem Nutzer nur die minimal notwendigen Berechtigungen zugeteilt werden. Somit lassen sich analog der folgenden Beispiele unterschiedliche Rollen definieren:

- Ein Read-Only Account dient dazu, die Einstellungen des Geräts einzusehen. Änderungen der Konfiguration sind nicht möglich.

- Der Read-Write Account erlaubt die Änderung und Betrachtung der meisten Einstellungen des Geräts, Sicherheits- und Passwort-Einstellungen gehören nicht dazu.
- Der Read-Write-All Account ist für die umfassende Kontrolle inklusive Sicherheitseinstellungen, Zugriffspassworte und Web-basierte Managementzugriffe vorgesehen.
- Zudem sind spezielle Accounts für die Verwaltung von Layer-2- und Layer-3-Funktionen möglich.

Ein Benutzer ist somit nach seiner Anmeldung am Gerät automatisch einer Berechtigungsstufe zugeordnet, alternativ muss er nach der Anmeldung dediziert die zu nutzende Berechtigungsstufe und das zugehörige Passwort eingeben. Für sicherheitskritische Rollen sollte stets eine Absicherung des Zugriffs über einen zentrale Authentisierungsserver eingerichtet werden.

Die Möglichkeiten der Zuordnung von Berechtigungen zu Benutzern und Rollen können sogar so weit gehen, dass für jeden einzelnen Befehl Berechtigungen vergeben werden können, die jedes Mal vor der Ausführung über den Autorisierungsserver überprüft werden.

Bei der Erstellung des Rechte- und Rollenkonzepts für die Administration der aktiven Netzkomponenten müssen die Möglichkeiten der einzelnen Systeme in Betracht gezogen werden. Wie fein die Berechtigungsstufen im Einzelfall unterschieden werden, sollte unter Berücksichtigung von Einsatzzweck und Schutzbedarf festgelegt werden. Als Faustregel kann dabei gelten: "So fein wie nötig, so einfach wie möglich." Zu grobe Unterteilungen bieten keine angemessene Sicherheit, andererseits können zu feine Unterteilungen die Effizienz der Arbeit beeinträchtigen und bringen die Gefahr von Fehlern mit sich.

Passwortverschlüsselung

Router und Switches sollten die Möglichkeit unterstützen, Passwörter verschlüsselt in Konfigurationsdateien abzulegen (siehe auch M 2.280 *Kriterien für die Beschaffung und geeignete Auswahl von Routern und Switches*). Beispielsweise kann dies bei Cisco-Geräten mit dem Befehl *enable secret* erreicht werden.

Die Verschlüsselung von Passwörtern ist insbesondere dann wichtig, wenn Konfigurationsdateien über das Netz übertragen oder in zentralen Servern gespeichert werden.

Wenn das Gerät die Passwortverschlüsselung unterstützt, sollte diese Funktion unbedingt genutzt werden. Dabei sollte das Verschlüsselungsverfahren berücksichtigt werden, da einige Geräte unterschiedliche Verfahren unterstützen. Insbesondere bei älteren Betriebssystemen werden noch schwache Verschlüsselungsverfahren angewendet, die eventuell aus Gründen der Kompatibilität auch in neueren Versionen noch unterstützt werden. Hier sollte bei einer Migration auf ein neues Gerät oder eine neue Betriebssystemversion geprüft werden, ob die neuere Version stärkere Verschlüsselungsverfahren unterstützt.

Zudem bestehen für alle Geräte Prozeduren, die es zwar nicht ermöglichen, verschlüsselte Passworte wieder lesbar zu machen, die aber das Rücksetzen von Passwörtern durchführen.

Einige Dienste können nicht durch eine Passwort-Verschlüsselung abgesichert werden. Hierzu gehören SNMPv1 und SNMPv2, RADIUS und TACACS+. Die Passwörter der letztgenannten Dienste sollten somit immer einmalig sein, für keinen weiteren Dienst verwendet und regelmäßig geändert werden. SNMPv1 und SNMPv2 sollten allenfalls in Verbindung mit Out-of-Band-Management (siehe oben: Administrationsnetz) genutzt werden und möglichst durch SNMPv3 ersetzt werden.

Session-Timeouts

Sämtliche Zugriffsarten können durch die Vergabe von Passwörtern geschützt werden. Diese Absicherung kann jedoch wirkungslos werden, wenn Sessions unbeaufsichtigt sind, beispielsweise wenn ein angemeldeter Administrator seinen Rechner verlässt und dabei vergisst, die Session zu beenden oder die Bildschirmsperre zu aktivieren. Aus diesem Grund ist es empfehlenswert, Time-Outs einzurichten, um Verbindungen nach einem definierten Zeitraum ohne Nutzeraktivität zu beenden oder zu sperren. Dabei sollte eine Timeout-Zeit von 10 Minuten nicht überschritten werden.

Ergänzende Kontrollfragen:

- Wie werden die aktiven Netzkomponenten administriert?
- Findet die Administration in Anlehnung an die Sicherheitsrichtlinie statt?
- Werden die o. a. Punkte bei der Administration berücksichtigt?

M 4.205 Protokollierung bei Routern und Switches

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Router und Switches bieten in der Regel Möglichkeiten zur Protokollierung. Die Auswertung dieser Informationen ermöglicht die Beurteilung der korrekten Funktion des Geräts und das Erkennen von Angriffsversuchen. Mit Hilfe der Protokollierungsinformationen kann oft auch die Art eines Angriffsversuches nachvollzogen und die Konfiguration entsprechend angepasst werden.

Daher sollte die Protokollierung immer genutzt und sorgfältig eingerichtet werden. Die sorgfältige Konfiguration ist besonders wichtig, da nur bei einer sinnvollen Filterung aus der Vielzahl von Informationen die relevanten Daten extrahiert werden können. Hierzu gehören vor allem das Erkennen abgewiesener Zugriffsversuche und Änderungen der Konfiguration.

Da Protokolldateien in den meisten Fällen personenbezogene Daten beinhalten, ist sicherzustellen, dass diese Daten nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet werden (M 2.110 *Datenschutzaspekte bei der Protokollierung*). Der Umfang der Protokollierung und die Kriterien für deren Auswertung sollte dokumentiert und innerhalb der Organisation abgestimmt werden. Gegebenenfalls sollten frühzeitig die jeweiligen Mitbestimmungsgremien beteiligt werden.

Folgende Informationen sollten nach Möglichkeit protokolliert werden:

- Konfigurationsänderungen
- Reboots
- Systemfehler
- Statusänderungen pro Interface, System und Netzsegment
- Login-Fehler (zumindest dann, wenn sie wiederholt auftreten)
- Verstöße gegen ACL-Regeln (abgewiesene Zugriffsversuche)

Insbesondere der letzte Punkt sollte für jede ACL aktiviert werden, um alle fehlgeschlagenen Versuche zu erfassen und falsch oder nicht korrekt konfigurierte Regeln erkennen zu können.

Je nach Hersteller können einige Aspekte möglicherweise nicht durch die Protokollierung erfasst werden. Beispiele sind

- Änderung von Berechtigungen
- Passwortänderungen
- Änderungen über SNMP
- Speicherung einer neuen Konfiguration in das NVRAM

In diesem Fall sollten andere Möglichkeiten der Überprüfung in Betracht gezogen werden, um zumindest feststellen zu können, dass Änderungen vorgenommen wurden.

In der Regel sind die zu protokollierenden Informationen unterschiedlichen Klassen zugeordnet. Dies ermöglicht eine Filterung der Protokollierung, indem in der Konfiguration die auszugebende Protokollierungsklasse angegeben wird.

Neben einer geeigneten Speicherung der Informationen kommt der möglichst zeitnahen Auswertung besondere Bedeutung zu. Hierfür existieren unterschiedliche Ausgabemöglichkeiten, die abgestimmt auf die individuellen Bedürfnisse auch in Kombination miteinander angewendet werden können:

Nutzersession

Die Protokollierungsinformationen können in einer bestehenden Nutzersession angezeigt werden. Hierzu müssen die Protokollierung und die Sitzung entsprechend konfiguriert werden.

Speicher

Protokollierungsinformationen lassen sich im systemeigenen RAM ablegen. Die Größe des dafür erforderlichen Speichers hängt stark vom Typ und Einsatzzweck des Gerätes ab, so dass an dieser Stelle keine konkreten Vorschläge gemacht werden können. Eine Speicherung der Protokollierungsinformationen auf einem zentralen Server (syslog) ist gegenüber der Speicherung im RAM zu bevorzugen.

SNMP

Herstellerabhängig lassen sich auf Routern und Switches für eine Vielzahl von Ereignissen SNMP-Nachrichten generieren, die von einem bestehenden Netzmanagementsystem erkannt, angezeigt und verarbeitet werden können. Dies ermöglicht eine automatisierte Auswertung.

Ausgabe an der Konsole

Die Ausgabe der Protokollierung an der Konsole erlaubt keine dauerhafte Speicherung kann daher lediglich eine Ergänzung zu anderen Methoden darstellen.

Zentraler Authentisierungsserver

Bei der Nutzung eines zentralen Authentisierungsservers, zum Beispiel mittels TACACS+ oder RADIUS, kann die dort implementierte Protokollierung (Accounting) genutzt werden, um Nutzeraktivitäten zu dokumentieren.

Syslog

Die Protokollierungsinformationen können über das Netz auf einen eigenen syslog-Server (beispielsweise auf einem Unix-Rechner) übertragen werden. Dies dient der zentralen Sammlung und Archivierung der Protokollierungsinformationen, da auf den Netzkomponenten oft keine ausreichenden Betriebsmittel dafür vorhanden sind. Dadurch können an einer zentralen Stelle relevante Informationen erfasst und ausgewertet werden. Außerdem bietet dies den Vorteil, dass bei einer Kompromittierung eines Gerätes die bereits übertragenen Protokollierungsinformationen vom Angreifer nicht verändert oder gelöscht werden können.

Die Übertragung zum syslog-Server erfolgt meist unverschlüsselt über TCP oder UDP, so dass ein Mithören auf dem Übertragungsweg möglich ist. Somit kann durch das Versenden von Informationen aus dem internen Netz die Vertraulichkeit der im internen Netz vorhandenen Informationen gefährdet werden. Daher sollte überlegt werden, die Übertragung über ein eigenes Netz (Administrationsnetz) abzuwickeln.

NTP

Alle Protokollierungsinformationen sollten mit einem korrekten Zeitstempel versehen sein. Nur so ist eine effektive Auswertung dieser Daten, insbesondere bei der Analyse von versuchten oder erfolgten Angriffen, sichergestellt. Aus diesem Grunde sollten im internen Netz entsprechende Server eingerichtet werden, die allen Systemen die korrekte Zeit bereitstellen. Dies kann beispielsweise auf Basis des NTP-Dienstes geschehen. Dazu sollte in Erwägung gezogen werden, im internen Netz einen eigenen Zeit-Server einzurichten, der beispielsweise auf einem eigenen Rechner angesiedelt ist, der mit einer Funkuhr verbunden ist. Alternativ kann ein geeigneter Rechner als NTP-Proxy dienen und die Zeitinformation seinerseits per NTP von einem Zeit-Server im Internet (beispielsweise von der Physikalisch-Technischen Bundesanstalt (PTB)) bezieht. Im Zweifelsfall sollte die erste Lösung (interner Zeitserver mit Funkuhr) bevorzugt werden, insbesondere in Netzen mit hohem Schutzbedarf. Keinesfalls sollten alle Geräte individuell per NTP direkt Anfragen an Zeitserver im Internet stellen.

Ergänzende Kontrollfragen:

- Ist der Umfang der Protokollierung auf Routern und Switches in der Sicherheitsrichtlinie beschrieben?
- Wie wird die Protokollierung auf Routern und Switches durchgeführt?
- Wie findet die Auswertung statt?
- Werden bei der Auswertung Datenschutzaspekte berücksichtigt?
- Wie wird sichergestellt, dass alle Geräte eine korrekte Systemzeit haben?

M 4.206 Sicherung von Switch-Ports

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

In Abhängigkeit vom Schutzbedarf eines Netzes ist es oft wünschenswert, dass nur ganz bestimmte vertrauenswürdige Clients Zugang zum Netz erhalten. Zu diesem Zweck bieten viele Switches eine Reihe von Möglichkeiten, mit denen selbst dann, wenn ein Angreifer beispielsweise Zugang zu einer Netz-Anschlussdose erlangt hat, ein Zugriff auf das Netz verhindert werden kann.

MAC-Address Notification

Viele Switches bieten die Möglichkeit zu protokollieren, wenn sich die an einem Port angeschlossene MAC-Adresse ändert. Diese Option bietet zwar keine Zugriffskontrolle, kann aber zur Entdeckung von Angriffen wichtig sein. Beispielsweise kann eine Nachricht an den Administrator verschickt werden, wenn sich eine MAC-Adresse ändert.

MAC-Locking

Die verbreitetste Methode zur Absicherung von Switch-Ports ist das sogenannte MAC-Locking. Dabei wird am Switch festgelegt, dass an einem bestimmten physikalischen Port des Switches nur Clients mit ganz bestimmten MAC-Adressen (im Extremfall nur eine einzige MAC-Adresse) zugelassen sind. Erhält der Switch einen Ethernet-Frame mit einer anderen MAC-Adresse, so wird dieser nicht in das Netz weitergeleitet, sondern verworfen. Auf diese Weise kann in "statischen" Netzen ein relativ guter Schutz erreicht werden.

Allerdings ist die Pflege der entsprechenden Tabellen aufwändig und MAC-Locking bietet keinen Schutz vor einem Angreifer, der zunächst eine zugelassene MAC-Adresse ermittelt hat und beim Anschluss seines Gerätes diese Adresse verwendet (siehe auch G 5.113 *MAC-Spoofing*).

IEEE 802.1x

Der Standard IEEE 802.1x (EAPoL, *EAP over LAN*) definiert eine Möglichkeit, Geräte mit Hilfe eines Authentisierungsservers (beispielsweise RADIUS) zu authentisieren. Die Authentisierung erfolgt dabei über EAP (Extensible Authentication Protocol, RFC 2284), das eine Reihe verschiedener Authentisierungsprotokolle (*EAP types*) mit unterschiedlichen Stärken bietet.

Um eine Client-Authentisierung über 802.1x zu nutzen, muss meist auf den Endgeräten ein entsprechendes Client-Programm installiert werden. Die verschiedenen Client-Programme unterscheiden sich nach den unterstützten Betriebssystemen und Authentisierungsprotokollen. Das einzige Authentisierungsprotokoll, das laut Standard von allen Client-Programmen unterstützt werden muss, ist MD5-Challenge. Da dieses Protokoll keine besonders hohe Sicherheit bietet, sollten nach Möglichkeit andere *EAP types* verwendet werden. Die Zugriffskontrolle über 802.1x bietet einen Schutz gegen MAC-Spoofing.

Andere Verfahren

Je nach Hersteller existieren andere Verfahren, über die eine Zugriffskontrolle auf Switch-Ports realisiert werden kann. Beispielsweise gibt es die Möglichkeit, dass der Benutzer sich über ein Web-Interface anmeldet. Dabei läuft auf dem Switch ein Webserver, der die eingegebenen Authentisierungsdaten an einen Authentisierungsserver weiterleitet. Dabei muss allerdings beachtet werden, dass durch den auf dem Switch laufenden Webserver eventuell neue Gefährdungen entstehen.

Bei Geräten, die IEEE 802.1x oder andere Verfahren zur Zugriffskontrolle unterstützen ist es außerdem wichtig, den Default-Status vorzugeben, in dem sich ein Port normalerweise befindet. Dabei sind die folgenden Möglichkeiten relevant:

Authentication off / Port on	Der Port ist aktiviert und es findet keine Authentisierung statt.
Authentication on / Port off	Der Port ist so lange deaktiviert, bis eine erfolgreiche Authentisierung stattgefunden hat.
Authentication on / Port on with default policy	Der Port ist aktiviert, aber so lange keine erfolgreiche Authentisierung stattgefunden hat, ist nur ein eingeschränkter Zugriff erlaubt. Erst nach erfolgreicher Authentisierung wird der uneingeschränkte Zugriff freigegeben.

Tabelle: Default Status

In einem Netz mit einem hohen Schutzbedarf bezüglich der Vertraulichkeit ist es empfehlenswert, eine port-basierte Zugriffskontrolle einzurichten.

Wenn eine port-basierte Zugriffskontrolle eingerichtet werden soll, so muss im Rahmen der Planung des Einsatzes der Switches geklärt werden, ob sowohl der Switch selbst als auch die vorgesehenen Clients die entsprechenden Protokolle und Authentisierungsmethoden unterstützen. Außerdem sollte vorab getestet werden, ob das Zusammenspiel von Clients, Switches und Authentisierungsserver reibungslos funktioniert. In der Sicherheitsrichtlinie und den Betriebsanweisungen für die aktiven Netzkomponenten sollten die zu verwendenden Verfahren und Default-Einstellungen dokumentiert werden.

Ergänzende Kontrollfragen:

- Wird eine port-basierte Zugriffskontrolle eingesetzt?
- Falls 802.1x eingesetzt wird: Welches Authentisierungsprotokoll wird verwendet?
- Wie ist der Default-Status der Switch-Ports?
- Sind die relevanten Informationen in der Sicherheitsrichtlinie und den Betriebsanweisungen dokumentiert?

M 4.207 Einsatz und Sicherung systemnaher z/OS-Terminals

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Die Steuerung und Kontrolle eines z/OS-Betriebssystems erfolgt über die *HMC*-Konsole (*Hardware Management Konsole),* über verschiedene *MCS*-Konsolen (*Multiple Console Support*), eventuell über *Extended MCS*-Konsolen und darüber hinaus, falls erforderlich, über Monitor-Konsolen. Weitere Informationen zu den Konsolen finden sich in der Maßnahme M 3.39 *Einführung in die zSeries-Plattform*.

HMC-Konsolen

HMC-Konsolen sind über ein LAN mit den *Support Elements* (SEs) des zSeries-Systems verbunden. Sie erlauben sicherheitskritische Eingriffe in die Hardware, den Microcode und die Konfiguration des gesamten z/OS-Systems. Die folgenden Hinweise sind zu beachten:

Voreingestellte IBM-Kennungen

Die mitgelieferten Passwörter der voreingestellten IBM-Kennungen müssen gegen neue Passwörter ausgetauscht werden (dies gilt auch für alle Kennungen von Nicht-IBM-Produkten). Hierbei ist M 2.11 *Regelung des Passwortgebrauchs* zu beachten.

Schutz der HMC-Konsole

Die HMC-Konsole sollte in einem Raum betrieben werden, der gegen unbefugten Zutritt geschützt ist.

Der Zugang zur HMC-Konsole muss logisch geschützt werden. Für den logischen Schutz sollte die Login-Funktion durch personenbezogene Kennungen mit Passwort gesichert werden.

Der *IBM Product Engineering* Zugriff ist während der normalen Produktion zu deaktivieren.

Verbindung mit den Support Elements

Dediziertes LAN

Die HMC-Konsole sollte über ein dediziertes LAN mit den *Support Elements* verbunden sein. Wenn ein anderes LAN mitbenutzt wird, sollte eine feste Zuordnung zwischen *Support Element* und HMC-Konsole definiert werden, z. B. durch entsprechende Einstellung in der *Domain-Security*-Funktion.

Remote-Anbindung

Wenn die HMC-Konsolen über eine Remote-Anbindung betrieben werden sollen, müssen entsprechende Schutzmaßnahmen für den Remote Access-Zugang vorgesehen werden. In diesem Fall ist Baustein B 4.4 *Remote Access* anzuwenden.

Autorisierungs-Modi

Das Personal sollte verschiedenen Autorisierungs-Modi zugeordnet werden. Diese Modi sollten wie folgt eingesetzt werden:

- Access Administrator

  Dieser Modus ist nur an die Administratoren der HMC-Konsolen zu vergeben. Er darf nicht für normale Benutzer vergeben werden. Dieser Modus sollte nur wenigen Mitarbeitern zur Verfügung stehen.

- Operator

  Dieser Modus ist den normalen Bedienern zuzuordnen, die z. B. ein zSeries-Betriebssystem starten oder stoppen sollen (Initial Microcode Load oder Initial Program Load).

- Advanced Operator

  Dieser Modus wird normalerweise nicht benötigt, da die wesentlichen Betriebs-Funktionen in *Operator* enthalten sind und die anderen Funktionen, wie z. B. *Customization*, normalerweise unter *System Programmer* angesiedelt werden.

- System Programmer

  Dieser Modus sollte nur den Bedienern zugeordnet werden, die als System-Programmierer tätig sind und in dieser Funktion Anpassungen in der HMC-Konsole vornehmen.

- Service Representative

  Dieser Modus ist nur dem Service-Techniker vorbehalten und darf nicht anderweitig vergeben werden.

Web-Server

Die HMC-Konsole besitzt einen eigenen Web-Server, der einen eingeschränkten Funktionsumfang der HMC-Konsole für den Zugang über einen Web-Browser anbietet. Auf Netzebene sollten alle nicht autorisierten Zugänge zum Web-Server der HMC-Konsole gesperrt werden. Der Web-Server der HMC-Konsole sollte deaktiviert werden, wenn die Web-Schnittstelle zur HMC-Konsole nicht genutzt wird.

Standard-Einstellungen

Die vom Hersteller mitgelieferten Standard-Einstellungen der HMC-Konsole sollten geändert werden, so dass Benutzern nur die Darstellungen zugeordnet werden, die sie für ihre Arbeit auch benötigen (*Customize User Control Process* in der *HMC*-Konsole).

Wartungsarbeiten

IBM Product Engineering Zugriff

Es ist eine Vorgehensweise für die Benutzung der HMC-Konsole, bzw. der *Support Elements*, durch Techniker für Wartungszwecke einzurichten. Es ist sicherzustellen, dass nach Beendigung der Wartungsarbeiten die HMC-Konsole mit einer Betriebskennung aktiviert wird und nicht weiter mit der hoch autorisierten Technikerkennung betrieben wird.

Schulung

Das für den Betrieb der *HMC*-Konsolen eingesetzte Personal ist für die Benutzung der Konsole zu schulen, besonders in Bezug auf die komplexeren Funktionen. Dadurch sollen gravierende Fehlbedienungen vermieden werden.

Es sollte überlegt werden, ob Übungen an der HMC-Konsole die Sicherheit erhöhen, da die Konsole im Betrieb nur selten benötigt wird.

Support Elements (SEs)

Die *Support Elements* (zwei IBM Laptops) befinden sich im Gehäuse der zSeries-Hardware und sind mit den Ressourcen der Hardware fest verbunden. Von diesen *Support Elements* aus können die gleichen Kommandos wie von der *HMC*-Konsole ausgeführt werden.

Zugang

Der Zugang zu den *Support Elements* muss physisch geschützt werden. Dies ist in der Regel dadurch gewährleistet, dass die zSeries-Systeme in einem Rechenzentrum betrieben werden, das gegen unbefugten Zutritt geschützt ist. Das Hardware-Schloss der zSeries-Hardware bietet keinen ausreichenden Schutz.

Wartung

Die *Support Elements* werden auch von den Hardware-Technikern des Herstellers zu Wartungszwecken genutzt. Nach Beendigung der Wartungstätigkeiten sollten die Türen der zSeries-Hardware abgeschlossen und ggf. weitere Sicherheitsmechanismen wieder aktiviert werden.

MCS-Konsolen (Multiple Console Support)

Die *MCS*-Konsolen (aus historischen Gründen auch immer noch MVS-Konsolen genannt) bieten direkten Zugriff auf das Betriebssystem (MCS mit eigenem Input/Output-Protokoll, SMCS via VTAM seit z/OS V1R1). Die folgenden Sicherheitsmechanismen sind für MCS- und SMCS-Konsolen vorzusehen:

Login

AUTH-Definition

Es ist zu prüfen, ob der Schutz über *AUTH*-Definition im Member *CONSOL00* ausreicht oder ob *MCS*-Konsolen so definiert werden, dass ein Login mit Kennung und Passwort erforderlich ist, bevor die Konsole benutzt werden kann. Für *SMCS*-Konsolen, die auch Remote eingesetzt werden, ist ein Login-Vorgang in jedem Fall notwendig.

Physischer Schutz

Wenn kein Login mit Kennung und Passwort für die MCS-Konsole eingerichtet wird, muss sie in einem Raum betrieben werden, der vor unbefugtem Zutritt geschützt ist. Ausgenommen hiervon sind Konsolen, die so definiert sind, dass nur unkritische *Display*-Funktionen möglich sind.

MCS-Masterkonsole

Da die *MCS-Masterkonsole* nicht über Kennung und Passwort geschützt werden kann, muss diese Konsole in jedem Fall in einem Raum betrieben werden, der vor unbefugtem Zutritt geschützt ist.

Das z/OS-Betriebssystem macht die erste verfügbare Konsole zur Masterkonsole, soweit keine anderen Definitionen vorliegen. Die Zuordnung der Masterkonsole ist im Member *CONSOL00* so vorzunehmen, dass eine physisch geschützte Konsole zur Masterkonsole wird. Eine zweite MCS-Konsole, die durch das automatische Umschalten der primären MCS-

Masterkonsole im Fehlerfall zum *Master* wird, ist auf die gleiche Weise wie die primäre MCS-Masterkonsole zu schützen.

Logischer Schutz

Es muss durch entsprechende Definitionen sichergestellt werden, dass MCS-Konsolen, die in nicht zutrittsgeschützten Räumen betrieben werden, nur von autorisierten Benutzern verwendet werden können. Dies kann über die Konfigurations-Parameter *AUTH=xxx* oder *LOGON=REQUIRED* im Member *CONSOL00* vorgenommen werden.

Sind die MCS-Konsolen auf andere Weise ausreichend geschützt und wird ein Audit der Operatoren nicht gefordert, kann statt *LOGON=REQUIRED* auch die Definition *LOGON=OPTIONAL* im Member *CONSOL00* verwendet werden.

Individuelle Autorisierungen

Für *MCS*-Konsolen mit *Login*-Prozess sollte überlegt werden, jeder Kennung individuelle Autorisierungen zuzuordnen. Dies ermöglicht die Einteilung in unterschiedliche Operator-Gruppen (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*), was bei der Vorgehensweise ohne Authentisierung nicht möglich ist. Ansonsten stehen die Funktionen der Konsole für jeden offen, der physischen Zugang zur MCS-Konsole hat.

Extended MCS-Konsolen

Über die *Extended MCS-Konsole* stehen zum Beispiel MCS-Konsolen unter TSO (*Time Sharing Option*) via *System Display and Search Facility* (für JES2) oder *Flasher* (für JES3) zur Verfügung. Für diese Konsolen sollten die folgenden Hinweise beachtet werden:

RACF-Definitionen

Zum Schutz der MVS-Kommandos sind entsprechende RACF-Definitionen (Klasse *OPERCMDS*) einzusetzen. Ob die *Extended MCS*-Konsole benutzt werden darf, welche Kennung die *Extended MCS*-Konsole benutzen darf und welche Kommandos verfügbar sind, muss separat in RACF definiert werden (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*). In jedem Fall muss sichergestellt sein, dass die Konsol-Services und die dabei verwendeten z/OS-Kommandos nur von Anwendern benutzt werden können, die in RACF entsprechend autorisiert worden sind. Dies gilt für alle Applikationen, die mit *Extended MCS*-Konsolen arbeiten.

RSF-Konsole (Remote Support Facility)

RSF (*Remote Support Facility*) ermöglicht es dem zSeries-System, automatisch mit dem Hersteller Verbindung aufzunehmen und den dortigen Technikern Fehler des laufenden Systems zu melden (Hard- und Software). Darüber hinaus erlaubt es die RSF-Funktion prinzipiell auch, dass der Hersteller Microcode-Modifikationen in das System laden kann. RSF ist eine zusätzliche Funktion der HMC-Konsole (*Host Management Console*) und ist über eine Wählverbindung an das Telefonnetz angeschlossen.

Für die RSF-Funktion sind die folgenden Hinweise zu berücksichtigen:

Grundsätzliche RSF-Überlegung

Es ist zu überlegen, ob eine Funktion wie RSF überhaupt gewünscht wird und welche Teilfunktionen davon benötigt werden. Der Einsatz der Funktion muss mit dem für die Systeme zuständigen Hardware-Support über den Wartungsvertrag abgestimmt werden. RSF (und ähnliche Funktionen bei Festplatten von anderen Herstellern) wird normalerweise für die Fehlererkennung von Hard- und Firmware eingesetzt und erhöht deutlich die Reaktionsfähigkeit auf auftretende Fehler. Ob die Fernwartung durch RSF aktiviert werden soll, muss der Betreiber des Rechenzentrums entscheiden.

Wählverbindung zum Hersteller

Fehlermeldungen werden von der HMC-Seite aus initiiert, dabei wird eine Wählverbindung zum Hersteller aufgebaut. Es ist im Rahmen der Anpassung der HMC-Definitionen sicherzustellen, dass die eingetragene Telefonnummer korrekt ist und nur von autorisiertem Personal geändert werden darf.

Microcode-Anpassung

Wird eine Microcode-Anpassung (oder sonstige Modifikation der Firmware) durch den Hersteller angefordert, so ist der *IBM Product Engineering* Zugriff für den vereinbarten Zeitraum zu aktivieren. Die Verbindung wird dabei durch *Dial-In* hergestellt. Nach Ablauf der Wartungsarbeiten ist er wieder zu deaktivieren, um das Missbrauchsrisiko zu minimieren.

Dokumentation

Die RSF-Installation und deren Einsatz ist nachvollziehbar zu dokumentieren.

Ergänzende Kontrollfragen:

- Ist die *MCS-Masterkonsole* physisch geschützt?
- Wurden die voreingestellten Passwörter geändert?
- Gibt es eine Verfahrensrichtlinie, in der die Wartung durch den Hersteller geregelt ist?
- Ist der *IBM Product Engineering* Zugriff in der HMC für Microcode-Anpassungen abgeschaltet?
- Gibt es eine RSF-Dokumentation?

M 4.208 Absichern des Start-Vorgangs von z/OS-Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der Startvorgang eines z/OS-Systems erfolgt beginnend mit dem IML-Ablauf (*Initial Microcode Load*) über den IPL-Ablauf (*Initial Program Load*) eines z/OS-Betriebssystems bis hin zum Starten der einzelnen *System Tasks*. Für den Startvorgang sollten die folgenden Hinweise beachtet werden:

IML- und IPL-Parameter

Die IML- und IPL-Parameter müssen dem *Operating*-Personal bekannt sein. Eine aktuelle Dokumentation muss vorliegen.

Fallback-Konfiguration

Es muss immer eine Fallback-Konfiguration vorliegen. Mit der Fallback-Konfiguration muss das System vor der letzten Änderung erfolgreich gestartet worden sein.

IOCDS-Datei

Es muss eine gültige IOCDS-Datei (*Input/Output Configuration DataSet*) im HMC-Dialog (*Host Management Console*) verfügbar sein, mit der das System gestartet werden kann.

LPAR

Das zu startende System muss als LPAR (*Logical Partition*) auf der zSeries-Hardware eingerichtet und entsprechend konfiguriert sein.

MVS-Master-Konsole

Es muss eine MVS-Master-Konsole (*Multiple Virtual Systems*) verfügbar sein, damit die Nachrichten während der NIP-Phase (*Nucleus Initialization Program*) kontrolliert werden können. Zusätzlich muss eine Backup-Konsole definiert sein, auf die der *Master* automatisch umgeschaltet werden kann, wenn die normale Master-Konsole aus technischen Gründen nicht verfügbar ist (siehe M 4.207 *Einsatz und Sicherung systemnaher z/OS-Terminals*).

Automationsverfahren

Werden Automationsverfahren eingesetzt, muss eine Dokumentation vorliegen, welche *System Tasks* in welcher Reihenfolgen zu starten sind. Auch die notwendigen Kommandos müssen dokumentiert sein, um eventuelle Fehler der Automation (oder auch deren Komplettausfall) zumindest teilweise kompensieren zu können.

Abschluss des Startvorgangs

Es sollte eine Nachricht an das Ende des Startvorgangs platziert werden, die anzeigt, dass der Startvorgang abgeschlossen ist.

Prüfliste

Es sollte eine aktuelle Prüfliste vorliegen, die nach dem Startvorgang zur Überprüfung des System-Status herangezogen werden kann. Die Überprüfung

stellt sicher, dass das z/OS-System wie vorgesehen ohne Fehler aktiviert worden ist (Soll/Ist-Vergleich). Wenn Automationsverfahren existieren, können auch Funktionen aus diesen Verfahren dazu benutzt werden.

Ergänzende Kontrollfragen:

- Sind die IML- und IPL-Parameter bekannt und dokumentiert?
- Sind die LPARs konfiguriert und im HMC-Dialog verfügbar?
- Gibt es eine Dokumentation aller *System Tasks* und Anweisungen, die darstellt, wie sie aktiviert werden müssen?

M 4.209 Sichere Grundkonfiguration von z/OS-Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

z/OS-Grundkonfiguration

Das z/OS-Betriebssystem verwaltet und benutzt verschiedene Autorisierungsmechanismen. Bei fehlerhaftem Einsatz oder Missbrauch dieser Mechanismen kann sich dies auf die Integrität des gesamten Systems auswirken. Sie müssen deshalb in der Grundkonfiguration berücksichtigt werden. Es handelt sich dabei im wesentlichen um die folgenden Funktionen:

- APF-autorisierte Dateien (*Authorized Program Facility*),
- SVCs (*SuperVisor Calls*),
- Ressourcen-Schutz,
- Parmlib-Definitionen,
- System Prozeduren (*Started Tasks*) und
- JES2-Definitionen.

Empfehlungen für das Sicherheitssystem RACF (*Resource Access Control Facility*) sind in M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF* beschrieben. Darüber hinaus ist M 4.220 *Absicherung von Unix System Services bei z/OS-Systemen* für die Grundkonfiguration zu berücksichtigen.

Um die Integrität des z/OS-Betriebssystems zu schützen, sind die folgenden Empfehlungen zu berücksichtigen:

APF-Autorisierungen

Über APF-autorisierte Dateien ist es möglich, sich Zugriff zu privilegierten Operationen zu verschaffen (z. B. *MODESET SVC*). In der Folge lassen sich dadurch Funktionen benutzen, für die der Anwender normalerweise nicht autorisiert ist. So ist es jederzeit möglich, sich im Supervisor-Modus Zugriff zu privilegierten Hauptspeicherbereichen zu verschaffen und dort hoch privilegierte Attribute (z. B. *SPECIAL* im *ACEE - Accessor Environment Element*) der eigenen Kennung zuzuordnen. Für APF-Dateien ist das Folgende zu beachten:

- Alle APF-Dateien müssen über vollqualifizierte generische RACF-Profile (wie auch in M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF* beschrieben) geschützt werden, d. h. trotz der Benutzung von generischen Profilen sollte der komplette Dateiname als Profilname benutzt werden.
- Alle APF-Dateien werden im Parmlib-Member *PROGnn* mit Volume-Angaben (bzw. Angabe *SMS*) definiert. Es dürfen keine Einträge existieren, zu denen es keine Datei gibt, da sonst die Gefahr besteht, dass eine andere Datei untergeschoben wird.
- Zugriff zu den APF-Dateien dürfen nur Mitarbeiter haben, zu deren Aufgaben die Wartung des Systems gehört. Die Anzahl dieser Mitarbeiter ist auf ein Minimum zu beschränken. Eine Vertreterregelung muss vorgesehen sein.

- APF-Dateien sind regelmäßig auf Veränderungen zu überprüfen, um Missbrauch und Missbrauchsversuche möglichst frühzeitig zu entdecken. Änderungen an diesen Dateien sollten unter Produktionsbedingungen nur über angemeldete Wartungsfenster erfolgen.
- Es ist zu überlegen, ob der Einsatz eines Real-Time-Monitors hilft, Missbrauch schneller zu entdecken, und somit zur Erhöhung der Sicherheit beitragen kann (siehe M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS*). In jedem Fall sollten mindestens manuelle Kontrollen der Zugriffe auf APF-Dateien durchgeführt werden, etwa durch Auswertung von SMF-Sätzen (*System Management Facility*).
- Alle APF-Dateien sollten ohne *Extents* angelegt werden.
- Es sollte berücksichtigt werden, dass alle in der *LINKLIST* definierten Dateien bei Benutzung des Parameters *LNKAUTH=LNKLST* im Member *IEASYSxx* vom System standardmäßig als APF-Dateien angesehen werden. Auch für diese Dateien müssen deshalb die oben beschriebenen Sicherheitsmechanismen aktiviert werden.

User SVCs (SuperVisor Calls)

User-SVCs (alle SVC-Nummern ab 200) erhalten die Kontrolle im *SuperVisor*-Status mit *Key 0* (dies entspricht dem *Kernel-Modus* bei einigen anderen Betriebssystemen), d. h. User-SVCs haben Zugriff auf alle Speicherbereiche und alle Operationen des z/OS-Betriebssystems. Für *User-SVCs* ist deshalb das Folgende zu beachten:

- Alle Dateien, die SVC-Programme bereitstellen, müssen über vollqualifizierte generische RACF-Profile (wie auch in M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF* beschrieben) geschützt werden.
- Alle SVCs werden im Parmlib-Member *IEASVCxx* definiert. Da ein SVC durch die notwendigen internen Sicherheitsmechanismen nicht sehr klein sein kann, deutet ein *User-SVC*-Modul mit kleiner Länge eventuell auf ein Sicherheitsproblem hin. Solche *User-SVCs* müssen von der Systemprogrammierung darauf untersucht werden, ob sicherheitskritische Lücken vorhanden sind. In früheren Jahren wurden oft SVCs mit unzureichenden Sicherheitsmechanismen eingesetzt, z.B. sogenannte *Autorisierungs-SVCs*, um autorisierte Funktionen aus nicht-autorisierten Umgebungen heraus ausführen zu können. Falls solche SVCs noch existieren, sollten sie nach Möglichkeit entfernt oder ersetzt werden.
- Werden *User-SVCs* im Rahmen von Produkten mitgeliefert, sollten beim Hersteller die Sicherheitsmechanismen der mitgelieferten SVCs erfragt werden. Dies ist besonders wichtig, wenn das gelieferte SVC-Modul sehr klein ist, denn das ist eventuell ein Hinweis auf fehlende interne Prüfungen.

- Zugriff auf SVC-Dateien dürfen nur Mitarbeiter haben, zu deren Aufgaben die Wartung des Systems gehört. Die Anzahl dieser Mitarbeiter ist zu minimieren. Dabei muss jedoch sichergestellt werden, dass mindestens ein Vertreter Zugriff hat.

Ressourcen

Ressourcen des z/OS-Betriebssystems (z.B. Dateien, Programme, Funktionen usw.) sind über RACF zu schützen (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*). Darüber hinaus sollten folgende Empfehlungen beachtet werden:

- Für die *Class Descriptor Table* (CDT) sollten installationsspezifische Einträge nur im Modul *ICHRRCDE* vorgenommen werden. Als wichtige Parameter sind *DFTUACC* (hier wird *NONE* empfohlen) und *OPER* (hier wird *NO* empfohlen) zu beachten. Die *Dataset Name Table* (DSNT) muss die Dateinamen der RACF-Datenbanken enthalten.
- Die *Authorized Caller Table* (AUT) sollte laut Empfehlung von IBM leer sein. Dabei handelt es sich um eine alte Funktion, die heute durch die Klasse *Program* ersetzt worden ist, aber noch existiert. Ausnahmen müssen begründet sein.
- Die *TSO Authorized command and program table* in der Parmlib (*IKJTSOxx*) darf nur die Kommando- und Programm-Namen enthalten, die für die Ausführung unter TSO (*Time Sharing Option*) notwendig sind.
- Die *Started Procedure Table* (*ICHRIN03*) sollte nur noch wenige Einträge für Notfälle enthalten, ansonsten sollte für die Definition der autorisierten *Started Tasks* die RACF Klasse *STARTED* benutzt werden. Das Attribut *PRIVILEGED* sollte vermieden, *TRUSTED* nur eingesetzt werden, wenn erforderlich (z.B. bei JES2). Die Tabelle sollte einen generischen Eintrag für alle *Started Tasks* enthalten, die nicht definiert sind, um sicherzustellen, dass diese Tasks nicht lauffähig sind.
- Die *RACF Router Table* muss synchron zur CDT gepflegt werden.
- RACF bietet zwei Algorithmen zum Verschlüsseln des Passwortes an, den *Masking Algorithm* und die DES-Verschlüsselung (*Data Encryption Standard*). Die RACF-Passwörter sollten DES-verschlüsselt werden, da dies einen besseren Schutz bietet als das *Masking*. Gesteuert wird dies über den RACF-Exit *ICHDEX01*. RACF-spezifische Empfehlungen sind in M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF* zu finden.

IPL-Parameter-Datei

In der IPL-Parameter-Datei (*Initial Program Load*) stehen die wesentlichen Informationen, die zum Initialisieren des z/OS-Betriebssystems benötigt werden. Diese Datei muss über RACF geschützt werden, die Zahl der für diese Datei autorisierten Mitarbeiter muss klein gehalten werden. Es ist jedoch darauf zu achten, dass Vertretungsregeln eingeführt sind.

Parmlib-Definitionen

In den Parameter-Dateien des z/OS-Betriebssystems (*SYSn.PARMLIBs*, es können mehrere vorhanden sein) werden wesentliche Definitionen des Betriebssystems abgelegt. Alle Parmlib-Dateien sind mittels RACF-Profil zu schützen. Der Zugriff darf nur den Mitarbeitern erlaubt sein, die im Rahmen ihrer Tätigkeit diese Dateien bearbeiten. Es ist zu überlegen, ob verschiedene Parameter-Dateien mit unterschiedlichem RACF-Schutz eingesetzt werden sollen, da in der Parmlib Definitionen mit unterschiedlichem Schutzbedarf existieren. Sicherheitskritische Member der Parmlib sind zum Beispiel (ohne Sortierung):

- BPXPRMxx
- CLOCKxx
- COMMNDxx
- CSVLLA00
- IEASYSxx
- IEFSSNxx
- IKJTSOxx
- MSTJCLxx
- PROGxx
- SCHEDxx
- SMFPRMxx

Der Zugriff auf diese Definitionen muss auf die notwendigen Mitarbeiter beschränkt werden. Vertretungsregeln müssen in Kraft sein.

System-Prozeduren

Alle wichtigen Prozeduren der *Started Tasks* stehen in speziellen Bibliotheken, die entweder über die MSTJCLxx-Definitionen, oder über die JES2/3-Definitionen dem System bekannt gegeben werden. Diese Dateien, z. B. *SYS1.PROCLIB*, müssen über RACF-Profile geschützt werden, die nur autorisierten Mitarbeitern Zugriff auf die Definitionen gewähren.

Login-Prozeduren

Besonders wichtig ist der Schutz von allgemeinen, d. h. von allen Mitarbeitern benutzten Login-Prozeduren, da hier die Gefahr des Missbrauchs besonders groß ist (siehe Maßnahme M 4.213 *Absichern des Login-Vorgangs unter z/OS*). Der schreibende/ändernde Zugriff sollte auf die Systemadministratoren beschränkt werden, darüber hinaus benötigt nur JES2/3 einen lesenden Zugriff.

System-Scripts

Diese Schutzvorkehrungen gelten auch für alle in allgemeinen Login-Prozeduren verwendeten Script-Dateien (TSO CLISTs oder REXX EXECs), da auch hier die Gefahr des Missbrauchs besonders groß ist.

JESx Definitionen (Job Entry Subsystem)

Zum Schutz der *Job Entry Subsysteme* JES2 und JES3 müssen hauptsächlich die folgenden Ressourcen durch RACF abgesichert werden:

- JES-eigene Dateien,
- Input von anderen Quellen (z. B. anderen Knoten),
- Jobnamen,

- System Input/Output auf der JES-Spool und
- Output für andere Knoten oder Remote Workstations.

Die folgenden RACF-Funktionen sollten eingesetzt werden, um die Sicherheit von JES2/3 zu erhöhen:

- BATCHALLRACF

  (Erzwingen der Kennung bei Batch-Jobs)

- EARLYVERIFY

  (nur noch *Early Verify* möglich)

- XBMALLRACF

  (Unterstützung des Execution Batch Monitors)

- NJEUSERID

  (Zuordnung der *Default Userid* bei *Network Job Entry* Funktionen)

- UNDEFINEDUSER

  (Zuordnung der *Undefined Userid* bei *Network Job Entry* Funktionen)

Darüber hinaus stellt RACF eine Reihe von *General Resource Classes* für JES2/3 zur Verfügung, die zum Schutz von JES-Funktionen eingesetzt werden sollten:

- OPERCMDS
- JESSPOOL
- SURROGAT
- NODES
- WRITER

Ergänzende Kontrollfragen:

- Sind die APF-Dateien über vollqualifizierte generische RACF-Profile geschützt?
- Werden die APF-Dateien überwacht?
- Werden die SVCs regelmäßig überprüft?
- Sind *Parmlib* und *Proclib* so geschützt, dass nur wenige, autorisierte Mitarbeiter und ihre Stellvertreter Zugriff darauf haben?
- Sind die RACF *Resource Classes* für JES2/3 aktiviert?

M 4.210 Sicherer Betrieb des z/OS-Betriebssystems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Ein z/OS-Betriebssystem läuft im Normalfall weitgehend autonom ohne Eingriffe durch das Bedienungspersonal. Zur Absicherung des Betriebes gibt es jedoch einige Maßnahmen, die notwendigerweise ergriffen werden müssen, wenn die Funktionalitäten eines z/OS-Betriebssystems ohne Probleme zur Verfügung stehen sollen:

Überwachung

HMC-Kontrolle

HMC-Fehlermeldungen

Die HMC (*Host Management Console*) ist regelmäßig auf dort gemeldete Fehler (Hardware, Microcode, Software) zu untersuchen. Fehler, die dem Hersteller durch die RSF-Funktion (*Remote Support Facility*) gemeldet werden, sollten in der Betriebsorganisation bekannt sein, bevor der Hersteller anruft.

WTOR-Überwachung

Überwachung der z/OS-Replies

WTOR-Nachrichten (*Write To Operator with Reply*) des z/OS-Betriebssystems müssen überwacht werden, um sicherzustellen, dass neu hinzugekommene Anfragen des Betriebssystems, falls erforderlich, sofort beantwortet werden. Analog gilt dies auch für wichtige WTO-Nachrichten (*Write To Operator*) des Betriebssystems oder seiner Komponenten, die unter Umständen ein sofortiges Reagieren erfordern.

System Tasks

Es muss sichergestellt werden, dass alle geplanten *System Tasks* aktiv sind. Dies ist meist an bestimmten Nachrichten während des Starts oder an Reaktionen der jeweiligen *System Task* auf Abfragen zu erkennen. Es reicht meist nicht aus, nur deren Vorhandensein durch *Display*-Kommandos zu kontrollieren, sondern es sollte auch die Reaktion der *System Task* geprüft werden.

Kapazitätskontrolle

Es muss sichergestellt werden, dass die Kapazitätsgrenzen des Systems nicht überschritten werden. Dies bedeutet, dass die planerischen Vorgaben eingehalten werden sollten, was regelmäßig zu überprüfen ist.

Überwachung der Sicherheitsverletzungen

Die Einhaltung der Sicherheitsvorgaben muss überwacht werden. Sicherheitsverletzungen müssen über die definierten Mechanismen gemeldet werden (siehe M 2.292 *Überwachung von z/OS-Systemen*).

System-Auslastung

Überwachung der Systemauslastung

Die Systemauslastung muss mit geeigneten Mitteln überwacht werden, bei Überlastung sind korrektive Maßnahmen erforderlich, z. B. das Reduzieren der JES2/3 *Initiators* (*Job Entry Subsystem*). Es ist zu überlegen, ob neben den standardmäßig vorhandenen Funktionen (RMF - *Resource Measurement*

Facility) zusätzliche, spezielle Monitore eingesetzt werden sollen, um das System noch effizienter zu überwachen.

Automation System

Überwachung durch Automationsfunktionen

Es ist zu überlegen, ob eine Automationsfunktion (als Eigenentwicklung oder als fertiges Produkt) eingesetzt werden sollte, um die trivialen Überprüfungen des Systems regelmäßig durchzuführen. Dazu gehört z. B. der Soll-/Ist-Vergleich aktiver Tasks und aktiver NJE-Verbindungen sowie offene Replies, System-Performance, JES2/3 Queue-Belegung und mehr. Dies ermöglicht eine einheitliche *System Alive*-Nachricht statt vieler unstrukturierter Nachrichten, wodurch die Kontrolle wesentlich erleichtert werden kann.

Werden mehrere z/OS-Systeme zentral von einer Funktion überwacht, sollte überlegt werden, die Ausnahme-Informationen (*Events*) an einer Konsole darzustellen (*Alert Management*). Verschiedene Hersteller bieten entsprechende Programme im Rahmen ihrer Automationspakete an.

Automation Batch-Jobs

Kontrolle der Batch-Jobs

Es ist zu überlegen, ob eine Automationsfunktion für die Kontrolle der Batch-Jobs eingesetzt werden soll. Ab einer bestimmten Anzahl von zu kontrollierenden Batch-Jobs ist dies unabdingbar, da sonst eine konsistente Überwachung nicht mehr zu realisieren ist. Job-Scheduler, die tausende von Batch-Jobs kontrollieren können, sind von verschiedenen Herstellern erhältlich.

Reduzieren der Systemnachrichten

Nachrichten nur, wenn wichtig

Systemnachrichten sollten so reduziert werden, dass nur wirklich wichtige Nachrichten dargestellt werden. Der Einsatz von Nachrichten-Filtern ist im Rahmen von Automationsfunktionen zu empfehlen (MPF - *Message Processing Facility*).

Focal Point Konzept

Zentrale Kontrolle

Wenn viele z/OS-Betriebssysteme eingesetzt werden, ist zu überlegen, eine zentrale Kontrollstelle (*Focal Point*) einzurichten.

Absicherung der Betriebsfunktionen

IT-Sicherheit ist keine Einmal-Angelegenheit, sie muss im laufenden Betrieb immer wieder überprüft und auch an die Gegebenheiten angepasst werden. Solche Anpassungen erfordern im laufenden Betrieb oft sicherheitsrelevante Aktionen, die entsprechend geschützt werden müssen. Für den sicheren Betrieb eines z/OS-Systems müssen deshalb folgende Empfehlungen berücksichtigt werden:

Kontrollierte Wartungsarbeiten

Keine Wartungsarbeiten außerhalb des Wartungsfensters

An einem laufenden z/OS-System dürfen keine die Produktion beeinflussenden Wartungsarbeiten und Änderungen außerhalb des Wartungsfensters durchgeführt werden. Alle Änderungen, ob geplant oder ungeplant, müssen über ein Change-Management-Verfahren mit allen beteiligten Fachverantwortlichen abgestimmt werden. Der Change-Plan sollte zur Nachverfolgbarkeit archiviert werden.

Software Installation durch SMP/E

Einsatz von SMP/E

Eine Software-Installation darf erst nach einer Anmeldung über das Change-Management-Verfahren durchgeführt werden. Um Fehler zu vermeiden, muss zur Software-Installation ein Verfahren wie SMP/E (*System Management Process Enhanced*) eingesetzt werden.

Dynamische Änderungen

Viele sicherheitsrelevante Änderungen lassen sich heute dynamisch, d. h. während des Betriebs, vornehmen, ohne dass ein IPL (*Initial Program Load*) notwendig wäre. Dynamische Änderungen am System dürfen nur während geplanter Wartungsarbeiten, bzw. auf Antrag, ausgeführt werden. Besonders sicherheitsrelevante dynamische Befehle, wie z. B. *SETAPF*, *REFRESH LLA*, *MODIFY*, *CONFIG*, *FORCE* oder *SET*, müssen über entsprechende RACF-Profile geschützt werden. Sie dürfen nur von geschultem Personal auszuführen sein.

SDSF

SDSF (*System Display and Search Facility*) muss so geschützt werden, dass Unberechtigte keine Systemkommandos missbrauchen können. So darf es z. B. nicht möglich sein, beliebig viele *Initiators* zu aktivieren. Weiterhin muss die Prioritäten-Steuerung für Jobs im System in SDSF geschützt werden (Zuordnung von *WLM-Service-Klassen*). Es darf Anwendern nicht erlaubt sein, die Priorität ihrer Batch-Jobs zu ändern, um z. B. für sich eine bessere Performance zu erhalten.

Diese Empfehlung gilt analog auch für *Flasher*, eine JES3-Unterstützung, die in dieser Hinsicht der SDSF-Funktionalität entspricht.

Schutz der Konsolen

Der Schutz der Konsolen ist in Maßnahme M 4.207 *Einsatz und Sicherung systemnaher z/OS-Terminals*) beschrieben. Es muss durch entsprechende RACF-Definitionen verhindert werden, dass sich Mitarbeiter unberechtigt Zugang zu einer EMCS (*Extended Multiple Console Support*) verschaffen können.

Schutz der MVS-Kommandos

System-Kommandos

z/OS-System-Kommandos dürfen nur von berechtigten Personen ausgeführt werden. Diese Kommandos müssen über entsprechende RACF-Profile geschützt sein. Es muss festgelegt werden, welche Mitarbeiter die Berechtigung für bestimmte System-Kommandos benötigen und diese ausführen dürfen. So ist zu überlegen, ob z. B. das Stoppen und Starten von Tasks allein durch das *Operating* zu erfolgen hat.

HCD

Hardware-Definition

Bestimmte Hardware-Einstellungen können während des Betriebs eines z/OS-Systems nachträglich definiert werden. Dies erfolgt durch den HCD-Prozess (*Hardware Configuration Definition*). Die Aktivierung des neuen IOCDS (*Input/Output Configuration Dataset*) sollte jedoch nur im Rahmen des Change-Managements durchgeführt werden. Bei der Definition von Hardware muss darauf geachtet werden, dass es nicht vorkommt, dass Ressourcen über

mehrere Einzelsysteme *Shared* definiert werden. Ein Zugriff auf die gleiche Festplatte von zwei unterschiedlichen Einzelsystemen aus sollte beispielsweise nicht möglich sein. Bei *Parallel-Sysplex*-Konfigurationen gehört *Resource-Sharing* zur Architektur und ist deshalb - bei sachgerechter Konfiguration - kein Problem.

Operation (Betrieb)

Es sollte überlegt werden, für das *Operating* zwei RACF-Gruppen einzurichten, eine für langjährig erfahrene Operatoren und eine zweite für neue (noch unerfahrene) Mitarbeiter. Alle Mitarbeiter sollten nur die Rechte erhalten, die sie benötigen. Sie müssen für ihre Aufgaben ausreichend geschult sein. Besonders sicherheitskritische Aufgaben sollten erfahrenen Mitarbeitern übertragen werden.

Ergänzende Kontrollfragen:

- Wird die HMC auf Fehler überwacht?
- Wird die Verfügbarkeit der *System Tasks* kontrolliert?
- Wird die Systemauslastung kontrolliert?
- Ist eine Automationsfunktion für die Überwachung des System-Zustands implementiert?
- Ist eine Automationsfunktion zum Betrieb und zur Kontrolle der Batch-Jobs vorhanden?
- Werden Änderungen nur über das Change Management aktiviert?
- Werden Wartungsarbeiten, wie z. B. Hardware-Definitionen, nur während der dafür vorgesehenen Zeitfenster durchgeführt?
- Sind die *EMCS*-Konsolen vor nicht-autorisiertem Zugriff geschützt?

M 4.211 Einsatz des z/OS-Sicherheitssystems RACF

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die sichere Konfiguration eines z/OS-Systems erfolgt durch Definitionen von Betriebssystem-Komponenten und zentral über das Sicherheitssystem RACF (*Resource Access Control Facility*). In dieser Maßnahme werden Empfehlungen für den Einsatz von RACF erläutert. Informationen für die Sicherung der z/OS-Definitionen können der Maßnahme M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen* entnommen werden.

In RACF werden die Kennungen der Anwender und die Zugriffsmöglichkeiten auf unterschiedliche Ressourcen in Form von Profilen verwaltet. Diese stehen als *Dataset* Profile, *General Resource* Profile, *Group* Profile und deren Verbindungen sowie als *User* Profile zur Verfügung.

Für die Verwaltung von RACF sind die folgenden Regeln zu berücksichtigen:

Wesentliche RACF-Einstellungen

SETROPTS Definitionen

Die zentrale Konfiguration des RACF erfolgt in den *SETROPTS* Einstellungen. Hier werden allgemeingültige systemweite Einstellungen für das RACF vorgenommen. Da hier sehr viele Parameter veränderbar sind und sich teilweise gegenseitig beeinflussen, müssen die Einstellungen gut konzipiert und durchdacht sein. Nachfolgend eine Aufzählung der wichtigsten Parameter, die über das Kommando *SETROPTS* gesetzt werden müssen.

- *Resource Access Policies* für allgemeine Resource-Klassen

CLASSACT	Access Authorization Checking
AUDIT	schaltet Protokollfunktion für Klassen an
RACLIST	definiert, welche Profile in den Speicher geladen werden
GENERIC	aktiviert *Generic Profile Checking*
NOADSP	verhindert diskrete Profile
PROTECTALL	stellt sicher, dass RACF-Profile erstellt werden
WHEN	erlaubt konditionalen Schutz für Programme
CMDVIOL	protokolliert alle RACF-Verstöße
OPERAUDIT	kontrolliert Kennungen mit Attribut *OPERATIONS*
ERASE	löscht Dateninhalt nach Löschen einer Datei
u. a.	

Tabelle: Resource Access Policies

- *Password Policies* für die Behandlung der Passwörter

INTERVAL	Gültigkeitsdauer des aktuellen Passworts
REVOKE	Anzahl ungültiger Anmelde-Versuche vor dem Sperren
RULE	definiert Passwort-Regeln
u. a.	

Tabelle: Password Policies

Die RACF-Grundeinstellung ist wesentlich für die Sicherheit des z/OS-Betriebssystems und relativ komplex. Da hier u. U. mehr als 30 Parameter definiert oder aktiviert werden müssen, ist eine ausführliche Planung notwendig. Diese stellt sicher, dass die Parameter richtig gesetzt werden und vermeidet so potentielle Sicherheitslücken. Zur Unterstützung des Planungsvorgangs bietet der Hersteller einen *RACF Security Planner* an (auch im Internet). Der *RACF Security Planner* gibt auch Empfehlungen für die RACF-Grundeinstellung.

Voreingestelltes RVARY-Passwort

Das voreingestellte Passwort für das RVARY-Kommando, z. B. für den SWITCH der RACF-Datenbanken, muss verändert werden und darf nicht auf dem voreingestellten Wert stehen.

Einsatz von RACF-Exits

Es ist zu untersuchen, ob *RACF-Exits* benötigt werden. Durch verschiedene *Exits* lässt sich erreichen, dass RACF Sicherheitsprüfungen übergeht oder zusätzliche Sicherheitsprüfungen durchführt. Geänderte und eigene *Exits* sind zu dokumentieren. Dabei sind Funktion und Grund für den Einsatz anzugeben. Werden *Exits* eingesetzt, sind sie zu überwachen (siehe M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS*).

RACF-Kennungen

Begrenzung der Anmeldeversuche

Eine in RACF angelegte Kennung erlaubt dem Anwender die Authentisierung gegenüber dem z/OS-System. Zum Schutz gegen Brute-Force-Attacken ist die Anzahl der Anmeldeversuche zu begrenzen, damit die Kennung automatisch gesperrt werden kann (maximal 3 bis 5 Versuche).

Anlegen einer Kennung

Für das Anlegen einer Kennung muss ein Verfahren existieren. Das Verfahren muss sicherstellen, dass nur Personen, die den Zugang zu dem jeweiligen System für ihre Arbeit benötigen, und deren Vertreter eine Kennung erhalten. Das Verfahren kann z. B. über ein Formblatt oder automatisiert ablaufen. In jedem Fall muss der Systemverantwortliche den Antrag genehmigen.

Segmente einer Kennung

Es sind nur die Segmente einer Kennung im RACF zu aktivieren, die der Anwender für seine Tätigkeit auch benötigt (z. B. *TSO*, *Netview*, *DCE* oder *OMVS*).

Freischaltung einer Kennung

Zum Freischalten einer gesperrten Kennung ist ein Verfahren einzuführen. Der Anwender muss sich gegenüber der freischaltenden Stelle, wie Call Center oder User Helpdesk, eindeutig identifizieren und seinen Anspruch nachweisen. Erst daraufhin darf die Kennung des Anwenders freigeschaltet werden.

TSO-Segment Daten

Die Daten aus dem TSO-Segment (*Time Sharing Option*), wie z. B. Name der Logon-Prozedur, Account-Nummer oder Speicherplatz, sollten durch RACF-Profile vor dem Überschreiben durch den Anwender geschützt werden. Dadurch kann der Anwender nur mit der vorgeschriebenen Umgebung arbeiten. Ausnahmefälle müssen begründet und dokumentiert werden.

Sperren wegen Inaktivität

Die Kennung eines Anwenders sollte aus Sicherheitsgründen nach einer bestimmten Zeitspanne der Inaktivität gesperrt werden, z. B. nach 90 Tagen. Von dieser Regelung auszunehmen sind Verfahrens-Kennungen, beispielsweise Notfall-Kennungen und STC-Kennungen. Es ist zu überlegen, nach einem noch längeren Zeitraum, z. B. 180 Tagen, die gesperrten Kennungen daraufhin zu überprüfen, ob sie gelöscht werden können. Wird ein solcher Löschvorgang durchgeführt, muss sichergestellt werden, dass die Ergebnisse des Löschvorgangs protokolliert werden und die RACF-Administration darüber informiert ist. Die Protokolle müssen gesichert abgespeichert werden und dienen der Nachvollziehbarkeit durch die RACF-Administration.

Löschen einer Kennung

Die Kennungen von Anwendern werden entweder auf Antrag gelöscht oder als Ergebnis von internen Überprüfungen. Beim Löschen einer Kennung muss darauf geachtet werden, dass neben der Kennung in RACF alle entsprechenden Zuordnungen und auch der ALIAS-Eintrag dieser Kennung im Masterkatalog gelöscht werden. Die Dateien dieser Kennung müssen entweder ebenfalls gelöscht oder einer anderen Kennung zugeordnet werden.

Limitierung restriktiver Kennungen

Kennungen mit hohen Rechten sollten nur dann vergeben werden, wenn die Mitarbeiter diese Berechtigungen tatsächlich für ihre Arbeit benötigen. Weitere Informationen hierzu finden sich in der Maßnahme M 2.289 *Einsatz restriktiver z/OS-Kennungen*.

RACF-Gruppen und -Gruppenstruktur

Berechtigungen sollten nicht direkt an eine Kennung vergeben werden. Anwender mit gleichen Aufgaben sollten in Gruppen zusammengefasst werden und über diese Gruppen die Berechtigungen erhalten. Eine Trennung der Gruppenstruktur ist zu empfehlen, z. B. nach dem folgenden Schema:

Organisationsgruppen	Zuordnung der Kennungen zu Organisationseinheiten der Behörde bzw. des Unternehmens, beispielsweise ORGA
Funktionsgruppen	Über diese Gruppen erhalten die Anwender ihre Rechte anhand der Aufgaben (Funktion) im System, beispielsweise FUNKT.
Ressourcen-Gruppen	zur Verwaltung der Datei-Ressourcen. Für jedes angelegte Dateiprofil im RACF muss eine Gruppe oder eine Kennung existieren. Gruppen sind zu empfehlen, da diese nicht zum Einstieg in das System missbraucht werden können, z. B. RES.

Tabelle: Trennung der Gruppenstruktur

Nachfolgend eine beispielhafte Darstellung der Gruppenstruktur:

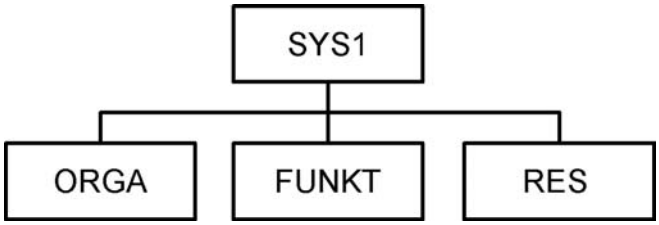


Abbildung: Prinzipaufbau der empfohlenen Gruppenstruktur im RACF

Der Name der Gruppe SYS1 ist fest vorgegeben. Sie ist immer die oberste Gruppe. In dieser Gruppe befindet sich nur der *IBMUSER*, der bei einer Neuinstallation benötigt wird. Zum Umgang mit dem *IBMUSER* siehe Maßnahme M 2.289 *Einsatz restriktiver z/OS-Kennungen*.

Die *Owner*-Struktur der Gruppen im RACF ist durchgängig anzulegen. In diesem Beispiel ist SYS1 der *Owner* der Gruppen ORGA, FUNKT und RES. Für weitere Untergruppen sollte als *Owner* der jeweilige Gruppenname der übergeordneten Gruppe gewählt werden. Der hierarchische Aufbau vereinfacht die Übersicht beim Einsatz der Berechtigungen *Group-Special*, *Group-Operations* und *Group-Auditor*.

Schutz durch RACF-Definitionen

Schutz von Started Tasks

Attribut PROTECTED

Started Tasks sind mit einer Kennung im RACF mit dem Attribut *PROTECTED* anzulegen. Das Attribut *PROTECTED* verhindert dabei den Missbrauch der Kennung zum normalen Login. *Started Tasks* sind in der RACF-Klasse *STARTED* zu definieren und zu schützen. Weitere Informationen über *Started Tasks* finden sich in der Maßnahme M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen*.

Schutz von sicherheitskritischen Programmen

Sicherheitskritische Programme sind mit der RACF-Klasse *PROGRAM* zu schützen. Der Zugang zu diesen Programmen ist nur Anwendern zu gewähren, die diese Programme für ihre Tätigkeit benötigen, sowie deren Vertretern. Weitere Informationen zum Umgang mit sicherheitskritischen Programmen sind in M 4.215 *Absicherung sicherheitskritischer z/OS-Dienstprogramme* zu finden.

Schutz von Dateien

Dateien werden im RACF über Dateiprofile geschützt. Dies betrifft sämtliche Systemdateien sowie alle Dateien der produktiven Anwendungen. Für den Schutz von Dateien sollten die folgenden Regeln beachtet werden:

- Dateien müssen generell über generische Dateiprofile im RACF geschützt werden. Diskrete Dateiprofile sind zu vermeiden.
- Kein Dateiprofil sollte mit *Universal Access* (UACC) größer *NONE* angelegt werden. Es sollte durch organisatorische oder technische Mechanismen verhindert werden, dass Anwender für die eigenen Dateiprofile den UACC-Wert verändern können.
- *General Resource*-Profile sollten nur dann mit UACC größer *NONE* angelegt werden, wenn dies unbedingt erforderlich ist. Dies sollte nachvollziehbar dokumentiert werden.
- In einem Produktions-System dürfen Dateiprofile und *General Resource*-Profile nicht im *Warning*-Modus laufen, da sonst kein echter Schutz der Ressourcen gewährleistet ist, denen diese Profile zugeordnet sind. Beim Einsatz des *Warning*-Modus auf einem Test-System ist darauf zu achten, dass die Performance des Systems nicht gravierend negativ beeinflusst wird (durch das Generieren von MVS-Nachrichten und SMF-Records).
- Um den Aufwand der RACF-Pflege zu begrenzen, sind Standards für die Erstellung und Benutzung von Dateinamen und RACF-*General Resources* notwendig (siehe M 2.285 *Festlegung von Standards für z/OS-Systemdefinitionen*).
- Hochautorisierte Dateien, wie z. B. APF-, SVC-Dateien, *Parmlibs* und *Proclibs*, dürfen nur über voll qualifizierte generische Dateiprofile geschützt werden. Weitere Informationen zum Schutz dieser Dateien sind in M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen* zu finden.
- Die RACF-Datenbank, die Backup-RACF-Datenbank und deren Sicherheitskopien sind mit UACC (*NONE*) zu schützen. Zugriffsrechte auf diese Dateien (selbst nur lesend) sind auf ein Minimum zu beschränken, um Brute-Force-Attacken auf die in der Datenbank gespeicherten Passwörter soweit wie möglich zu verhindern.

HFS-Dateien

Die HFS-Dateien (*Hierarchical File System*) des USS-Subsystems (*Unix System Services*) müssen im z/OS wie normale MVS-Datasets über RACF geschützt werden. Informationen zum Schutz der Files im USS sind in M 4.220 *Absicherung von Unix System Services bei z/OS-Systemen* enthalten.

Mandantenfähigkeit unter z/OS

In vielen Installationen ist es üblich, dass sich mehrere Kunden (Mandanten) ein z/OS-System teilen. Da sie somit auf dem gleichen System arbeiten, muss das z/OS-System mandantenfähig sein. Dies bedeutet unter anderem, dass ein Kunde nicht auf die Daten eines anderen Kunden zugreifen und somit auch nicht deren Vertraulichkeit, Integrität oder Verfügbarkeit beeinträchtigen kann.

Für die Mandantenfähigkeit sind folgende Hinweise zu beachten:

Trennung durch RACF-Profile

Die Daten und Anwendungen der Mandanten müssen durch RACF-Profile getrennt werden. Hierzu ist ein RACF-Konzept zur Mandantentrennung zu erstellen.

Absicherung der Betriebssysteme

Keiner der Mandanten darf ändernden Zugriff auf Dateien des z/OS-Betriebssystems haben. Solche Änderungen dürfen nur durch den Betreiber des z/OS-Systems erfolgen.

Kennungen mit hohen Berechtigungen

Hohe Berechtigungen im RACF (*SPECIAL, OPERATIONS, AUDITOR*) dürfen nur von Mitarbeitern des System-Betreibers verwendet werden. Es sollte überlegt werden, dem Kunden auf Wunsch die Berechtigungen *Group-Special*, *Group-Operations* und *Group-Auditor* zur Verfügung zu stellen. Hierzu muss ein Gruppenkonzept (*Owner*-Konzept) speziell für jeden Kunden erstellt werden.

Einsatz von RACF-Security-Labels

Es ist zu überlegen, *RACF-Security-Labels* für die Trennung der Kundenumgebungen zu verwenden, um die Mandantentrennung genauer durchsetzen zu können.

Abstimmung Wartungsfenster

Die Wartungsfenster, in denen das z/OS-System nicht zur Verfügung steht, sind mit allen Kunden, die auf dem betroffenen System arbeiten, abzustimmen.

Ergänzende Kontrollfragen:

- Sind die wichtigsten *SETROPTS*-Werte geeignet gesetzt?
- Ist das *RVARY*-Passwort neu gesetzt?
- Ist die Anzahl der ungültigen Login-Versuche begrenzt?
- Gibt es ein Verfahren zum Freischalten gesperrter Kennungen?
- Werden Kennungen ohne Aktivitäten nach Ablauf einer festgelegten Frist im System gesperrt?
- Sind die eingesetzten *RACF-Exits* dokumentiert?
- Sind die Wartungsfenster mit allen Kunden abgestimmt?

- Sind die Daten der unterschiedlichen Kunden ausreichend über RACF geschützt?

M 4.212 Absicherung von Linux für zSeries

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Verfahrensverantwortlicher, Administrator

Auf zSeries-Systemen kann auch das Betriebssystem Linux eingesetzt werden. Zur Absicherung des Betriebssystems ist in diesem Fall zusätzlich der Baustein B 3.102 *Unix-Server* bzw. Baustein B 3.206 *Unix-System* anzuwenden. Darüber hinaus sind im Folgenden einige zSeries-spezifische Besonderheiten beschrieben, die zu berücksichtigen sind.

Betriebsarten von Linux unter zSeries

Es sind drei unterschiedliche Methoden zum Betrieb von Linux unter zSeries möglich.

Linux Native auf zSeries Hardware

Das Linux-Betriebssystem wird als Single-System auf der zSeries-Hardware betrieben. Dies bedeutet, dass die gesamte zSeries-Hardware vom Linux-System benutzt wird.

Linux in einer zSeries LPAR

Bei dieser Variante erfolgt der Betrieb von Linux in einer *LPAR* (*Logical Partition*) auf der zSeries-Maschine. Der *LPAR*-Mode erlaubt den Betrieb von mehreren unabhängigen Betriebssystem-Installationen auf der gleichen zSeries-Hardware. Jede einzelne Partition verhält sich wie eine unabhängige Hardware. Auf diesen *LPARs* können unter anderem *z/OS* oder *Linux* als Betriebssystem installiert werden.

Linux unter dem Träger-System z/VM

Es können mehrere Linux-Installationen auf einem zSeries-Rechner oder innerhalb einer LPAR unter dem Träger-System z/VM betrieben werden. Das z/VM stellt sogenannte virtuelle Maschinen zur Verfügung, unter denen die einzelnen Linux-Installationen unabhängig von einander betrieben werden können.

Absicherung der Terminals

Die SE (*Support Elements*) und die HMC (*Hardware Management Console*) sind, wie in Maßnahme M 4.207 *Einsatz und Sicherung systemnaher z/OS-Terminals* empfohlen, zu sichern.

Absicherung von Linux unter z/VM

Für den Betrieb von Linux unter z/VM sollten zusätzlich folgende Empfehlungen berücksichtigt werden:

- Für z/VM müssen die aktuellen Patch-Stände eingehalten werden. Es ist darauf zu achten, nicht mit veralteten Systemen zu arbeiten.
- Die Berechtigungen des z/VM Systemadministrators sind sehr hoch. Er kann unter z/VM weitere virtuelle Maschinen einrichten oder löschen. Dies beinhaltet eine Vertrauensstellung, in der dem Administrator bewusst sein muss, dass er für die Sicherheit der Systeme mitverantwortlich ist.

- Nach der Installation von z/VM müssen das voreingestellte Login-Passwort und das voreingestellte *Minidisk*-Passwort sofort geändert werden.
- Unter z/VM definierte virtuelle Maschinen sollten nur die für die jeweiligen Aufgaben notwendigen Ressourcen erhalten, beispielsweise *Minidisks*, Adressen usw. Die Zugriffe werden über z/VM kontrolliert. Die strenge Trennung der virtuellen Maschinen muss eingehalten werden.
- Auch unter z/VM dürfen nur die benötigten Dienste gestartet werden. Nicht benötigte Dienste sind zu deaktivieren.
- Die Sicherheitsadministration von z/VM muss über *RACF für z/VM* erfolgen. *RACF für z/VM* dient als Security Manager und kann nur die Rechte der z/VM-Benutzer verwalten. Darüber hinaus sollten *Virtual Machines*, *Minidisks* und - falls gewünscht - auch Terminals über RACF *Resource Profile* geschützt werden. Zugriff auf diese Ressourcen dürfen nur diejenigen Anwender erhalten, die diese Rechte im Rahmen ihrer Tätigkeit benötigen. RACF kann jedoch nicht die Rechte der Linux-Benutzer und deren Zugriffe auf Systemressourcen innerhalb des Linux-Betriebssystems verwalten. Linux-Benutzer werden nach erfolgreichem Aktivieren des virtuellen Linux-Systems von den normalen Linux-Sicherheitsmechanismen kontrolliert. Sicherheitskritische System-Kommandos von z/VM (wie z. B. *CP DIAL*) sollten über RACF geschützt werden.
- Zur Verwaltung der Dateien und Verzeichnisse von z/VM ist zu überlegen, das Utility *DIRMAINT* einzusetzen. Es erlaubt eine übersichtliche Verwaltung der Anwenderverzeichnisse und hilft dadurch bei der Vermeidung von Administrationsfehlern. *DIRMAINTs* Sicherheitsmechanismen sollten immer auf *RACF für z/VM* basieren. Kommandos und Nachrichten im Rahmen der *DIRMAINT*-Administration sollten unter Audit-Kontrolle stehen.
- Die *Journaling*-Funktion von z/VM und die *Audit*-Funktionen von RACF sollten für Audits eingesetzt werden (siehe auch M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS*).
- Es sollten die unter Unix bzw. Linux üblichen Standardmechanismen zur Absicherung von TCP/IP-Anbindungen eingesetzt werden. Darüber hinaus ist zu überlegen, ob zusätzlich die von Linux unterstützten *KERBEROS Authentication Services* oder *Secure Socket Layer* (SSL) eingesetzt werden sollen.
- Die Linux-Definitionen sollten so eingestellt sein, dass der Aufruf rekursiver Funktionen nicht zur Überlastung des Betriebssystems führen kann (siehe auch G 3.69 *Fehlerhafte Konfiguration der Unix System Services unter z/OS*).

Linux-Authentisierung über z/OS RACF

Es ist zu überlegen, die Authentisierung von Linux-Benutzern über ein zentrales z/OS RACF mittels LDAP (*Lightweight Directory Access Protocol*) und ein Linux PAM (*Pluggable Authentication Module*) durchzuführen. Dies kann besonders bei einer hohen Anzahl zu administrierender Linux-Systeme zu einer erheblichen Reduzierung des Verwaltungsaufwands für die Kennungen führen.

Linux und Krypto-Hardware von zSeries-Maschinen

zSeries-Systeme können mit optionalen kryptographischen Prozessor-Karten vom Typ PCICA (*Peripheral Component Interconnect Cryptographic Accelerator*) oder PCICC (*Peripheral Component Interconnect Cryptographic Coprocessor*) ausgestattet werden. Diese Karten dienen der Performance-Verbesserung von Krypto-Funktionen und zur sicheren Verwahrung von digitalen Schlüsseln. Beide Karten werden auch von Linux unterstützt. Da Linux das CCF (*Cryptographic Coprocessor Feature*) nicht unterstützt, sollte überlegt werden, diese Krypto-Karten einzusetzen. Dies kann unter allen oben beschriebenen Installationsvarianten erfolgen. Unter z/VM können die Krypto-Karten von mehreren Linux-Systemen gleichzeitig und unabhängig von einander verwendet werden.

Kommunikation von Linux unter zSeries-Hardware

Die Kommunikation von Betriebssystemen, *z/OS* oder *Linux*, die entweder im *LPAR-Mode* oder unter *z/VM* auf derselben zSeries-Hardware installiert sind, sollte über interne Kanäle erfolgen, d. h. über *HiperSockets* oder virtuelle CTC-Verbindungen (*Channel-to-Channel*). Diese ermöglichen eine schnelle TCP/IP-Verbindung zwischen den Betriebssystem-Installationen. Im Vergleich mit der Kommunikation über das lokale Netz werden hierdurch die Fehler- und Angriffsmöglichkeiten reduziert, da die Informationen direkt innerhalb derselben Hardware von System zu System fließen.

Ergänzende Kontrollfragen:

- Ist die Hardware ausreichend gegen unberechtigte Zugriffe geschützt?
- Wird *RACF für z/VM* als Sicherheitssystem eingesetzt?
- Erfolgt die Kommunikation von Betriebssystemen, die auf der gleichen zSeries-Hardware installiert sind, über interne Verbindungen (*Hiper-Sockets*, virtuelle CTC)?

M 4.213 Absichern des Login-Vorgangs unter z/OS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der Zugang zu z/OS-Systemen - insbesondere der Login-Vorgang - muss geschützt werden. Hierzu sind folgende Empfehlungen zu beachten:

- Alle nicht für den Zugang benötigten Dienste und Ports sollten gesperrt sein. Es sollte überlegt werden, den Zugriff auf die benötigten Dienste und Ports durch RACF-Profile auf die autorisierten Zugriffsmöglichkeiten zu beschränken.
- Der Umgang mit Passwörtern sollte wie in Maßnahme M 2.11 *Regelung des Passwortgebrauchs* beschrieben erfolgen. Beim Zugang aus öffentlichen Netzen (Internet) zu z/OS-Systemen muss verhindert werden, dass alle Kennungen durch Falscheingabe von Passwörtern gesperrt werden. Dies kann zur Zeit nur durch den Einsatz von digitalen Zertifikaten gelöst werden. Es ist zu überlegen, ob die Automation des *RACF Reply* bei Kennungen mit dem Attribut *SPECIAL* aus Sicherheitsgründen unterbleiben sollte. Dies verhindert, dass alle Kennungen mit *SPECIAL* Attribut automatisch gesperrt werden können.
- Die Datei *SYS1.UADS* dient dazu, dass beim Ausfall des RACF noch eine Möglichkeit zum Systemzugang besteht. In diese Datei darf nur der *IBMUSER* oder ein (oder mehrere) *Notuser* eingetragen sein.

Darüber hinaus gelten die in M 4.15 *Gesichertes Login* beschriebenen Empfehlungen.

Ergänzende Kontrollfragen:

- Gibt es Notkennungen in *SYS1.UADS*?
- Sind die nicht benötigten TCP/IP-Dienste für Logins gesperrt?

M 4.214 Datenträgerverwaltung unter z/OS-Systemen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator

Um den Schutz von Festplatten und Bändern in z/OS-Systemen gewährleisten zu können, sind die nachfolgenden Empfehlungen zu berücksichtigen.

Festplatten

- Die Festplatten sind über entsprechende RACF-Profile (*Resource Access Control Facility*) und RACF-Klassen zu schützen. Es ist im RACF ein Profil für den Schutz des VTOC (*Volume Table of Content*) der Festplatte anzulegen. Das Arbeiten mit generischen Profilen - z. B. VTOC.** - ist möglich und zu überlegen.
- Der *Master-Katalog* ist durch ein RACF-Profil zu schützen, Mitarbeiter sind mit *READ* zu autorisieren. Ein schreibender Zugriff ist nur den Mitarbeitern zu erlauben, die dies im Rahmen ihrer Tätigkeit wirklich benötigen (z. B. beim Anlegen eines *ALIAS*).
- Zur Verwaltung und Erhaltung der Übersicht über die Festplatten in den Festplattenschränken ist ein Plattenbelegungsplan notwendig. Dieser Plattenbelegungsplan muss mindestens folgende Informationen enthalten:
  - Adresse der Festplatte,
  - Name der Festplatte,
  - Name des SMS-Festplatten-Pools, zu dem die Festplatte gehört (wenn SMS) und
  - Name des Plattenschranks, in dem die Festplatte generiert wurde.

  Dies ist schriftlich zu dokumentieren.
- Die Programme zum Verwalten der Festplatten (z. B. Initialisieren, Umkopieren von Daten u. a.) müssen geschützt werden. Die Programme dürfen nur von Mitarbeitern ausführbar sein, die diese Berechtigung für ihre Tätigkeit benötigen. Die Benutzung des Attributs *OPERATIONS* durch Programme sollte vermieden werden, weitere Informationen über dieses Attribut sind in M 2.289 *Einsatz restriktiver z/OS-Kennungen* zu finden, wenn es doch benötigt wird.
- Die Administrationsfunktion des ISMF (*Interactive Storage Management Facility*) muss über RACF-Profile geschützt sein. Nur berechtigte Anwender dürfen diese Funktionalitäten nutzen.
- z/OS-Befehle, mit denen Festplatten und Bänder in das System eingefügt, bzw. aus dem System herausgelöst werden können, sind über entsprechende RACF-Profile zu schützen. Sie dürfen nur von berechtigten Anwendern ausgeführt werden (siehe auch M 4.210 *Sicherer Betrieb des z/OS-Betriebssystems*).

- Die ACS-Routinen (*Automatic Class Selection*) des SMS (*System Managed Storage*) müssen geschützt sein und dürfen nur von berechtigten Anwendern angepasst werden. Es sollten Sicherungskopien der ACS-Dateien zur Verfügung stehen, die in einer Notfall-Situation zurückgespielt werden können.

Magnetbänder

- Der Schutz von Magnetbändern muss über entsprechende RACF-Profile und RACF-Klassen gewährleistet werden.
- Beim Einsatz von Verwaltungsprogrammen für Magnetbänder sind die Besonderheiten dieser Programme beim Schutz von Magnetbändern zu beachten (z. B. Einsatz von *TAPEVOL* und *TAPEDSN* Klasse).
- Durch entsprechende Vorkehrungen und Regelungen muss gewährleistet werden, dass genügend Bandstationen zur Verfügung stehen und diese nicht unnötig lange durch Belegung blockiert werden.
- Um den Schutz der Daten auf Magnetbändern zu gewährleisten, muss die Funktion *Bypass Label Processing* bei z/OS-Systemen gesperrt werden. Hierzu ist in der *General Ressource* Klasse *FACILITY* ein Profil mit dem Namen *ICHBLP* einzutragen. Dieses Profil ist mit *UACC=NONE* zu schützen. Zugang zu dieser Funktion darf nur in begründeten Ausnahmefällen temporär gewährt werden.

HSM (Hierarchical Storage Manager)

- Die Konfiguration des HSM erfolgt in einem Member (*ARCCMDxx*). Hier müssen auch die Kennungen der Administratoren für den HSM eingetragen sein. Die Datei, die dieses Member enthält, muss durch ein entsprechendes RACF-Profil geschützt werden, so dass nur die zuständigen Mitarbeiter Zugriff haben.
- Die Dateien, die auf Migrationsstufe 2 sind, befinden sich auf Magnetbändern. Diese Bänder müssen geschützt werden und dürfen nur von HSM bearbeitet werden.
- Es ist zu überlegen, wann die Backup-Sicherungen durch den HSM ausgeführt werden, um Behinderungen der Produktion durch *ENQUEUES* und *RESERVES* zu vermeiden. Ferner ist festzulegen, welche Platten gesichert werden sollen und wie die Plattensicherung erfolgen soll (*Full Volume* oder *Incremental* Speicherung).

Ergänzende Kontrollfragen:

- Ist die Funktion *Bypass Label Processing* deaktiviert?
- Gibt es einen Plattenbelegungsplan?
- Ist der Magnetbandschutz aktiv?
- Ist das Definitions-Member des HSM ausreichend geschützt?

M 4.215 Absicherung sicherheitskritischer z/OS-Dienstprogramme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

In z/OS-Systemen stehen den Systemprogrammierern, RACF-Administratoren und Storage-Managern Dienstprogramme zur Verfügung, über die bei entsprechender Autorisierung tiefgreifende Änderungen am z/OS-System durchgeführt werden können. Für eine sichere Benutzung dieser Programme müssen folgende Empfehlungen berücksichtigt werden:

Absichern sicherheitskritischer Programme

Sicherheitskritische Dienstprogramme müssen über das RACF-Sicherheitssystem (*Resource Access Control Facility*) entsprechend geschützt werden. Sie dürfen nur von den dafür vorgesehenen Mitarbeitern benutzt werden können. Ebenso sind die *Alias*-Namen der Programme zu schützen.

Nachfolgend eine Auswahl sicherheitskritischer Dienstprogramme:
- AMASZAP, AMASPZAP, IMASZAP
- ADRDSSU
- SYSIEH
- SMFDUMP
- ICKDSF
- IEHATLAS
- IEHINITT
- PGTFPF00
- IRRDBU00
- ICHDSM00
- IRRUT100, IRRUT200, IRRUT300, IRRUT400
- RESOLVE

Schutz von kritischen TSO-Kommandos

TSO-Kommandos (*Time Sharing Option*), hinter denen sich sicherheitskritische Programme verbergen, müssen über das Member *TSOKEY00* (in der z/OS *Parmlib*) entsprechend gesichert werden, damit nur autorisierte Mitarbeiter diese Kommandos benutzen können.

Unerlaubtes Installieren sicherheitskritischer Programme

Es muss sichergestellt werden, dass Fremdprogramme nicht unerlaubt installiert werden können. So sind im Internet einige Programme erhältlich, die sehr tief in das z/OS-System eingreifen können. Auch haben viele Systemprogrammierer selbstgeschriebene Programme, die ihre Arbeit erleichtern, aber u. U. sehr tiefgreifende Änderungen am z/OS-System vornehmen können. Ein unkontrolliertes Installieren und Ausführen dieser Programme muss durch entsprechende Schutzvorkehrungen unterbunden werden (siehe hierzu Maßnahmen M 4.209 *Sichere Grundkonfiguration von z/OS-Systemen* und M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*). Werden solche Programme dennoch benötigt, so dürfen sie nur über den offiziellen Installationsprozess in das System eingebracht werden.

Ergänzende Kontrollfragen:

- Ist sichergestellt, dass sicherheitskritische Dienstprogramme und TSO-Kommandos nur von entsprechend autorisierten Mitarbeitern benutzt werden können?

M 4.216 Festlegung der Systemgrenzen von z/OS

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Administrator

Für den Betrieb eines z/OS-Systems ist es wichtig, die Systemgrenzen für die maximale Belastung der Ressourcen festzulegen. Folgende Hinweise sind zu beachten:

Kommunikation der Systemgrenzen

Die Systemgrenzen, deren Planung in Maßnahme M 2.286 *Planung und Einsatz von zSeries-Systemen* beschrieben wird, müssen den betroffenen Administratoren und Anwendungseignern bekannt sein. Zu den Systemgrenzen zählen Angaben wie die maximale Größe einer Datei, der maximal zur Verfügung stehende Hauptspeicher, die maximale Größe von Dateien für FTP-Übertragungen (*File Transfer Program*), die Anzahl von LPARs (*Logical Partitions* auf einem zSeries-Mainframe), die Anzahl von Systemen in einem *Parallel-Sysplex-Cluster* und ähnliche Festlegungen. Systemgrenzen müssen bekannt sein und berücksichtigt werden, um Fehler beim Ablauf von Anwendungen zu vermeiden.

Magnetband-Stationen

Die Anzahl der zur Verfügung stehenden Magnetband-Stationen sollte mit den Anforderungen der betroffenen Anwendungseigner abgestimmt sein. Damit nicht zu viele gleichzeitige Belegungen von Magnetband-Stationen erfolgen, müssen die Zeiten, an denen Anwendungen auf Magnetband-Stationen zugreifen, unter den betroffenen Anwendungsentwicklern und -verantwortlichen abgestimmt sein.

Festplatten

Die benötigte Kapazität an Festplatten muss von den Anwendungseignern geplant und festgelegt sein. Das *Space-Management* muss darauf achten, dass der Speicherplatz auf den Festplatten ausreicht. Ist dies nicht der Fall, so ist der jeweilige Anwendungseigner zu informieren (zu *Space Management* siehe M 2.295 *Systemverwaltung von z/OS-Systemen*).

Initiators

Die *Initiators*, die im JES2 (*Job Entry Subsystem*) aktiviert sind, steuern die parallele Verarbeitung von Batch-Jobs. Ihre Anzahl muss an die Hardware-Voraussetzungen angepasst sein. Die Zahl und die damit verbundenen Restriktionen müssen den Anwendungseignern bekannt sein.

TSO-Anwender und Adressräume

Die maximale Anzahl der TSO-Anwender und die maximale Anzahl der zu startenden Adressräume müssen an die Hardware-Voraussetzungen angepasst sein.

Einsparungspotential

Es ist zu überlegen, ob System-Ressourcen eingespart werden können, wenn nach einer Zeit der Inaktivität eines Anwenders (z. B. 30 Minuten) dieser Anwender automatisch durch das System abgemeldet wird. Dabei ist zu

prüfen, ob dies zu Problemen mit den betriebenen Applikationen führt. Die Anwender sind über eine entsprechende Regelung zu informieren.

Ergänzende Kontrollfrage:

- Sind die Systemgrenzen den Administratoren und den Anwendungseignern bekannt?
- Wird die freie Kapazität der Festplatten regelmäßig überprüft?

M 4.217 Workload Management für z/OS-Systeme

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: IT-Verfahrensverantwortlicher, Administrator

Die Verwaltung der Ressourcen in einem *Parallel Sysplex Cluster* (aber auch in einem Einzelsystem) erfolgt durch die Komponente WLM (*Work Load Manager*) des z/OS-Betriebssystems. Für die Sicherheit des WLM-Einsatzes sind die folgenden Hinweise zu beachten:

Schutz der *Couple-Datasets*

Die für WLM notwendigen *Couple-Datasets* sind durch entsprechende RACF-Profile (*Resource Access Control Facility*) zu schützen. Für die WLM-Arbeitsdateien - ein oder mehrere PDS-Dateien (*Partitioned Datasets*) - gelten die gleichen Regeln. Das Dienstprogramm zum Anlegen der Dateien ist über das RACF *Facility*-Profil *MVSADMIN.WLM.POLICY* zu schützen.

Schutz des Modify-Kommandos

Es ist möglich, WLM-Optionen dynamisch durch ein *Modify*-Kommando zu verändern. Dieses Kommando darf nur autorisierten Mitarbeitern, wie entsprechend geschulten Operatoren oder Systemprogrammierern, zur Verfügung stehen.

Schutz des Reset-Kommandos

Das *Reset*-Kommando muss so geschützt werden, dass nur autorisierte Mitarbeiter WLM-Regeln für laufende Jobs ändern können.

Schutz der WLM-Applikation

Die WLM-Definitionen werden durch einen ISPF-basierenden WLM-Dialog gepflegt (*Interactive System Productivity Facility*). Der Zugang zu der WLM-Applikation sollte über das RACF *Facility*-Profil *MVSADMIN.WLM.POLICY* geschützt werden und nur autorisierten Mitarbeitern zur Verfügung stehen (Service- und Kapazitäts-Management).

Übereinstimmende Autorisierung

Definierte WLM-Vorgaben (z. B. die *Service Class*) können sowohl über MVS-Kommandos als auch über die SDSF-Schnittstelle (*System Display and Search Facility*) geändert werden. Es muss sichergestellt werden, dass die Berechtigungen zum Ändern des WLM über MVS-Kommandos und über das SDSF gleich sind.

Ergänzende Kontrollfragen:

- Sind die *Couple-Datasets* durch RACF-Profile geschützt?
- Ist die WLM-Applikation so geschützt, dass nur autorisierte Mitarbeiter Zugriff darauf haben?
- Sind die Kommandos, die den WLM beeinflussen können, hinreichend geschützt?

M 4.218 Hinweise zur Zeichensatzkonvertierung bei z/OS-Systemen

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Anwendungsentwickler, Administrator

Das z/OS-System arbeitet in der Regel mit dem EBCDIC-Zeichensatz (*Extended Binary Coded Decimal Interchange Code*). Dies gilt sowohl für die MVS-Dateien (*Multiple Virtual Storage*), als auch für die HFS-Dateien (*Hierarchical File System*). Ausnahmen sind lediglich im zFS-Filesystem möglich. Windows- und Unix-Systeme arbeiten meist mit dem ASCII-Zeichensatz (*American Standard Code for Information Interchange*). Bei der Kommunikation zwischen den unterschiedlichen Systemen müssen folgende Regeln beachtet werden:

- Sollen Textdateien übertragen werden, müssen Umsetzungs-Tabellen eingesetzt werden, die eine Zeichensatz-Konvertierung durchführen. Diese Tabellen werden im z/OS-Betriebssystem mitgeliefert. Es ist jedoch darauf zu achten, dass die richtige Tabelle verwendet wird.
- Bei der Übertragung von Binärdaten muss sichergestellt werden, dass die Konvertierung ausgeschaltet ist, da sonst die Daten nachher unbrauchbar sind.
- Beim Daten-Transfer von Unix- oder Windows-Systemen in ein HFS (*Hierarchical File System*) des z/OS-Systems - und umgekehrt - über FTP (*File Transfer Program*) muss darauf geachtet werden, dass die richtige Konvertierungs-Option beim Transfer aktiviert ist.
- Es ist besonders beim Übertragen von Programm-Quellcode zu überprüfen, dass wirklich alle Zeichen (und hier speziell einige Sonderzeichen) richtig übersetzt werden, damit nicht unbemerkte Programmfehler durch die Konvertierung entstehen. Beispielsweise führen falsche Zeichen in Konstantendefinitionen in einigen Fällen nicht zu einem Compiler-Fehler, sondern machen sich erst bei der Ausführung eventuell sehr viel später bemerkbar.

Ergänzende Kontrollfragen:

- Werden die richtigen Tabellen zur Zeichensatzkonvertierung verwendet?
- Sind die FTP-Jobs mit den richtigen Transfer-Optionen versehen?

M 4.219 Lizenzschlüssel-Management für z/OS-Software

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Verantwortliche der einzelnen IT-Anwendungen

Einige Software-Hersteller benutzen sogenannte *Activation-Keys* (Lizenzschlüssel), um die Nutzung ihrer Programme zu steuern. Diese Lizenzschlüssel laufen oft nach bestimmten Zeiten ab und müssen durch den Systembetreiber erneuert werden. Die folgenden Hinweise sind hierbei zu berücksichtigen:

Erneuerung von Lizenzschlüsseln

Es ist ein Verfahren einzurichten, so dass Lizenzschlüssel rechtzeitig erneuert werden. Andernfalls besteht die Gefahr, dass Software-Funktionen durch abgelaufene Lizenzschlüssel plötzlich nicht mehr zur Verfügung stehen.

Die Laufzeiten der Lizenzschlüssel sind zu dokumentieren. Die Dokumentation muss allen betroffenen Administratoren zur Verfügung stehen.

Es ist zu überlegen, ob die Gültigkeit der Lizenzschlüssel regelmäßig kontrolliert werden sollte.

Warnung vor Ablauf der Lizenz

Sollte Software im Einsatz sein, die ohne Warnung nach Ablauf des Lizenzschlüssels die Funktion einstellt, sollte mit dem Hersteller verhandelt werden, um eine Verbesserung der Situation zu erreichen. Die Software sollte z. B. rechtzeitig vor dem Ablaufen des Lizenzschlüssels warnen oder den Einsatz von Notschlüsseln erlauben.

Ergänzende Kontrollfragen:

- Ist ein Lizenzschlüssel-Management eingerichtet?
- Wird die Gültigkeit der Lizenzschlüssel regelmäßig kontrolliert?

M 4.220 Absicherung von Unix System Services bei z/OS-Systemen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: IT-Verfahrensverantwortlicher, Administrator

Unix System Services (USS) ist ein *Posix*-kompatibles Subsystem, das unter dem z/OS-Betriebssystem läuft. Für den generellen Schutz der *Unix System Services* müssen die im Baustein B 3.102 *Unix-Server* beschriebenen Maßnahmen umgesetzt werden. Weiterhin müssen einige zusätzliche Sicherheitsaspekte berücksichtigt werden:

Doppelte UID-Vergabe

Es muss sichergestellt werden, dass UIDs nicht doppelt vergeben werden, da sonst keine genaue Zuordnung zur MVS-User-ID möglich ist.

HFS-Dateien

RACF-Datei-Profile

HFS-Dateien (*Hierarchical File System*), die das Unix-Dateisystem beinhalten, sind über RACF-Datei-Profile zu schützen. Auf diese RACF-Profile sollte nur die *Unix Started Task* Zugriff erhalten. Ein Backup der HFS-Dateien sollte über HSM-Funktionen (*Hierarchical Storage Manager*) erfolgen. HFS-Dateien sollten jedoch nicht durch HSM migriert werden. Diese Empfehlungen gelten ebenfalls für zFS-Dateien.

ROOT-Dateisystem als READ-ONLY

Das *ROOT*-Dateisystem sollte mit der Option *READ-ONLY* gemounted sein.

Es ist zu überlegen, HFS-Dateien von Anwendern über die RACF-Profile der Kennung des jeweiligen Anwenders zu schützen. Um zu verhindern, dass jeder Anwender mit eigener HFS-Datei die Befehle *mount* und *umount* ausführen muss, sollte überlegt werden, die *Automount*-Funktion einzusetzen.

Member BPXPRMxx

Die wesentlichen USS-Parameter werden in der *Parmlib* im Member *BPXPRMxx* definiert. Einige Parameter beschreiben die zur Verfügung stehenden Ressourcen (z. B. *MAXPROCSYS* oder *MAXPROCUSER*). Diese Parameter müssen entsprechend der Leistungsfähigkeit der zSeries-Hardware bzw. LPAR eingestellt werden, um eine Überlastung des Systems zu verhindern.

Es sollten symbolische Variablen zur Definition dieses Members verwendet werden.

APF-Autorisierung

Es sollte im USS-Dateisystem keine APF-Autorisierung (*Authorized Program Facility*) über das *File Security Packet* (FSP) geben. Statt dessen sollten die Module von APF-Dateien des z/OS-Betriebssystems geladen werden.

Superuser UID(0) und UNIXPRIV

Viele System-Kommandos, für deren Nutzung unter anderen Unix-Systemen die Berechtigung *Superuser* (UID 0) nötig ist, können bei USS über die RACF-Profile in der RACF-Klasse *UNIXPRIV* geschützt werden. Dies

bedeutet, dass die Rechte der Administration durch RACF verwaltet werden können und so die *Superuser*-Berechtigung nur in sehr wenigen Ausnahmefällen vergeben werden muss. Die Empfehlungen zum Umgang mit *Superuser*-Rechten sind in M 2.289 *Einsatz restriktiver z/OS-Kennungen* aufgeführt.

RACF-Profile BPX.xxx der Klasse FACILITY

Zur Absicherung vieler USS-Funktionen sollten zusätzlich zu den Profilen in der Klasse *UNIXPRIV* die RACF-Profile *BPX.xxx* der Klasse *FACILITY* eingesetzt werden. Dadurch können in vielen Fällen höhere Autorisierungen vermieden werden (z. B. UID 0).

Audit und Monitoring

Für das Audit und Monitoring der USS sollten die gleichen Mechanismen wie für z/OS genutzt werden. Die Vorgänge im USS schreiben SMF-Sätze. Zugriffsverletzungen werden in RACF-Nachrichten übersetzt und erzeugen Meldungen im *Syslog*. Beide Quellen sollten, wie in Maßnahme M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS* beschrieben, ausgewertet werden. Einige Unix-Tasks, wie z. B. der mitgelieferte Webserver, schreiben Protokoll-Informationen in eigene Dateien. Diese sollten ebenfalls ausgewertet werden, falls die entsprechenden Programme aktiviert sind.

Zeichensatzkonvertierung

Es sollten die Empfehlungen in M 4.218 *Hinweise zur Zeichensatzkonvertierung bei z/OS-Systemen* beim Einsatz des USS-Subsystems beachtet werden.

Ergänzende Kontrollfragen:

- Wird auf APF-autorisierte Dateien im USS-Filesystem verzichtet?
- Ist das *ROOT*-Verzeichnis mit der Option *READ-ONLY* gemounted?
- Sind alle HFS-Dateien über RACF-Profile geschützt?
- Wird das USS-Subsystem auditiert?

M 4.221 Parallel-Sysplex unter z/OS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Verfahrensverantwortlicher, Administrator

Ein *Parallel-Sysplex-Cluster* ist ein Systemverbund aus mehreren z/OS-Systemen, die nach außen hin als ein System erscheinen. Dabei können die z/OS-Systeme auf einer oder auch auf mehreren LPARs (*Logical Partitions*) laufen. Zur Synchronisierung sind alle Systeme dieses Verbunds über eine *Coupling Facility* verbunden. Bei der Benutzung mehrerer LPARs muss zur Synchronisierung der System-Zeit (*Clock*) ein sogenanntes *Timer Facility* eingesetzt werden. Weitere Informationen hierzu finden sich in M 3.39 *Einführung in die zSeries-Plattform*. *Parallel-Sysplex-Cluster* kommen zum Einsatz, wenn hohe Anforderungen an die Verfügbarkeit und Skalierbarkeit bestehen.

Alle z/OS-Systeme eines *Parallel-Sysplex-Clusters* werden vom gleichen Festplattensatz geladen. Die einzelnen z/OS-Betriebssysteme werden über individuelle Systemdefinitionen unterschieden.

Beim Einsatz von *Parallel-Sysplex-Clustern* sollten folgende Empfehlungen beachtet werden:

Einsatz der Coupling Facility

Die *Coupling Facility* (CF) verbindet die LPARs untereinander. Sie stellt auch einen gemeinsam nutzbaren Speicher zur Verfügung, der in verschiedene Objekte, sogenannte *Coupling Facility Structures*, aufgeteilt ist. Der Zugriff auf die CF erfolgt über XES (*Cross-System Extended Services*). Es gibt drei verschiedene Speichertypen, die in der CF definiert werden können:

Cache Structures

Diese Struktur stellt hochperformanten Speicher für die gemeinsame Nutzung durch mehrere Anwender zur Verfügung. Werden Daten von der Festplatte gelesen, wird eine Kopie in den eigenen lokalen Speicherpuffer geschrieben. Darüber hinaus kann optional eine weitere Kopie in die *Cache Structure* der *Coupling Facility* gestellt werden.

List Structures

Diese Struktur erlaubt es mehreren Anwendern, Informationen miteinander zu teilen, die in Listen (*Message passing*) oder Warteschlangen (*Queues of work*) verfügbar sind.

Lock Structures

Diese Struktur kann verwendet werden, um die Benutzung von Ressourcen im *Shared*- oder *Exclusive*-Modus über alle LPARs zu steuern.

Einsatz

Wird der Betrieb eines *Parallel-Sysplex-Clusters* erwogen, z. B. aus Verfügbarkeitsgründen, sollte die *Coupling Facility* möglichst mit *Data Sharing* eingesetzt werden. Dies gilt zumindest für JES2/3 (*Job Entry Subsystem*), RACF (*Resource Access Control Facility*), VTAM (*Virtual Telecommunication Access Method*), *System Logger*, CICS, IMS und DB2. Es sollte geprüft werden, ob eine redundante Auslegung der *Coupling Facility* erforderlich ist,

um den Anforderungen an die Verfügbarkeit des Gesamtsystems Rechnung zu tragen.

Coupling Facilities werden über die HMC (*Host Management Console*) definiert und initialisiert. Empfehlungen zum Einsatz dieser Konsole finden sich in M 4.207 *Einsatz und Sicherung systemnaher z/OS-Terminals*.

Couple Datasets

Die *Couple Datasets* werden von XCF (*Cross-System Coupling Facility*) benutzt, um Informationen über die LPARs, Gruppen oder Member zu kontrollieren. Alle LPARs des *Parallel-Sysplex*-Verbundes müssen auf diese Datasets zugreifen können. Der Einsatz von *Alternate Couple Datasets* ist zu empfehlen. Unter z/OS müssen die *Couple Datasets* über RACF geschützt werden. Es sollten nur die Mitarbeiter verändernden Zugriff darauf erhalten, die im Rahmen ihrer Tätigkeit die Dateien bearbeiten, sowie deren Vertreter (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).

Zum Formatieren der *Couple Datasets* steht das Utility *IXCL1DSU* zur Verfügung. Dieses Programm sollte über RACF geschützt werden (Class *PROGRAM*). Das administrative Utility *XCMIAPU* erlaubt die Definition der *CFRM-Policy* (*Coupling Facility Resource Management*). Es sollte über ein entsprechendes *Facility*-Profil im RACF geschützt werden, so dass nur autorisiertes Personal Zugriff darauf hat. Weitere Empfehlungen zum Schutz kritischer Programme finden sich in M 4.215 *Absicherung sicherheitskritischer z/OS-Dienstprogramme*.

Sysplex-Kommandos

Zur Administration und Kontrolle stellt das z/OS-Betriebssystem das System-Kommando *SETXCF* zur Verfügung. Es unterstützt unter anderem die folgenden Aktivitäten:

- Definieren der *Couple Datasets*
- Umschalten zwischen *Primary*- und *Backup-Couple Dataset*
- Aktivieren einer neuen *CFRM-Policy*
- Start der *PATHIN*- oder *PATHOUT*-Verbindung
- Ändern der Struktur-Größe (*Structure Size*)
- *Rebuild* der Struktur nach Struktur-Fehlern

Zum Schutz dieses Kommandos (und aller anderen den *Parallel-Sysplex-Cluster* unterstützenden Kommandos) müssen entsprechende RACF-Profile definiert werden (siehe M 4.210 *Sicherer Betrieb des z/OS-Betriebssystems*).

XCF Kontrolle

RMF (*Resource Measurement Facility*) erzeugt einen sogenannten *XCF Activity Report*. Es ist zu überlegen, diesen Report zur Überwachung des Nachrichtenverkehrs zwischen den z/OS-Betriebssystemen einzusetzen, um Kommunikationsengpässe und *Deadlock*-Situationen rechtzeitig erkennen und präventive Maßnahmen ergreifen zu können.

Einheitliche RACF-Datenbank

Für alle LPARs des gesamten *Parallel-Sysplex-Clusters* sollte eine RACF-Datenbank mit einheitlichen RACF-Definitionen verwendet werden.

Standards

Um die Übersichtlichkeit und Wartbarkeit zu verbessern, sollten in folgenden Bereichen Standards eingeführt werden:

- Die Parameter-Member der *PARMLIBs* sollten standardisiert werden. Alle Namen müssen im *Parallel-Sysplex*-Verbund eindeutig sein. Hierzu gehören: Dataset-Namen, Subsystem-Namen, Prozedur-Namen, VTAM *Application IDs* (siehe M 2.285 *Festlegung von Standards für z/OS-Systemdefinitionen*).
- Sämtliche Systemeinstellungen der lokalen Definitionen in *PARMLIB* und *PROCLIB* sollten einheitlich sein. Es ist empfehlenswert, dass der strukturelle Aufbau der einzelnen Definitions-Member identisch ist.
- Die SMS-Struktur (*System Managed Storage*) muss im gesamten *Parallel-Sysplex*-Verbund einheitlich sein.
- Auf allen LPARs sollte eine möglichst einheitliche System-Software eingesetzt werden (eventuell ist hierdurch eine Anpassung der Software-Lizenzen notwendig).

Dimensionierung

Es muss auf die richtige Dimensionierung der Caches der Festplatten-Steuereinheiten, der Work-Platten, der Strukturen in der *Coupling Facility* und der *SPOOL*-Platten geachtet werden. Die Größe der Bereiche ergibt sich in erster Linie aus der Art und den Anforderungen der Anwendungen, die auf dem *Parallel-Sysplex*-Verbund laufen. In vielen Fällen enthalten auch die Dokumentationen der Software-Hersteller Hinweise hierzu.

Serialisierung

Es muss ein GRS-Verbund (*Global Resource Serialization*) eingerichtet werden, um die System-Aktionen serialisieren zu können. Der GRS-Modus muss im Member *IEASYSnn* der *PARMLIB* definiert sein (*RING*- oder *STAR*-Modus). Es sollte, wenn möglich, der modernere *STAR*-Modus gewählt werden, da diese Topologie durch die auf den *Couple Datasets* gespeicherten *Resource Name Lists* (RNLs) meist eine schnellere Verarbeitung bietet. Auch in Bezug auf die Verfügbarkeit ist der *STAR*-Modus in der Regel vorteilhafter.

Achtung: Der *STAR*-Modus ist nur mit *Coupling Facility* möglich.

Hochverfügbarkeit durch Redundanz

Bei hohen oder sehr hohen Anforderungen an die Verfügbarkeit sollte geprüft werden, ob die folgenden Redundanzmechanismen zweckmäßig sind:

- RACF mit Primary- und Backup-Datenbank
- Zweite Coupling Facility
- Alternate Couple Datasets

- Zweiter Timer (gekoppelt über Hochverfügbarkeitseinrichtung *FC 4048*, mit eigenem Stromkreis)
- Backup-Systemumgebung, damit im Fehlerfall ein System-Reboot ohne Zeitverzögerung erfolgen kann
- CTC-GRS-Ring (Kanalverbindung *ESCON* / *General Resource Serialization*)
- Backup-MCS-Masterkonsole (*Multiple Console Support*)
- Datensicherung von wichtigen Kontrolldateien, wenn möglich, mit der Option *Concurrent Copy* realisieren (Utility *ADRDSSU*)

Weitere Hinweise finden sich in M 6.93 *Notfallvorsorge für z/OS-Systeme*.

Festplattenzugriffe

Bei den Festplattenzugriffen sind folgende Empfehlungen zu beachten:

- Im *Parallel-Sysplex*-Verbund sollten keine Festplatten außerhalb des Verbundes zur Verfügung stehen. Festplatten, die nicht zum Verbund gehören, sollten nur für Recovery-Maßnahmen *Online* gesetzt werden können.
- Der Zugriff auf Festplatten des *Parallel-Sysplex*-Verbundes von anderen, nicht zum Verbund gehörenden Systemen sollte unter Produktionsbedingungen nicht möglich sein.
- Es ist zu überlegen, ob die Option *Enhanced Catalog Sharing* eingesetzt werden soll, wenn hohe Performance-Anforderungen vorliegen.
- Test-/Entwicklungs-Systeme und Produktions-Systeme sollten möglichst nicht im selben *Parallel-Sysplex-Cluster* betrieben werden.
- Das Betriebssystem sollte für alle z/OS-Systeme im *Parallel-Sysplex-Cluster* von einem Systemplatten-Satz geladen werden.

Symbolische Variablen

Es sollten symbolische Variablen an möglichst vielen Stellen der *PARMLIB*-Definitionen genutzt werden. Dies hilft, Fehler bei der Systemadministration zu vermeiden und erleichtert das *System-Cloning*.

System Logger

Der *System Logger* sollte mit *Staging Dataset* eingesetzt werden. (Im Fehlerfall wird auf diese Datasets von anderen Systemen im Verbund aus zugegriffen.)

Reduzierung der Konsol-Nachrichten

Um die Konsol-Meldungen zu reduzieren und überschaubar zu halten, wird empfohlen, die Message-Filterung zu aktivieren (siehe M 4.210 *Sicherer Betrieb des z/OS-Betriebssystems*). Dies ist besonders wichtig, da alle Nachrichten von allen z/OS-Betriebssystemen eines *Parallel-Sysplex-Clusters* auf einer MVS-Konsole angezeigt werden.

Ergänzende Kontrollfragen:

- Ist eine *Coupling Facility* im Einsatz?

- Sind die wichtigen Komponenten des *Parallel-Sysplex-Clusters* redundant ausgelegt?
- Existiert ein GRS-Verbund im *STAR*-Modus?
- Werden die Konsol-Nachrichten gefiltert?

M 4.222 Festlegung geeigneter Einstellungen von Sicherheitsproxies

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsbeauftragter

Verantwortlich für Umsetzung: Administrator

In dieser Maßnahme werden Empfehlungen zu Standardeinstellungen der wichtigsten Sicherheitsproxies zusammengestellt. Die vorgeschlagenen Einstellungen können allerdings die Funktionalität der betreffenden Inhalte einschränken (z. B. können eventuell Web-Seiten aufgrund des fehlenden JavaScript nicht mehr bedient werden) und müssen deshalb auf die eigenen Bedürfnisse angepasst werden.

HTTP

Aktive Inhalte filtern

Die Filterung aktiver Inhalte in Webseiten ist ein zentraler Punkt bei der Sicherheit der Clients (siehe auch M 4.100 *Sicherheitsgateways und aktive Inhalte*). Für Clients mit hohem Schutzbedarf bezüglich der Vertraulichkeit sollten aktive Inhalte in Webseiten grundsätzlich ausgefiltert werden. Gegebenenfalls können in Einzelfällen für vertrauenswürdige Websites aktive Inhalte zugelassen werden (Whitelist Strategie). Die entsprechenden Whitelists dürfen aber nicht zu umfangreich werden und müssen regelmäßig überprüft und gepflegt werden.

Folgende weitergehende Einstellungen werden für HTTP-Proxies empfohlen:

- Sperrung des HTTPS-Verkehrs, falls kein HTTPS-Proxy eingesetzt wird,
- Komplette Sperrung von Cookies (eventuell Freischaltung einzelner Webseiten),
- Filtern bzw. Ersetzen der Browserkennung,
- Filtern folgender Informationen aus dem Request-HTTP-Header:
  - Referer (falls beim Surfen eine Domain verlassen wird),
  - Via,
  - From,
- Filtern folgender Informationen aus dem Response-HTTP-Header:
  - Server,
- Prinzipiell Freigabe aller URLs. Ggf. Sperrung einzelner, bedenklicher URLs und
- Einschränkung auf notwendige MIME-Typen.

  Hinweis: Die Whitelist-Strategie "Alles sperren, was nicht explizit erlaubt ist" kann auf die Sperrung bzw. Freigabe von MIME-Typen nur schlecht angewendet werden. Aufgrund der Vielzahl der von Web-Seiten verwendeten MIME-Typen ist sehr schwierig, die relevanten Typen zu sperren und gleichzeitig die Funktionalität des Dienstes WWW wenigstens einigermaßen zu erhalten. Eine pragmatische Vorgehensweise ist die Sperrung besonders bedenklicher MIME-Typen. Um einen hohen Schutz zu erhalten, muss eine solche Sperrliste allerdings ständig vom Administrator auf dem Laufenden gehalten werden.

HTTPS

Bezüglich der Filterung von Schadprogrammen sollte wie beim HTTP-Proxy verfahren werden.

Ein HTTPS-Proxy ist die zentrale Entscheidungsinstanz für die Akzeptanz von Zertifikaten und nimmt den Benutzern weitgehend die Kontrolle über die Zertifikate ab. Aus diesem Grunde sind die Einstellungen des HTTPS-Proxies bezüglich der Vorgehensweise bei "problematischen" Zertifikaten besonders wichtig. Die folgende Tabelle gibt Vorschläge zur Einstellung in verschiedenen Fällen:

Entscheidung	**Vorschlag zur Einstellung**
Akzeptieren von Zertifikaten, die von einer Zertifizierungsstelle ausgestellt wurden.	Den in weit verbreiteten Browsern eingetragenen Zertifizierungsstellen kann vertraut werden. Dabei wird davon ausgegangen, dass die Vertrauenswürdigkeit der Zertifizierungsstellen durch den Hersteller der Browser überprüft wurde. Trotzdem sollte regelmäßig geprüft werden, ob alle Zertifizierungsstellen noch vertrauenswürdig sind. Gegebenenfalls können zusätzliche Zertifizierungsstellen hinzugefügt werden. Dies darf aber nur nach sorgfältiger Prüfung der Vertrauenswürdigkeit der Zertifizierungsstelle geschehen.
Akzeptieren von Zertifikaten, die nicht von einer Zertifizierungsstelle ausgestellt wurden ("self signed certificates").	Selbst erstellte Zertifikate dienen ausschließlich zur Verschlüsselung und bieten keine Funktionen zur Sicherstellung der Authentizität einer Web-Site. Solche Zertifikate sollten nur in Ausnahmefällen nach einer expliziten Überprüfung akzeptiert werden.
Tunneln von Webseiten (d. h. bei diesen besteht Ende-zu-Ende-Verschlüsselung).	Beim Tunneln wird die Filterung auf Schadprogramme umgangen. Daher sollte Tunneln nur ausnahmsweise zugelassen werden, wenn zu der betreffenden Gegenseite ein besonders hohes Vertrauen besteht.

Akzeptieren von Zertifikaten, bei denen der "Common Name" des Zertifikats nicht mit der aufgerufenen URL übereinstimmt.	Stimmen der "Common Name" des Zertifikats und URL nicht überein, so ist dies prinzipiell ein Indiz für eine Manipulation. Solche Zertifikate sollten prinzipiell nicht akzeptiert werden.
Akzeptieren von Zertifikaten trotz abgelaufenen Gültigkeitszeitraums.	Vertrauenswürdige Web-Sites sind gut betreut und besitzen immer ein gültiges Zertifikat. Zertifikate mit abgelaufenen Gültigkeitszeitraum sollten daher prinzipiell nicht akzeptiert werden.

Tabelle: Vorschläge zur Einstellung

SMTP

Auch im Zusammenhang mit SMTP (d. h. dem Dienst E-Mail) sollte M 4.100 *Sicherheitsgateways und aktive Inhalte* beachtet werden.

In verschiedene Sicherheitsproxies sind Spam-Filter integriert. Allerdings reichen die Fähigkeiten dieser Filter oft nicht an die Funktionalität dedizierter Spam-Filter (d. h. eigenständiger Komponenten) heran. Die Integration eines dedizierten Spam-Filters in das Sicherheitsgateway ermöglicht somit oft eine effektivere Filterung von E-Mails.

Derzeit existieren keine Verfahren, die "nützliche" E-Mails von Spam-Mails sicher unterscheiden können. Der Einsatz eines Spam-Mail-Filters ist deshalb nur dann zu empfehlen, wenn die Liste der verworfenen E-Mails ständig (in der Regel täglich) von einem Mitarbeiter nach versehentlich verworfenen E-Mails ("false positives") durchsucht wird.

Vorschläge zu Konfiguration und Betrieb des Spam-Filters:

- Der Spam-Filter sollte gesperrte E-Mails nicht an den Absender zurückschicken bzw. eine Meldung über die Tatsache der Sperrung ausgeben, da der Spam-Absender in diesem Fall weitere Informationen über die Existenz seiner Adressaten erhält.
- Ein automatisches Löschen von E-Mails kann aus verschiedenen (unter anderem aus rechtlichen) Gründen problematisch sein. Der Spam-Filter sollte daher keine E-Mails automatisch löschen, sondern sie stattdessen mit einem Hinweis versehen, dass es sich vermutlich um eine Spam-Mail handelt. Anhand dieses Hinweises kann der Mail-Client bzw. der Benutzer selbst eine Sortierung in unterschiedliche Postfächer oder Verzeichnisse vornehmen.
- Die Betreuung des Spam-Filters sollte durch organisationsinterne Mitarbeiter erfolgen. Wird die Filterung als Dienst eingekauft, ergeben sich eventuell (datenschutz-) rechtliche Probleme.
- Vor dem Einsatz von Spam-Filtern sollte eine umfassende rechtliche Zulässigkeitsprüfung im Einzelfall vorgenommen werden. Die allgemeine rechtliche Lage beim Einsatz von Spam-Filtern ist derzeit noch unklar. Die

Einführung von Spam-Filtern sollte zudem mit der Betriebsleitung und dem Betriebrat abgesprochen werden.

- Appliances zur Spam-Filterung können den Installationsaufwand verringern. Diese Produkte bieten oft umfassende Updatemöglichkeiten zur Verbesserung der Erkennungsrate.
- Bei eingehenden E-Mails sollte kontrolliert werden, ob Server des vertrauenswürdigen Netzes als Mail-Relay missbraucht werden. Dabei wird bei eingehenden E-Mails überprüft, ob die Empfängerdomain zum vertrauenswürdigen Netz gehört. Bei ausgehenden E-Mails sollte die Absenderdomain zum vertrauenswürdigen Netz gehören.
- Ausgehende E-Mails sollten ebenfalls kontrolliert werden. Dadurch kann der Schaden begrenzt werden, wenn trotz aller Sicherheitsmaßnahmen ein Client im internen Netz mit einem E-Mail-Wurm infiziert wird. Auf diese Weise kann eine Infektion oft auch sofort entdeckt werden.
- Auffällige E-Mail-Adressen sollten gesperrt werden.

Wird kein Spam-Filter in das Sicherheitsgateway integriert, so sollten die Mitarbeiter beim sicheren Umgang mit Spam-Mails geschult werden. Hinweise an die Mitarbeiter könnten sein:

- Spam-Mails ungelesen löschen,
- Unsubscribe-Funktion von Spam-Mails nicht verwenden,
- Mit dem Absender "fraglicher" vor dem Öffnen Rücksprache halten, falls dieser bekannt ist und
- Einige Provider wünschen die Zusendung von besonders auffälligen bzw. gefährlichen Spam-Mails. In Ausnahmefällen kann auch eine Benachrichtigung des Providers sinnvoll sein.

Filterung von Dateianhängen

Folgende Dateianhänge werden in den meisten Arbeitsumgebungen nicht benötigt und könnten gefiltert werden (geordnet nach der Art der Bedrohung):

Zugriff auf das gesamte System:

- * .bat (DOS-Batch-Datei)
- * .vbx (Visual-Basic-Datei)
- * .com (Windows-Anwendung)
- * .hta (HTML-Applikationen)
- * .inf (Installationsskript)
- * .js (Jscript-Datei)
- * .jse (Kodierte Jscript-Datei)
- * .wsh (Windows-Scripting-Host-Skript)
- * .vbs (Visual-Basic-Datei)
- * .vbe (Kodierte Visual-Basic-Datei)

Ausführung beliebiger Anwendungen:

- * .lnk (Link-Datei)
- * .chm (Kompilierte HTML-Datei)
- * .pif (Programm-Information-File)
- * .rm (RealMedia-Datei)

Weitere Probleme:

- * .mdb (Access-Datenbank. Können Makroviren beinhalten.)
- * .reg (Registry-Datei. Kann Veränderungen an der Registry vornehmen.)

Diese Liste ist zwangsläufig unvollständig. Es existieren viele weitere Dateitypen, mit denen ein Endgerät kompromittiert werden kann, die teilweise für Arbeitsvorgänge unbedingt benötigt werden (z.B. .html, .xls, .pdf). Das Filtern von Dateien alleine anhand von Dateiendungen oder MIME-Typen kann alleine keine ausreichende Sicherheit erzeugen, da Dateien mit Schadprogrammen oft mit unbedenklichen Endungen versehen und trotzdem ausgeführt werden.

Telnet

Telnet sollte nur noch in Ausnahmefällen verwendet und nach Möglichkeit durch ein sichereres Protokoll wie beispielsweise SSH ersetzt werden. Muss Telnet aus zwingenden Gründen trotzdem noch eingesetzt werden, so müssen mit Hilfe des ALG oder der Paketfilter die erlaubten Verbindungen auf ein Minimum beschränkt werden.

FTP

FTP sollte wie Telnet ebenfalls nur noch in Ausnahmefällen verwendet und die erlaubten Verbindungen müssen ebenfalls mit entsprechenden Filterregeln oder Acess-Control-Lists auf ein Minimum beschränkt werden.

Folgende Protokollbefehle sollten gefiltert werden:

- PORT (Filterung verhindert aktives FTP)

POP3

Bei POP3 sollte M 4.100 *Sicherheitsgateways und aktive Inhalte* beachtet werden.

Ergänzende Kontrollfragen:

- Für welche Protokolle werden Proxies eingesetzt?
- Falls Telnet oder FTP eingesetzt wird: Sind die erlaubten Verbindungen mit Hilfe entsprechender Filterregeln auf ein Minimum beschränkt?

M 4.223 Integration von Proxy-Servern in das Sicherheitsgateway

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsbeauftragter

Verantwortlich für Umsetzung: Administrator

HTTPS-Sicherheitsproxy

Der HTTPS-Proxy sollte den eintreffenden Datenverkehr entschlüsseln, der Inhaltefilterung zuleiten und daraufhin den Datenverkehr wieder verschlüsseln. Der temporär unverschlüsselte Datenverkehr kann auf unerwünschte Inhalte untersucht werden.

Im besten Fall wird ein HTTPS-Proxy vom angeschafften ALG unterstützt. Dann bietet sich der in Abbildung dargestellte, relativ einfache Aufbau an. Hier wird der Übersichtlichkeit halber der Fall betrachtet, in dem die Filterung auf einer eigenen Komponente durchgeführt wird. Vielfach wird die Filterung jedoch vom Hersteller bereits in das ALG integriert.

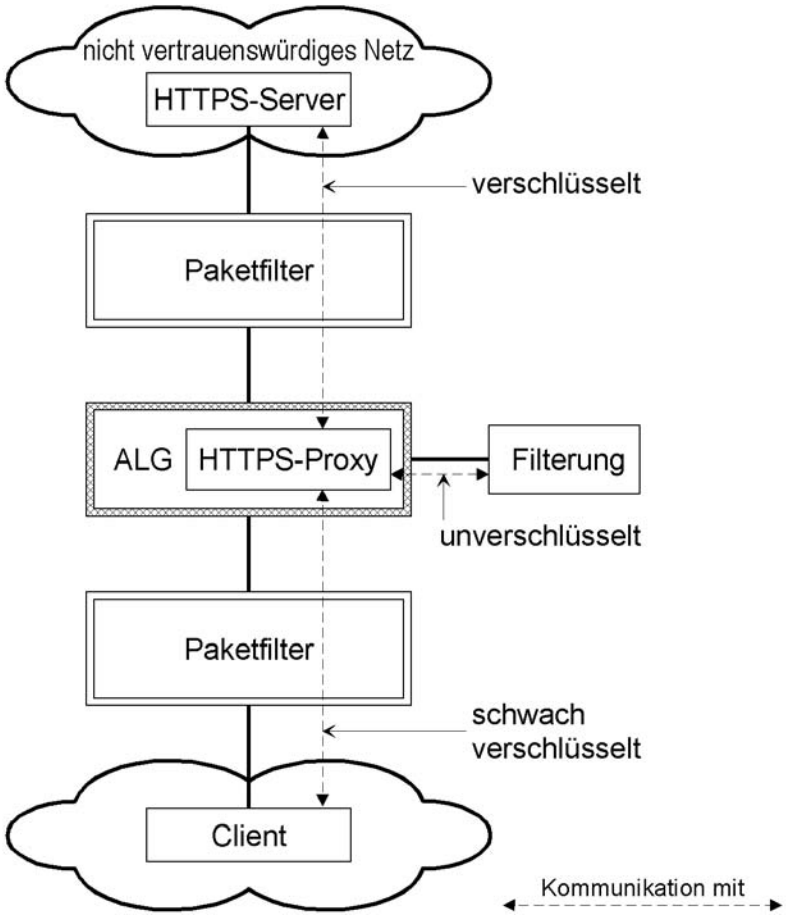


Abbildung: Integration eines internen HTTPS-Proxies

Vorteile "HTTPS-Proxy auf ALG"	Nachteile "HTTPS-Proxy auf ALG"
- Einfache Einrichtung, da in der Regel Konfigurationsoberflächen zur Verfügung stehen. - Gegenüber einem externen HTTPS-Proxy ergibt sich eine geringere Anzahl an Kommunikationsbeziehungen zwischen den an der SSL-Entschlüsselung und an der Inhaltefilterung beteiligten Modulen (da die Daten das ALG nicht verlassen müssen).	- Die Komplexität von SSL begünstigt Fehler bei der Entwicklung der Proxy-Software, was zu Schwachstellen führen kann. Durch Fehler in der SSL-Implementierung kann dann möglicherweise das gesamte ALG übernommen werden. - Der maximale Datendurchsatz wird aufgrund der rechenintensiven Schlüsselverarbeitung und der daraus resultierenden verstärkten Auslastung des ALG verringert.

Tabelle: Vorteile und Nachteile von HTTPS-Proxy auf ALG

Falls das ALG keinen HTTPS-Proxy anbietet, ergibt sich der in der Abbildung dargestellte Aufbau. Der HTTPS-Proxy befindet sich hier in einer eigenen DMZ. In der Abbildung ist abweichend von der vorhergehenden Abbildung der Fall dargestellt, bei dem die Filterung von Schadinhalten vom ALG wahrgenommen wird.

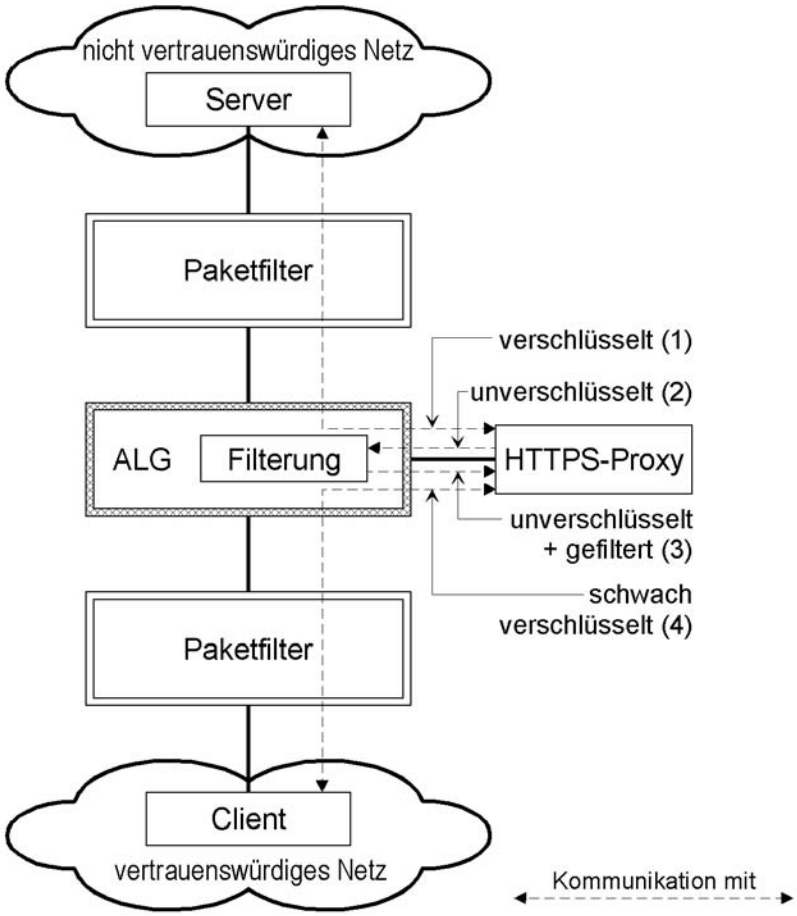


Abbildung: Integration eines externen HTTPS-Proxies

Vorteile "HTTPS-Proxy in DMZ"	Nachteile "HTTPS-Proxy in DMZ"
- Die Produktauswahl ist unabhängig vom ALG möglich. - Entlastung des ALGs, da die rechenintensive Schlüsselverwaltung auf einem eigenen Rechner stattfindet.	- Auf dem ALG müssen mehrere Proxies eingerichtet werden. - Fehlkonfigurationen werden aufgrund der komplexen Kommunikationsbeziehungen der beteiligten Komponenten begünstigt. - Erhöhte Latenzzeiten gegenüber einem auf dem ALG integrierten HTTPS-Proxy beim Abruf von Daten, da mehrere TCP- bzw. UDP-Verbindungen zwischen den einzelnen Modulen aufgebaut werden müssen.

Tabelle: Vorteile und Nachteile von HTTPS-Proxy in DMZ

Die Stärke der Verschlüsselung innerhalb des vertrauenswürdigen Netzes könnte bei beiden vorgestellten Lösungen dem Schutzbedarf und der Vertrauenswürdigkeit der Teilnehmer angepasst werden, ggf. kann hier zur Steigerung der Performance auf eine Verschlüsselung im vertrauenswürdigen Netz verzichtet werden oder ein weniger rechenintensives, schwächeres Verschlüsselungsverfahren eingesetzt werden.

Caching-Proxy

Bei der Nutzung von Diensten könnte der Zugriff auf das nicht-vertrauenswürdige Netz auf bestimmte Proxies (z. B. Caching-Proxy für HTTP) beschränkt werden. Ein Client-Zugriff nach außen unter Umgehung des ("Zwangs-") Proxies ist dann nicht möglich, da die IP-Adresse des Clients vom Sicherheitsgateway abgewiesen wird (nur die IP-Adresse des Caching-Proxy wird vom Sicherheitsgateway akzeptiert).

Vorteile von ("Zwangs-") Caching-Proxies	**Nachteile von ("Zwangs-") Caching-Proxies**

- Umfangreiche Möglichkeiten zur Protokollierung des HTTP-Verkehrs, falls nur ein einstufiges Sicherheitsgateway verwendet wird (bestehend aus einem Paketfilter).
- Erweiterte Filtermöglichkeiten, falls nur ein einstufiger Aufbau bestehend aus einem Paketfilter eingesetzt wird. Mit einem Caching-Proxy lassen sich beispielsweise filtern:
  - Cookies,
  - URLs,
  - HTTP-Referrer,
  - HTTP-Via und
  - HTTP-Server.
- Reduzierung des übertragenen Datenvolumens aufgrund der Caching-Funktionalität.
Anmerkung: In der Regel werden Caching-Proxies nicht unter Sicherheitsaspekten entwickelt. Ein dedizierter Sicherheitsproxy sollte den Caching-Proxies nach Möglichkeit vorgezogen werden.
	- Kompletter Ausfall von HTTP/HTTPS bei Ausfall des Proxies. Eine vorübergehende Inbetriebnahme unter Verzicht auf den Proxy erfordert umfangreiche Konfigurationsarbeiten (die Sperrlisten auf dem Paketfilter müssen geändert werden und die Proxyeinstellungen der Clients müssen angepasst werden, falls der Caching-Proxy nicht transparent betrieben wurde). In der Regel ist deshalb eine redundante Auslegung des Proxies notwendig.

Tabelle: Vorteile und Nachteile von Zwangs-Caching-Proxies

Reverse Proxy

"Reverse Proxies" werden im Zusammenhang mit der Bereitstellung von (Web-) Servern auch zur Erreichung folgender Sicherheitsziele verwendet:

1. Einschränkung der Kommunikationsverbindungen, die aus dem nicht-vertrauenswürdigen Netz kommend über einen Sicherheitsproxy geleitet werden müssen. Dadurch wird die Administration des Sicherheitsgateways erleichtert und die Wahrscheinlichkeit von Fehlkonfigurationen verringert.
2. Verschleierung der Identität des Web-Servers (mehrere, zur Lastverteilung genutzte Web-Server erscheinen vom nicht-vertrauenswürdigen Netz aus gesehen unter einer IP-Adresse).
3. Abfangen von Fehlermeldungen des Web-Servers, die einem Angreifer Hinweise zur Kompromittierung des Systems liefern könnten (eigentlich handelt es sich hierbei um einen Workaround, da der Web-Server dieses Problem selber abfangen sollte).
4. Zusätzliche Abschottung des Web-Servers, d. h. ein Angreifer kann u. U. die Informationen einer Transaktion mitlesen, aber keinen Zugriff auf den Web-Server erlangen.
5. Abkoppelung des IP-Stacks des Servers vom nicht-vertrauenswürdigen Netz.
6. Filterung unerwünschter, aus dem nicht-vertrauenswürdigen Netz stammender Anfragen an den Web-Server.
7. Erhöhung der Verfügbarkeit aufgrund von Lastverteilung und Lastminderung durch Caching.

In der folgenden Abbildung ist eine Situation dargestellt, in der zwei Server zum Zugriff aus dem nicht-vertrauenswürdigen Netz bereitgestellt werden. In dem abgebildeten Szenario müssen zwei Kommunikationsverbindungen über das ALG und den externen Paketfilter hinweg freigeschaltet werden.

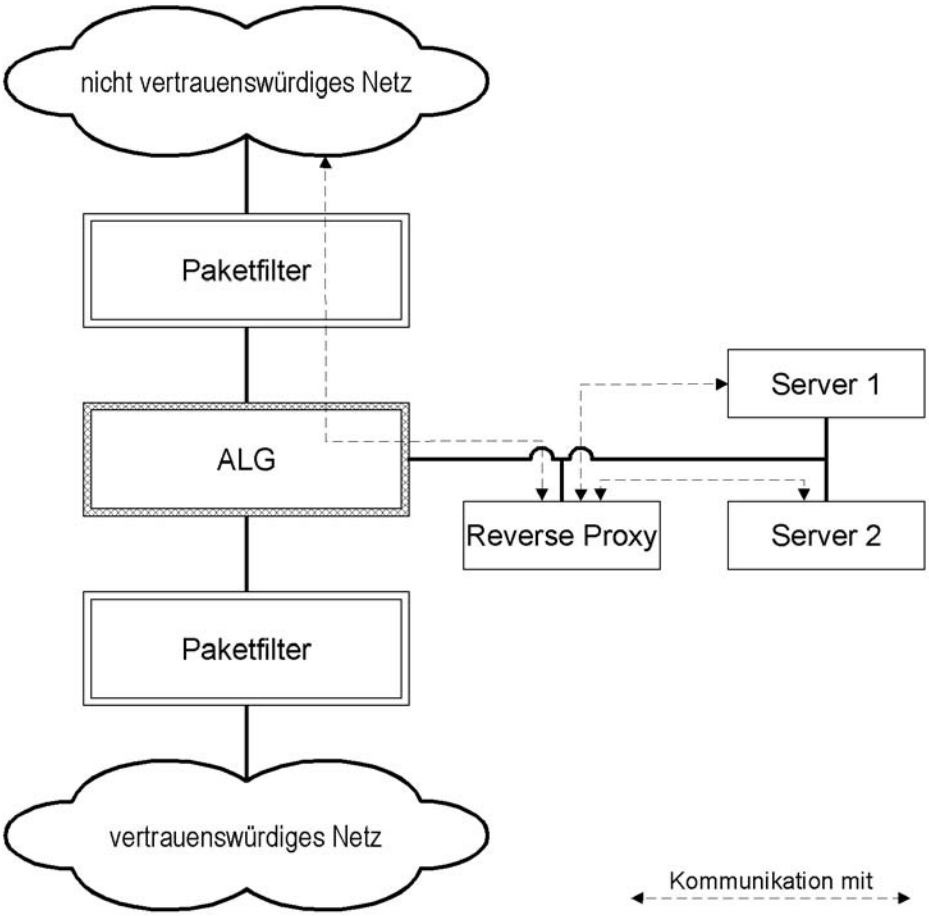


Abbildung: Reverse Proxy zur Vermeidung vieler Kommunikationsbeziehungen über das ALG hinweg. Reverse Proxy und die Server stehen in einer DMZ.

Die in der vorigen Abbildung dargestellten Kommunikationsbeziehungen lassen sich mit Hilfe eines Reverse Proxy reduzieren. In Abbildung ist aus dem nicht-vertrauenswürdigen Netz nur der Zugriff auf den Reverse Proxy gestattet, Server 1 und 2 sind vor Zugriff gesperrt. Auf beide Server kann nur der Reverse Proxy zugreifen.

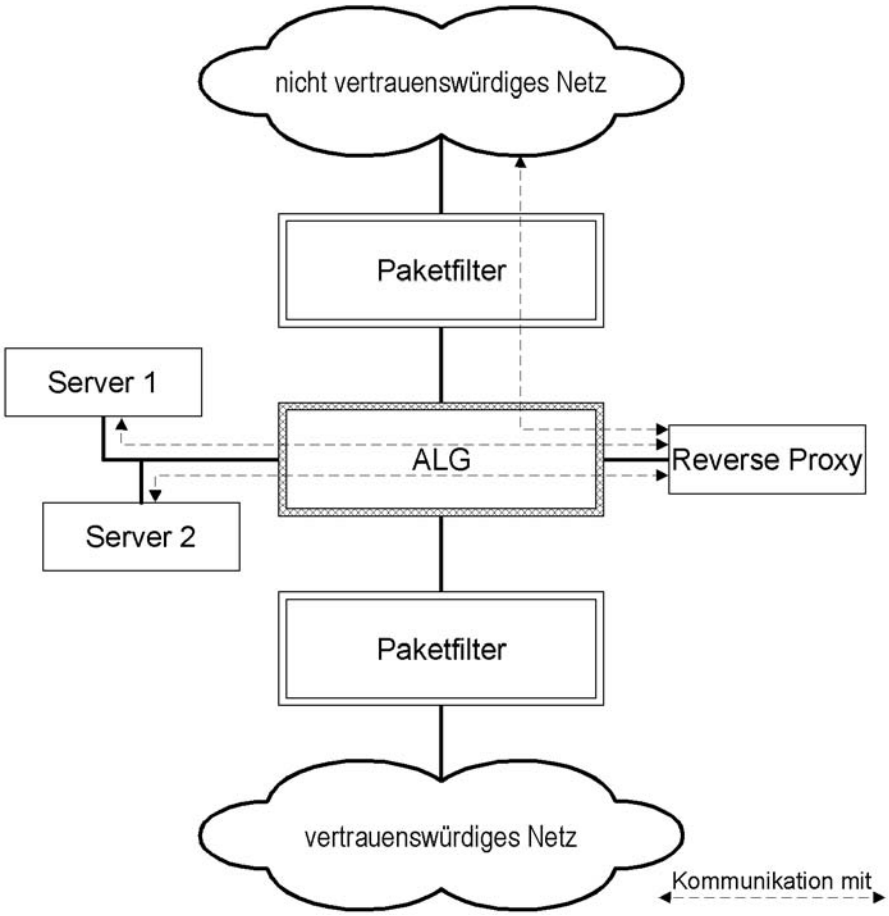


Abbildung: Reverse Proxy zur Vermeidung vieler Kommunikationsbeziehungen über das ALG hinweg. Reverse Proxy und die Server stehen in verschiedenen DMZ.

Zur Erhöhung der Serversicherheit können die Server auch in einer eigenen DMZ (oder auch im vertrauenswürdigen Netz) betrieben werden, wo sie durch einen Sicherheitsproxy vom Reverse Proxy getrennt werden. Die Übernahme eines Servers wird hierdurch zusätzlich erschwert, allerdings erhöht sich die Anzahl der Kommunikationsbeziehungen über das ALG.

Ergänzende Kontrollfragen:

- Welche Proxies werden eingesetzt?

M 4.224 Integration von Virtual Private Networks in ein Sicherheitsgateway

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsbeauftragter

Verantwortlich für Umsetzung: Administrator

Virtual Private Networks (VPNs) werden häufig mittels IPSec oder SSL aufgebaut. Vor der Beschreibung der Realisierungsformen werden grundlegende Anforderungen an VPNs bzw. Schwachpunkte von VPNs beschrieben.

Anforderungen

- Für den Aufbau von VPNs sollten nur sichere Verschlüsselungsverfahrens verwendet werden.
- Beim Einsatz von proprietären Verschlüsselungsverfahren sollte das Verschlüsselungsverfahren offen gelegt sein. Dies ermöglicht unter anderem die Fehlersuche durch unabhängige Experten.
- In der Regel sollten verfügbare, offen gelegte Verschlüsselungsverfahren der Eigenentwicklung eines Herstellers vorgezogen werden.
- Bei vielen VPN-Implementierungen findet die gesamte VPN-Kommunikation über eine zentrale Verschlüsselungskomponente statt. Im Falle einer Störung (beispielsweise wegen eines Hardwarefehlers) ist dann das gesamte VPN angreifbar oder nicht verfügbar. Dies ist besonders dann problematisch, wenn eine VPN-Gegenstelle von einem externen Dienstleister betrieben wird und Verfügbarkeitsanforderungen nicht vertraglich fixiert wurden.
- Beim Betrieb eines VPNs mittels IPSec im Transportmodus ist zu beachten, dass die IP-Adressen der Rechner in den zu schützenden Netzen prinzipiell mitgelesen werden können und somit nicht auf eine "Network Address Translation" verzichtet werden kann. Beim Betrieb im Tunnelmodus stellt die VPN-Komponente die NAT-Funktion durch Hinzufügen neuer TCP/IP-Header und Verschlüsselung des kompletten gekapselten Ursprungspakets implizit bereit.

Im Zusammenhang mit Sicherheitsgateways bietet sich der Tunnelmodus zum Betrieb eines VPNs an, da die VPN-Funktion von einem zentralen Gateway übernommen werden kann und keine Anpassungen der Rechner in den vertrauenswürdigen Netzen notwendig ist. Zudem sind bei Verwendung des Tunnelmodus in der Regel weniger Paketfilterregeln als beim Transportmodus notwendig (dies entfällt, falls je nach der gewählten Integrationsvariante der VPN-Verkehr keinen Paketfilter mehr passiert, siehe später).

- Bei der Wahl der Verschlüsselungskomponente sollte ein dediziertes Gerät einem selbst erstellten System (z. B. mit Linux und IPSec) normalerweise vorgezogen werden, da Appliances viele Funktionalitäten mittels manipulationssicherer und performanter Hardware realisieren.
- Zum sicheren Betrieb von VPNs ist meist der Aufbau einer vertrauenswürdigen Schlüsselinfrastruktur notwendig (PKI).

- Von der Erzeugung von "Pseudo-VPNs" innerhalb einer Organisation durch die Nutzung der VLAN-Funktionalität von Switches wird abgeraten, da es derzeit noch einfache Angriffe auf Switches gibt, die unberechtigten Nutzern Zugriff auf das VLAN gestattet. VLANs sind keine Technik zur sicheren Trennung von Netzen (siehe auch M 2.277 *Funktionsweise eines Switches*)

Nach den allgemeinen Hinweisen zu VPNs werden im Folgenden Realisierungsformen von VPNs anhand von IPSec und SSL vorgestellt.

VPNs mittels IPSec

Vor und Nachteile von VPNs mittels IPSec stellen sich wie folgt dar:

Vorteile von VPNs mittels IPSec	**Nachteile von VPNs mittels IPSec**
Bereitstellung ganzer Netze über eine zentrale VPN-Komponente möglich.	Integration einer Hardware-Komponente in das Sicherheitsgateway notwendig. Die Platzierung der VPN-Komponente ist im Einzelfall zu betrachten, da aufgrund der unterschiedlichsten Anwendungszusammenhänge keine allgemeingültigen oder grundlegenden Aussagen zur Platzierung möglich sind.
Einmalige Integration des VPN-Gateways an zentraler Stelle.	Ausfall des zentralen VPN-Gateways verursacht Komplettausfall des (VPN-) Netzwerks.

Tabelle: Vorteile und Nachteile von VPNs mittels IPSec

Im Zusammenhang mit VPNs muss zwischen einem Trusted-VPN und einem Secure-VPN unterschieden werden:

- Nutzung eines Trusted-VPN

  Da sowohl bei der Verbindung zweier Standorte als auch bei der Verbindung von Telearbeitern mit Standorten die Daten vom Dienstleister oftmals nicht verschlüsselt werden und die gesamte Betreuung beim externen Dienstleister liegt, sollten sie nur bei wenig schutzwürdigen Daten verwendet werden. Bei höherem Schutzbedarf ist vor Übertragung der Daten eine Verschlüsselung notwendig (die faktisch ein Secure-VPN darstellt, so dass das Trusted-VPN überflüssig wird). Zudem ist eine regelmäßige Revision mindestens der Zugangssysteme beim Dienstleister notwendig, um Fehler in der Konfiguration aufdecken zu können.

- Integration eines Secure-VPN

  Die folgenden Betrachtungen beziehen sich ausschließlich auf den Betrieb im Tunnel-Modus. Diese Betriebsart ist im Zusammenhang mit der sicheren Verbindung von Standorten im Vergleich zum Transport-Modus die leichter zu administrieren.

Der Ort der Integration des VPN-Gateways relativ zum Paketfilter des Sicherheitsgateways hängt davon ab, wie wenig vertrauenswürdig das externe Netz ist. Prinzipiell existieren dabei (auch dann, wenn nur ein einstufiges

Sicherheitsgateway bestehend aus einem Paketfilter eingesetzt wird) drei Möglichkeiten:

1. Bei einem hohen Angriffspotenzial sollte das VPN-Gateway durch einen Paketfilter geschützt, also zwischen ALG und äußerem Paketfilter platziert werden.

   In diesem Fall wird einerseits das VPN-Gateway geschützt, andererseits ist es aber nicht mehr möglich, den eintreffenden Datenverkehr auf dem Paketfilter portabhängig zu filtern. Da der über das VPN kommende Verkehr ebenfalls aus einem vertrauenswürdigen Netz kommt, kann dieser Nachteil aber normalerweise in Kauf genommen werden.

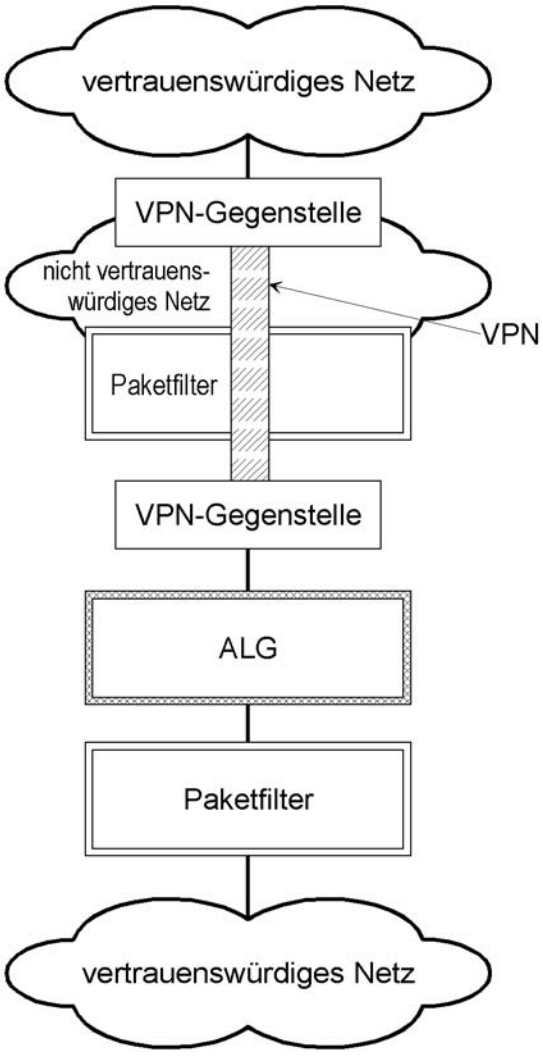


Abbildung: Platzierung der VPN-Komponente "hinter" dem Paketfilter.

Vorteile	Nachteile
Das VPN-Gateway (insbesondere der TCP/IP-Stack des VPN-Gateways) wird durch den Paketfilter geschützt.	Filterung durch den Paketfilter nur anhand der Informationen des IP-Headers möglich. Einige grundlegende Portfilterfunktionen können allerdings von einem ALG wahrgenommen werden.
Einfache Administration des Paketfilters, da nur die IP-Adresse des VPN-Gateways als Absenderadresse erscheint.	Der Paketfilter darf keine NAT vornehmen.

Tabelle: Vorteile und Nachteile von VPN-Gateways

2. Ist die Angriffswahrscheinlichkeit auf das Sicherheitsgateway gering, weil das externe Netz "relativ vertrauenswürdig" ist, so kann das VPN-Gateway auch "vor" dem Paketfilter platziert werden:

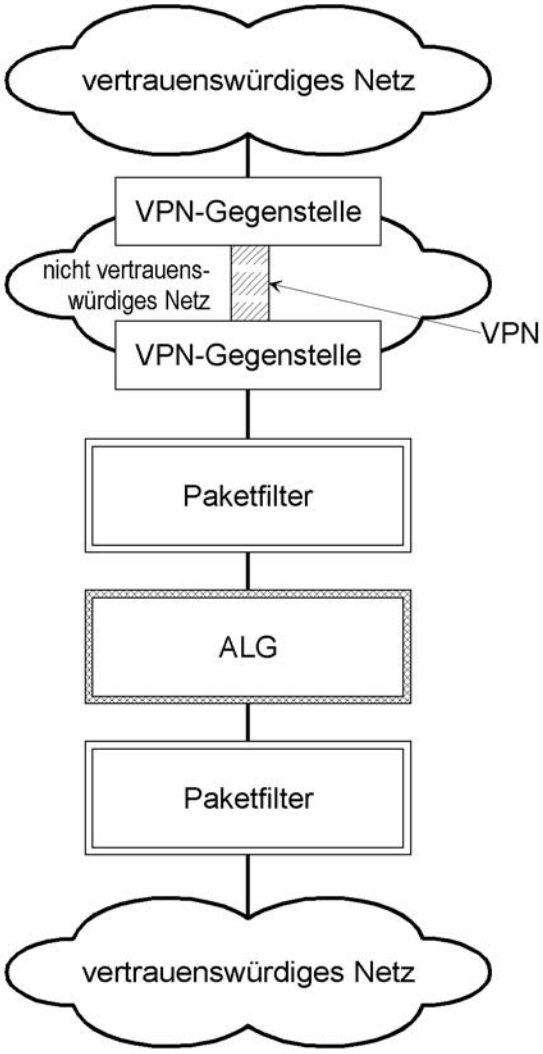


Abbildung: Platzierung der VPN-Komponente "vor" dem Paketfilter.

Vorteile	Nachteile
Filterung anhand der Informationen des TCP-Headers möglich.	Kein Schutz des VPN-Gateways durch den Paketfilter. (Werden dedizierte VPN-Komponenten eingesetzt, ist ein Schutz durch einen Paketfilter in der Regel nicht notwendig.)
Möglichkeit zur NAT durch den Paketfilter.	
VPN-Komponente kann durch einen externen Dienstleister betrieben werden.	

Tabelle: Vorteile und Nachteile von VPN-Gateway vor dem Paketfilter

3. Alternativ zur Platzierung vor dem äußeren Paketfilter kann das VPN-Gateway auch an eine weitere Netzschnittstelle des ALG angeschlossen werden. Ist das zur Übertragung der Daten genutzte Netz nur in sehr geringem Maße nicht vertrauenswürdig, kann eventuell sogar auf den Einsatz eines Paketfilters verzichtet werden. Ein konkreter Einsatzzweck hierfür ist beispielsweise die Kopplung zweier räumlich getrennter LANs, die über gemietete, nur von einem Nutzer bzw. Betreiber verwendete Leitungen verbunden werden sollen. In diesem Fall braucht die Verbindung nicht unbedingt durch einen Paketfilter vor Angriffen auf Dienste geschützt zu werden.

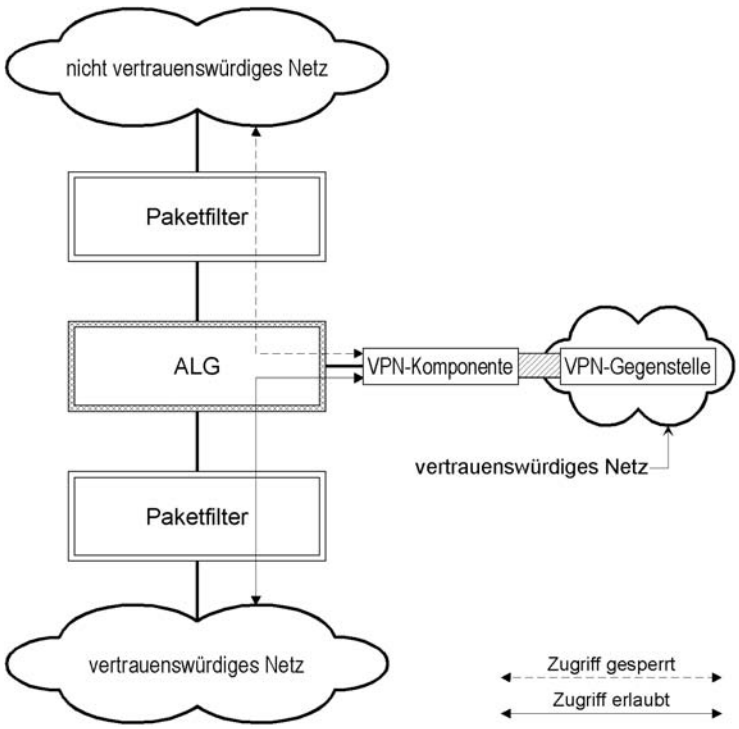


Abbildung: Platzierung der VPN-Komponente zwischen ALG und vertrauenswürdigem Netz ohne Verwendung eines Paketfilters.

Vorteile	Nachteile
Keine Einschränkungen der Paketfilterfunktionalität, da über den Paketfilter kein verschlüsseltes Protokoll geleitet wird.	Einsatz nur bei Verbindung zweier vertrauenswürdiger Netze.
Keine Einschränkungen der VPN-Funktionalität, da die VPN-Kommunikation nicht über einen Paketfilter geleitet wird.	

Tabelle: Vorteile und Nachteile von VPN-Gateways zwischen ALG und vertrauenswürdigem Netz

Neben dem Aufbau von VPNs mittels IPSec können sichere Zugänge zu Anwendungen in vertrauenswürdigen Netzen auch mittel SSL-VPNs hergestellt werden. Diese werden im folgenden Abschnitt vorgestellt.

VPNs mittels SSL

Vor- und Nachteile von VPNs mittels SSL stellen sich wie folgt dar:

Vorteile von VPNs mittels SSL	Nachteile von VPNs mittels SSL
Gezielte Bereitstellung einzelner Server für einzelne Nutzer möglich.	Evtl. hohe Performanceeinbußen auf dem Server, da der Server die Verschlüsselungsfunktion übernehmen muss (falls hierfür keine eigene Komponente verwendet wird).
Bereitstellung von Servern mit fast jedem ALG möglich.	Nicht web-basierte Anwendungen erfordern oftmals die Ausführung von ActiveX-Komponenten oder Java-Applets im Browser des Nutzers.
Einfache (aber auch eventuell unsichere) Integration in Web-Browser möglich.	Nicht web-basierte Anwendungen erfordern die Integration von SSL-Unterstützung auf dem Server, was aufgrund der Komplexität von SSL zur Fehladministration führen kann.
Für web-basierte Anwendungen sind keine Clients außer dem Browser notwendig.	Anpassung an neu eingeführte Applikationen/Protokolle notwendig.
Gegenüber IPSec feinere Abstimmung von Zugriffsregelungen möglich.	

Tabelle: Vorteile und Nachteile von VPNs mittels SSL

Die Kommunikationsbeziehung zwischen Client und Server ist in Abbildung ersichtlich. Der SSL-verschlüsselte Datenverkehr sollte über jedes verfügbare ALG mittels generischer Proxies geleitet werden können.

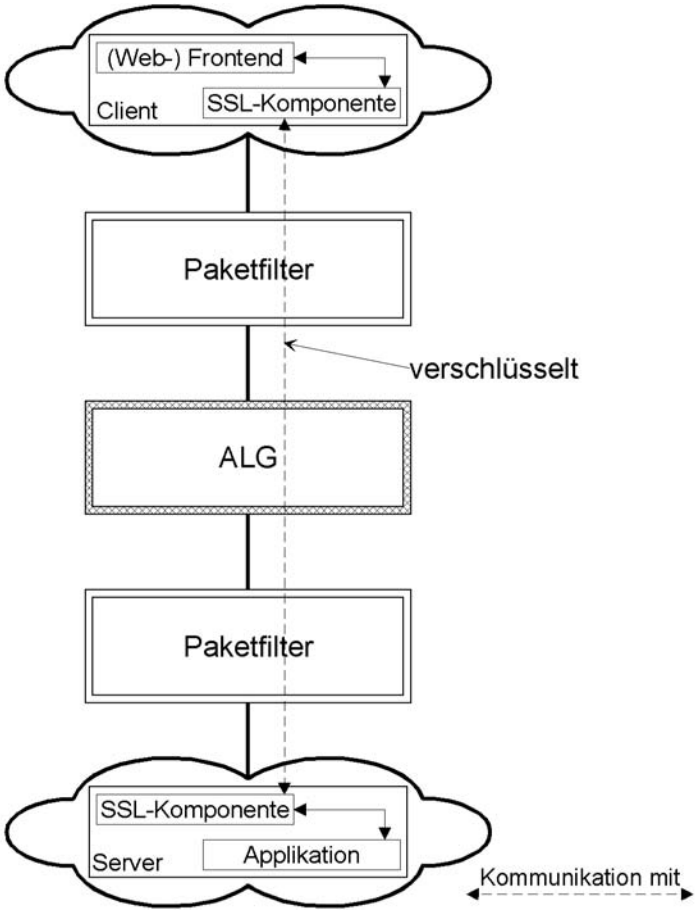


Abbildung: Überblick über VPNs mit SSL

Existieren dedizierte Sicherheitsproxies für eine mittels SSL bereitgestellte Anwendung, so kann deren Funktionalität zur Durchsetzung von Sicherheitsleitlinien genutzt werden, wenn die verschlüsselte Verbindung aufgebrochen, gefiltert und wieder verschlüsselt wird. Dieses Szenario stimmt - abgesehen vom Typ des verwendeten Sicherheitsproxies - mit dem Einsatz eines HTTPS-Proxies überein.

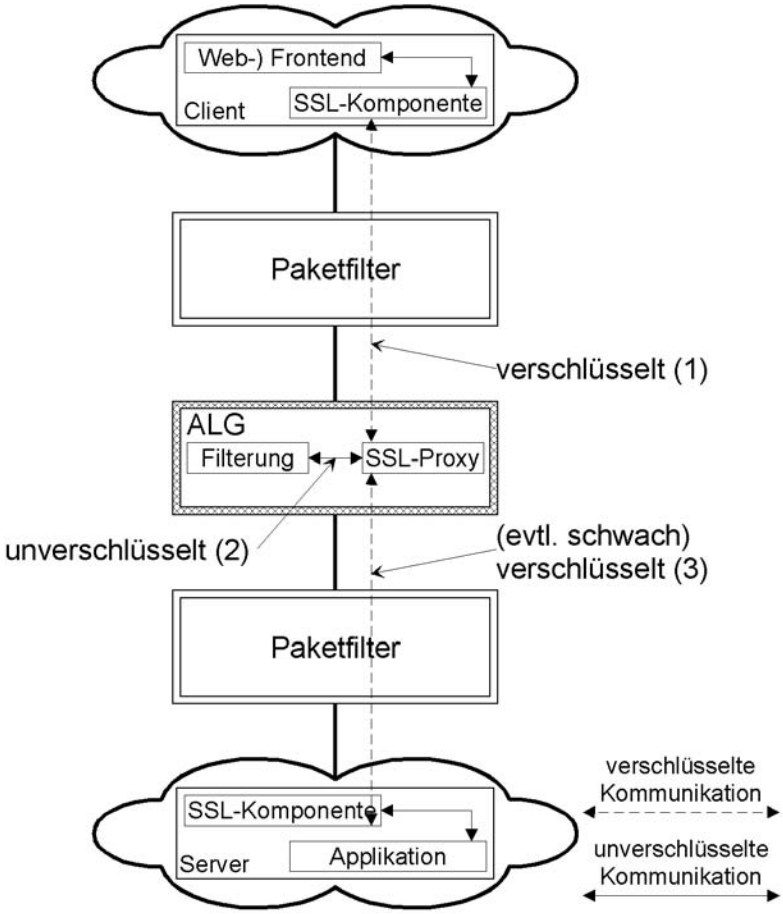


Abbildung: Überblick über VPNs mit SSL. Die Verbindung wird temporär zur Kontrolle der übertragenen Daten entschlüsselt.

Bei der Anbindung verschiedener Nutzergruppen mit verschiedenen Rechten sollte jeder Nutzergruppe ein eigener Schlüsselkreis zugeordnet werden, um die Vertraulichkeit der übertragenen Daten zwischen den Nutzergruppen sicherzustellen.

In der Regel bieten sich zur Erstellung eines VPN der Einsatz einer dedizierten Lösung eines Herstellers oder der Einsatz der Implementierung eines offenen Standards (z. B. FreeS/WAN bzw. IPSec) an. Die Vor- und Nachteile beider Lösungen sind im Folgenden beschrieben.

Proprietäre Lösungen

In der folgenden Tabelle werden Vor- und Nachteile von dedizierten Modulen zum Aufbau eines VPN vorgestellt:

Vorteile	Nachteile
Geringer Installationsaufwand bis zur Inbetriebnahme, da die Produkte zur schnellen Inbetriebnahme entsprechend vorbereitet sind (oder im Einzelfall vom Hersteller entsprechend vorbereitet werden).	Möglicherweise Schwächen im Verschlüsselungsverfahren, wenn proprietäre Verschlüsselungsverfahren eingesetzt werden. Offengelegte Verschlüsselungsverfahren sind in der Regel den proprietären Verfahren vorzuziehen, da bei offengelegten Verfahren in der Regel mehr Teilnehmer an der Schwachstellenanalyse beteiligt sind.
Hoher Schutz vor Kompromittierung des Systems, da viele Funktionen in die Hardware integriert sind.	Softwarefunktionen sind durch Angriffe leichter zu kompromittieren. Programmierfehler bleiben unter Umständen lange unentdeckt, falls ein Produkt nur eine geringe Verbreitung besitzt. Bei wenig verbreiteten Produkten werden Hinweise zu Schwachstellen und Patches möglicherweise nicht von bekannten Medien publiziert, so dass das Auftreten von Sicherheitslücken unbekannt bleiben kann.
Evtl. höhere Geschwindigkeit, da dedizierte Produkte oft auf hohe Geschwindigkeit hin optimiert sind.	Aufgrund proprietärer Bauteile und der hohen Integration von Funktionen in Hardware resultieren geringe Erweiterungsmöglichkeiten.
Geringer Wartungsaufwand, falls das Produkt (vom Hersteller) ferngewartet werden kann und z. B. Patches automatisch über das Internet installiert werden können.	

Tabelle: Vorteile und Nachteile von dedizierten Modulen

Offene Standards

In der folgenden Tabelle sind Vor- und Nachteile der Implementation eines offenen Standards am Beispiel von IPSec aufgelistet:

Vorteile	Nachteile
Da IPSec-Implementierungen oft im Quelltext vorliegen, eine große Verbreitung und somit viele "Tester" besitzen, handelt es sich um eine vergleichsweise ausgereifte, fehlerarme Software.	Hoher Installations- und Wartungsaufwand, da der Rechner, auf dem IPSec betrieben werden soll, oftmals selbst installiert und gehärtet werden muss.
Das Verschlüsselungsverfahren wurde von einer großen Zahl an Entwicklern diskutiert und sollte somit als relativ sicher gelten.	Schwieriges Recovery bei Systemausfall, da selbst installierte Systeme hierfür keine Standardverfahren vorsehen. Ggf. muss ein Cold-Standby-System bereitgehalten werden.
Geringe Investitionskosten für Software, insbesondere falls VPNs zwischen einzelnen Rechnern (zwecks Ende-zu-Ende-Verschlüsselung) gebildet werden. In diesem Fall muss nicht für jeden Client kostenpflichtige, proprietäre Software beschafft werden.	Mögliche Inkompabilitäten beim Einsatz verschiedener Implementierungen von IPSec (wenn optionale Bestandteile der Spezifikation unterschiedlich ausgenutzt wurden).

Tabelle: Vorteile und Nachteile der Implementation eines offenen Standards am Beispiel von IPSec

Ergänzende Kontrollfragen:

- Welche VPN-Technik wird eingesetzt?
- Wo ist der VPN-Endpunkt platziert?

M 4.225 Einsatz eines Protokollierungsservers in einem Sicherheitsgateway

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsbeauftragter

Verantwortlich für Umsetzung: Administrator

Bei komplizierteren Sicherheitsgateways fallen oft große Mengen verschiedener Protokollierungsinformationen der verschiedenen Komponenten an. Um die Auswertung der Protokolle zu erleichtern ist es empfehlenswert, an zentraler Stelle einen Protokollierungsserver (Loghost) zu betreiben, der die Protokolldaten der an das Sicherheitsgateway angeschlossenen Komponenten aufnimmt. Die Daten lassen sich so einfach zueinander in Beziehung setzen und erleichtern damit die regelmäßige, anlassunabhängige Auswertung und ermöglichen im Falle eines Ausfalls das Auffinden des Verursachers (siehe auch M 4.47 *Protokollierung der Sicherheitsgateway-Aktivitäten*).

Problematisch ist die Platzierung des zentralen Loghosts, denn er muss einerseits von sämtlichen Komponenten des Sicherheitsgateways aus zu erreichen sein, andererseits darf er keinen unberechtigten Zugriff aus dem nicht-vertrauenswürdigen Netz ermöglichen.

Keine zusätzlichen Aufgaben auf dem Loghost

Wird der Loghost kompromittiert, so erleichtert er aufgrund der zentralen Aufstellung im Sicherheitsgateway die Kompromittierung der anderen Komponenten erheblich. Ein zentraler Loghost im Sicherheitsgateway sollte daher nur diese Funktion wahrnehmen und nicht noch für weitere Aufgaben (etwa als Administrationsrechner) verwendet werden.

Im Zusammenhang mit Logdaten sollte folgendes beachtet werden:

- Der zentrale Loghost sollte die Daten redundant ablegen.
- Die Protokollierung sollte, wenn möglich, zusätzlich lokal auf den einzelnen Komponenten des Sicherheitsgateways erfolgen. Da hierdurch die Leistung der Komponente nicht merklich sinkt, sollte diese Sicherung als zusätzlicher Ausfallschutz eingeschaltet werden.

Ein weiteres wichtiges Element der Protokollierung stellt die Alarmierung bei definierten, kritischen Ereignissen dar. Auch hier ist darauf zu achten, dass die Weiterleitung der Alarmmeldungen zu einer zentralen Instanz möglich ist.

Wichtigstes Kriterium bei der Platzierung eines Loghosts ist, dass keine zusätzlichen Schwachstellen entstehen, wie z. B. die Möglichkeit zur Umgehung von Sicherheitskomponenten. Zudem ist zu berücksichtigen, dass die Protokolldaten zur Speicherung auf einem zentralen Loghost möglichst wenige Komponenten des Sicherheitsgateways überqueren müssen. Werden Protokolldaten über Proxies versendet, so erscheinen diese in den Protokolldateien mit der IP-Adresse des Proxies, so dass der eigentliche Absender nicht mehr unmittelbar zu erkennen ist, wenn nicht die Protokollierungsfunktionen auf den einzelnen Komponenten eine entsprechende Kennzeichnung der Daten ermöglichen

Im Idealfall werden Loghosts in einem eigenen Administrationsnetz platziert. Auf den Loghost wird dann ausschließlich aus dem Adminstrationsnetz heraus zugegriffen.

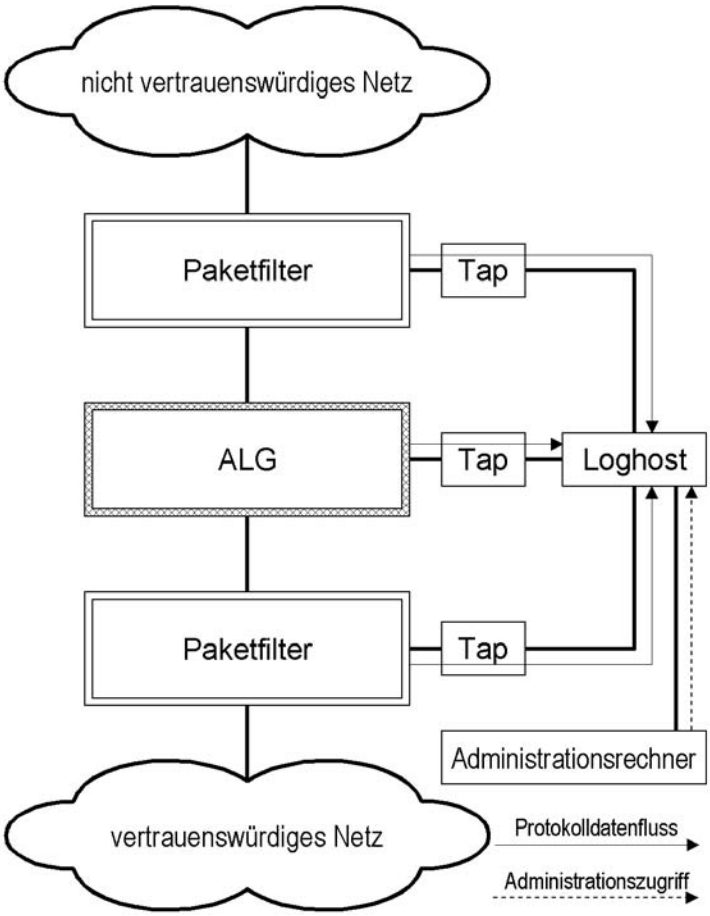


Abbildung 1: Platzierung des Loghost im Administrationsnetz.

Steht kein eigenes Administrationsnetz zur Verfügung, so muss der Loghost im Produktivnetz betrieben werden. In Abhängigkeit von der Struktur des Sicherheitsgateways ergeben sich damit zwei empfohlene Platzierungen für einen zentralen Loghost:

Platzierung bei einfachen Sicherheitsgateways

Bei einem einfachen Sicherheitsgateway, das nur aus einem einzelnen Paketfilter besteht, bietet es sich an, den Loghost in einer eigenen DMZ des Paketfilters zu platzieren. In der Regel bieten Paketfilter eine ausreichende Anzahl an Netzschnittstellen oder sind leicht erweiterbar, so dass eine spezielle Loghost-DMZ zum Einsatz kommen kann.

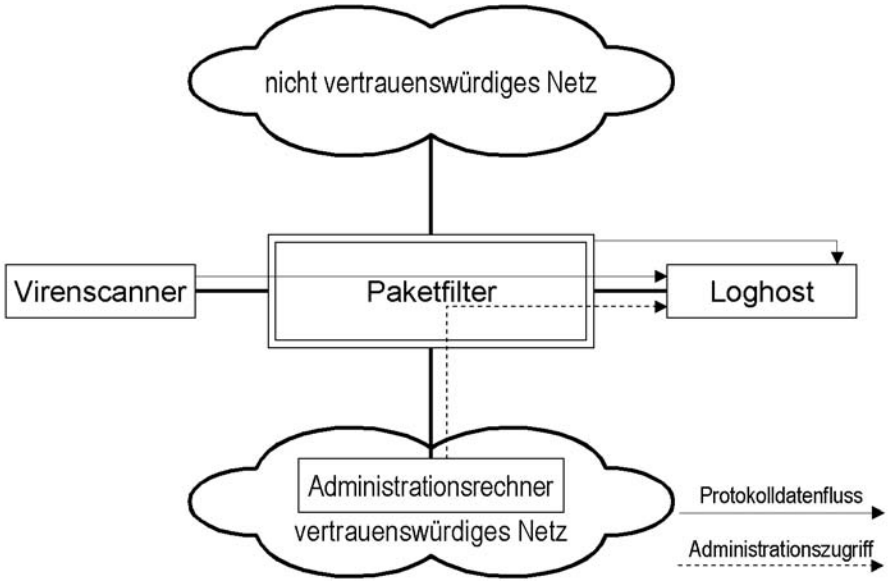


Abbildung 2: Platzierung des Loghost bei einfach strukturierten Sicherheitsgateways.

Platzierung bei komplexen Sicherheitsgatways

Bei komplexeren Strukturen von Sicherheitsgateways ist es in der Regel notwendig, die Protokolldaten über einen Proxy zum Loghost zu leiten.

Prinzipiell ist dabei zwischen der Platzierung des Loghosts in einer eigenen DMZ und der Platzierung des Loghosts in einer gemeinsamen DMZ mit anderen Modulen des Sicherheitsgateways zu unterscheiden.

Die folgende Abbildung zeigt eine Lösung, bei der ein zentraler Loghost in einer eigenen DMZ platziert wurde und von zwei getrennten Sicherheitsgateways gemeinsam genutzt wird.

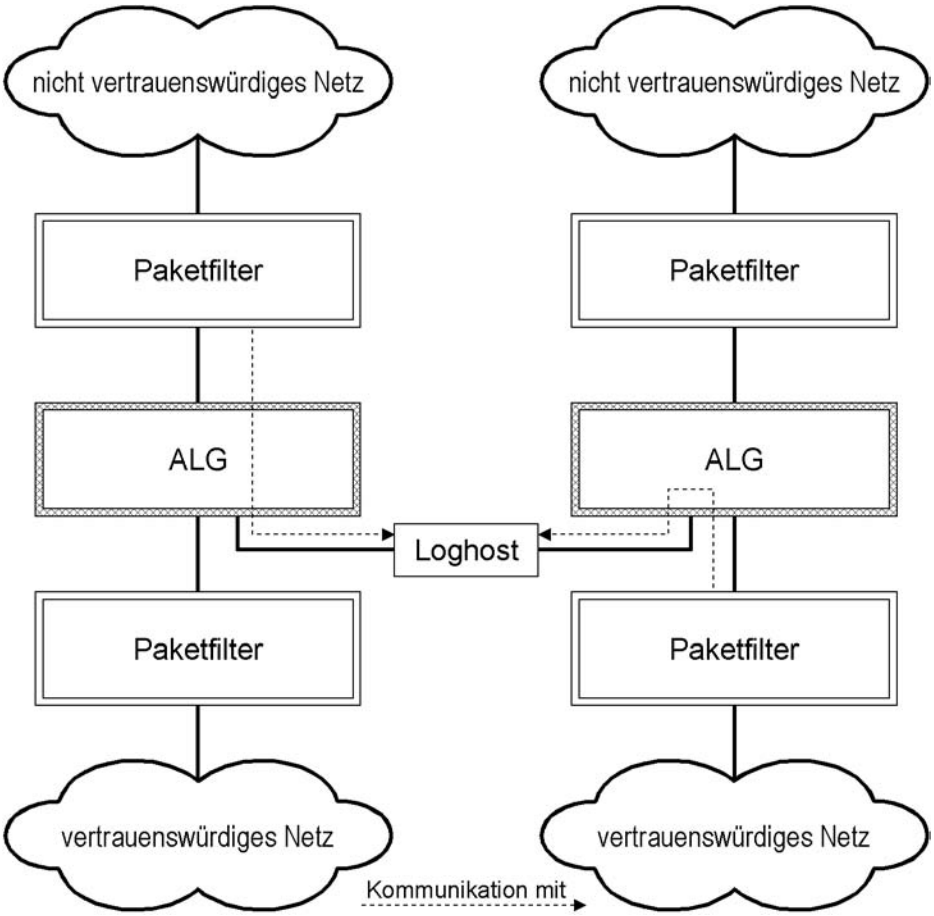


Abbildung 3: Platzierung des Loghost in einer dedizierten DMZ.

Die Platzierung des Loghost in einer eigenen DMZ hat den Vorteil, dass sie bei einer Kompromittierung des Loghosts dem Angreifer nur wenig weitere Angriffsmöglichkeiten eröffnet, da die einzigen direkt erreichbaren Module des Sicherheitsgateways die ALGs sind. Diese sind in der Regel jedoch besonders gegen Angriffe geschützt.

Bei der abgebildeten Lösung ist zudem zu beachten, dass durch die Integration des Loghost eine "Querverbindung" zwischen den beiden vertrauenswürdigen Netzen geschaffen wurde, die ohne Integration des Loghost nicht existiert hätte. Hierzu ist eine eigene Risikoabschätzung notwendig. Gegebenenfalls muss auf die Querverbindung verzichtet werden, was den Einsatz von zwei getrennten Loghosts zur Folge hat, deren Protokolldaten eventuell zu Analysezwecken zusammengeführt werden müssen.

Bei der Lösung, die in der folgenden Abbildung dargestellt ist befinden sich weitere Module des Sicherheitsgateways in der gleichen DMZ wie der Loghost. Diese können weitere Angriffspunkte nach der Übernahme des Loghost bieten, da es sich nicht notwendigerweise um speziell entwickelte Sicherheitsprodukte handelt. Möglicherweise können diese Module deshalb besonders einfach übernommen werden.

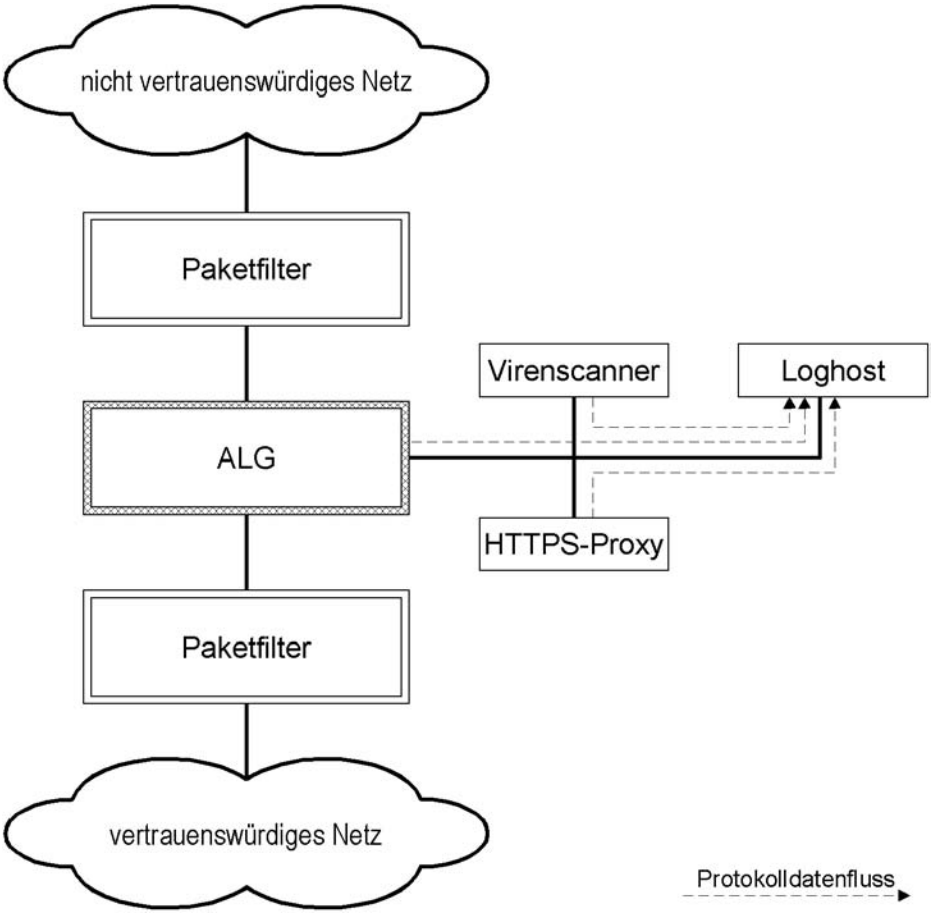


Abbildung 4: Platzierung des Loghost in einer DMZ, die weitere Komponenten des Sicherheitsgateways enthält.

Die Lösung, bei der der Loghost in einer eigenen DMZ platziert wird, ist deshalb dieser Lösung vorzuziehen.

Die Platzierung des Loghost in einer DMZ mit weiteren Komponenten ist nur dann ratsam, wenn das ALG keine ausreichende Anzahl an Netzschnittstellen zur Verfügung stellt.

Die folgende Tabelle fasst die Empfehlungen zusammen:

Struktur des Sicherheitsgateway	**Schutzbedarf**	**Platzierung des Loghosts**
Nur Paketfilter	normal	Loghost in einer eigenen DMZ des Paketfilters
Komplexes Sicherheitsgateway (P-A-P)	- normal - hoch	- Loghost in einer gemeinsamen DMZ mit anderen Komponenten akzeptabel. Eigene DMZ für den Loghost empfohlen - Loghost einer eigenen DMZ
Gemeinsame Nutzung eines Loghosts durch mehrere Sicherheitsgateways	-	Loghost in einer eigenen DMZ

Tabelle: Empfehlungen

M 4.226 Integration von Virenscannern in ein Sicherheitsgateway

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsbeauftragter

Verantwortlich für Umsetzung: Administrator

Schadsoftware wie Viren, Würmer und Trojaner (im Folgenden vereinfachend unter dem Begriff "Viren" zusammengefasst) können zum einen zentral auf dem Sicherheitsgateway und zum anderen verteilt auf den Arbeitsplatz-PCs und Servern (d. h. den Endsystemen von Kommunikationsbeziehungen über das Sicherheitsgateway hinweg) gefiltert werden.

Eine zentrale Filterung auf dem Sicherheitsgateway kann einen dezentralen Virenschutz nicht vollständig ersetzen, da unter Umständen Schadsoftware auch auf anderen Wegen (beispielsweise über Wechseldatenträger) auf die Systeme gelangen kann.

Eine zentrale Filterung ist derzeit in der Regel nur beim Einsatz eines Application-Level-Gateways möglich.

Filterung direkt durch das ALG

Sofern das eingesetzte ALG eine entsprechende Option anbietet ist es meist sinnvoll, die Prüfung auf Schadsoftware direkt auf dem ALG durchzuführen.

Filterung durch das Sicherheitsgateway beim Einsatz eines ALG

ALGs bieten oft eine Schnittstelle, mit denen sich Virenschutzprogramme von Drittanbietern anbinden lassen. Das Virenschutzprogramm nimmt die Daten entgegen und übergibt dem ALG eine Meldung über das Ergebnis der Virenfilterung. Das ALG verarbeitet die Daten dann in Abhängigkeit vom Ergebnis der Überprüfung.

Somit bietet sich für die Integration des Virenscanners der in der nachfolgenden Abbildung dargestellte Aufbau an, in dem der Virenscanner "neben" dem ALG in der DMZ des Sicherheitsgateway platziert wird. Bei diesem Aufbau sollten einige Punkte beachtet werden, da der Rechner mit dem Virenschutzprogramm durch diese Aufgabe besonders stark gefährdet ist:

- Der Rechner mit dem Virenschutzprogramm muss besonders sicher konfiguriert werden, beispielsweise durch eine besonders restriktive Konfiguration des Betriebssystems ("Härten"). Die Sicherheitsanforderungen sind (mindestens) genau so hoch wie an die sonstigen Komponenten des Sicherheitsgateway.
- Der Rechner muss durch entsprechende Paketfilterregeln möglichst gut vom Rest des Netzes getrennt werden. Insbesondere sollten von diesem Rechner keine ausgehenden Verbindungen, weder ins interne noch ins externe Netz, von den Paketfiltern erlaubt werden. Im Idealfall kann der Rechner direkt mit dem ALG kommunizieren, über den er den zu prüfenden Datenstrom erhält und an den er die gefilterten Daten zurück liefert. Darüber hinaus sind nur noch Verbindungen aus einem gesonderten Administrationsnetz zu dem Rechner erlaubt.
- Die regelmäßige Integritätsprüfung des Systems sollte in kurzen Abständen erfolgen.

- Eventuell sollte der Rechner mit einem host-basierten Intrusion-Detection-System ausgerüstet werden, so dass eine eventuelle Kompromittierung möglichst sofort erkannt werden kann.
- Die Administration des Rechners muss über eine entsprechend abgesicherte Verbindung erfolgen.

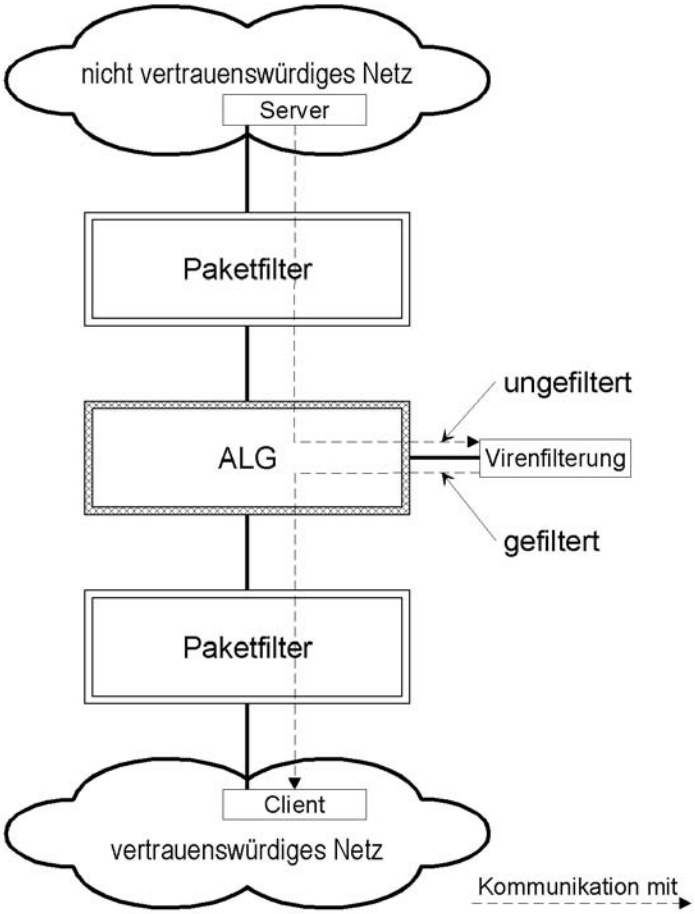


Abbildung: Integration einer Viren-Filterung

Filterung auf den Endgeräten (beim Einsatz eines Paketfilters)

Da Paketfilter keine Schnittstelle zu Virenfiltern besitzen, ist beim Einsatz eines einstufigen Sicherheitsgateways, das nur aus einem Paketfilter besteht normalerweise keine zentrale Virenfilterung durch das Sicherheitsgateway möglich. In diesem Fall kann der Schutz vor Schadprogrammen nur durch den Einsatz von Virenfiltern auf den Arbeitsplatzrechnern oder den jeweiligen Servern des vertrauenswürdigen Netzes (beispielsweise E-Mail-Server, Newsserver) realisiert werden.

Zum Thema Virenschutz ist außerdem Baustein B 1.6 *Computer-Virenschutzkonzept* zu berücksichtigen.

M 4.227 Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsbeauftragter

Verantwortlich für Umsetzung: Administrator

In vielen Situationen ist es bei vernetzten Systemen wichtig, dass alle bei einem Vorgang betroffenen Rechner eine korrekte Systemzeit besitzen. Insbesondere bei der Auswertung von Protokollierungsinformationen ist dies von zentraler Bedeutung, beispielsweise um Fehlermeldungen, die auf einen Angriff über das Netz hindeuten, richtig korrelieren zu können, oder wenn bei Anwendungen, die über mehrere Rechner verteilt sind, Synchronisationsprobleme auftreten. Auch verteilte Dateisysteme und zentrale Authentisierungsdienste sind auf Zeitsynchronizität angewiesen.

Network Time Protocol NTP

Für die korrekte Einstellung der Systemzeit bieten die meisten Betriebssysteme die Möglichkeit, über das Protokoll NTP (Network Time Protocol Version 3, RFC 1305) oder SNTP (Simple Network Time Protocol Version 4, RFC 2030) auf einen externen Zeitserver zuzugreifen. Windows-Rechner in einer Active Directory Infrastuktur gleichen zudem die Systemzeit mit dem Domänencontroller ab.

Im Internet existiert eine verteilte Infrastruktur von öffentlichen NTP Zeitservern. In Deutschland bieten beispielsweise die Physikalisch-Technische Bundesanstalt (PTB) in Braunschweig und verschiedene Universitäten einen solchen Dienst an.

NTP nicht direkt auf allen Rechnern

Da NTP ein Klartextprotokoll ohne kryptographische Sicherungen ist, sollte es nur innerhalb des eigenen Netzes eingesetzt werden. Falls die Zeitserver-Infrastruktur im Internet genutzt werden soll, so sollte dafür ein eigener Rechner vorgesehen werden, der als einziger die NTP-Informationen von den ausgewählten Zeitservern bezieht. Die Rechner im lokalen Netz synchronisieren ihre Systemuhr dann mit dem lokalen NTP-Proxy. Am Sicherheitsgateway sollte NTP in diesem Fall nur für den NTP-Proxy-Server freigeschaltet werden. Insbesondere in Netzen mit hohem Schutzbedarf sollten keinesfalls alle Geräte individuell per NTP direkt Anfragen an Zeitserver im Internet stellen.

Sichere Alternative: Lokaler Zeitserver mit Funkuhr

Alternativ kann ein Rechner im internen Netz mit einem Funkuhr-Modul ausgestattet als lokaler Zeitserver eingesetzt werden. Im Zweifelsfall sollte dieser Lösung der Vorzug gegeben werden.

Plausibilitätsprüfungen aktivieren

Falls für die Zeitsynchronisation auf externe Quellen (Funkuhren, öffentliche NTP-Zeitserver, etc.) zurückgegriffen wird, muss sichergestellt werden, dass die empfangenen Zeit-Informationen nicht ungeprüft übernommen werden. Die Software des lokalen Zeit-Servers beziehungsweise NTP-Proxys muss eine Plausibilitätsprüfung vornehmen, bevor sie die empfangenen Zeit-Informationen übernimmt und an die anderen Rechner im Netz weitergibt. Ein Beispiel für eine solche Plausibilitätsprüfung ist, dass sprunghafte Änderungen, die eine vorher festgelegte maximale Zeitdifferenz überschreiten, nicht übernommen werden.

Ergänzende Kontrollfragen:

- Woher werden Zeitinformationen bezogen?

M 4.228 Nutzung der Sicherheitsmechanismen von PDAs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

PDAs und zugehörige Anwendungen können an verschiedenen Stellen durch PINs oder Passwörter abgesichert werden. Hierzu gehören:

Zugriffsschutz für den PDA

Egal welche PDA-Variante eingesetzt wird, eine Zugriffssicherung haben alle. Im Allgemeinen ist diese über eine Passwortabfrage realisiert.

Leider sind nicht alle vom Hersteller angebotenen Sicherheitsmechanismen so sicher, wie es wünschenswert wäre. Daher sollten sich PDA-Benutzer informieren, wie zuverlässig die vorhandenen Sicherheitsmechanismen sind, z. B. über das Internet.

Solange keine besseren Sicherheitstools installiert sind, sollten aber auf jeden Fall die vorhandenen Sicherheitsmechanismen genutzt werden. Alle Benutzer sollten sich aber über deren Wirkung und insbesondere deren Grenzen im Klaren sein. Dabei sollten die Passwörter und PINs sorgfältig ausgewählt werden, also auch lang genug sein, damit sie nicht einfach überwunden werden können. Die Passwörter dürfen keinesfalls zusammen mit dem PDA aufbewahrt werden.

Einschalte-Passwort aktivieren

Bei der Auslieferung ist meist die Passwortabfrage deaktiviert und ein triviales Passwort voreingestellt. Bei der ersten Benutzung sollte unbedingt das Passwort geändert und aktiviert werden, so dass zumindest bei jedem Einschalten des Gerätes eine Passwort-Eingabe erforderlich ist. Für diese Passwörter sollten dieselben Regeln gelten wie für Passwörter zu sonstigen IT-Systemen (siehe auch M 2.11 *Regelung des Passwortgebrauchs*). Auf keinen Fall dürfen sie zu kurz oder zu einfach gewählt sein.

Automatische Sperre / Pausenschaltung

PDAs sehen im Allgemeinen auch die Möglichkeit einer automatischen Sperre vor, die sich bei Arbeitsunterbrechungen nach einem kurzen Moment selbst aktiviert. Erst nach Eingabe des entsprechenden Passwortes ist die weitere Nutzung des PDAs möglich. Ist eine Pausenschaltung vorhanden, so sollte sie unbedingt genutzt werden. Der Zugriffsschutz sollte sich bereits nach einer kurzen Phase von Inaktivität einschalten, zu empfehlen sind hier maximal 5 Minuten. Ist es absehbar, dass die Unterbrechung länger dauert, ist der PDA direkt auszuschalten.

Benutzer-Information

Damit ein ehrlicher Finder eines PDAs weiß, an wen er sich wenden kann, sollte dieser so eingerichtet werden, dass nach dem Einschalten eine entsprechende Information auf dem Bildschirm erscheint. Bei privat genutzten PDAs sollte hier möglichst nicht die vollständige Privatadresse angegeben werden, damit ein Dieb nicht auch noch diese Information für einen Einbruch bei einer naheliegenden Abwesenheit des Benutzers ausnutzen kann (alle Kalenderinformationen liegen ihm ja vor).

Weitere Sicherheitsmechanismen

Es gibt viele verschiedene Sicherheitsmechanismen bei PDAs wie Verschlüsselung oder zeitgesteuerte Deaktivierung. Welche hiervon vorhanden sind bzw. wie diese aktiviert werden können, ist abhängig vom eingesetzten PDA. Daher sollte die Bedienungsanleitung sorgfältig daraufhin ausgewertet werden. Sollen auf einem PDA Daten mit hohem Schutzbedarf bezüglich der Vertraulichkeit gespeichert werden, so sollten diese verschlüsselt werden. Bietet der PDA keine "eingebaute" Verschlüsselungsfunktion, so sollte ein zusätzliches Verschlüsselungsprodukt eingesetzt werden.

Beim Einsatz von PDAs in Behörden oder Unternehmen empfiehlt es sich, die wichtigsten Sicherheitsmechanismen sowohl vorzukonfigurieren als auch auf einem übersichtlichen Handzettel verständlich für die Benutzer zu dokumentieren.

Ergänzende Kontrollfragen:

- Verfügen die eingesetzten PDAs über Einschalte-Passwörter? Sind diese aktiviert?

M 4.229 Sicherer Betrieb von PDAs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Die sinnvolle Nutzung von PDAs erfordert im Allgemeinen eine Kopplung mit anderen IT-System, beispielsweise dem Arbeitsplatzrechner. Die Installation und Konfiguration der dafür benötigten Hard- und Software sollte zentral geregelt sein und durchgeführt werden. Ohne entsprechende Tests und Freigaben sollte keinerlei Installation erfolgen.

Es sind Vorgaben zu den Sicherheitsmechanismen und -einstellungen der eingesetzten PDAs notwendig. Diese müssen in einer PDA-Sicherheitsrichtlinie für Benutzer verständlich dokumentiert werden, da deren korrekte Nutzung stark in der Hand der Benutzer liegt. Daher ist explizit zu verbieten, dass die Konfiguration geändert wird. Außerdem müssen die Benutzer für Sinn und Zweck der gewählten Einstellungen sensibilisiert werden. Soweit technisch möglich, sollten Sicherheitsmechanismen so gewählt und konfiguriert werden, dass die Benutzer möglichst wenig Einflussmöglichkeiten haben.

PDAs sind nicht dafür konzipiert, dass verschiedene Benutzer damit arbeiten sollen. Daher gibt es auch im allgemeinen keine ausgefeilten Mechanismen zur Rollentrennung. Das bedeutet insbesondere, dass es keine nur für Administratoren zugreifbare Bereiche gibt. Benutzer können also nicht daran gehindert werden, sicherheitsrelevante Konfigurationsänderungen durchzuführen. Dies kann nur durch entsprechende Regelungen und Sensibilisierung der Benutzer erreicht werden. Hilfreich ist es außerdem, regelmäßig die Einstellungen zu kontrollieren bzw. diese durch Administrationstools bei der Synchronisierung wieder auf die vorgegebenen Werte zurückzusetzen.

Sicherheit der gekoppelten Endgeräte

Die Sicherheit **aller** zur Synchronisation mit dem PDA benutzten Endgeräte ist wesentlich für die Sicherheit des PDAs selber. Wenn auf den Endgeräten Daten oder Programme manipuliert worden sind, können diese auf den PDA durchgereicht werden, ohne das erkannt werden kann.

Daten oder Programme, die auf einem PDA installiert werden sollen, können in speziellen Verzeichnissen auf dem Benutzer-PC abgelegt werden, so dass sie bei der nächsten Synchronisation automatisch auf den PDA transferiert werden. Der Zugriff auf diese Verzeichnisse sollte soweit wie möglich beschränkt werden. Die Benutzer sollten außerdem regelmäßig diese Verzeichnisse daraufhin inspizieren, ob sich dort ihnen unbekannte Dateien befinden. Die Synchronisationssoftware sollte so konfiguriert werden, dass vor der Installation von Programmen eine Rückfrage beim Benutzer erfolgt. Der Synchronisationsvorgang sollte nicht unbeobachtet ablaufen, auch die Informationen, welche Dateien jeweils transferiert werden, können entscheidende Hinweise enthalten.

Test- und Freigabe neuer Applikationen

Bei der Installation von Applikationen sind natürlich die üblichen Vorgaben zu beachten, d. h. es muss ein geordnetes Test- und Freigabeverfahren erfolgen.

Die Synchronisation sollte protokolliert werden, bei nahezu allen PDAs kann dies entsprechend konfiguriert werden. Die Synchronisationsprotokolle sollten

dann regelmäßig zumindest überflogen werden, um festzustellen, ob unbefugte Synchronisationsvorgänge stattgefunden haben.

In der Sicherheitsrichtlinie sollte festgehalten werden, welche Daten und Programme auf den PDAs gespeichert werden dürfen. Davon hängen auch weitere Sicherheitsmaßnahmen ab. Beispielsweise hat ein PDA, auf dem ausschließlich Termine und Adressen gespeichert werden, einen niedrigeren Schutzbedarf als ein PDA, auf dem kryptographische Schlüssel und Zugangsparameter für andere IT-Systeme und Netze abgelegt sind.

Virenschutz

Die ersten Viren und Trojanischen Pferde, die speziell für PDAs konzipiert worden sind, sind bereits veröffentlicht worden. Diese haben zwar noch keine großen Schäden verursacht, zeigen aber auf, dass Vorbeugung notwendig ist. Die meisten Hersteller von Virenschutz-Programmen haben mittlerweile auch PDA-Virenscanner in die Produktpalette mitaufgenommen. Nicht vergessen werden darf in diesem Zusammenhang auch der Virenschutz auf Seiten der zur Synchronisation eingesetzten PCs. Auch diese müssen mit aktuellen Virenschutz-Programmen ausgestattet sein. Im Büro sollte das eine Selbstverständlichkeit sein, nicht vergessen werden dürfen allerdings die Privat-PCs, mit denen eventuell noch synchronisiert wird.

Internet-Anbindung

Wenn über PDAs Internet-Dienste genutzt werden sollen, sollte neben einem E-Mail-Client ein Web-Browser installiert sein. Dieser sollte SSL bzw. TSL beherrschen, damit verschlüsselte Verbindungen hergestellt werden können, beispielsweise für den Zugriff auf unternehmens- oder behördeninterne Server. Einige der für PDAs verfügbaren Browser unterstützen auch aktive Inhalte, also Java, ActiveX und/oder Javascript. Wie bei anderen IT-Systemen ist aber auch hier zu beachten, dass je nach Art dieser Programme mit ihrem Ausführen eventuell ein Sicherheitsrisiko verbunden sein kann. Daher sollten aktive Inhalte im WWW-Browser im Regelfall abgeschaltet sein und nur aktiviert werden, wenn diese aus einer vertrauenswürdigen Quelle kommen, also z. B. von den WWW-Seiten eines ihnen bekannten Anbieters.

Auch wenn für fast alle PDAs Web-Browser verfügbar sind, kann die Nutzung von WAP-Browsern die bessere Alternative sein, da über WAP häufig dieselben Informationen kompakter und weniger grafiküberfrachtet angeboten werden. Dies gilt ebenso für Notebooks und sogar stationäre PCs, wenn die verfügbare Bandbreite der Internet-Anbindung zu wünschen übrig lässt. WAP-Browser sollten über WTLS (Wireless Transport Layer Security) verfügen. WTLS bietet die Überprüfung der Datenintegrität, Abhörsicherheit und Authentikation von Server und Client mittels Verschlüsselung und dient als Schutz vor Denial-of-Service-Attacken. WTLS basiert auf dem Industrie-Standard TLS, der eine Erweiterung des SSL-Protokolls ist.

Inventarisierung

Da kleine und mobile Geräte häufig aus den Augen verloren werden, müssen für den Einsatz in einer Institution Bestandsverzeichnisse über diese angelegt werden. Die Bestandsverzeichnisse sollten mindestens folgende Informationen enthalten: Identifizierungsmerkmale wie Gerätenummern oder Inventarnummern, Art des Gerätes, Betriebssystem, Installationsdatum und Konfigurationsbesonderheiten, Aufstellungsort (wenn stationär), Benutzer sowie Administratoren.

Ergänzende Kontrollfrage:

- Wie werden PDAs administriert?

M 4.230 Zentrale Administration von PDAs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Administration für mobile Endgeräte ist keine einfache Aufgabe, vor allem bei großen Institutionen und bei Benutzern, die sich häufig und in aller Welt bewegen. Es gibt Tools, die eine zentrale Administration und die Umsetzung von Sicherheitsrichtlinien erleichtern. Mit solchen Tools können dann beispielsweise zentrale Vorgaben an die Passwortgestaltung umgesetzt werden oder auch der Zugriffsschutz beim Synchronisationsvorgang verbessert werden.

Grundsätzlich ist eine gut überlegte Einbindung in die vorhandene IT-Umgebung notwendig, um die Benutzer durch den Komfort von einer gut administrierten PDA-Anbindung davon abzuhalten, weitere, unkontrollierte und damit potentiell unsichere PDAs mit einzuschleppen. Durch eine zentrale Administration können nicht nur Software und Informationen verteilt, sondern auch die organisationseigenen Sicherheitsrichtlinien durchgesetzt werden, z. B. für Authentikation, Zugriff oder Datensicherung.

Beim Einsatz von Software zum zentralen PDA-Management erfolgt die Synchronisation der PDAs dann typischerweise nicht mehr mit einem lokalem Endgerät, sondern mit einem Server. Daher können Daten dann nicht nur von einer Station aus abgeglichen werden, sondern von allen mit dem Server verbundenen. (Hinweis: Daher ist hierbei natürlich der Zugriffsschutz auf die Dockingstationen besonders wichtig, um zu verhindern, dass Unbefugte hierüber Zugriff auf die gesammelten Synchronisationsdaten nehmen.)

Bei der Synchronisation über einen Server lassen sich aber auch Sicherheitsvorgaben technisch forcieren, indem sicherheitsrelevante Einstellungen auf ihre vorgegebenen Werte zurückgesetzt werden. Typische Funktionen solcher Tools zum zentralen PDA-Management sind unter anderem:

- Über Personal Information Manager (PIM) können Termine verwaltet und Adressenbücher geführt werden, und dies nicht nur für einzelne Benutzern, sondern für Arbeitsgruppen. Die bekanntesten Anwendungen von PIMs sind Microsoft Outlook und Lotus Notes. Bei PDAs werden PIMs für die gesteuerte Synchronisation mit den Hintergrundsystemen eingesetzt. Das Management der PIM-Daten, anderer Informationen und der Applikationen, die auf den diversen PDAs vorhanden sein sollen, kann zentral gesteuert werden. Dadurch können z. B. Applikationen remote installiert und konfiguriert werden.
- Es können aber auch zentrale Adressen-Sammlungen und andere Daten gepflegt und weitergegeben werden. Dies erleichtert besonders bei einer Vielzahl von mobilen Mitarbeitern, die unterwegs eingepflegten Daten den anderen Mitarbeitern schnell und komfortabel zur Verfügung zu stellen.
- Datensicherungen können zentral durchgeführt werden, ohne dass die Benutzer sich darum kümmern müssen. Ebenso können Vorgaben gemacht werden, wann bzw. wie oft Daten zu sichern oder zu synchronisieren sind und welche Randbedingungen dabei eingehalten werden müssen.

- Es besteht die Möglichkeit, Rückmeldungen über den Status der PDAs zu erhalten und Diagnosen remote durchführen zu können.
- Es können Benutzerprofile angelegt werden, um die Benutzerverwaltung zu vereinfachen.
- Es lassen sich organisationsspezifisch einstellbare Passwortregeln und andere Sicherheitsregeln vorgeben.

Diese Funktionen können im Allgemeinen nicht nur über Dockingstationen, sondern auch über andere Schnittstellen wie Infrarot oder Bluetooth angeboten werden, so dass auch diese Zugriffe zum einem unterstützt und zum anderen abgesichert werden können.

Ein Tool zum zentralen PDA-Management sollte möglichst alle in der Organisation eingesetzten PDA-Betriebssysteme unterstützen, damit nicht mehrere solcher Tools parallel eingesetzt werden müssen. Dasselbe gilt ebenso natürlich für die eingesetzte Groupware und E-Mail-Plattform.

M 4.231 Einsatz zusätzlicher Sicherheitswerkzeuge für PDAs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer, Administrator

Es gibt diverse Zusatzwerkzeuge, mit denen die Sicherheit von PDAs verbessert werden kann. Diese bieten erweiterte Sicherheitsfunktionen wie beispielsweise

- Verschlüsselung des Dateisystems und der Speicherkarteninhalte oder auch nur einzelner Dateien oder Datenbanken,
- Verbesserung der Authentisierung, z. B. durch einfachere oder sicherere Authentisierungsverfahren,
- Absicherung der Verbindung zu anderen Komponenten, z. B. durch Verschlüsselung der Kommunikation oder durch Erzeugung von Einmalpasswörtern für die Anmeldung über externe IT-Systeme,
- Virenschutz und
- Verhinderung des unautorisierten Zugriffs auf das Gerät.

Dadurch kann die PDA-Sicherheit bis zu einem gewissen Grad erhöht werden. Dafür müssen die Benutzer die erweiterten Sicherheitsmechanismen aber auch genau kennen. Sie sollten zum einen über deren Nutzen und Schwächen informiert sein und zum anderen über deren Handhabung. Generell sollte aber allen Anwendern klar sein, dass es nahezu unmöglich ist, auf einer unsicheren Plattform mit schwachen Sicherheitsmechanismen eine zuverlässig sichere Applikation zu implementieren. Für viele der PDA-Sicherheitsprodukte sind schon Warnmeldungen über Sicherheitslücken herausgegeben worden. Auch mit der verfügbaren Zusatz-Sicherheitssoftware für PDAs werden nur einige, aber nicht alle vorhandenen Sicherheitsprobleme beim PDA-Einsatz behoben.

Trotzdem sollte geprüft werden, inwieweit solche Tools für den jeweiligen Einsatzzweck sinnvoll sind, da sie helfen, das Gefährdungspotential zu senken. Der Einsatz solcher Tools ist vor allem dann anzuraten, wenn PDAs als Sicherheitstoken oder für die Speicherung sensibler Daten eingesetzt werden. So gibt es beispielsweise Tools zur Verbesserung des Zugriffsschutzes, zur Verschlüsselung einzelner Dateien oder des gesamten Systems und für eine zentrale Administration.

Ergänzende Kontrollfragen:

- Werden die Benutzer im Umgang mit den zusätzlichen Sicherheitswerkzeugen geschult?
- Werden PINs und kryptographische Schlüssel für die Nutzung zusätzlicher Sicherheitswerkzeuge sicher und sorgfältig erzeugt?

M 4.232 Sichere Nutzung von Zusatzspeicherkarten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Da bei mobilen Endgeräten wie PDAs der vorhandene Speicherplatz beschränkt ist, können die meisten Modelle mit externen Speichermedien erweitert werden. Verbreitet sind hierfür Speicherkarten, z. B. SD-, MMC-Cards oder auch Compact Flash Cards, die den Vorteil haben, schnell gewechselt werden zu können. Diese Karten benötigen keine Batterie zur Datenspeicherung, wodurch der Verlust der gespeicherten Daten durch Strommangel wegfällt. Sie eignen sich dadurch auch, um unterwegs Backups durchzuführen, was vor allem dann sinnvoll ist, wenn ein PDA-Benutzer häufig lange abwesend ist. Wie generell für Datensicherungen gilt auch hier, dass diese sicher verwahrt werden müssen. Wenn die Memory-Cards im PDA oder anderswo unbeaufsichtigt zurückgelassen werden können, können Unbefugte diese benutzen, um die darauf gespeicherten Daten auszulesen. Dies geht mit einem Laptop und einem geeigneten Adapter im Handumdrehen. Wenn anschließend die Memory-Card wieder zurückgelegt wird, werden dabei nicht einmal Spuren hinterlassen.

Um die Daten auf externen Speicherkarten zu schützen, ist es empfehlenswert, diese mit entsprechenden Zusatztools zu verschlüsseln. Solange dies nicht der Fall ist, sollten die Speicherkarten auch unterwegs immer beaufsichtigt werden.

Ergänzende Kontrollfrage:

- Werden Zusatzspeicherkarten immer sicher aufbewahrt?

M 4.233 Sperrung nicht mehr benötigter RAS-Zugänge

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Nutzung eines entfernten Zugangs ist in regelmäßigen Zeitabständen zu überprüfen. Bestehende, in Vergessenheit geratene RAS-Zugänge stellen unnötige Sicherheitslücken dar und sind schnellstmöglich zu sperren, falls ihre Nutzung nicht mehr erwünscht ist.

Auch die Anforderungen für den Remote Access Zugang sollen in regelmäßigen Abständen überprüft und das RAS-Konzept daraufhin angepasst werden. Besonders ist dabei darauf zu achten, ob die Berechtigungen für den RAS-Zugang der einzelnen Mitarbeiter zu ihren aktuellen Aufgaben passen.

Die Überprüfung der Anforderungen gilt ebenfalls für die einzelnen Systeme, die in dem RAS-Konzept beteiligt sind. Hier ist auch nach dem Minimalprinzip zu handeln.

Ergänzende Kontrollfragen:

- Wird regelmäßig überprüft, ob die bestehenden RAS-Zugänge noch sinnvoll sind?
- Existiert ein Verfahren, um die Remote Access Zugriffsrechte von Mitarbeitern bei Aufgabenänderungen anzupassen?

M 4.234 Aussonderung von IT-Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

IT-Systeme sind dem ständigen Wandel der Technik unterworfen. Daher werden sie häufiger ausgetauscht als viele andere Arbeitsmaterialien. Da sich auf IT-Systemen aber schutzbedürftige Daten und Anwendungen befinden können, ist die Weitergabe oder Aussonderung von IT-Systemen zu regeln.

Unabhängig davon, ob ausrangierte IT-Systeme an andere Abteilungen weitergegeben werden, an Mitarbeiter verschenkt, verkauft oder verschrottet werden, muss sichergestellt sein, dass alle Daten und Anwendungen vorher sorgfältig gelöscht wurden (siehe auch M 2.167 *Sicheres Löschen von Datenträgern*).

Vorher ist zu überprüfen, ob die Daten gesichert wurden, soweit sie noch benötigt werden.

Es empfiehlt sich, dass beide Schritte vom jeweils Zuständigen schriftlich bestätigt werden.

Ergänzende Kontrollfragen:

- Werden vor einer Aussonderung alle gespeicherten Daten und Anwendungen sorgfältig gelöscht?

M 4.235 Abgleich der Datenbestände von Laptops

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Benutzer, Administrator

Wenn ein Laptop unterwegs eingesetzt wird, ist es wichtig, alle erforderlichen Daten und Anwendungen in der aktuellsten Version verfügbar zu haben. Ebenso sollten unterwegs bearbeitete Daten zügig auf IT-Systemen innerhalb des IT-Verbunds der Behörde bzw. des Unternehmens gespeichert werden, damit es nicht zu inkonsistenten Datenbeständen kommt. Der einfachste Weg hierfür ist der regelmäßige Abgleich der Datenbestände von Laptops, beispielsweise über Tools zur Synchronisation von Dateien und Verzeichnissen zwischen Laptops und Arbeitsplatzrechnern oder Servern.

Dafür sollte überlegt werden, welche Informationen an welchen Stellen gespeichert sind, also auf welchen Servern und in welchen Verzeichnissen. Bei der ersten Sichtung zeigt sich meist, an wie vielen verschiedenen Stellen in einem IT-Verbund sich die für einen Arbeitsplatz relevanten Informationen befinden.

Damit Synchronisationsvorgänge nicht zu lange dauern, sollten dafür Tools ausgewählt werden,

- über die Dateien und Verzeichnisse nach vorher festgelegten Kriterien automatisch abgeglichen und aktualisiert werden können,
- die über Filtermöglichkeiten komplette Verzeichnisse oder auch einzelne Dateien von einem Kopiervorgang ausschließen können,
- die Synchronisationskonflikte auflösen können. Synchronisationskonflikte können auftreten, wenn seit der letzten Synchronisation eine Datei in verschiedenen Verzeichnissen geändert wurde.

Synchronisationstools sollten außerdem möglichst benutzerfreundlich sein und trotzdem einen guten Schutz vor fehlerhafter Bedienung gewährleisten. Synchronisationsvorgänge sollten zugriffsgeschützt sein, bei Laptops kann dies über bereits vorhandene Zugriffsschutz-Verfahren erfolgen.

Damit über die Synchronisation keine Manipulationen vorgenommen werden können, sollten die Benutzer regelmäßig die relevanten Verzeichnisse daraufhin inspizieren, ob sich dort ihnen unbekannte Dateien befinden. Die Synchronisationssoftware sollte so konfiguriert werden, dass vor der Installation von Programmen eine Rückfrage beim Benutzer erfolgt. Der Synchronisationsvorgang sollte nicht unbeobachtet ablaufen, auch die Informationen, welche Dateien jeweils transferiert werden, können entscheidende Hinweise enthalten. Die Synchronisation sollte protokolliert werden. Die Synchronisationsprotokolle sollten dann regelmäßig zumindest überflogen werden, um festzustellen, ob unbefugte Synchronisationsvorgänge stattgefunden haben.

Ergänzende Kontrollfragen:

- Existieren Tools oder Verfahren für die Synchronisation von Datenbeständen zwischen Laptops und stationären IT-Systemen?

M 4.236 Zentrale Administration von Laptops

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator

Die Administration für mobile Endgeräte ist keine einfache Aufgabe, vor allem bei großen Institutionen und bei Benutzern, die sich häufig und in aller Welt bewegen. Es gibt Tools, die eine zentrale Administration und die Umsetzung von Sicherheitsrichtlinien erleichtern. Durch eine zentrale Administration können nicht nur Software und Informationen verteilt, sondern auch die organisationseigenen Sicherheitsrichtlinien durchgesetzt werden, z. B. für Authentisierung, Zugriff oder Datensicherung.

Beim Einsatz von Software zum zentralen Laptop-Management erfolgt die Synchronisation der Laptops dann typischerweise nicht mehr mit einem lokalem Endgerät, sondern mit einem Server. Daher können Daten dann nicht nur von einer Station aus abgeglichen werden, sondern von allen mit dem Server verbundenen.

Bei der Synchronisation über einen Server lassen sich aber auch Sicherheitsvorgaben technisch forcieren, indem sicherheitsrelevante Einstellungen auf ihre vorgegebenen Werte zurückgesetzt werden. Typische Funktionen solcher Tools zum zentralen Laptop-Management sind unter anderem:

- Datensicherungen können zentral durchgeführt werden, ohne dass die Benutzer sich darum kümmern müssen. Ebenso können Vorgaben gemacht werden, wann bzw. wie oft Daten zu sichern oder zu synchronisieren sind und welche Randbedingungen dabei eingehalten werden müssen.
- Es besteht die Möglichkeit, Rückmeldungen über den Status der Laptops zu erhalten und Diagnosen remote durchführen zu können.
- Es können Benutzerprofile angelegt werden, um die Benutzerverwaltung zu vereinfachen.
- Es lassen sich organisationsspezifisch einstellbare Passwortregeln und andere Sicherheitsregeln vorgeben.

Ein Tool zum zentralen Laptop-Management sollte möglichst alle in der Organisation eingesetzten Laptop-Betriebssysteme unterstützen, damit nicht mehrere solcher Tools parallel eingesetzt werden müssen. Dasselbe gilt ebenso natürlich für die eingesetzte Groupware und E-Mail-Plattform.

M 4.237 Sichere Grundkonfiguration eines IT-Systems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Grundeinstellungen, die vom Hersteller oder Distributor eines Betriebssystems vorgenommen werden, sind meist nicht auf Sicherheit optimiert, sondern auf eine einfache Installation und Inbetriebnahme sowie oft darauf, dass jeder Anwender möglichst einfach auf möglichst viele Features des Betriebssystems zugreifen kann. Beim Einsatz von IT-Systemen (egal, ob als Client oder Server) in Behörden oder Unternehmen ist dies oft nicht wünschenswert.

Der erste Schritt bei der Grundkonfiguration muss daher sein, die Grundeinstellungen zu überprüfen und nötigenfalls entsprechend den Vorgaben der Sicherheitsrichtlinie anzupassen. Die Grundkonfiguration ist naturgemäß relativ stark vom eingesetzten Betriebssystem abhängig. Aus diesem Grund sind in den betriebssystemspezifischen Bausteinen entsprechende detailliertere Maßnahmen enthalten.

Ziele einer sicheren Grundkonfiguration sollten sein, dass

- das System gegen "einfache" Angriffe über das Netz abgesichert ist,
- ein normaler Benutzer durch reine Neugierde oder gar zufällig keinen Zugriff auf sensitive Daten erlangen kann, die nicht für ihn bestimmt sind,
- kein normaler Benutzer beim normalen Arbeiten mit dem System durch reine Bedienungsfehler oder Leichtsinn ("Was passiert eigentlich, wenn ich diese Datei lösche?") schwerwiegenden Schaden am System oder an Daten anderer Benutzer verursachen kann, und dass
- auch für die Arbeiten des Systemadministrators die Auswirkungen kleinerer Fehler so weit wie möglich begrenzt sind.

Die Einstellungen, die im Rahmen der Grundkonfiguration überprüft und angepasst werden sollten betreffen insbesondere die folgenden Bereiche:

- **Einstellungen für den Systemadministrator**

  Für das Konto des Systemadministrators müssen besonders sichere Einstellungen gewählt werden. Dies betrifft beispielsweise die Einstellungen für die Benutzerumgebung wie

  - Suchpfade für Programme und Dateien,
  - Umgebungsvariablen und die
  - Konfiguration bestimmter Programme.

  Diese Einstellungen sollten überprüft und gegebenenfalls angepasst werden. Außerdem sollten die Einstellungen für das Benutzerverzeichnis des Systemadministrators so gewählt werden, dass normale Benutzer keinen Zugriff darauf haben.

- **Einstellungen für die Systemverzeichnisse und -dateien**

  Bei der Grundkonfiguration muss überprüft werden, ob die Berechtigungen für Systemverzeichnisse und -dateien den Vorgaben der Sicherheitsrichtlinie entsprechen. Auf einem Server sollten für die Berechtigungen der Systemverzeichnisse und -dateien relativ restriktive Einstellungen gewählt werden.

- **Einstellungen für Benutzerkonten**

  Im Rahmen der Grundkonfiguration sollte überprüft werden, welche Standardeinstellungen für Benutzerkonten gelten. Die Einstellungen müssen gegebenenfalls entsprechend der Sicherheitsrichtlinie angepasst werden. Dies betrifft im wesentlichen die selben Parameter wie für das Konto des Systemadministrators, für normale Benutzer können aber unter Umständen andere Einstellungen sinnvoll sein.

- **Bereinigung der Benutzerdatenbank**

  Oft wird im Rahmen der Standardinstallation eines Betriebssystems eine größere Anzahl von Benutzerkonten eingerichtet, die für den Betrieb nicht in jedem Fall notwendig sind. Daher sollte im Rahmen der Grundkonfiguration geprüft werden, welche Benutzerkonten wirklich gebraucht werden. Nicht benötigte Benutzerkonten sollten entweder gelöscht oder zumindest so deaktiviert werden, so dass unter dem betreffenden Konto keine Anmeldung am System möglich ist.

- **Überprüfung der Netzdienste**

  Die Standardinstallation eines Betriebssystems enthält oft eine Reihe von Netzdiensten, die normalerweise nicht benötigt werden und die gerade deswegen eine Quelle von Sicherheitslücken sein können. Nach der Installation sollte deswegen überprüft werden, welche Netzdienste auf dem System installiert und aktiviert sind. Nicht benötigte Netzdienste sollten deaktiviert oder ganz deinstalliert werden.

  Die Überprüfung auf laufende Dienste kann einerseits lokal mit den Mitteln des installierten Betriebssystems und andererseits von außen durch einen Portscan von einem anderen System aus erfolgen. Durch eine Kombination beider Methoden kann weitgehend ausgeschlossen werden, dass das System noch weitere ungewollte Netzdienste anbietet.

- **Einstellungen für den Zugriff auf das Netz**

  Im Rahmen der Grundkonfiguration sollten auch die Einstellungen für den Zugriff auf das Netz sowie wichtige externe Dienste getroffen und dokumentiert werden. Dies betrifft beispielsweise (sofern nicht bereits bei der Installation geschehen):

  - Vergabe der IP-Adresse und Konfiguration der grundlegenden Netzparameter oder Konfiguration des Zugriffs auf einen Server, der automatisch, beispielsweise über DHCP (Dynamic Host Configuration Protocol) Netzeinstellungen verteilt. Für Server wird allerdings von der Verwendung von DHCP abgeraten.

- Konfiguration des Zugriffs auf einen DNS-Server und gegebenenfalls andere Namensdienste und die
- Konfiguration des Zugriffs auf verteilte Dateisysteme, Datenbanken oder sonstige externe Dienste.

- **Zusätzlicher Schutz durch einen lokalen Paketfilter**

  Server und Clients mit hohem Schutzbedarf sollten zusätzlich zum Schutz durch die organisationsweiten Sicherheitsgateways oder Paketfilter, die das interne Netz segmentieren, mit einem lokalen Paketfilter abgesichert werden. Entsprechende Funktionalitäten sind in praktisch allen modernen Betriebssystemen vorhanden.

  Im Rahmen der Grundkonfiguration sollte zumindest für Server mit hohem Schutzbedarf ein entsprechender Schutz durch einen lokalen Paketfilter realisiert werden. Auch für Server mit normalem Schutzbedarf wird der Schutz durch einen lokalen Paketfilter empfohlen. Gegebenenfalls kann in diesem Fall eine "liberalere" Konfiguration gewählt werden.

  Für Clients wird der Einsatz eines lokalen Paketfilters zumindest dann empfohlen, wenn diese einen hohen oder sehr hohen Schutzbedarf im Bezug auf die Vertraulichkeit oder Integrität besitzen.

  Genauere Informationen zur Einrichtung eines lokalen Paketfilters finden sich in M 4.238 *Einsatz eines lokalen Paketfilters*.

- **Anlegen einer Integritätsdatenbank**

  Nach Abschluss der Grundkonfiguration wird empfohlen, mit einem entsprechenden Tool eine Integritätsdatenbank anzulegen. Bei manchen Betriebssystemen gehören entsprechende Programme bereits zum Umfang einer Standardinstallation. Die Integritätsdatenbank sollte nicht auf dem System selbst, sondern auf einem schreibgeschützten Datenträger (beispielsweise CD-R) oder einem anderen, besonders gesicherten System gespeichert werden. Bei einem Verdacht auf eine Kompromittierung des Systems lassen sich anhand der erzeugten Prüfsummen Dateien identifizieren, die von einem Angreifer modifiziert wurden. Bei den regelmäßigen Überprüfungen der Systemintegrität (siehe auch M 5.8 *Regelmäßiger Sicherheitscheck des Netzes*) dient diese Datenbank als Referenz für einen definierten, sicheren Zustand des Systems.

Dokumentation ist wichtig

Es sollte dokumentiert werden, welche Einstellungen im Rahmen der Grundkonfiguration überprüft, sowie ob und gegebenenfalls wie sie geändert wurden. Die Dokumentation muss so beschaffen sein, dass im Notfall auch eine andere Person als der eigentliche Administrator ohne vorherige Kenntnis des Systems anhand der Dokumentation nachvollziehen kann, was getan wurde. Im Idealfall sollte es möglich sein, alleine mit Hilfe der Dokumentation das System wiederherzustellen.

Ergänzende Kontrollfragen:

- Wie sind die Einstellungen für die Benutzerumgebung des Systemadministrators?
- Wurden nicht benötigte Benutzerkonten deaktiviert oder gelöscht?
- Wurden nicht benbötigte Netzdienste deaktiviert oder deinstalliert? Wurde ein Portscan durchgeführt?
- Wurde eine Integritätsdatenbank erzeugt? Welches Tool wurde benutzt?

M 4.238 Einsatz eines lokalen Paketfilters

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Das gesamte Netz einer Organisation sollte durch ein entsprechendes Sicherheitsgateway geschützt sein. Server, die Dienste nach außen hin anbieten, sollten in einer Demilitarisierten Zone (DMZ) aufgestellt werden. Trotzdem ist es empfehlenswert, auch auf jedem Rechner entsprechende Zugriffsbeschränkungen auf Anwendungs- oder Netzebene einzurichten. Dies gilt auch für Server, die nur intern genutzt werden und nicht zuletzt auch für Clients.

Ein lokaler Paketfilter kann einen Rechner gegen Angriffe schützen, die aus dem selben Subnetz heraus gestartet werden. Außerdem kann ein solcher Paketfilter dazu benutzt werden, eine feiner abgestufte Zugriffskontrolle für einzelne Dienste zu realisieren, als dies beispielsweise mit Paketfiltern nur an Netzübergängen möglich ist.

Darüber hinaus kann ein lokaler Paketfilter auch dazu benutzt werden, ausgehende Netzverbindungen zu beschränken und so die Folgen einer Kompromittierung des Systems zu begrenzen. Ein solcher Schutz kann zwar eventuell von einem Angreifer nach einer erfolgreichen Kompromittierung des Rechners deaktiviert werden, andererseits wird ein Angreifer auf diese Weise zumindest behindert. Auf diese Weise kann entscheidende Zeit bei der Entdeckung und für mögliche Reaktionen gewonnen werden.

Zuletzt kann die Protokollfunktion eines lokalen Paketfilters es ermöglichen, bestimmte Angriffe überhaupt zu entdecken.

Zugriffsbeschränkugen auf Betriebssystem-ebene

Praktisch alle aktuellen Betriebssysteme bieten die Möglichkeit, Filter zu definieren, die alle empfangenen oder zu sendenden Pakete nach bestimmten Regeln untersuchen und behandeln. Die Filtermöglichkeiten unterscheiden sich dabei zwischen den einzelnen Betriebssystemen teilweise erheblich. Praktisch immer können jedoch Regeln basierend auf der Quell- und Zieladresse des Pakets sowie auf dem verwendeten Protokolltyp (TCP/IP, UDP/IP, ICMP etc.) sowie gegebenenfalls dem Quell- oder Zielport definiert werden. Mit Hilfe von Paketfilterregeln können so beispielsweise Pakete, die von bestimmten Rechnern oder aus bestimmten Subnetzen stammen, gezielt verworfen werden.

Manche Serveranwendungen besitzen eigene Mechanismen, um den Zugriff auf den Dienst für einzelne IP-Adressen oder Adressbereiche zu erlauben oder zu verbieten. Gegenüber diesen Mechanismen hat ein lokaler Paketfilter auf Betriebssystemebene den Vorteil, dass er den Dienst selbst gegen mögliche Angriffe schützt, die zu einer Kompromittierung führen, bevor die eingebaute Zugriffsbeschränkung überhaupt wirksam werden kann.

Prinzipiell sollten alle Server mit hohem Schutzbedarf mit einem lokalen Paketfilter geschützt werden.

Freizügig vs. restriktiv

Es gibt zwei allgemeine Strategien, mit der Paketfilter-Regeln implementiert werden können: Die Blacklist-Strategie erlaubt alle Arten von Verbindungen, die nicht bestimmte Ausschlusskriterien erfüllen (Freizügige Strategie: "Alles ist erlaubt, was nicht explizit verboten ist"). Der Vorteil liegt dabei in einem

eventuell geringeren Aufwand bei der Administration und der Fehlersuche. Ein schwerwiegender Nachteil ist jedoch, dass vergessene Regeln, die den Zugriff auf nicht geschützte Netzdienste ermöglichen, als Grundlage für einen Angriff dienen können.

Demgegenüber werden bei der Whitelist-Strategie alle Arten von Verbindungen blockiert, die nicht zu einer Liste erlaubter Dienste gehören (Restriktive Strategie: "Alles ist verboten, was nicht explizit erlaubt ist").

Die Whitelist-Strategie bietet die größere Sicherheit und sollte daher grundsätzlich verwendet werden, wenn nicht wichtige Gründe dagegen sprechen. Der Nachteil liegt in einem tendenziell höheren Administrationsaufwand, da bei jeder Änderung der Anforderungen neue Regeln definiert werden müssen. In Ausnahmefällen, beispielsweise wenn ein Protokoll nicht auf fest definierten Ports arbeitet, kann auf die Blacklist-Strategie zurückgegriffen werden.

Es ist empfehlenswert, auf allen Servern im Rahmen der Grundkonfiguration einen lokalen Paketfilter mit einem Basis-Regelwerk einzurichten, bei dem grundsätzlich alle Verbindungsanfragen von außen abgewiesen werden. Dieses Regelwerk sollte aktiv sein, wenn das System ans Netz angeschlossen wird. Je nachdem welche Dienste von dem System angeboten werden sollen, können nach deren Konfiguration die dafür benötigten Protokolle und Ports freigeschaltet werden. Auch für Clients sollte dieses Vorgehen zumindest dann in Betracht gezogen werden, wenn diese besondere Anforderungen an die Sicherheit stellen.

Logging

Paketfilter erlauben meist ein detailliertes Protokollieren des Netzverkehrs. Das Aufsetzen eines lokalen Paketfilters ist daher auch in sicheren Netzen, die mit einem Sicherheitsgateway von einem unsicheren Netz wie dem Internet getrennt sind, sinnvoll, denn gewonnen Informationen können für die Erkennung von Angriffen hilfreich sein. Allerdings muss dabei darauf geachtet werden, dass keine Datenschutzbestimmungen verletzt werden. Gegebenenfalls sollten die entsprechenden Stellen (Datenschutzbeauftragter, Belegschaftsvertretung oder andere) beteiligt werden.

Problem ICMP

Das *Internet Control Message Protocol* ICMP wird dazu verwendet, Nachrichten über Fehler bei der Übertragung von IP-Paketen zu übermitteln. Beispielsweise existieren Nachrichten, die dem Sender eines Pakets mitteilen, dass das Zielnetz nicht erreichbar ist oder dass das Paket zu groß war, um an das Zielsystem weitergeleitet zu werden. Die Funktion der Tools *ping* und *traceroute* beruhen ebenfalls auf ICMP.

Neben vielen nützlichen Eigenschaften gibt es jedoch einige ICMP-Nachrichtentypen, mit denen Angreifer sich wichtige Informationen über ein Netz verschaffen und diese direkt für Angriffe benutzen können. Leider ist der radikale Ansatz, ICMP grundsätzlich am Sicherheitsgateway zu blockieren, ebenfalls keine befriedigende Lösung, da bestimmte Funktionen dann nicht mehr verfügbar sind. Auf *ping* und *traceroute* kann zwar in der Regel auf normalen Arbeitsplatzrechnern und Servern verzichtet werden, eine globale Blockierung von ICMP kann aber zu Beeinträchtigungen führen, die schwer zu diagnostizieren sind. Daher sollte überlegt werden sowohl am

Sicherheitsgateway, als auch beim lokalen Paketfilter eine selektive ICMP-Filterung vorzunehmen, sofern dieser die entsprechenden Möglichkeiten zur Verfügung stellt. Dies sollte stets unter der Berücksichtigung des Einsatzzweckes des Rechners (Server oder Arbeitsplatzrechner), dessen Schutzbedarfs und die am Sicherheitsgateway getroffenen Maßnahmen geschehen. Beispielsweise kann für das interne Netz eine größere Zahl von Nachrichtentypen zugelassen werden, als für das externe Netz.

Mehr Informationen zur Filterung von ICMP finden sich im Baustein B 3.301 *Sicherheitsgateway (Firewall)* und speziell in M 5.120 *Behandlung von ICMP am Sicherheitsgateway*.

Umsetzung und Überprüfung

Welche Möglichkeiten der Filterung und Protokollierung zur Verfügung stehen, unterscheidet sich je nach Betriebssystem. Vor dem Aufsetzen eines lokalen Paketfilters sollte die vorhandene Dokumentation zu Rate gezogen werden.

Vorsicht bei Einrichtung und Test

Bei der Einrichtung von Paketfilterregeln sollte mit großer Sorgfalt vorgegangen werden, da ein Fehler in einer Regel unter Umständen dazu führen kann, dass sich ein Administrator, der über das Netz auf dem Rechner arbeitet, auf diese Weise "aussperrt" und die Korrekturen von der Systemkonsole aus vornehmen muss.

Nach dem Aktivieren des lokalen Paketfilters sollte einerseits geprüft werden, ob die benötigten Dienste noch erreichbar sind, andererseits sollte mit einem Portscan überprüft werden, ob die restlichen Ports alle blockiert sind.

Beispiel: lokale Paketfilterregeln für einen Webserver

Im nachfolgenden Beispiel werden lokale Paketfilterregeln für einen Rechner vorgeschlagen, der als Webserver in einer DMZ aufgestellt ist. Dabei wird davon ausgegangen, dass die Administration des Servers von einem Arbeitsplatzrechner aus über eine ssh-Verbindung erfolgt und die Dateien für das Webangebot ebenfalls über eine ssh-Verbindung auf den Rechner übertragen werden.

Für den Webserver wurde die Namensauflösung per DNS abgeschaltet, daher ist kein Zugriff auf einen DNS-Server erforderlich. UDP kann daher vollständig blockiert werden. Vom Webserver aus wird normalerweise kein *ping* oder *traceroute* benötigt, sondern es wird nur der ICMP-Nachrichtentyp 3 (*Destination unreachable*) zugelassen. Für eine leichtere Diagnose im internen Netz können eventuell noch andere ICMP-Nachrichtentypen (beispielsweise Typ 8 und Typ 0: *Echo request* und *Echo reply*) erlaubt werden. Im Beispiel werden für das interne Netz eingehende *Echo requests* und ausgehende *Echo replies* erlaubt: Dies ermöglicht es, den Webserver aus dem internen Netz heraus "anzupingen".

Wichtig ist weiter, dass die ssh-Verbindungen nur zum Webserver hin erfolgen, und nicht von diesem ausgehen. Das gleiche gilt für Verbindungen zum TCP-Port 80, der zum Webserver-Prozess gehört: Es werden eingehende Verbindungen zu diesem Port zugelassen, aber keine ausgehenden Verbindungen. Dies bedeutet, dass prinzipiell keine ausgehenden Verbindungsanfragen (nur das TCP SYN-Flag ist gesetzt) benötigt werden,

sondern dass nur ausgehende TCP-Pakete erlaubt sind, die zu einer bestehenden Verbindung gehören (das TCP ACK-Flag ist gesetzt). Das Sperren ausgehender Verbindungsanfragen dient, wie oben erläutert, dem Zweck, einen Angreifer, der sich beispielsweise über eine Sicherheitslücke im Webserver-Dienst Zugang zum Rechner verschafft hat, zumindest aufzuhalten. Der Angreifer kann diese Sperre zwar deaktivieren, sie bietet aber insbesondere dann einen zusätzlichen Sicherheitsgewinn, wenn sie mit entsprechenden Protokollierungs- und Alarmierungsfunktionen kombiniert wird.

Quell-Adresse:Port	**Ziel-Adresse:Port**	**Protokoll**	**TCP-Flags oder ICMP-Typ**	**Entscheidung**
intern:*	Webserver:22 (ssh)	TCP	SYN oder ACK	Akzeptieren
extern:*	Webserver:22	TCP	alle	Blockieren
Webserver:22	intern:*	TCP	ACK	Akzeptieren
alle:*	Webserver:80 (http)	TCP	SYN oder ACK	Akzeptieren
Webserver:80	alle:*	TCP	ACK	Akzeptieren
alle	Webserver, nicht 22 oder 80	TCP	alle	Blockieren
Webserver:*	alle:*	TCP	ohne ACK	Blockieren
alle	alle	UDP	-	Blockieren
alle	Webserver	ICMP	Typ 3	Akzeptieren
Webserver	alle	ICMP	Typ 3	Akzeptieren
intern	Webserver	ICMP	Typ 8	Akzeptieren
Webserver	intern	ICMP	Typ 0	Akzeptieren
Webserver	alle	ICMP	andere	Blockieren
alle	Webserver	ICMP	andere	Blockieren

Tabelle: Beispielkonfiguration für einen Paketfilter

In der Tabelle steht * für einen beliebigen Port.

Eine noch höhere Sicherheit kann in diesem Beispiel erreicht werden, wenn die internen Adressen, von denen aus ein Zugriff per ssh erlaubt sein soll, weiter eingeschränkt werden. Falls beispielsweise nur zwei Administratoren von ihren beiden Arbeitsplatzrechnern aus zugreifen, dann könnte der Zugriff auf die Adressen dieser beiden Rechner beschränkt werden.

Detailliertere Informationen zu Paketfiltern finden sich im Baustein B 3.301 *Sicherheitsgateway (Firewall)*.

Ergänzende Kontrollfragen:

- Werden als Standardeinstellung alle Verbindungsanfragen von externen Systemen im Netz abgewiesen?
- Sollen alle empfangenen und gesendeten Pakete protokolliert werden oder ist eine Selektion sinnvoll?
- Falls Netzdienste bereitgestellt werden sollen, wie ist eine Beschränkung der Zielgruppe auf Grund von IP-Adressen oder Netzmasken möglich und wie wurde diese implementiert?
- Können Pakete empfangen werden, die als Antwort einer vom lokalen System initiierten Verbringungsanfrage vom Kommunikationspartner gesendet wurden?
- Wurde nach dem Aufsetzen des Regelwerks diese mit einem Portscanner von einem externen System überprüft?

M 4.239 Sicherer Betrieb eines Servers

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der sichere Betrieb eines Servers hängt von einer Reihe von Faktoren ab. Besonders wichtig ist dabei, dass die Administration des Servers mit der gebotenen Sorgfalt auf einem sicheren Zugang erfolgt.

Im Folgenden werden einige allgemeine Punkte beschrieben, die für einen sicheren Betrieb eines Servers beachtet werden sollten. Für einzelne Betriebssysteme werden in entsprechenden Maßnahmen der betreffenden Bausteine spezifischere Hinweise gegeben.

Administrationszugänge

Es gibt unterschiedliche Zugriffsmöglichkeiten um Server zu administrieren. Abhängig von der genutzten Zugriffsart müssen eine Reihe von Sicherheitsvorkehrungen getroffen werden. Bei größeren Netzen ist es empfehlenswert, auch die Server in ein zentrales Netzmanagement-System einzubinden, da sonst eine sichere und effiziente Administration kaum gewährleistet werden kann. Die zur Administration verwendeten Methoden sollten in der Sicherheitsrichtlinie festgelegt werden und die Administration darf nur entsprechend der Sicherheitsrichtlinie durchgeführt werden.

Allgemein ist es wichtig, einen Überblick darüber zu erhalten, welcher Teil der Administration eines Servers normalerweise

- lokal über die Konsole,
- remote über das Netz, aber unter Nutzung der Standardmechanismen des Betriebssystems, oder
- über ein zentrales netzbasiertes Administrationswerkzeug

durchgeführt werden soll. Es wird empfohlen, für die verschiedenen Nutzungsarten eine Übersicht zu erstellen, welche Administrationstätigkeiten auf welchem Weg durchgeführt werden können. Insbesondere ist es wichtig festzuhalten, ob bestimmte Tätigkeiten auf einem bestimmten Weg normalerweise nicht durchgeführt werden dürfen.

- Lokale Administration

  Ein Server sollte prinzipiell in einem Serverraum oder zumindest einem abschließbaren Serverschrank aufgestellt sein. Für den Teil der Administration, der trotzdem teilweise lokal über die Konsole erfolgen soll oder muss, müssen entsprechende Vorgaben dafür gemacht werden, wer Zugang zur Konsole erhält, welche Art der Authentisierung für den lokalen Zugang genutzt werden darf und welche anderen Vorgaben berücksichtigt werden müssen.

- Remote-Administration

  Meist wird ein Server nicht lokal an der Konsole sondern von einem Arbeitsplatzrechner aus über das Netz administriert. Um zu verhindern, dass dabei Authentisierungsinformationen der Administratoren und Konfigurationsdaten der Server abgehört oder gar von einem Angreifer

manipuliert werden, sollte die Administration nur über sichere Protokolle (beispielsweise nicht über Telnet, sondern über SSH, nicht über HTTP, sondern über HTTPS) erfolgen. Alternativ kann ein eigenes Administrationsnetz eingerichtet werden, das vom dem restlichen Netz getrennt ist.

Keine ungesicherte Remote-Administration über externe Netze!

Eine ungesicherte Remote-Administration über externe (unsichere) Netze hinweg darf in keinem Fall erfolgen. Dies muss bereits bei der Festlegung der Sicherheitsrichtlinie berücksichtigt werden. Auch im internen Netz sollten, soweit möglich, keine unsicheren Protokolle verwendet werden.

- Administration über ein zentrales Managementsystem

  Falls für die Administration des Servers ein zentrales Managementsystem genutzt werden soll, so sollten für diesen Zugangsweg analoge Vorüberlegungen angestellt werden, wie für die Remote-Administration. Zusätzlich ist es wichtig, dass das zentrale Managementsystem selbst entsprechend sicher konfiguriert und administriert wird. Entsprechende Hinweise finden sich im Baustein B 4.2 *Netz- und Systemmanagement*.

Routinetätigkeiten bei der Administration

Es wird empfohlen, für die üblichen Routinetätigkeiten der Administratoren entsprechend der Sicherheitsrichtlinie für den Server Hinweise für die Administration zu erstellen. Dies umfasst beispielsweise Tätigkeiten wie

- Anlegen und Löschen von Benutzern,
- Installation und Deinstallation von Programmen,
- Einspielen von Sicherheitsupdates und Patches (siehe auch M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*),
- Einspielen sonstiger Updates und Patches,
- Regelmäßige Überprüfung des Betriebszustandes des Systems (beispielsweise Auslastung des Systems, verbleibender freier Plattenplatz),
- Überprüfung der Logdaten auf ungewöhnliche Einträge (siehe auch M 5.9 *Protokollierung am Server*) und
- Regelmäßiger Integritätscheck mit entsprechenden Tools (siehe auch M 4.93 *Regelmäßige Integritätsprüfung* und M 5.8 *Regelmäßiger Sicherheitscheck des Netzes*).

Tests von Konfigurationsänderungen

Verschiedene Serverprogramme bieten die Möglichkeit, Konfigurationsänderungen vor dem Wirksamwerden zumindest auf technische Korrektheit zu überprüfen. Dies hilft zu vermeiden, dass ein Serverprogramm nach einer fehlerhaften Konfigurationsänderung nicht mehr startet und so zu einem Ausfall des betreffenden Dienstes führt. Sofern solche Möglichkeiten vorhanden sind, sollten die Administratoren mit deren Benutzung vertraut sein und sie auch tatsächlich wahrnehmen.

Dokumentation von Arbeiten am System

Änderungen an der Systemkonfiguration oder an der Konfiguration von Serverprogrammen müssen dokumentiert werden. Die Dokumentation muss so beschaffen sein, dass im Falle von Problemen nachvollziehbar ist, was die letzte Änderung war und wann sie von wem durchgeführt wurde. Dabei ist es wichtig, dass die Dokumentation so beschaffen ist, dass sie nicht nur von den Administratoren selbst nachvollzogen werden kann, sondern notfalls auch von einem "fachkundigen Dritten", der mit dem täglichen Betrieb des betreffenden Systems nichts zu tun hat. Außerdem sollte es anhand der Dokumentation möglich sein, eine frühere Konfiguration zu reproduzieren.

Für Änderungen an textbasierten Konfigurationsdateien bieten sich zu diesem Zweck Revisionsverwaltungssysteme an. Zusätzlich sollte direkt in den Konfigurationsdateien durch kurze Kommentare die Auswirkungen und die Funktionsweise der neuen Konfigurationseinstellungen erläutert werden. Für andere Konfigurationsmechanismen existieren teilweise ähnliche Werkzeuge oder die betreffende Software bietet bereits standardmäßig entsprechende Funktionalitäten an. Wird ein zentrales Administrationssystem genutzt, so sollten entsprechende Funktionen vorhanden sein und auch genutzt werden.

Ergänzende Kontrollfragen:

- Auf welchen Wegen wird zur Administration auf das System zugegriffen?
- Wie werden Konfigurationsänderungen getestet?
- Wie werden Änderungen dokumentiert?

M 4.240 Einrichten einer Testumgebung für einen Server

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Für Server mit hohen Sicherheitsanforderungen sollte eine Testumgebung eingerichtet werden, in der Konfigurationsänderungen, Updates und Patches vor dem Einspielen auf dem Produktionssystem vorab getestet werden können. Dies betrifft sowohl Sicherheitspatches und -updates als auch normale Updates, die vom Hersteller herausgegeben werden.

Funktional äquivalente Testumgebung

Die Testumgebung muss so beschaffen sein, dass sie eine "funktional äquivalente" Installation von Hard- und Software erlaubt. Dies bedeutet nicht notwendigerweise, dass zu einem teuren Serverrechner ein zweites, identisch konfiguriertes System beschafft werden muss. Zum Testen von Konfigurationsänderungen, Updates und Patches von Anwendungsprogrammen und Serversoftware genügt meist ein technisch deutlich sparsamer ausgestattetes System.

Es sollte jedoch auch die Möglichkeit bestehen, neue Gerätetreiber vor dem Einspielen zu testen. Daher kann es gegebenenfalls vorteilhaft sein, für verschiedene Arten von Tests unterschiedliche Testsysteme zu nutzen, etwa ein System für Tests systemnaher Programme oder von Betriebssystempatches und ein anderes für Tests im Zusammenhang mit der eigentlichen Serversoftware. In einem solchen Fall ist es jedoch wichtig sich bewusst zu sein, dass auf diese Weise gewisse Arten von Wechselwirkungen zwischen Betriebssystemumgebung und Serversoftware nicht abgedeckt werden können. Bei besonderen Anforderungen an die Sicherheit und Zuverlässigkeit eines Servers kann es deswegen erforderlich werden, tatsächlich ein zweites, identisch konfiguriertes System als Testumgebung zur Verfügung zu haben.

Checklisten helfen

Für verschiedene typische und häufiger wiederkehrende Testfälle sollten Checklisten erstellt werden, die beim Testen abgearbeitet werden können und die neben der reinen Dokumentation des Tests oft auch zu einer Erhöhung der Effizienz und zur Vermeidung von Fehlern beitragen können.

Dokumentation ist wichtig

Alle Tests sollten so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

Ergänzende Kontrollfragen:

- Werden Konfigurationsänderungen sowie Updates und Patches vorab getestet?
- Wie werden Tests dokumentiert?

M 4.241 Sicherer Betrieb von Clients

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der sichere Betrieb von Clients hängt von einer Reihe von Faktoren ab. Besonders wichtig ist dabei auch bei Clients, dass einerseits die Administration mit der gebotenen Sorgfalt und andererseits über einen sicheren Zugang erfolgt.

Im folgenden werden einige allgemeine Punkte beschrieben, die für einen sicheren Betrieb beachtet werden sollten. Für einzelne Betriebssysteme werden in den entsprechenden Maßnahmen der betreffenden Bausteine spezifischere Hinweise gegeben.

Administrationszugänge

Es gibt unterschiedliche Zugriffsmöglichkeiten, um Clients zu administrieren. Abhängig von der genutzten Zugriffsart müssen eine Reihe von Sicherheitsvorkehrungen getroffen werden. Bei größeren Netzen ist es empfehlenswert und oft unumgänglich, die Clients in ein zentrales Netzmanagement-System einzubinden, da sonst eine sichere und effiziente Administration nicht gewährleistet werden kann. Die zur Administration verwendeten Methoden sollten in der Sicherheitsrichtlinie festgelegt und die Administration nur entsprechend der Sicherheitsrichtlinie durchgeführt werden.

Es wird empfohlen, für die verschiedenen Administrationstätigkeiten eine Übersicht zu erstellen, welche Arbeiten auf welchem Weg durchgeführt werden können. Vor allem ist es wichtig festzuhalten, ob bestimmte Tätigkeiten auf einem bestimmten Weg normalerweise nicht durchgeführt werden dürfen.

- Lokale Administration

  Die Administration von Clients direkt durch Zugriff über die Konsole ist nur für eine kleine Zahl von Rechnern handhabbar und wird in Umgebungen mit einer größeren Anzahl von Clients meist einen Ausnahmefall darstellen. Muss ein Administrator ausnahmsweise doch lokal an einem Client-Rechner arbeiten, ist es beispielsweise wichtig, dass der Administrator bei der Eingabe des Passworts darauf achtet, dass dieses nicht ausgespäht werden kann. Gegebenenfalls sollte überlegt werden, für solche Arbeiten Einmalpasswörter oder ähnliches zu verwenden.

- Administration mit Hilfe eines Bootmediums

  Für bestimmte Administrationsarbeiten, die lokal an einem Client-Rechner vorgenommen werden sollen kann es vorteilhaft sein, ein externes Boot-Medium einzusetzen, von dem der Rechner gestartet wird (siehe auch M 6.24 *Erstellen eines Notfall-Bootmediums*). Dies bietet den Vorteil, dass der Administrator sich einer "sauberen" Systemumgebung sicher sein kann. Allerdings hat diese Methode auch eine Reihe von Nachteilen, beispielsweise einen höheren Aufwand. Außerdem ist es auf diese Weise meist nicht möglich, bestimmte Fehlermeldungen, die im laufenden Betrieb auftreten, nachzuvollziehen.

- Remote-Administration

  Auch Clients werden häufig von einem Administrationsrechner aus über das Netz administriert. Um zu verhindern, dass dabei Authentisierungsinformationen der Administratoren abgehört oder gar von einem Angreifer manipuliert werden, sollte die Administration nur über sichere Protokolle (beispielsweise nicht über Telnet, sondern über SSH, nicht über HTTP, sondern über HTTPS) erfolgen.

  Keine ungesicherte Remote-Administration über externe Netze!

  Eine ungesicherte Remote-Administration über externe (unsichere) Netze hinweg darf in keinem Fall erfolgen. Dies muss bereits bei der Festlegung der Sicherheitsrichtlinie berücksichtigt werden. Auch im internen Netz sollten soweit möglich keine unsicheren Protokolle verwendet werden.

- Administration über ein zentrales Managementsystem

  Falls für die Administration ein zentrales Managementsystem genutzt werden soll, so müssen für diesen Zugangsweg analoge Vorüberlegungen angestellt werden, wie für die Remote-Administration. Zusätzlich ist es wichtig, dass das zentrale Managementsystem selbst entsprechend sicher konfiguriert und administriert wird. Entsprechende Hinweise finden sich im Baustein B 4.2 *Netz- und Systemmanagement*.

Routinetätigkeiten bei der Administration

Es wird empfohlen, für die üblichen Routinetätigkeiten der Administratoren entsprechend der Sicherheitsrichtlinie Hinweise für die Administration zu erstellen. Dies umfasst beispielsweise Tätigkeiten wie

- Anlegen und Löschen von Benutzern,
- Installation und Deinstallation von Programmen,
- Einspielen von Sicherheitsupdates und Patches (siehe auch M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*),
- Einspielen sonstiger Updates und Patches oder
- Regelmäßiger Integritätscheck mit entsprechenden Tools (siehe auch M 4.93 *Regelmäßige Integritätsprüfung* und M 5.8 *Regelmäßiger Sicherheitscheck des Netzes*).

Tests von Konfigurationsänderungen

Konfigurationsänderungen an Clients sollten nach Möglichkeit auf einem Referenzsystem getestet werden, bevor sie auf die einzelnen Rechner verteilt werden (siehe auch M 4.242 *Einrichten einer Referenzinstallation für Clients*). Werden (etwa im Rahmen einer Fehlersuche) Änderungen lokal auf einzelnen Clients durchgeführt, so sollte auf jeden Fall geprüft werden, ob durch die Änderungen die sonstigen Funktionen des Clients nicht beeinträchtigt werden.

Dokumentation von Arbeiten an den Systemen

Änderungen an der Systemkonfiguration der Clients oder an der Konfiguration von Anwendungen müssen dokumentiert werden. Die Dokumentation sollte auch bei Clients idealerweise so beschaffen sein, dass im Falle von Problemen nachvollziehbar ist, was die letzte Änderung war und wann und von wem sie durchgeführt wurde. Bei Clients ohne hohe

Sicherheitsanforderungen kann aber auch die Dokumentation einzelner funktionierender Konfigurationsstände (beispielsweise zu bestimmten Zeitpunkten) ausreichend sein, ohne dass es unbedingt notwendig ist, jeden einzelnen Schritt nachzuvollziehen. Trotzdem wird empfohlen, die Dokumentation so zu gestalten, dass alle Änderungen nachvollziehbar sind.

Ergänzende Kontrollfragen:

- Auf welchen Wegen wird zur Administration auf das System zugegriffen?
- Wie werden Konfigurationsänderungen getestet?
- Wie werden Änderungen dokumentiert?

M 4.242 Einrichten einer Referenzinstallation für Clients

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Es wird empfohlen, für Clients eine Referenzinstallation zu erstellen, in der die Grundkonfiguration und alle Konfigurationsänderungen, Updates und Patches vor dem Einspielen auf den Clients bei den Anwendern vorab getestet werden können. Dies betrifft die Grundeinstellungen des Systems, Sicherheitspatches und -updates und auch normale Updates, die vom Hersteller herausgegeben werden.

Mögliche Effizienzsteigerung bei der Installation

Darüber hinaus kann eine solche Referenzinstallation gegebenenfalls auch dazu genutzt werden, die Installation neuer Clients zu vereinfachen, indem eine entsprechend vorkonfigurierte Installation auf geeignete Art und Weise auf den zu installierenden Rechner überspielt wird ("klonen"). Im Idealfall brauchen anschließend nur noch wenige Einstellungen angepasst zu werden. Eine Referenzinstallation, die zum Klonen von Clients verwendet wird, muss mit besonderer Sorgfalt konfiguriert und getestet werden.

Funktional äquivalente Testumgebung

Die Referenzinstallation muss so beschaffen sein, dass die wesentlichen Parameter der Hard- und Softwareplattform für alle Systeme, die von dieser Referenzinstallation abgeleitet werden, die selben sind. Dies bedeutet nicht notwendigerweise, dass deswegen auf sämtlichen Clients eine identische Hard- und Softwarekonfiguration bestehen muss. Die Konfiguration verschiedener Clients muss aber hinreichend ähnlich sein, damit der Referenzcharakter der Installation erhalten bleibt.

Anwendungsprogramme nicht mit Administrator-rechten testen

Bei Tests von Anwendungsprogrammen und Einstellungen, die die Anwender auf den Clients betreffen, ist es darüber hinaus besonders wichtig, dass die Administratoren diese nicht mit Administratorrechten durchführen, sondern unter einer Benutzerkennung, der die selben Berechtigungen besitzt und für den die selben Einstellungen für die Benutzerumgebung gewählt wurden, wie die Anwender, die mit dem System arbeiten sollen.

Gegebenenfalls kann es vorteilhaft sein, für verschiedene Arten von Tests unterschiedliche Testsysteme zu nutzen, etwa ein oder mehrere Systeme für Tests von Gerätetreibern oder systemnaher Programme und von Betriebssystempatches, und ein anderes für Tests im Zusammenhang mit Anwendungsprogrammen. In einem solchen Fall ist es jedoch wichtig, sich bewusst zu sein, dass auf diese Weise gewisse Arten von Wechselwirkungen zwischen Betriebssystemumgebung und Anwendungsprogrammen nicht abgedeckt werden können. Bei besonderen Anforderungen an die Sicherheit der Clients kann es deswegen erforderlich werden, tatsächlich für bestimmte Einsatzszenarien nur identisch ausgestattete und konfigurierte Systeme einzusetzen.

Checklisten helfen

Für verschiedene typische und häufiger wiederkehrende Testfälle sollten Checklisten erstellt werden, die beim Testen abgearbeitet werden können und die neben der reinen Dokumentation des Tests oft auch zu einer Erhöhung der Effizienz und zur Vermeidung von Fehlern beitragen können.

Dokumentation ist wichtig

Alle Tests sollten so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können. Dies ist insbesondere bei Tests von Sicherheitsupdates und von neuen Gerätetreibern notwendig, bei denen eine fehlerhafte Konfiguration oder ein Fehlschlagen der Installation dazu führen kann, dass die betroffenen Clients keinen Zugang mehr zum Netz erhalten oder gar überhaupt nicht mehr starten. Gerade in solchen Fällen kann eine aussagekräftige Dokumentation die notwendige Zeit für die Fehlersuche und -beseitigung wesentlich verkürzen.

Ergänzende Kontrollfragen:

- Werden Konfigurationsänderungen sowie Updates und Patches vorab getestet?
- Wie werden Tests dokumentiert?

M 4.243 Windows XP Verwaltungswerkzeuge

Verantwortlich für Initiierung: Administrator

Verantwortlich für Umsetzung: Administrator

Das kommandozeilenbasierte Tool *secedit* ist bereits aus Windows 2000 bekannt. Es ermöglicht das Automatisieren von Aufgaben bei der Konfiguration der Sicherheitseinstellungen. Mit diesem Tool können unter anderem Vorlagen automatisch erstellt, angewandt und analysiert werden. Eines seines wichtigsten Merkmale ist die Fähigkeit, einen Abgleich der geltenden Gruppenrichtlinieneinstellungen mit einem Mustersatz zu erstellen. Es sollte beachtet werden, dass ein Teil der *secedit*-Funktionalität unter Windows XP ausgelagert wurde (*gpupdate*).

Die Analyse der aktuell geltenden Einstellungen kann auch mit dem MMC Snap-In *Sicherheitskonfiguration und -analyse* durchgeführt werden. Die Ergebnisse werden im Gegensatz zu *secedit* graphisch aufbereitet und präsentiert. Es ist zu beachten, dass sowohl das *secedit* Tool als auch das MMC Snap-In *Sicherheitskonfiguration- und -analyse* nicht zur Konfiguration und Analyse der in administrativen Vorlagen definierten Parameter verwendet werden können.

Die Bearbeitung von Sicherheitsvorlagen erfolgt unter Windows XP mit dem MMC Snap-In *Sicherheitsvorlagen*. Da die Sicherheitsvorlagen jedoch einfache Textdateien sind, können sie auch mit einem gewöhnlichen Texteditor bearbeitet werden. Dies kann unter anderem für die Spezifizierung zusätzlicher Registry-Schlüssel notwendig sein.

Ändern sich die Einstellungen einer Gruppenrichtlinie, so werden die Konfigurationsänderungen nur mit einer Verzögerung wirksam, die durch die Verarbeitungseinstellungen der Gruppenrichtlinien vorgegeben wird. Um die Änderungen für einen Benutzer oder Computer unverzüglich zu verbreiten, kann das Kommandozeilenwerkzeug *gpupdate* benutzt werden. Dieses Tool ersetzt das von Windows 2000 bekannte Kommando *secedit /refreshpolicy*.

Das Kommandozeilentool *gpresult* kann auf einem Windows XP Client benutzt werden, um das Resultat aller eingerichteten Gruppenrichtlinien aufzulisten. Es dient unter anderem auch dazu herauszufinden, was bei der Anmeldung eines bestimmten Benutzers auf einem bestimmten Computer passiert (*gpresult /s:computername /u:benutzername*). Dieses Werkzeug kann vor allem zur Fehlersuche oder zur Dokumentation der geltenden Einstellungen verwendet werden.

Eine ähnliche Funktionalität wie *gpresult* bietet auch das MMC Snap-in *Richtlinienergebnissatz* (*rsop.msc*). Dieses Tool kann nicht nur zur Dokumentation der aktuell geltenden Einstellungen verwendet werden (Protokollierungsmodus), sondern auch, um mögliche andere Szenarien durchzuspielen (Planungsmodus). Damit lässt sich eine Richtlinienimplementierung simulieren, die vor allem in der Design-Phase immens wichtig ist und vor vielen Implementierungsfehlern, insbesondere bei komplexen Gruppenrichtlinien-Strukturen und -Hierarchien, bewahren kann.

Das von Microsoft frei verfügbare Tool *Group Policy Management Console* (*GPMC*) bietet deutlich bessere Verwaltungsmöglichkeiten für Gruppenrichtlinien im Active Directory als die Standard-Snap-Ins von Windows 2000. Dieses Tool stellt weitergehende Funktionalitäten zur Verfügung, welche für die Verwaltung der Gruppenrichtlinien im Active Directory sehr wichtig sind: das Erstellen, Verlinken und Löschen von GPOs, Importieren der Einstellungen aus gesicherten Gruppenrichtlinienobjekten, Erstellung von GPO-Reports (die unter anderem für Dokumentationszwecke verwendet werden können), Sichern und Wiederherstellen von GPOs. Nicht zuletzt bietet *GPMC* eine Scripting-Schnittstelle, die bei einer Vielzahl administrativer Aufgaben sinnvoll eingesetzt werden kann. Der Einsatz von *GPMC* wird daher in Active Directory Umgebungen dringend empfohlen.

Ein weiteres sinnvolles Tool ist der Migrationstabellen-Editor *mtedit*, das im Lieferumfang des *GPMC* enthalten ist. Dieses Tool ermöglicht eine bequeme Erstellung von Migrationstabellen, die beim domänenübergreifenden Kopieren oder Importieren einer Sicherheitsrichtlinie verwendet werden können. Durch die Verwendung von Migrationstabellen lassen sich domänenspezifische Informationen modifizieren (z. B. Gruppennamen oder SIDs).

Microsoft stellt mit dem Baseline Security Analyzer (MBSA) ein Tool zur Verfügung, das für die automatische Auswertung der Patch-Stände eingesetzt werden kann. Der Einsatz dieses Tools verschafft den Administratoren einen aktuellen Überblick über den Patch-Stand der Systeme und trägt somit wesentlich zur Gesamtsicherheit bei (siehe auch M 4.249 *Windows XP Systeme aktuell halten*).

Alle diese Werkzeuge sollten unbedingt von Administratoren bei der Fehlersuche oder während der Design- und Test-Phasen eingesetzt werden. Die Verwendung dieser Tools hilft, Konfigurationsschwächen zu entdecken und zu vermeiden.

Ergänzende Kontrollfragen:

- Werden die Werkzeuge entsprechend den Anforderungen in der Planungsphase bzw. im Betrieb eingesetzt?

M 4.244 Sichere Windows XP Systemkonfiguration

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Sicherheit eines Arbeitsplatzrechners hängt im Wesentlichen davon ab, ob ein Benutzer administrativ auf den Rechner einwirken kann, welche Funktionen den Benutzern verfügbar gemacht werden und ob die Benutzer die ihnen zur Verfügung gestellten Sicherheitsmechanismen korrekt nutzen.

Bei der Konfiguration von Windows XP sind folgende Aspekte aus Sicherheitssicht zu berücksichtigen:

- Die entsprechenden Überwachungsrichtlinien (siehe M 4.148 *Überwachung eines Windows 2000/XP Systems*) müssen definiert sein. Die gesammelten Protokollierungsdaten müssen auch regelmäßig ausgewertet werden.
- Beim Einsatz in einer Active-Directory-basierten Umgebung sollten die Rechte zum Hinzufügen von Arbeitsstationen zur Domäne eingeschränkt werden. Ausschließlich berechtigte administrative Benutzer dürfen diese Zuständigkeit besitzen. Die Einschränkung des entsprechenden Rechts erfolgt über die entsprechende Richtlinie (*Zuweisen von Benutzerrechten* | *Hinzufügen von Arbeitsstationen zur Domäne*) auf Domain Controllern.
- Beim Einsatz eines Windows XP Systems als mobiler Rechner entstehen zusätzliche Sicherheitsrisiken, die durch besondere Vorkehrungen gemindert werden sollten (siehe dazu Maßname M 2.328 *Einsatz von Windows XP auf mobilen Rechnern,* sowie den Baustein B 3.203 *Laptop*).

Datenhaltung und Verarbeitung

Es empfiehlt sich, bei vernetzten Clients keine lokalen Daten auf Arbeitsplatzrechnern zu halten. Dies erleichtert die zentrale Administartion und Steuerung von Sicherheitsvorgaben, ebenso wie die Datensicherung. Daneben ergibt sich der Sicherheitsvorteil, dass bei Kompromittierung des Systems lokal keine sensitiven Daten vorzufinden sind, da sie auf einem Server befinden, der in der Regel besser als ein Client-Rechner geschützt ist. In Einzelfällen kann es notwendig sein, dass Daten aus Sicherheitsgründen lokal auf dem Arbeitsplatz gespeichert werden müssen, wenn z. B. nur der Arbeitsplatzbenutzer darauf zugreifen darf und/oder eine Übertragung über das Netz nicht erfolgen soll. Dann ist der Arbeitsplatz jedoch nicht als Standardarbeitsplatz anzusehen, so dass besondere Regelungen für solche Arbeitsplätze geplant und umgesetzt werden müssen. Beispiele für entsprechende Maßnahmen sind eine starke Absicherung der Clients sowohl lokal als auch im Netz, eine Festplattenverschlüsselung und die Einbindung in der Clients in ein zentrales Backup-Konzept.

Vertrauliche Daten müssen sicher verarbeitet werden. Nicht nur der direkte Zugriff auf die Daten muss entsprechend dem Berechtigungskonzept eingeschränkt sein, es muss auch dafür Sorge getragen werden, dass kein unautorisierter Zugriff auf die temporären Inhalte möglich ist. Viele Anwendungen (unter anderem auch Microsoft Office) erstellen bei der Verarbeitung temporäre Dateien, die im Gegensatz zu Originaldaten möglicherweise nicht ausreichend geschützt sind. Daher ist die Bereinigung von Verzeichnissen, in denen temporäre Dateien abgelegt werden (z. B. *Temp*, *Tmp* und das Drucker-Spool-Verzeichnis), sehr empfehlenswert. Dies kann unter anderem auch mit einem Skript realisiert werden, das beim Herunterfahren des Systems ausgeführt wird (siehe M 2.326 *Planung der Windows XP Gruppenrichtlinien*). Das Löschen der Auslagerungsdatei beim Herunterfahren des Systems wird durch die Richtlinie *Auslagerungsdatei des virtuellen Arbeitsspeichers beim Herunterfahren des Systems löschen* in Gruppenrichtlinienobjekten unter *Computerkonfiguration* | *Windows Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* aktiviert.

Softwareeinschränkungen

Durch die gezielte Systemkonfiguration soll vermieden werden, dass normale Benutzer administrative Tätigkeiten ausführen können. Dies kann durch die Zugriffsrechte auf Dateien und die Registry, Berechtigung zum Starten der Konfigurationswerkzeuge, wie z. B. der MMC-Konsole erreicht werden. Diese Einstellungen werden über Gruppenrichtlinien verwaltet und sollten schon in die Planung der Gruppenrichtlinien einfließen (siehe M 2.326 *Planung der Windows XP Gruppenrichtlinien*). Der Einsatz von Richtlinien für Softwareeinschränkungen (englisch Software Restriction Policies, SRP) kann in dieser Hinsicht zusätzliche Sicherheit bringen.

Software-Installationen sind ausschließlich von berechtigten Administratoren durchzuführen. Die Installationsmöglichkeiten für normale Benutzer sind daher soweit wie möglich einzuschränken (siehe auch M 2.9 *Nutzungsverbot nicht freigegebener Hard- und Software*). Die Installationen, die mittels des Windows Installers durchgeführt werden, lassen sich durch die Definition geeigneter Gruppenrichtlinien unter *Computerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Windows Installer* einschränken. Ob und in welchem Umfang Installationen eingeschränkt werden sollten, hängt von der Software-Installationsrichtlinie eines Unternehmens bzw. einer Behörde ab. Es sollte bedacht werden, dass diese Einstellungen nur den Windows Installer betreffen und nicht verhindern können, dass Benutzer anderweitig Programme installieren oder aktualisieren können.

Die mit Windows XP eingeführte Technologie der Softwareeinschränkungen ermöglicht es, die auf einem Computer ausführbaren Programme zu begrenzen. Durch die Definition spezieller Regeln in Softwareeinschränkungen-Richtlinien im Computerteil einer GPO (*Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Richtlinien für Softwareeinschränkungen*) wird entweder die Menge der erlaubten (Positivliste) oder der verbotenen Programme (Negativliste) spezifiziert. Bei der Definition einer Positivliste sollten nicht nur die Anwendungen, sondern auch alle für den Regelbetrieb benötigten Systemprogramme erlaubt sein.

Programme können in einer Regel durch einen voll- oder teilqualifizierten Pfad-Namen, einen Hashwert, eine digitale Signatur bzw. Zertifikat oder die Programmzone (beispielsweise *Internet*, *Lokaler Rechner*) identifiziert werden. Eine Regel ist nicht nur auf gewöhnliche ausführbare Dateien, sondern unter anderem auch auf DLLs, ActiveX Steuerelemente, Windows Installer Dateien sowie auf VBScript Dateien anwendbar.

Die zur Verfügung stehenden Konfigurationsmöglichkeiten für Ausführungsbeschränkungen mittels SRP sind sehr variabel und ermöglichen die Realisierung einer Vielzahl von Einsatzszenarien. Dieser Vorteil wird jedoch mit einem entsprechenden Administrationsaufwand erkauft, da die definierten Regeln schnell komplex und unübersichtlich werden. Umfangreiche Planung und ausgiebiges Testen sind unabdingbar, wenn ein Unternehmen bzw. eine Behörde Richtlinien zur Softwareeinschränkungen implementieren möchte.

Dienste

Windows XP ist kein Server-Betriebssystem und sollte daher nur für Clients verwendet werden. Windows XP Clients sollten keine Anwendungen oder Dienste im Netz zur Verfügung stellen. Mehr dazu findet sich in M 2.67 *Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste* und M 5.37 *Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz*. Unter anderem sollten die normalen Arbeitsplatzrechner neben den administrativen Standardfreigaben keine Verzeichnisfreigaben zur Verfügung stellen. Auch die administrativen Freigaben sollten deaktiviert werden, wenn sie nicht zur Administration verwendet werden (*HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks*=0). Sind jedoch aus bestimmten Gründen Freigaben auf den Clients erforderlich, so darf in diesem Fall der Mechanismus der einfachen Dateifreigabe nicht benutzt werden, um die hiermit verbundenen Sicherheitsrisiken zu vermeiden. Mit Windows XP wurde auch das Konzept der "einfachen Dateifreigabe" eingeführt. Ist die einfache Dateifreigabe auf einem Rechner aktiviert, so werden alle Benutzer, die über das Netz auf diesen Computer zugreifen, dem Gastkonto zugeordnet. Die entsprechenden Berechtigungen für den Zugriff auf die Freigabe müssen jedoch sehr restriktiv vergeben werden. Es ist zu beachten, dass die einfache Freigabe standardmäßig nur auf Einzelrechnern aktiviert wird, die keiner Domäne angehören (auf Rechnern, die als Domänenmitglieder installiert wurden, ist die einfache Dateifreigabe standardmäßig deaktiviert).

Die Gesamtsicherheit eines Systems hängt auch von eingesetzten Systemdiensten ab. Hinweise zu sicheren Dienstkonfiguration können in Maßnahme M 4.246 *Konfiguration der Systemdienste unter Windows XP*, gefunden werden.

Benutzerkonten

Windows XP Benutzerkonten dürfen nur von einer dazu berechtigten Person verwendet werden, d. h. das Benutzerkonto ist einem Benutzer eindeutig zuzuordnen. Dies hat vor allem aus Gründen der Nachvollziehbarkeit zu erfolgen. Sammelkonten sollten nach Möglichkeit keine Verwendung finden. Dies ist auf organisatorischer Ebene zu gewährleisten.

Erfolgt das Anlegen eines neuen Benutzerkontos im Active Directory, so ist auf die richtige Zuordnung zu einer Organisationseinheit zu achten, da hierüber die korrekten Sicherheitseinstellungen für dieses Benutzerkonto festgelegt werden. Die an einen Benutzer vergebenen Rechte resultieren neben den Gruppenmitgliedschaften unter anderem aus den Gruppenrichtlinien, die an die Organisationseinheit des Benutzers gelinkt sind.

Erfolgt die Administration des Windows XP Systems über personalisierte Benutzerkonten, so kann das integrierte Administratorkonto gesperrt werden. In jedem Fall sollte das Administratorkonto umbenannt werden. Das Deaktivieren und/oder Umbenennen des integrierten Benutzerkontos kann in der Benutzerverwaltung oder durch die Richtlinien der *Konten: Administratorkontostatus* und *Konten: Administrator umbenennen* (unter *Computereinstellungen* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen*) erfolgen. Vor dem Deaktivieren des Administratorkontos ist eine Testphase empfehlenswert, in der ausschließlich über die personalisierten Benutzerkonten administriert wird.

Wie alle anderen Windows Versionen enthält auch Windows XP standardmäßig ein Gastkonto, das deaktiviert ist. Das Gastkonto soll nicht genutzt werden, Benutzer sollten immer ein dediziertes Konto verwenden. Das Gastkonto ist zu deaktivieren, wobei trotzdem ein komplexes Kennwort für das Konto vergeben werden sollte. In diesem Fall besteht auch im Falle eines zufälligen oder unberechtigten Aktivierungsversuchs des Kontos ein Kennwortschutz. Um das Gastkonto umzubenennen und zu deaktivieren, können entweder die lokale Benutzerverwaltung oder die Richtlinien *Konten: Gastkontenstatus* und *Konten: Gastkonto umbenennen* (unter *Computereinstellungen* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen*) verwendet werden.

Das unter Windows XP standardmäßig angelegte Konto für den Support-Benutzer (*SUPPORT_388945a0*) wird normalerweise in Behörden- und Unternehmensumgebung nicht verwendet und sollte daher gelöscht werden. Zum Löschen dieses Kontos dient die lokale Benutzerverwaltung.

Beim Betrieb eines Windows XP Systems in der Domäne sollten nach Möglichkeit keine weiteren lokalen Benutzerkonten angelegt werden. Generell sollten lokal nur die unbedingt notwendigen Konten angelegt sein. Eine Überprüfung lokaler Benutzerkonten hat in regelmäßigen Abständen zu erfolgen.

Entsprechend der Maßnahme M 4.2 *Bildschirmsperre* muss für jeden Benutzer der Kennwortschutz für den Bildschirmschoner aktiviert werden. Ist der Standby-Modus möglich, so muss die Kennworteingabe auch beim Reaktivieren des Systems aus dem Standby-Modus erforderlich sein (*Energieoptionen* | *Erweitert* | *Kennwort beim Reaktivieren aus dem Standbymodus anfordern*).

Die Anforderungen in Maßnahmen M 2.11 *Regelung des Passwortgebrauchs* und M 4.15 *Gesichertes Login* müssen umgesetzt werden. Dies betrifft vor allem die Länge, Qualität sowie Änderungsintervalle der Kennwörter sowie die Anzahl der Fehlversuche und das Sperren der Benutzerkonten.

Anmeldung absichern

Der Systemzugang muss auf autorisierte Personen beschränkt sein. Die Vergabe entsprechender Benutzerrechte hat dementsprechend restriktiv zu erfolgen (siehe auch die Maßnahme M 4.247 *Restriktive Berechtigungsvergabe unter Windows XP*). Administrative Zugriffe vom Netz sollten grundsätzlich nur berechtigten administrativen Personal erlaubt werden. Des weiteren muss die Anmeldung über das Netz an lokalen Benutzerkonten ohne Kennwort untersagt werden. Dies wird durch das Aktivieren der Richtlinie *Konten: Lokale Kontenverwendung von leeren Kennwörtern auf Konsolenanmeldung beschränken* (unter *Computereinstellungen* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen*) erreicht.

Die automatische Benutzeranmeldung muss auf allen Windows XP deaktiviert sein. Ein automatischer Login in der Wiederherstellungskonsole darf ebenfalls nicht gestattet werden. Administrative Benutzer müssen sich explizit authentisieren. Der Zugriff auf Daten außerhalb der Systemverzeichnisse sollte in der Wiederherstellungskonsole eingeschränkt werden. Anderenfalls können unautorisierte Datenzugriffe stattfinden, die zudem nicht einmal protokolliert werden können. Um dies zu erreichen, sind Richtlinien *Wiederherstellungskonsole: Automatische administrative Anmeldungen zulassen* und *Wiederherstellungskonsole: Kopieren von Disketten und Zugriff auf alle Laufwerke und alle Ordner zulassen* (unter *Computereinstellungen* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen*) zu deaktivieren.

Alle Benutzer müssen explizit authentisiert werden, bevor ihnen der Zugang zum System gewährt wird. Die Tastenkombination STRG+ALT+ENTF sollte bei der Anmeldung erzwungen werden (Richtlinie *Computereinstellungen* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Interaktive Anmeldung: Kein STRG+ALT+ENTF erforderlich*). Dies gewährleistet, dass tatsächlich das originale Anmeldefenster und kein "Nachbau" benutzt wird. Außerdem sollte der Name des zuletzt angemeldeten Benutzers in der Anmeldemaske nicht angezeigt werden (Richtlinie *Computereinstellungen* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen*).

Es wird weiterhin empfohlen, allen Benutzern, die sich lokal anzumelden versuchen, eine Warnmeldung anzuzeigen. Der genaue Text der Warnmeldung ist anhand der konkreten Umstände und im Einzelfall festzulegen. Der Text der Warnmeldung und der Nachrichtentitel werden mit Hilfe der Richtlinien *Interaktive Anmeldung: Nachricht für Benutzer, die sich anmelden wollen* und *Interaktive Anmeldung: Nachrichtentitel für Benutzer, die sich anmelden wollen* unter *Computereinstellungen* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* eingerichtet.

Anmeldeinformationen für Domänenkonten werden standardmäßig zwischengespeichert, so dass ein Benutzer sich an seinen Client auch bei Nichtverfügbarkeit des Domain Controllers anmelden kann. Die Anzahl solcher zwischengespeicherten Kontoinformationen wird in der Richtlinie *Computereinstellungen* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Interaktive Anmeldung: Anzahl zwischenzuspeichernder vorheriger Anmeldungen* festgelegt und sollte nach Möglichkeit minimiert werden. Die Parametereinstellung ist anhand konkreter Umstände und im Einzelfall festzulegen.

Systemeinstellungen

Die Autoplay-Funktionalität ist in der Standardinstallation von Windows XP nicht deaktiviert und stellt ein Sicherheitsrisiko dar, da gefährliche Inhalte ohne Benutzerinteraktion zur Ausführung kommen können. Aus diesem Grund ist die Autoplay-Funktionalität für alle Laufwerke zu deaktivieren (siehe auch Maßnahme M 4.57 *Deaktivieren der automatischen CD-ROM-Erkennung*). Hierfür muss die Richtlinie *Computerkonfiguration* | *Administrative Vorlagen* | *System* | *Autoplay deaktivieren* aktiviert und der Wert *Alle Laufwerke* eingestellt werden.

Interne Systemobjekte (wie z. B. Mutexe und Semaphore, die zur Synchronisation unterschiedlicher Threads und Prozesse dienen) besitzen eigene Zugriffsrechte. Diese Zugriffsrechte können durch die Definition einer speziellen Richtlinie verstärkt werden, so dass nicht-administrative Benutzer keine Änderungsrechte an Objekten haben, die nicht von ihnen erstellt wurden (*Computereinstellungen* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Systemobjekte: Standardberechtigungen interner Systemobjekte (z. B. symbolischer Verknüpfungen) verstärken*.

Normalerweise erlaubt Windows XP sowohl lokalen als auch entfernten Zugriff auf Disketten und CD-ROMs. Wie in der Maßname M 4.52 *Geräteschutz unter Windows NT/2000/XP* empfohlen wird, sollte der Zugriff jedoch auf den gerade eingeloggten Benutzer beschränkt werden.

Selbständige Windows XP Internetkommunikation unterbinden

Mehrere Windows XP Dienste und Anwendungen nehmen in der Standardkonfiguration selbsttätig und vom Benutzer unbemerkt Kontakt zu Servern im Internet auf. Dabei werden system- und/oder benutzerspezifische Daten an Microsoft oder andere Anbieter übermittelt.

Die nachfolgende Liste gibt einen Überblick über Dienste und Anwendungen, die selbsttätig Daten an Microsoft übertragen. Diese Liste erhebt keinen Anspruch auf Vollständigkeit (weitere Informationen können im Dokument *Microsoft Windows XP Professional sicher konfigurieren, http://www.microsoft.com/austria/technet/articles/windowsxp_konfig.mspx* gefunden werden).

- Internet Explorer
- Windows Media Player
- Windows Messenger
- Windows Zeitdienst
- Hilfe- und Supportcenter
- Windows Update
- Gerätemanager
- Windows Aktivierung und Registrierung
- Aktualisierung der Stammzertifikate
- Ereignisanzeige
- Webdienst Assoziation
- Fehlerberichterstattung

Für die meisten der oben aufgeführten Dienste und Anwendungen wird das Abschalten der Datenübertragung empfohlen. Dies kann durch entsprechendes Umkonfigurieren von Registry und Programmoptionen sowie Änderungen im Dateisystem erfolgen. Nach Einführung von Service Pack 2 wurde die Verwaltbarkeit dieser Funktionalitäten deutlich verbessert. Eine neue Kategorie der Gruppenrichtlinien wurde unter *Computerkonfiguration* | *Administrative Vorlagen* | *System* | *Internetkommunikationsverwaltung* eingeführt.

Basiseinstellungen für GPOs

Die Basiseinstellungen für Windows XP Gruppenrichtlinienobjekte sind in der Maßnahme M 4.245 *Basiseinstellungen für Windows XP GPOs* beschrieben.

Ergänzende Kontrollfragen:

- Wie wird die Sicherheit und Vertraulichkeit der lokal verarbeiteten Daten gewährleistet?
- Wie ist der Umgang mit lokalen Benutzerkonten geregelt?
- Wie werden Softwareeinschränkungen technisch und organisatorisch umgesetzt?
- Wurde eine entsprechende Warnmeldung für Benutzer konfiguriert, die sich lokal anzumelden versuchen?
- Ist sichergestellt, dass nur autorisierte Benutzer einen Rechner in die Domäne aufnehmen dürfen?
- Wird die selbstständige Kommunikation von Windows XP Diensten und Anwendungen unterbunden?

M 4.245 Basiseinstellungen für Windows XP GPOs

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Unter den Hilfsmitteln des IT-Grundschutzes befinden sich Vorgaben für die Sicherheitseinstellungen in Tabellenform. Diese können als Ausgangsbasis für die Sicherheitseinstellungen innerhalb einer Gruppenrichtlinie dienen. Die vorgeschlagenen Werte resultieren unter anderem aus Anforderungen in den Maßnahmen M 4.244 *Sichere Windows XP Systemkonfiguration* und M 5.123 *Absicherung der Netzwerkkommunikation unter Windows XP*. Die Vorgaben für die Berechtigungsvergabe sind in der Maßnahme M 4.247 *Restriktive Berechtigungsvergabe unter Windows XP* und in den Hilfsmitteln des IT-Grundschutzes zu finden.

Die angegebenen Werte müssen auf jeden Fall an die lokalen Bedingungen angepasst werden. Im Rahmen des Gruppenrichtlinienkonzeptes sind die einzelnen Werte zudem auf unterschiedliche Gruppenrichtlinienobjekte zu verteilen und jeweils an den Verwendungszweck anzupassen. Dadurch können für einzelne Einträge auch jeweils unterschiedliche Werte zustande kommen.

Werden die angegebenen Basiseinstellungen angepasst und insbesondere abgeschwächt, so sind mögliche sicherheitsrelevante Auswirkungen zu untersuchen, die aus diesen Änderungen resultieren.

Ergänzende Kontrollfragen:

- Wurden die Basiseinstellungen an eigene Anforderungen angepasst?
- Wurden mögliche sicherheitsrelevante Auswirkungen untersucht, die sich aus dem Abschwächen der Basiseinstellungen ergeben?

M 4.246 Konfiguration der Systemdienste unter Windows XP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die sichere Konfiguration einzelner Systemdienste, die auf einem Rechner ausgeführt werden, trägt wesentlich zur Gesamtsicherheit eines Systems bei. Jeder nicht benötigte, aber aktivierte Dienst kann eine Gefahrquelle sein. Daher muss bei der Konfiguration von Windows XP Systemen darauf geachtet werden, dass ausschließlich benötigte Dienste zur Ausführung kommen. Um eine zentralisierte Konfiguration der Dienste zu ermöglichen, wird in einer Active Directory Umgebung der Einsatz entsprechender Gruppenrichtlinien empfohlen. Dafür werden einzelne Dienste im Computerteil eines Gruppenrichtlinienobjektes unter *Computereinstellungen* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Systemdienste* aktiviert oder deaktiviert.

Unter den Hilfsmitteln zum IT-Grundschutz werden Vorgaben für die Konfiguration der Systemdienste aufgezeigt, die als Ausgangsbasis für die Sicherheitseinstellungen dienen können. Es sei darauf hingewiesen, dass die Konfiguration einzelner Systemdienste immer von lokalen Gegebenheiten oder Anforderungen abhängt und daher immer in diesem spezifischen Kontext zu sehen ist. Im Einzelfall muss gegebenenfalls sogar aufgrund lokaler Gegebenheiten auf weniger sichere Konfigurationen ausgewichen werden. Dann sollten aber zusätzliche Schutzmaßnahmen eingeleitet werden, die die fehlende Sicherheit in der Dienstkonfiguration ausgleichen. Beispiele hierfür sind der Einsatz einer zusätzlichen Firewall oder auch organisatorische Maßnahmen.

Ergänzende Kontrollfragen:

- Wurde eine Bedarfsanalyse bezüglich der erforderlichen Systemdienste durchgeführt?
- Sind alle nichtbenötigten Dienste deaktiviert?
- Wurden verschiedene Client-Ausprägungen beim Festlegen der auszuführenden Systemdienste und der Definition entsprechender GPOs berücksichtigt?

M 4.247 Restriktive Berechtigungsvergabe unter Windows XP

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Insgesamt können unter Windows XP Berechtigungen in folgenden Bereichen vergeben werden:
- Dateisystem,
- Registrierung,
- Systemberechtigungen bzw. Benutzerberechtigungen,
- Berechtigungen für den Zugriff auf die Freigaben.

Alle Berechtigungen sind grundsätzlich restriktiv zu vergeben, d. h. die sog. Need-to-know- bzw. Least-Privilege-Strategien müssen umgesetzt werden (siehe auch M 4.149 *Datei- und Freigabeberechtigungen unter Windows 2000/XP*). Dies betrifft ausnahmslos alle Bereiche, in denen Berechtigungen vergeben werden können. Das im Vorfeld der Windows XP Einführung spezifizierte Berechtigungskonzept (siehe M 2.325 *Planung der Windows XP Sicherheitsrichtlinie*) muss umgesetzt werden.

Im Allgemeinen wird empfohlen, die Vergabe von Berechtigungen an einzelne Benutzer zu vermeiden, da dies zu komplexen und unübersichtlichen Strukturen führt, die gegen eine Fehlkonfiguration anfällig sind. Die Zuweisung der Berechtigungen sollte nach Möglichkeit ausschließlich auf Gruppenbasis erfolgen. Auf diese Weise müssen die meisten Berechtigungen nur einmal vergeben werden, die Konfiguration im Betrieb erfolgt über die Gruppenzugehörigkeit.

Weiterhin wird empfohlen, dedizierte Gruppen für einzelne Anwendungen zu definieren. Entsprechend sind die Zugriffsberechtigungen auf Software und Daten im Dateisystem und in der Registrierung zu vergeben.

Sind die Benutzer für Berechtigungsvergabe z. B. auf eigenen oder Projektdateien zuständig, so müssen sie entsprechend geschult werden. Anderenfalls können unsichere Dateizugriffsrechte unter Umständen zur Kompromittierung eines Einzelsystems oder im schlimmsten Fall zur Kompromittierung des gesamten Netzes führen.

Nach der Installation und insbesondere nach einem Upgrade oder einer größeren Systemänderung (z. B. dem Einspielen eines neuen Service Packs) ist die Korrektheit der vergebenen Berechtigungen zu verifizieren.

Eine Berechtigungsvergabe an die eingebaute Benutzergruppe *Jeder* (insbesondere *Vollzugriff*, *Schreiben/Ändern* Rechte) sollte grundsätzlich vermieden werden. Soll der Zugriff für alle Benutzer möglich sein, empfiehlt sich stattdessen die Verwendung der ebenfalls eingebauten Gruppe *Authentifizierte Benutzer*.

Unter Windows XP werden in den Standardeinstellungen restriktivere Berechtigungen vergeben als es unter Windows 2000 der Fall war. Dennoch sind weitere Verbesserungen möglich. Die nachfolgenden Basiseinstellungen sind anhand konkreter Umstände und im Einzelfall anzupassen.

Basiseinstellungen Benutzerrechte/Systemberechtigungen

Eine Beispieltabelle mit den lokalen Richtlinien und der Zuweisung von Benutzerrechten findet sich in den Hilfsmitteln zum IT-Grundschutz.

Diese Vorgaben zeigen Sicherheitseinstellungen auf, die als Ausgangsbasis für die Sicherheitseinstellungen in der Windows XP Umgebung eines Unternehmens bzw. einer Behörde dienen können. Diese sollten vor dem Einsatz gegebenenfalls angepasst werden.

Basiseinstellungen Dateisystem und Registrierung

Die notwendigen Einschränkungen der Zugriffsrechte sind anhand der konkreten Umstände und im Einzelfall festzulegen, so dass an dieser Stelle keine allgemein gültigen Empfehlungen möglich sind. Dabei sind nicht nur systemspezifische, sondern auch anwendungsspezifische Verzeichnisse und Dateien zu identifizieren, die einem besonderen Schutzbedarf unterliegen. Um unautorisierten Zugriff zu verhindern, müssen die Zugriffsrechte dann geeignet eingeschränkt werden. Die Einschränkungen der Zugriffsrechte können mit Hilfe der Gruppenrichtlinien definiert und verteilt werden.

Eine Beispieltabelle mit den lokalen Richtlinien und der Zuweisung von Benutzerrechten findet sich in den Hilfsmitteln zum IT-Grundschutz. Diese Vorgaben zeigen Sicherheitseinstellungen für die Registrierung sowie Systemverzeichnisse und -dateien auf, die als Ausgangsbasis für die Sicherheitseinstellungen in der Windows XP Umgebung eines Unternehmens bzw. einer Behörde dienen können. Diese Einstellungen können bei Bedarf an die lokalen Gegebenheiten angepasst und erweitert werden. Die vorgeschlagenen Vorgaben basieren auf folgenden Dokumenten:

- NSA Guide to securing Microsoft Windows XP (*http://www.nsa.gov/snac/downloads_all.cfm*),
- Microsoft Windows XP security guide (*http://go.microsoft.com/fwlink/?LinkId=14840*).

In diesen Dokumenten können auch weitere Informationen zu einzelnen Sicherheitseinstellungen gefunden werden.

Tabellen zu

- Zugriffsrechte für Systemverzeichnisse und -dateien, sowie
- Zugriffsrechte Registrierung

finden sich unter den Hilfsmitteln zum IT-Grundschutz.

In den Tabellen werden folgende Methoden verwendet:

- Propagieren: Die Zugriffsrechte werden zusätzlich zu existierenden vererbt, sofern anwendbar.
- Ersetzen: Die Zugriffsrechte werden ersetzt, sofern anwendbar.
- Ignorieren: Die bestehenden Zugriffsrechte sollen nicht ersetzt werden.

Ergänzende Kontrollfragen:

- Wurde ein entsprechendes Berechtigungskonzept definiert und umgesetzt?
- Werden die Berechtigungen auf Gruppenbasis vergeben?
- Wird die Korrektheit der vergebenen Berechtigungen regelmäßig kontrolliert?
- Wurden Benutzer in Sachen sicherer Berechtigungsvergabe geschult, wenn sie für Berechtigungsvergabe zuständig sind (z. B. auf eigenen oder Projektdateien)?

M 4.248 Sichere Installation von Windows XP

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Während der Installationsphase ist ein Windows XP System nicht vollständig konfiguriert (siehe Planungsmaßnahmen), so dass auch die gewünschten Sicherheitseinstellungen noch nicht aktiviert sind. Die Installation und die initiale Konfiguration eines Windows XP Systems sollte daher nach Möglichkeit in einer geschützten Umgebung erfolgen. Wo dies nicht möglich ist, beispielsweise bei der Vor-Ort-Installation von Arbeitsplatzrechnern (lokal oder über das Netz), sollte alternativ eine vorbereitete (und vorkonfigurierte) Standardkonfiguration aufgespielt werden (Imaging). Vor allem sollte ein Windows XP System komplett aktualisiert sein, bevor es produktiv geht, insbesondere bevor es sich mit dem Internet verbinden darf.

Wird ein Windows XP System außerhalb einer Active Directory-basierten Umgebung betrieben, muss die Konfiguration der Gruppenrichtlinien, die auch die Sicherheitseinstellungen enthalten, lokal auf dem Rechner erfolgen. Dies kann manuell oder skriptbasiert erfolgen. Wie genau die Einstellungen vorgenommen werden, ist in der Planungsphase zu entscheiden.

Der Mechanismus der Gruppenrichtlinien ermöglicht eine schnellere initiale Konfiguration, wenn der Rechner in die Domäne aufgenommen wird. Nach dem Beitritt zur Domäne muss das Rechner-Objekt in die entsprechende Organisationseinheit im Active Directory verschoben werden. Bleibt der Rechner im standardmäßig zugewiesenen AD-Container *Computer*, werden ausschließlich Standort- und Domänen-GPOs aber keine OU-GPOs angewandt, da an diesen AD-Container keine OU-Gruppenrichtlinienobjekte angehängt werden können. Es ist auch darauf zu achten, dass der Rechner nach dem Verschieben in eine neue OU neu gestartet wird. Auf diese Weise werden an diese OU gelinkte GPOs auf den Rechner geladen und angewandt.

Nach der erfolgten Installation sollte sichergestellt werden, dass die entsprechenden Sicherheitseinstellungen auch tatsächlich angewandt worden sind. Dabei sind installierte Komponenten, angewandte Richtlinien, Berechtigungen im Dateisystem und Registrierung, zugewiesene Benutzerrechte und erlaubte Systemdienste zu überprüfen.

Domänenmitgliedschaft

Beim Hinzufügen eines Rechners zu einer Domäne muss entweder ein entsprechendes Computerkonto in der Domäne vorbereitet werden oder das Computerkonto wird beim Beitritt erzeugt. Dazu sind dann entsprechende administrative Berechtigungen notwendig, mit denen restriktiv umgegangen werden muss. Ob das Computerkonto vor oder während der Installation erstellt werden soll, ist in Abhängigkeit von der gängigen Praxis des Unternehmens bzw. der Behörde zu entscheiden.

Zukünftige Domänenmitglieder sollten direkt während der Installation in die Domäne aufgenommen und nicht erst als Einzelrechner installiert werden. Dadurch wird beispielsweise gewährleistet, dass die einfache Dateifreigabe deaktiviert bleibt und keine zusätzlichen lokalen Benutzer mit administrativen Berechtigungen angelegt werden.

Unbeaufsichtigte Installationen

Windows XP bietet einen Mechanismus zur unbeaufsichtigten Installation des Betriebssystems an (d. h. unter Verwendung einer vorgefertigten Antwortdatei und ohne Interaktion mit dem Administrator, der die Installation durchführt). Dabei wird im Vorfeld einer Installation eine sog. Antwortdatei mit dem Installations-Manager *Setup Manager* erstellt, die die notwendigen Installationseingaben beinhaltet.

Werden Windows XP Systeme unbeaufsichtigt installiert, so ist Folgendes zu berücksichtigen:

- Sensitive Informationen wie Kennwörter in Antwortdateien müssen vor unberechtigter Einsichtnahme geschützt sein. So sind die verwendeten Kennwörter beim Erstellen der Antwortdatei mit dem Installations-Manager *Setup Manager* zu verschlüsseln.
- Der Umgang mit Kennwörtern für die Aufnahme in die Domäne, die in einem Installationsskript oder einer Antwortdatei verwendet werden, muss definiert werden.
- Das Administrator-Kennwort darf nicht leer sein, da sonst das Autologon-Feature automatisch aktiviert wird.
- Nach der Installation müssen die Skripte sowie alle Dateien mit vertraulichem Inhalt umgehend sicher gelöscht werden (siehe auch M 4.56 *Sicheres Löschen unter Windows-Betriebssystemen*).

Angepasste Installationsmedien

Wenn Windows XP von möglicherweise veralteten Originalmedien installiert wird, müssen dabei nach der Installation die existierenden Service Packs und Updates gesondert eingespielt werden. Dies verlängert die Installationszeit und erhöht das Risiko einer erfolgreichen Attacke auf den Computer, da er sich eine gewisse Zeit nicht auf dem aktuellen Stand befindet. Um die Updates gleich bei der Installation einzuspielen und somit das Risiko einer Attacke zu mindern, kann eine der beiden mit Windows XP eingeführten Installationsfunktionen verwendet werden:

- integrierte Installation (auch Slipstream-Installation bezeichnet) oder
- kombinierte Installation.

Mit der integrierten Installation wird das Betriebssystem zusammen mit einem Service Pack installiert. Die kombinierte Installation ermöglicht die Installation von Windows XP zusammen mit Hotfixes und zusätzlichen Anwendungen im unbeaufsichtigten Modus.

Für eine integrierte Installation wird ein neues Installationsmediums erstellt. Dabei werden die Originaldateien durch Dateien des Service Packs überschrieben. Mögliche Installationsmedien sind CD-ROM, Netz-Distributionsfreigabe oder Installationsordner der Remoteinstallationsdienste (RIS). Es ist zu beachten, dass ein Service Pack, das im integrierten Modus installiert wurde, nicht deinstalliert werden kann.

Ein kombiniertes Installationsmedium wird erstellt, indem zusätzliche Installationsdateien in das Original-Installationsmedium integriert werden. Die Antwortdatei für die unbeaufsichtigte Installation (standardmäßig wird sie *Unattend.txt* genannt) und *cmdlines.txt* müssen dann entsprechend angepasst werden. Die genaue Vorgehensweise ist der Dokumentation von Microsoft zu entnehmen.

Der Einsatz von angepassten Installationsmedien ist grundsätzlich zu empfehlen. Welches der beiden Verfahren bei einem Unternehmen bzw. einer Behörde eingesetzt werden soll, ist im Einzelfall zu entscheiden. Die Maßnahme M 2.329 *Einführung von Windows XP SP2* ist dabei zu beachten.

Systemkomponenten

Bei der Installation des Systems ist zu gewährleisten, dass nur die benötigten Systemkomponenten installiert werden. In Beispieltabellen unter den Hilfsmitteln zum IT-Grundschutz werden Komponenten aufgezählt, die für eine Basis-Installation von Windows XP verwendet werden sollten (Status: *Aktiviert*). Je nach existierenden geschäftlichen Anforderungen können weitere Komponenten installiert werden, die in der nachfolgenden Tabelle als *Optional* markiert wird. Von der Installation der Windows-Komponenten, die mit *Deaktiviert* markiert sind, ist aus Sicherheitssicht abzuraten.

Ergänzende Kontrollfragen:

- Wurde sichergestellt, dass die entsprechenden Sicherheitseinstellungen nach der Installation auch tatsächlich angewandt worden sind (installierte Komponenten, angewandte Richtlinien, Berechtigungen im Dateisystem/Registry, zugewiesene Benutzerrechte, erlaubte Systemdienste usw.)?
- Sind Kennwörter in Installationsskripten bzw. Konfigurationsdateien geschützt?
- Sind Installationsskripte und/oder Konfigurationsdateien mit vertraulichen Informationen unmittelbar nach der Installation vom System gelöscht worden?
- Werden angepasste Installationsmedien verwendet?

M 4.249 Windows XP Systeme aktuell halten

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator

Die Vergangenheit hat gezeigt, dass sicherheitsrelevante Updates bzw. Patches, die Microsoft regelmäßig veröffentlicht, zeitnah installiert werden sollten. In der Praxis führt dies jedoch öfter zu Problemen, da einerseits die Updates so schnell wie möglich eingespielt werden müssen, sie andererseits vor der Installation ausgiebig getestet werden sollen. Für dieses Problem existiert keine allgemeingültige Lösung, hier ist ein geeigneter Kompromiss einzugehen, der den Anforderungen an Sicherheit und Praktikabilität gerecht wird.

Die Maßnahme M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates* muss bei der Planung berücksichtigt sein.

- Es muss ein Prozess für den Umgang mit Patches und Updates auf organisatorischer Ebene etabliert sein (z. B. im Rahmen des Änderungsmanagements).
- Der Prozess muss nicht nur Updates und Patches für Windows XP Systeme, sondern auch eingesetzte Anwendungen (z. B. Microsoft Internet Explorer, Microsoft Office) berücksichtigen.
- Administratoren müssen sich regelmäßig über Schwachstellen und verfügbare Sicherheits-Updates informieren.
- Einspielen und Prüfen der Updates im Test-System muss sichergestellt werden.
- Eine Strategie zum Wiederherstellen der Funktionsfähigkeit der Systeme im Problemfall muss vorhanden sein.

Überprüfung des Patch-Standes

Um existierende Windows XP Systeme aktuell zu halten, muss der aktuelle Patch-Stand der Systeme mit den von Microsoft verfügbaren Updates verglichen werden. Microsoft stellt mit dem Baseline Security Analyzer (MBSA) ein Tool zur Verfügung, das für die automatische Auswertung der Systemstände eingesetzt werden kann. Der Einsatz dieses oder eines vergleichbaren Tools verschafft den Administratoren einen aktuellen Überblick über den Patch-Stand der Systeme und trägt somit wesentlich zur Gesamtsicherheit bei. Das MBSA Tool kann so konfiguriert werden, dass die Überprüfung nicht gegen einen Microsoft-Server im Internet, sondern gegen einen intern aufgesetzten Microsoft SUS (Software Update Server) erfolgt. Auf diese Weise wird der Ist-Zustand der Systeme mit dem unternehmensspezifischen Soll-Zustand verglichen. Diese Vorgehensweise wird vor allem für Tests verwendet, ob die im Unternehmen freigegebenen Patches und Updates auf allen Systemen installiert sind. Durch die Integration von MBSA in Microsoft SMS können die Testergebnisse auch direkt in der SMS Datenbank gespeichert werden.

Das MBSA Tool besitzt eine graphische Bedienungsoberfläche (*mbsa.exe*), kann aber auch über die Kommandozeile gesteuert werden (*mbsacli.exe*). Mit Letzterem lässt sich das Tool in einen automatisierten Prozess integrieren, so dass die Ergebnisse ebenfalls automatisch (z. B. mit Skripten) weiterverarbeitet werden können.

Die MBSA Utility ist im Stande, den Patch-Stand des Betriebssystems und weitere Microsoft Anwendungen wie z. B. Microsoft Office, Exchange Server 2003, Microsoft Internet Explorer (hier speziell auch die Zonen-Konfiguration) zu überprüfen. Es sollte jedoch berücksichtigt werden, dass die Version 1.2.1 nur lokale Überprüfungen von Windows-Firewall und Microsoft Office durchführen kann. Die restlichen Überprüfungen können sowohl lokal als auch entfernt durchgeführt werden.

Aktualisierungsmethoden

Zum Aktualisieren eines Windows XP Systems kann die integrierte *Automatische Updates* Funktionalität von Windows XP verwendet werden oder die Updates und Patches werden mittels eines anderen (externen) Software-Verteilungsmechanismen installiert. Nach welcher Strategie verfahren werden soll, ist anhand der konkreten Umstände und im Einzelfall festzulegen. Wird ein externer Software-Verteilungsmechanismus verwendet, so ist die *Automatische Updates* Funktionalität zu deaktivieren, so dass durch ihren parallelen Einsatz keine negativen Wechselwirkungen entstehen können.

Wird die automatische Aktualisierung von Windows XP verwendet, so stehen folgende Konfigurationsmöglichkeiten zur Verfügung:
- Updates werden automatisch heruntergeladen und entsprechend dem definierten Zeitplan installiert (diese Funktionalität steht erst der aktualisierten Version von *Automatische Updates* Software zur Verfügung).
- Updates werden automatisch heruntergeladen, es findet jedoch keine automatische Installation statt.
- Beim Vorhandensein neuer Updates erfolgt lediglich eine Benachrichtigung des Administrators, die Updates werden nicht heruntergeladen.

Von der manuellen Installation eines Updates sollte abgesehen werden. Um die Zeitspanne zwischen dem Bekanntwerden und dem Schließen einer Sicherheitsschwäche möglichst kurz zu halten, wird die automatische Installation von freigegebenen Updates mit dem *Automatische Updates* Mechanismus oder einem externen Software-Verteilungsmechanismus empfohlen.

Da aus Sicherheitssicht direkte Verbindungen ins Internet zu vermeiden sind und die zu installierenden Updates zuerst in Testsystemen getestet werden sollten, wird eine direkte Aktualisierung von Windows XP Systemen von externen Quellen (z. B. Microsoft) beim Einsatz des *Automatische Updates* Mechanismus nicht empfohlen. Stattdessen sollten die Windows XP Systeme durch die entsprechende Konfiguration angewiesen werden, einen unternehmensinternen Update Server zu benutzen. Auf diese Weise lässt der folgende sinnvolle Ablauf einer Aktualisierung realisieren:

- Administratoren werden über die Bereitstellung eines Updates benachrichtigt.
- Das Update wird heruntergeladen und auf Testsystemen installiert.
- Nach erfolgreich abgeschlossenen Tests wird das Update für interne Update Server freigegeben.
- Windows XP Rechner laden das freigegebene Update von einem internen Update Server herunter und installieren es.

Ergänzende Kontrollfragen:

- Ist die Strategie für die Aktualisierung festgelegt?
- Berücksichtigt die definierte Update-Strategie auch anwendungsspezifische Updates?
- Ist die Vertrauenswürdigkeit der Update-Quellen gewährleistet?
- Wird gewährleistet, dass nur getestete und freigegebene Updates installiert werden?

M 4.250 Auswahl eines zentralen, netzbasierten Authentisierungsdienstes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

IT-Systeme aller Art sollten grundsätzlich sicherstellen, dass sich alle Benutzer, die darauf zugreifen möchten, authentisieren müssen. Nur so kann verhindert werden, dass unautorisierte Personen Zugriff auf die Dienste erlangen, die das System anbietet, oder auf die Daten, die auf dem System gespeichert sind. Eine Ausnahme bilden nur solche IT-Systeme, die allgemein zugänglich sein sollen wie öffentliche Informationsdienste (beispielsweise öffentliche Webserver) oder Ähnliches.

Nachdem die Authentisierung erfolgreich abgelaufen ist, muss das System sicher stellen, dass die Benutzer nur auf solche Dienste und Daten Zugriff erhalten, für die sie entsprechende Berechtigungen besitzen.

Oft soll die Authentisierung nicht lediglich für einen einzelnen Dienst oder auf einem einzelnen System erfolgen, sondern es sollen zumindest für verschiedene Dienste und auf unterschiedlichen Systemen dieselben Authentisierungsdaten (etwa Benutzername und Passwort) genutzt werden können. In einem solchen Fall ist ein zentraler, netzbasierter Authentisierungsdienst erforderlich, damit die Authentisierungsdaten nicht auf jedem beteiligten System einzeln verwaltet und aktualisiert werden müssen.

Den Extremfall stellt hier das sogenannte "Single Sign-On" dar, bei dem eine Authentisierung zentral für alle Dienste eines IT-Verbunds erfolgt. Dies hat den Vorteil, dass die Benutzer sich nur einmal anmelden müssen. Die Benutzer benötigen nur jeweils ein Passwort oder Token und müssen sich somit nicht verschiedene Passwörter merken oder eine Vielzahl von Token aufbewahren. Andererseits wird einem Angreifer aber der Zugriff auf alle Dienste des IT-Verbunds ermöglicht, wenn er sich einmal als Benutzer anmelden konnte.

Soll ein zentrales, netzbasiertes Authentisierungssystem eingesetzt werden, so ist eine sorgfältige Planung besonders wichtig, da die Funktion und die Sicherheit eines solchen Systems entscheidende Faktoren für die Sicherheit des gesamten IT-Verbundes sind.

Die zentrale Authentisierung kann durch einen Einsatz eines zentralen Authentisierungssystems wie Kerberos erreicht werden. Kerberos bietet im weiterem den Vorteil, dass neben Unix-Systemen auch unter Windows-Betriebssysteme eine Kerberos-Authentisierung verwendet werden kann.

Auf wichtige Empfehlungen, die für die Auswahl und den Einsatz eines netzbasierten Authentisierungsdienstes berücksichtigt werden müssen, wird im Folgenden tiefer eingegangen:

Verschlüsselung der Netz-Protokolle

Im Gegensatz zu einer lokalen Benutzerverwaltung werden kritische Informationen, die für eine netzbasierte Authentisierung benötigt werden, über ein LAN oder WAN übertragen. Daher ist es zwingend erforderlich, dass diese Informationen nicht mitgelesen oder verändert werden können. Außerdem

muss sichergestellt werden, dass ein Angreifer sich nicht anmelden kann, indem er aufgezeichnete Anmeldeinformationen wieder einspielt. Daher müssen die Anmeldeinformationen, die für die Authentisierung zwischen Server und Client ausgetauscht werden, verschlüsselt und zusätzlich, beispielsweise mit Challenge-Response-Verfahren, dynamisiert werden.

Schutz des Authentisierungsservers

Generell werden alle für eine Authentisierung benötigten Informationen auf einem zentralen Server abgelegt. Daher ist sicherzustellen, dass keine unautorisierten Personen an diese kritischen Informationen gelangen können. Ein Authentisierungsserver muss also auf allen Ebenen sorgfältig geschützt werden (der Schutzbedarf ist vergleichbar mit dem eines Sicherheitsgateways). Hierzu gehört unter anderem:

- Er sollte in einem separaten Serverraum aufgestellt werden. Hierbei zu realisierende Maßnahmen sind in Baustein B 2.4 *Serverraum* beschrieben. Wenn kein Serverraum zur Verfügung steht, kann der Authentisierungsserver alternativ in einem Serverschrank aufgestellt werden (siehe Baustein B 2.7 *Schutzschränke*).
- Er darf sich nur innerhalb eines geschützten Netzes befinden.
- **Härtung des Servers**
  Auf einem Authentisierungsserver sollten nur die dafür erforderlichen Dienste verfügbar sein und möglichst keine weiteren Dienste angeboten werden, zumindest keine mit niedrigerem Schutzbedarf, wie z. B. ein Webserver. Außerdem dürfen nur Programme installiert sein, die für die Funktionsfähigkeit nötig sind.
- Für die Konzeption und den Betrieb eines Authentisierungsservers muss geeignetes Personal mit ausreichend Ressourcen zur Verfügung stehen. Der zeitliche Aufwand für den Betrieb eines Authentisierungsservers darf nicht unterschätzt werden. Alleine die Auswertung der angefallenen Protokolldaten nimmt oft viel Zeit in Anspruch. Die Administratoren müssen fundierte Kenntnisse der eingesetzten IT-Komponenten besitzen und entsprechend geschult werden.
- Nur Administratoren dürfen sich auf diesem System anmelden können. Die Vergabe von Administrationsrechte muss sorgfältig dokumentiert sein. Besonders sicherheitskritische Eingriffe sollten möglichst im Vieraugenprinzip erfolgen. Administratoren sollten für die Anmeldung starke Authentisierungsmethoden benutzen.
- Die Administration des Authentisierungsservers darf nur über einen gesicherten Zugang möglich sein, also z. B. über eine gesicherte Konsole, eine verschlüsselte Verbindung oder ein separates Netz (Administrationsnetz).
- **sorgfältige Konfiguration**
  Die korrekte Konfiguration eines Authentisierungsservers ist wesentlich für dessen sicheren Betrieb. Fehler in der Konfiguration können zu Sicherheitslücken oder Ausfällen führen. Die bestmögliche Konfiguration muss sorgfältig dokumentiert sein.
- Betriebssystem und Programme eines Authentisierungsservers müssen jederzeit auf einem sicheren Patch-Stand sein.

- Es müssen in regelmäßigen Abständen Integritätstests der eingesetzten Software durchgeführt werden (siehe auch M 4.93 *Regelmäßige Integritätsprüfung*). Im Fehlerfall muss der Authentisierungsserver abgeschaltet werden.
- Es muss klar dokumentiert sein, welche Ereignisse protokolliert werden müssen (M 5.9 *Protokollierung am Server*), wo diese gespeichert werden und wie und in welchen Abständen sie ausgewertet werden.
- Authentisierungsserver müssen in das organisationsweite Datensicherungskonzept sowie in das Notfallvorsorgekonzept integriert sein. Beim Wiedereinspielen von gesicherten Datenbeständen muss darauf geachtet werden, dass Benutzer- und Rechteverwaltung auf dem aktuellsten Stand sind.
- Für einen sicheren Betrieb eines Authentisierungsservers sind die umgesetzten Sicherheitsmaßnahmen regelmäßig auf ihre korrekte Einhaltung zu überprüfen. Durch regelmäßige Audits muss der sichere Betrieb überprüft werden.

Weiterhin ist bei einer zentralen Verwaltung ein Ausfall des Servers oder des Netzes zu berücksichtigen, was nach einem Denial-Of-Service-Angriff der Fall sein kann. Wenn alle weiteren Rechner im Netz von dem Server für eine Authentisierung abhängig sind, weitet sich der Denial-Of-Service-Angriff auf alle Systeme im Netz aus. Daher wird der Einsatz eines hochverfügbaren Systems empfohlen, das mit dem Einsatz eines redundanten Servers (siehe M 6.43 *Einsatz redundanter Windows NT/2000 Server*) realisiert werden kann.

Da eine verlässliche Authentikation für die Sicherheit jedes Netzes eine zentrale Rolle spielt, ist der sichere und ordnungsgemäße Betrieb des Authentisierungsservers besonders wichtig. Daher muss das gewählte Vorgehen in die bestehende organisationsweite Sicherheitsleitlinie integriert werden.

Passwörter

Analog zur Maßnahme M 2.11 *Regelung des Passwortgebrauchs* sind geeignete Vorkehrungen für eine hohe Passwortgüte zu treffen.

Protokollierung

Das Authentisierungssystem muss die aus der Maßnahme M 5.9 *Protokollierung am Server* bekannten Ereignisse erfassen können.

Alle Logdateien sollten zentral auf dem Server abgelegt werden. Da dies die Erstellung detaillierter Benutzerprofile ermöglicht, muss aus Gründen des Datenschutzes verhindert werden, dass diese Informationen von unautorisierten Personen ausgelesen werden können.

Wird ein zentraler Protokollierungsserver eingesetzt, sollte gewährleistet werden, dass die übertragenen Daten nicht abgehört werden können. Dies kann beispielsweise durch den Einsatz von Übertragungsprotokollen, die die Verschlüsselung der Daten ermöglichen, eine VPN-Verbindung oder durch ein separates Netz zwischen den zentralen Authentisierungsserver und dem Protokollierungsserver erfolgen.

Ergänzende Kontrollfragen:

- Welche Dienste im IT-Verbund unterstützen den Einsatz eines zentralen Authentisierungsservers?
- Wird Single Sign-On eingesetzt?
- Wie werden die Authentisierungsinformationen bei der Übertragung geschützt?
- Wie werden Angriffe auf den Authentisierungsserver verhindert?

M 4.251 Arbeiten mit fremden IT-Systemen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Benutzer, Vorgesetzte

Verantwortlich für Umsetzung: Benutzer

Häufig ist es erforderlich, auch unterwegs auf elektronische Informationen verschiedenster Art zugreifen zu können, z. B. um Terminkalender abgleichen zu können, E-Mails zu verschicken oder einzelne Dateien abrufen zu können. Hierfür ist es häufig das einfachste, fremde IT-Systeme oder Kommunikationsanbindungen zu benutzen, also beispielsweise

- aus einem Internet-Cafe Dateien herunterzuladen,
- in einem Büro einer besuchten Institution über deren PCs oder deren Intranet oder
- über WLAN über einen Hotspot im Hotel auf das Firmennetz zuzugreifen.

Hierbei sollte sich aber jeder Benutzer darüber im Klaren sein, das dies fremd-administrierte IT ist und daher zusätzliche Sicherheitsmaßnahmen zu ergreifen sind. Es sollte immer davon ausgegangen werden, dass das Sicherheitsniveau der fremden Umgebung nicht bekannt ist und damit als niedrig eingeschätzt werden muss. Jeder Mitarbeiter sollte sich bewusst sein, dass fremde Rechner und fremde Umgebungen grundsätzliche höhere IT-Sicherheitsrisiken darstellen. Selbst wenn das Sicherheitsniveau einen ausgezeichneten Eindruck macht, kann dies ein Trugschluß sein.

Beispielsweise kann die momentane Netzumgebung schlechter geschützt sein als der eigene Laptop, so dass damit Probleme wie z. B. Computer-Viren oder Trojanische Pferde importiert werden können. Es kann sich auch herausstellen, dass in einer besuchten Institution ein völlig anderes Verständnis von Sicherheit herrscht, so dass kein Konsens über Sicherheitsziele, Sicherheitsniveau und Sicherheitsmaßnahmen existiert.

Wechselnde Benutzer

In mobilen Netzen kann es passieren, dass die Netzteilnehmer ständig wechseln, also neue hinzukommen und andere das Netz verlassen. Damit ist es schwer, nachzuvollziehen, wer zu einem bestimmten Zeitpunkt ebenfalls in diesem Netz aktiv war. Mobile Netze sind dadurch anfällig für Angriffe, die unter Umständen nicht einmal nachvollziehbar sind, und alle Aussagen über ein vorhandenes Sicherheitsniveau sind sehr schwierig.

Trau, schau wem!

Bevor sich Benutzer in fremden Netzen anmelden oder Dienstleistungsangebote nutzen, sollten sie sich darüber Gedanken machen, wie vertrauenswürdig diese sind. Extrem günstige Angebote könnten speziell dazu eingerichtet worden sein, um Daten auf mobilen Endgeräte auszuspähen oder zu manipulieren. Beispielsweise könnte ein Angreifer einen kostenfreien Internet-Zugang oder WLAN-Zugang zur Verfügung stellen, um so auf einfache Weise die von dort übertragenen Daten mitlesen zu können.

Auch bei der Nutzung verhältnismäßig einfacher, überschaubarer Dienstleistungen müssen die Benutzer die unerlässliche Sorgfalt bewahren. Beispielsweise kann es unterwegs erforderlich sein, Ausdrucke vom Laptop aus anzufertigen. Dazu können dann etwas Druckdienste in Hotels, in

Internetcafes oder Kopierläden genutzt werden oder auch auf die Drucker in einer besuchten Firma zugegriffen werden. Dabei werden allerdings mit dem Druckjob zumindest auch die gedruckten Informationen Externen zugänglich gemacht, nämlich den jeweiligen Dienstleistern. Die zu druckende Datei muss an den Drucker übertragen werden und wird dabei unter Umständen auf IT-Systemen zwischengespeichert. Ausdrücke können unbemerkt mehrfach angefertigt werden oder es kann schlicht Papier am Drucker liegen bleiben.

Daher sollten Benutzer folgende Empfehlungen beachten, bevor sie mit fremden IT-Systemen arbeiten oder Dienstleistungsangebote nutzen:

- Sie sollten sich über vorhandene Sicherheitsmaßnahmen informieren.
- Sie sollten sich genau überlegen bzw. sich an den Vorgaben und Regelungen für die mobile IT-Nutzung orientieren und fremde IT-Systeme oder Dienstleistungsangebote nicht für alle denkbaren Aktionen und Daten benutzen.
- Sobald die Arbeit beendet wurde, sollten bei einem fremden Rechner grundsätzlich alle währenddessen entstandenen temporären Daten gelöscht werden. Dies ist allerdings meistens nicht einfach, da bei vielen Betriebssystemen temporäre Daten an einer Vielzahl von Stellen entstehen. Außerdem kann es bei fremden IT-Systemen auch vorkommen, dass die Zugriffsrechte ein Löschen aller entstandenen Daten nicht zulassen. Zumindest sollte der Zwischenspeicher (Cache) gelöscht werden.

Temporäre Daten löschen

- Auf keinen Fall sollten Browser-Funktionen zur "Auto-Vervollständigung" von Benutzernamen und Passwörtern genutzt werden, damit nachfolgende Benutzer keine einfache Möglichkeit vorfinden, sich unter diesem Benutzernamen irgendwo anzumelden.

Ergänzende Kontrollfragen:

- Werden alle Mitarbeiter darüber informiert, was sie bei der Nutzung fremder IT beachten sollten?

M 4.252 Sichere Konfiguration von Schulungsrechnern

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator

Um Sicherheitsprobleme und die ungewünschte Nutzung von Schulungsrechnern zu vermeiden, sind eine minimale Konfiguration der Rechner und eine restriktive Rechtevergabe (siehe M 2.63 *Einrichten der Zugriffsrechte* und M 4.135 *Restriktive Vergabe von Zugriffsrechten auf Systemdateien*) erforderlich. Empfehlungen zur Konfiguration von Schulungsrechnern können der Maßnahme M 4.95 *Minimales Betriebssystem* entnommen werden.

Vor dem Einsatz von Schulungsrechnern sollte festgelegt werden, welche Anwendungen und Kommunikationsschnittstellen in der jeweiligen Schulung genutzt werden sollen. Durch die Festlegung einer Standardkonfiguration für die Schulungsrechner (siehe M 2.69 *Einrichtung von Standardarbeitsplätzen)* kann der Installationsaufwand minimiert und ein Mindestniveau an Sicherheit für die Schulungsrechner gewährleistet werden. Vor jeder Schulung muss überprüft werden, ob die Konfiguration der Rechner für die Zwecke der Schulung geeignet ist. Um hier auf langwierige Prüfungen verzichten zu können, ist es sinnvoll, Schulungsrechner vor jedem Einsatz über entsprechend vorbereitete Pakte neu zu installieren (siehe M 4.109 *Software-Reinstallation bei Arbeitsplatzrechnern*).

Von Schulungsrechnern sollten Informationen wie Schulungs- oder Prüfungsunterlagen nicht unkontrolliert kopiert werden können und es sollten auch keine zusätzlichen Dateien oder Programme aufgespielt werden können (z. B. Spickzettel für Prüfungen). Daher sollten einerseits restriktive Zugriffsrechte für die Benutzer dieser Rechner vergeben werden und andererseits das Überspielen von Daten auf externe Medien verhindert werden (siehe auch M 4.4 *Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern*).

Es ist außerdem zu überlegen, ob und in welchem Umfang es notwendig ist, Datensicherungen durchzuführen, beispielsweise wenn Übungsaufgaben oder Prüfungsergebnisse gesichert werden sollen.

Auf den Schulungsrechnern sollten zusätzliche Sicherheitsprogramme installiert werden, falls diese nicht schon Teil des Betriebssystems sind. Vor allem sinnvoll sind ein Integritätsprüfprogramm (siehe M 4.93 *Regelmäßige Integritätsprüfung*) und ein Softwarepaketfilter. Empfehlenswert sind zusätzlich Programme zur Virensuche und zur Auswertung der Protokolleinträge.

Ergänzende Kontrollfragen:

- Sind alle Schulungsrechner sicher konfiguriert?

M 4.253 Schutz vor Spyware

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Bei Spyware handelt es sich um eine Schadsoftware, die private und vertrauliche Daten heimlich sammelt und an einen Angreifer bzw. an Dritte übermittelt. Durch folgende Mechanismen kann die Gefahr vor Spyware erheblich minimiert werden:

- **Aktualisierung der Sicherheitsrichtlinien**

  Die aktuelle Sicherheitsrichtlinie einer Behörde bzw. eines Unternehmens muss auf die zusätzlichen Gefahren durch Spyware aktualisiert werden. Hierbei sollte auch klar definiert werden, wie bei einem Spyware-Befall eines IT-Systems vorgegangen werden muss.

- **Sensibilisierung der Benutzer**

  Die Mitarbeiter sind in geeigneten Schulungen oder durch ein Informationsportal im Intranet über die Problematik von Spyware zu unterrichten. Ebenso ist auf die entsprechenden Inhalte in der Sicherheitsrichtlinie hinzuweisen.

- **Vermeidung der Darstellung von Webseiten mit aktiven Inhalten**

  Bei der Internetnutzung sollten Webseiten mit aktiven Inhalten (ActiveX, JavaApplets bzw. JavaScript) vermieden werden. Dies kann durch geeignete Einstellungen im Browser oder durch den Einsatz eines Web-Proxies geschehen. Hierbei ist zunächst zu klären, ob eine strikte Einhaltung dieser Richtlinie eventuell die eigentliche Arbeit nicht behindert.

- **Regelmäßiges Einspielen von Software-Updates**

  Viele Hersteller veröffentlichen regelmäßig Aktualisierungspakete für ihre Software, um bekannte oder mögliche Fehlerquellen und Schwachstellen zu beheben. Diese Updates sollten relativ zeitnah auch eingespielt werden, um der Spyware diesen Zugang zum IT-System zu verwehren. Vorerst muss allerdings geklärt werden, ob durch die Aktualisierung der Software nicht noch andere Probleme entstehen. Die Aktualisierung eines Testsystems wird daher dringend empfohlen, bevor ein Produktivsystem aktualisiert wird.

- **Beobachtung der Netz-Protokolle**

  Ein regelmäßiger Blick in die Protokolldateien des Netzes bringt ebenfalls viele Hinweise zu Tage. Oft sind verhältnismäßig große Datenmengen innerhalb bestimmter Zeitintervalle, z. B. alle 15 Minuten, ein Anzeichen für unerwünschten Datenverkehr. Stellt sich heraus, dass diese Datenmengen immer zu der gleichen Gegenstelle geschickt werden, so ist es wahrscheinlich, dass eine Spyware im internen Netz aktiv ist. Intrusion Detection Systeme (IDS) unterstützen hier die automatische Suche nach solchen Ungewöhnlichkeiten.

Heute erkennen viele Anti-Viren-Programme bereits Spyware, bevor sich diese unbemerkt auf dem IT-System installieren kann. Deshalb sollte stets

darauf geachtet werden, dass das eingesetzte Anti-Viren-Programm, wenn möglich täglich, mit aktuellen Viren-Informationen ausgestattet wird. Unterstützt das eingesetzte Anti-Viren-Programm nicht die Erkennung von Spyware, so ist es empfehlenswert, ein eigenes Anti-Spyware-Programm als Einzelprodukt auf den einzelnen IT-Systemen oder als Gateway-Lösung zu installieren.

Zusätzliche Kontrollfragen:

- Wurden die Sicherheitsrichtlinien mit den Gefahren und Maßnahmen zu Spyware aktualisiert?
- Sind alle Mitarbeiter auf die Gefahren von Spyware ausreichend sensibilisiert?
- Unterstützt das eingesetzte Anti-Viren-Programm die Erkennung von Spyware? Wenn nein, gibt es ein geeignetes Anti-Spyware-Programm für die Institution?

M 4.254 Sicherer Einsatz von drahtlosen Tastaturen und Mäusen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Drahtlose Tastaturen und Mäuse sind Peripheriegeräte, die kabellos über Funk- oder Infrarot-Schnittstellen mit einem Empfängermodul kommunizieren, das über COM-Port, PS2-Schnittstelle oder USB-Anschluss mit dem Rechner verbunden ist.

Da keine galvanische Verbindung zum Rechner besteht, müssen kabellose Eingabegeräte über eine eigene Spannungsversorgung in Form von Batterien oder Akkus verfügen. Für eine lange Betriebsdauer ist eine geringe Leistungsaufnahme dieser Geräte unumgänglich. Nach dem heutigen Stand der Technik haben Geräte mit Infrarot-Technik einen höheren Energieverbrauch als solche mit Funkschnittstelle.

Die Betriebsfrequenzen der Systeme liegen alle in lizenzfreien Frequenzbereichen. Die Mehrzahl der Funkmäuse und Funktastaturen senden im 27 MHz-Band und verfügen über zwei Funkkanäle, einige kabellose Geräte arbeiten im 2,4 GHz-Bereich.

Die Reichweite der Funksysteme beträgt typischerweise 2 bis 5 Meter. Hier ist im Gegensatz zu den Systemen auf Basis der Infrarot-Technik keine direkte Sichtverbindung zwischen Sender und Empfänger notwendig. Die Reichweite ist extrem abhängig von den Umgebungsbedingungen. Andere im gleichen Frequenzbereich sendende Geräte wie z. B. Sprechfunkgeräte, Funkspielzeug, funkgesteuerte Antriebe für Garagentore oder WLAN-Verbindungen im 2,4 GHz-Bereich können den Betrieb der Systeme empfindlich stören und die Reichweite reduzieren. Metallische Hindernisse (Stahlarmierungen, Stahlschränke und Ähnliches) können zum Versagen der Technik führen.

Hersteller von Funk-Anwendungen geben als Reichweite Entfernungen an, in denen die Datenübertragung ihrer Geräte sicher funktioniert. Diese Funktionalitätsreichweite ist aber im Falle von Geräten, die nur mit billiger Empfangstechnik ausgestattet sind, in der Regel kleiner als die Entfernung, in der die ausgesendeten Signale mit Hilfe von Richtantennen und hochwertiger Empfängerelektronik noch empfangen, aufgezeichnet und ausgewertet werden können. Eine Abhörgefährdung in einer größeren Entfernung als die Funktionalitätsreichweite kann daher nicht ausgeschlossen werden.

mangelnde Abhörsicherheit

Ein Problem der funkbasierten Eingabegeräte ist die mangelnde Abhörsicherheit. Die ausgesendeten Funksignale können von Dritten empfangen und aufgezeichnet werden. Sind diese Funksignale nicht sicher verschlüsselt, können diese Daten leicht ausgewertet werden. Es gibt auf dem Markt zahlreiche Funktastatursysteme, welche die aus den Tastenanschlägen resultierenden Signale völlig unverschlüsselt und damit für Dritte abhörbar übertragen. Hier reicht häufig schon ein zweiter Empfänger vom selben Hersteller aus, um die empfangenen Signale auf einem anderen Rechner sichtbar zu machen.

Systeme, die auf Basis der Infrarot-Technik kommunizieren, verwenden meistens den IrDA-Standard der Infrared Data Association. Im IrDA-Standard sind keine Sicherheitsmechanismen gegen ein Mithören des Datenverkehrs

spezifiziert. Die Daten werden nur auf Protokollebene gegen Übertragungsfehler mittels Prüfsummenverfahren gesichert. Sicherheitsmechanismen wie Authentisierung, kryptographischer Integritätsschutz und Verschlüsselung sind nicht vorhanden. In gewissem Rahmen wird die Übertragung durch die sehr eingeschränkte Reichweite der Infrarotstrahlen und die benötigte Sichtverbindung geschützt. Das Sicherheitsniveau dieser Systeme liegt allerdings, aufgrund der möglichen Streustrahlung, unter dem der kabelgebundenen Eingabegeräte.

Einige Hersteller bieten Produkte mit proprietären Sicherheitslösungen an. Über die Sicherheit solcher Lösungen kann keine Aussage getroffen werden, da die eingesetzten Algorithmen in der Regel von den Herstellern unter Verschluss gehalten werden.

Damit baugleiche Geräte nebeneinander betrieben werden können, haben die meisten Hersteller ihre Geräte mit verschiedenen Erkennungsnummern ausgerüstet. Hierbei werden verschiedene Prinzipien verwendet, z. B. wird aus einem Pool von IDs ein bestimmter Wert fest für ein Gerät vergeben oder es wird bei einem Batteriewechsel die ID durch die Software neu erwürfelt.

Auf dem Markt sind erste Produkte erhältlich, die über Bluetooth kommunizieren. Bei korrekter Implementierung und Konfiguration der Bluetooth-Sicherheitsmerkmale bieten diese im Allgemeinen einen höheren Schutz als Funksysteme mit proprietärer Technik. Eine Zusammenstellung der Gefährdungen und mögliche Sicherheitsmaßnahmen zum Thema Bluetooth ist im Baustein x.y Bluetooth zu finden.

Abschließend sei erwähnt, dass bei Tastaturen durch die elektromagnetische Abstrahlung der Tastaturmatrix und des Verbindungskabels eine Abhörgefährdung besteht (siehe auch M 4.89 *Abstrahlsicherheit*). Dies gilt auch für kabellose Tastaturen. Die Abhörgefährdung ist aber bei kabelgebundenen Tastaturen im Allgemeinen wesentlich geringer als die Abhörgefahr durch den Einsatz von Funkkommunikationsstrecken bei kabellosen Eingabegeräten.

Auf Funktastaturen und -mäuse sollte verzichtet werden!

Zahlreiche Funktastaturen und Funkmäuse senden ihre Informationen über Funk oder Infrarot-Licht ohne Sicherheitsvorkehrungen zu den Rechnern. Ohne großen Aufwand können diese Informationen von Dritten mitgelesen oder gegebenenfalls sogar manipuliert werden. Vom Einsatz solcher Systeme ist aus Sicht der IT-Sicherheit daher generell abzuraten.

Für Systeme mit proprietären Sicherheitsmaßnahmen, die kein Sicherheitszertifikat aufweisen, ist der Sicherheitswert nicht einschätzbar. Der Nutzer geht hierbei das Risiko ein, dass die nicht evaluierte Lösung des Herstellers nur eine minimale Sicherheit bietet, die aber bei weitem nicht ausreicht, um seine Daten effektiv zu schützen.

Drahtlose Systeme, die auf Standards wie Bluetooth basieren und bei denen die Sicherheitsmechanismen korrekt implementiert und aktiviert worden sind, bieten im Vergleich einen höheren Schutz. In sensiblen Bereichen sollten jedoch grundsätzlich besser keine Funk-Tastaturen, Funk-Mäuse und Infrarot-Produkte eingesetzt werden.

M 4.255 Nutzung von IrDA-Schnittstellen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Die Infrared Data Association (IrDA) hat Spezifikationen veröffentlicht, in der zunächst die unteren Schichten eines Protokolls für eine Infrarot-Schnittstelle definiert wurden, bei der Licht in Form von Infrarotstrahlung als Träger für den Datenaustausch über kurze Distanzen verwendet wird. Mittlerweile stellt IrDA auch höhere Protokolle für unterschiedliche Einsatzbereiche zur Verfügung. IrDA wird heute von allen gängigen Betriebssystemen unterstützt, die Kommunikation von Geräten wie PDAs und Mobiltelefonen mit dem PC oder untereinander via Infrarot-Schnittstelle ist in der Praxis etabliert.

Im IrDA-Standard sind keine Sicherheitsmechanismen gegen ein Mithören des Datenverkehrs spezifiziert. Die Daten werden nur auf Protokollebene gegen Übertragungsfehler mittels Prüfsummenverfahren gesichert. Sicherheitsmechanismen wie Authentisierung, kryptographischer Integritätsschutz und Verschlüsselung sind nicht vorhanden. Diese müssten gegebenenfalls auf Applikationsebene implementiert werden. In gewissem Rahmen wird die Übertragung durch die sehr eingeschränkte Reichweite der Infrarotstrahlen und die benötigte Sichtverbindung geschützt. Das Sicherheitsniveau dieser Systeme liegt allerdings, aufgrund der möglichen Streustrahlung, unter dem der kabelgebundenen Eingabegeräte.

Beim Betrieb von Geräten mit IrDA-Schnittstelle ist darauf zu achten, dass diese nur im Bedarfsfall aktiviert wird. Da im Protokoll keine Authentisierung vorgesehen ist, kann ein beliebiger Partner Daten über die IrDA-Schnittstelle an ein Gerät senden. So nimmt beispielsweise ein Mobiltelefon mit aktivierter IrDA-Schnittstelle SMS-Mitteilungen zum Versand an. An einen PDA oder Laptop können auch Programme über IrDA geschickt werden, die unter Umständen Schadfunktionen enthalten können. Außerdem belastet eine eingeschaltete IrDA-Schnittstelle die Batterie bzw. den Akku des mobilen Gerätes zusätzlich.

Da die Kopplung nur in einem sehr eingeschränkten Bereich möglich ist, ist ein Mithören der Kommunikation meist ausgeschlossen. Das bestehende geringe Restrisiko aufgrund der Streustrahlung der IrDA-Komponenten kann durch den Einsatz von zusätzlichen Sicherheitsmechanismen (z. B. Authentisierung und Verschlüsselung auf Applikationsebene) oder den Ersatz von IrDA durch leitungsgebundene Übertragung weiter minimiert werden.

Ergänzende Kontrollfragen:

- Werden IrDA-Schnittstellen bei allen IT-Komponenten deaktiviert, solange sie nicht benötigt werden?

M 4.256 Sichere Installation von SAP Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement,

Verantwortlich für Umsetzung: Administrator

Für die Installation eines SAP Systems sind die nachfolgend beschriebenen Aspekte zu berücksichtigen, denn schon in der Installationsphase werden wichtige Weichen für dessen Sicherheit gestellt.

Verwendete Betriebssysteme absichern

Die Komponenten eines SAP Systems werden als Programme auf einem IT-System installiert und in Form von Prozessen ausgeführt. Damit ist die Sicherheit des genutzten Betriebssystems auch wichtig für die Sicherheit des SAP Systems (siehe auch M 4.257 *Absicherung des SAP Installationsverzeichnisses auf Betriebssystemebene)*. Die Bausteine der IT-Grundschutz-Kataloge, die für die genutzten IT-Systeme relevant sind, müssen daher in die Modellierung einbezogen und angewendet werden. Außerdem sollten die IT-Systeme gehärtet werden (Hardening), also nicht benötigte Dienste und Programme deaktiviert oder besser entfernt werden.

SAP Informationsquellen

Hinweise auf weitere Informationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Nur benötigte Komponenten installieren

Ein SAP System besteht potentiell aus vielen Komponenten unterschiedlichster Ausprägung. Ungenutzte Komponenten jeglicher Art bergen jedoch Sicherheitsrisiken, da diese oftmals vergessen werden und daher ohne angepasste Konfiguration sind.

Für ein SAP System muss insbesondere entschieden werden, ob nur ein oder beide Stacks benötigt werden, sofern die eingesetzte Systemversion die separate Installation noch unterstützt. Ist dies nicht der Fall, muss der nicht benötigte Stack-Teil so abgesichert werden, dass dessen Funktionen nicht unberechtigt genutzt werden können.

Wahl von sicheren Passwörtern

Schon während der Installation müssen wichtige Authentisierungsdaten eingegeben werden. Dies sind beispielsweise Passwörter für technische Benutzer, die von den SAP Systemkomponenten (z. B. der Komponente, die die Verbindung zwischen Java-Stack und ABAP-Stack realisiert) zur Authentisierung bei internen Kommunikationsverbindungen genutzt werden.

Es ist darauf zu achten, dass dabei sichere Passwörter gewählt werden. Die Passwörter sollten sich an den internen Passwortvorgaben orientieren. Es ist auch dann ein neues Passwort einzugeben, falls die Installationsroutine bereits ein Passwort vorgibt.

Im Rahmen der Risikobetrachtung für das SAP System ist zu bedenken, dass der Administrator, der das SAP System installiert und die Passwörter festlegt, dadurch die Möglichkeit besitzt, die Sicherheitsmechanismen des SAP Systems zu unterwandern. Die technischen Benutzer, für die die Passwörter anzugeben sind, besitzen in der Regel hohe Privilegien. Daher müssen die Passwörter nach der Installation durch vertrauenswürdige Administratoren

verändert werden. Alternativ kann die Passworteingabe im Vier-Augen-Prinzip erfolgen, wobei je einer von zwei Administratoren die Hälfte des Passwortes eingibt. Dies gilt insbesondere in Outsourcing-Szenarien.

Bei der Passwortlänge ist zu beachten, dass ABAP- und Java-Stack unterschiedliche Restriktionen besitzen: Für den ABAP-Stack können Passwörter maximal aus 8 Zeichen bestehen. Groß- und Kleinschreibung wird dabei nicht unterschieden. Für den Java-Stack gelten diese Beschränkungen nicht. Bei der Passworteingabe ist daher zu berücksichtigen, ob der zugehörige technische Benutzer im ABAP- oder Java-Stack angelegt wird.

Die eingestellten Passwörter sind gemäß der geltenden Passwortrichtlinie zu dokumentieren und aufzubewahren. Hinweise zur Passwortgestaltung finden sich auch in M 2.11 *Regelung des Passwortgebrauchs*.

Installationsquellen absichern

In der Regel werden SAP Systeme nicht direkt von CD oder DVD installiert. Vielmehr wird eine Verzeichnisstruktur lokal oder im Netz genutzt, um die Daten anzubieten, die zur Installation benötigten werden. Die Daten der CD- bzw. DVD-Medien werden dann dorthin kopiert. Es wird empfohlen, die Daten nicht lokal auf dem Rechner zu halten, auf dem das SAP System installiert wird, sondern auf einem separaten Rechner. Auf die Daten kann dann über das Netz zugegriffen werden. In großen Behörden und Unternehmen kann dieses Verzeichnis genutzt werden, um zusätzliche SAP Systeme zu installieren. Werden die Systeme nicht in einem separaten und abgeschirmten Netzsegment installiert, so ist es sinnvoll, den Installationsrechner vom Netz zu nehmen, solange er nicht benötigt wird.

Es wird empfohlen den Zugriff auf die Installationsquellen mit Mitteln des Betriebssystems abzusichern, so dass nur berechtigte Administratoren darauf zugreifen können. Unberechtigte Benutzer dürfen insbesondere keine schreibenden Rechte auf die Installationsquellen besitzen, damit die enthaltenen Daten nicht verändert werden können.

Werden die Installationsquellen lokal auf den Rechnern des SAP Systems vorgehalten, so wird empfohlen, diese nach Abschluss der Installation zu löschen.

SAP Hinweise für die Installation umsetzen

Die Installationsanleitung eines SAP Systems enthält in der Regel eine Vielzahl von Verweisen auf SAP Hinweise, in denen wichtige Informationen für eine reibungslose Installation oder zur Problemlösung bei Installationsproblemen enthalten sind. In der Regel verweisen die in der Dokumentation genannten SAP Hinweise selbst auch wieder auf weitere SAP Hinweise, so dass eine beträchtliche Informationsmenge zusammenkommen kann. Die Hinweise sind im Vorfeld der Installation zu besorgen. In der Regel ist es zunächst ausreichend, ausgehend von der Installationsdokumentation die dort angegebenen Hinweise zu lesen und einen weiteren Iterationsschritt durchzuführen. Oft wird bei Referenzen auf weitere Informationen explizit angegeben, ob diese verpflichtend abzuarbeiten sind oder nur unter bestimmten Bedingungen angewandt werden sollen. Es wird dringend

empfohlen, alle relevanten Informationen tatsächlich abzuarbeiten, da es sonst leicht zu Fehlinstallationen kommen kann.

Insbesondere wenn die Installation zwar abgeschlossen wird, dabei jedoch Fehler aufgetreten sind, ist es möglich, dass Teilfunktionen eines SAP Systems nicht korrekt arbeiten. Dies kann auch sicherheitsrelevante Auswirkungen haben, so dass immer eine fehlerfrei abgeschlossene Installation anzustreben ist. Fehlermeldungen können nur dann ignoriert werden, wenn dies explizit durch die Installationsanleitung oder SAP Hinweise angegeben wird.

SAP Informationsquellen

SAP Hinweise sind über den SAP Service Marktplatz (siehe M 2.265 *Geeigneter Einsatz digitaler Signaturen bei der Archivierung*) zu erreichen. Es wird empfohlen, die SAP Hinweise auszudrucken und nach der Abarbeitung der Systemdokumentation beizulegen.

Aktuelle SAP Sicherheitsleitfäden berücksichtigen

Für immer mehr Produkte von SAP stehen Sicherheitsleitfäden zur Verfügung. Obwohl diese unterschiedlich in der Qualität der Sicherheitsempfehlungen sind, ist es sinnvoll, die Leitfäden für die zu installierenden SAP Komponenten zu verwenden. Die Sicherheitsleitfäden werden in Abständen aktualisiert, so dass es sich lohnt, neuere Leitfäden für bereits installierte Systeme zu berücksichtigen.

Die Sicherheitsleitfäden stehen vornehmlich für aktuelle System- und Produktversionen zur Verfügung. Es lohnt sich jedoch auch für Betreiber von älteren R/3 Systemen, die Sicherheitsleitfäden für neuere Produkt-Versionen zu nutzen, da viele Empfehlungen direkt anwendbar sind oder leicht adaptiert werden können.

SAP Informationsquellen

Die existierenden SAP Sicherheitsleitfäden sind über den SAP Service Marktplatz (siehe M 2.346 *Nutzung der SAP Dokumentation)* erreichbar.

Sichere Installation und Konfiguration der Datenbank

Die Datenbank, die das SAP System nutzt, um alle Informationen persistent zu speichern, ist eine kritische Komponente, die vor unberechtigtem Zugriff unbedingt geschützt werden muss. Neben den allgemeinen Aspekten einer sicheren Datenbank-Installation sind die spezifischen Empfehlungen in der Maßnahme M 4.269 *Sichere Konfiguration der SAP System Datenbank* zusammengefasst. Die Sicherheit von Datenbanken wird auch im Baustein B 5.7 *Datenbanken* behandelt.

Sichere Installation und Konfiguration der SAP Systemlandschaft

Entsprechend der Planung der Systemlandschaft (siehe M 2.341 *Planung des SAP Einsatzes*) müssen die betroffenen SAP und Nicht-SAP Komponenten (z. B. Firewalls) installiert und konfiguriert werden.

Ergänzende Kontrollfragen:

- Sind alle Passwörter während der Installation sicher gewählt worden?
- Wurden die Installationsquellen gegen unbefugten Zugriff gesichert?

- Sind alle relevanten SAP Hinweise in der Installation umgesetzt worden?
- Sind die SAP Empfehlungen aus den relevanten Sicherheitsleitfäden umgesetzt worden?

M 4.257 Absicherung des SAP Installationsverzeichnisses auf Betriebssystemebene

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator

Während der SAP Installation werden durch das Installationsprogramm zunächst Daten aus den Installationsquellen (z. B. Verzeichnis im Netz, CD/DVD) in ein Installationsverzeichnis (z. B. /sapinst) extrahiert. In diesem werden auch alle Aktivitäten während der Installation protokolliert.

Je nach Installationsprogramm können in den Protokolldateien auch schützenswerte Informationen enthalten sein. Dazu zählen die Informationen über die gewählten SAP System-IDs (SAPSID), Informationen über den lokalen Rechner (z. B. IP-Adresse, Rechnername), Namen der gewählten technischen Benutzer. Aber auch die Passwörter, die während der Installation eingegeben wurden, können im Klartext enthalten sein. Dies gilt insbesondere für ältere Installer-Versionen.

Daher wird nach Abschluss der Installation folgendes Vorgehen empfohlen:

- Das gesamte Installationsverzeichnis ist zu sichern. Die Sicherung sollte so erfolgen, dass auf die Daten nicht von unberechtigten Personen zugegriffen werden kann.
- Bei Problemen mit der SAP Installation müssen die gesicherten Daten und Protokolle durch SAP Experten gesichtet werden. Hierfür können diese an SAP gesandt oder durch SAP Berater eingesehen werden. Daher müssen in diesem Fall berechtigte Administratoren auf die Daten zugreifen können. Werden die Daten an SAP gesandt oder von Dritten eingesehen, so ist zu bedenken, dass damit diese Personen schützenswerte Systeminformationen erhalten. Daher muss eine entsprechende Vertraulichkeitsvereinbarung geschlossen werden.
- Das gesicherte Installationsverzeichnis kann danach auf dem installierten System gelöscht werden.

Je nach Schutzbedarf des SAP Systems kann es sinnvoll sein, die Protokolldaten vor dem Zugriff durch Dritte auf Klartextpasswörter zu untersuchen und diese zu löschen oder zu maskieren. Dies wird von neueren Installer-Versionen bereits bei der Protokollerstellung umgesetzt, so dass dadurch keine Beeinträchtigung der Support-Leistung erfolgt, falls die so veränderten Protokolldateien im Support-Fall genutzt werden.

Ergänzende Kontrollfragen:

- Wurde das Installationsverzeichnis gesichert und im Dateisystem gelöscht?

M 4.258 Sichere Konfiguration des SAP ABAP-Stacks

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der ABAP-Stack ist die traditionelle Ausführungsumgebung eines SAP Systems. Dies trifft insbesondere auf die Systemversionen zu, die allgemein mit dem Begriff SAP R/3 bezeichnet werden, da die R/3 Komponenten und Module im ABAP-Stack ausgeführt werden.

Die initiale Konfiguration des ABAP-Stacks ist aufwendig und umfasst viele Einzelschritte. Der Aufwand erhöht sich, wenn neben der Konfiguration der reinen SAP Basis auch Applikationen und Module konfiguriert werden müssen, wie das in R/3-Systemen notwendig ist. Hier müssen alle relevanten Behörden- oder Unternehmensprozesse durch Konfiguration (Customizing) oder Anpassungen im ABAP-Code nachgebildet werden.

Im Folgenden werden die aus Sicherheitssicht wichtigsten Schritte aufgezeigt, die bei der initialen Konfiguration des ABAP-Stacks durchzuführen sind. Die Darstellung beschränkt sich auf die Konfiguration der SAP Basis und geht damit nicht auf Module oder Applikationen ein.

Mandant für den Betrieb festlegen

Zunächst muss ein Mandant für den Betrieb des SAP Systems festgelegt werden. Als "Mandant" (engl. Client) wird in einem SAP System eine technische Unterteilung verstanden. Dies ist nicht mit dem Mandantenbegriff im Sinne von "Kunde" zu verwechseln. Nach der Installation dürfen die existierenden Standardmandaten mit den Nummern 000 (SAP Referenzmandant), 001 (Produktionsvorbereitungsmandant), und 066 (Earlywatch-Mandant) nicht genutzt werden.

Ein SAP System kann mehrere Mandanten mit unterschiedlichen Verwendungszwecken enthalten. Alle Mandanten eines SAP Systems hängen jedoch über den SAP Referenzmandanten zusammen, in dem Konfigurationen erfolgen, die global für das gesamte SAP System gelten.

Aus Sicherheitssicht ist zu fordern, dass Mandanten mit sehr unterschiedlichen Sicherheitsanforderungen nicht zusammen in einem SAP System betrieben werden. So darf etwa ein Produktivmandant nie zusammen mit einem Entwicklungsmandanten in einem SAP System betrieben werden. Beim gemeinsamen Betrieb können Entwickler auch mandanten-unabhängige Objekte ändern, so dass dies direkt Auswirkungen auf den Produktivmandanten hat. Daher ist eine Separation zwingend erforderlich.

Sicherheitsrelevante IMG-Aktivitäten durchführen

SAP Informationsquellen

Der SAP Implementation Guide (IMG, SAP Reference IMG) ist eine von SAP vordefinierte, systeminterne Liste, die die Konfigurationsschritte enthält, die zur Konfiguration eines SAP Systems durchzuführen sind. Die Liste ist hierarchisch aufgebaut und jeweils auf die verwendete Systemversion und die installierten Komponenten abgestimmt. Daneben besteht die Möglichkeit, eigene IMGs zu erstellen (Projekt IMGs), in denen nur die im Rahmen der Systemverwendung notwendigen Konfigurationsschritte aus dem SAP Reference IMG enthalten sind. IMGs bieten zudem die Möglichkeit

festzuhalten, welche Konfigurationen bereits durchgeführt wurden, so dass dadurch der Konfigurationsstatus vorgehalten werden kann.

In M 2.346 *Nutzung der SAP Dokumentation* findet sich ein Hinweis auf die SAP IMG Dokumentation, die zu beachten ist. Alle im Rahmen der Planung festgelegten IMG-Aktivitäten (siehe auch M 2.341 *Planung des SAP Einsatzes*) müssen abgearbeitet werden.

Folgende IMG-Aktivitäten sind immer durchzuführen:

- HTTP-Services aktivieren bzw. deaktivieren, falls diese für den späteren Einsatz nicht benötigt werden (Transaktion: SICF), siehe dazu auch , M 5.127 *Absicherung des SAP Internet Connection Framework (ICF)*.
- Berechtigungen für IDOC-Schnittstelle vergeben (Transaktion: PFCG), siehe dazu auch M 5.128 *Absicherung der SAP ALE (IDoc/BAPI) Schnittstelle*.
- Berechtigungen für RFC-Schnittstellen vergeben (Transaktion PFCG), siehe dazu auch M 2.342 *Planung von SAP Berechtigungen* und , M 5.126 *Absicherung der SAP RFC-Schnittstelle*.
- IDOC-Administration einstellen (Transaktion: OYEA), siehe dazu auch , M 5.128 *Absicherung der SAP ALE (IDoc/BAPI) Schnittstelle.*
- Content-Server Administration (Transaktion: CSADMIN), siehe dazu auch M 5.129 *Sichere Konfiguration der HTTP-basierten Dienste von SAP Systemen*.
- Profilparameter für den Internet Connection Manager (ICM) konfigurieren (Transaktion SMICM, Springen, Parameter)
- Proxy-Konfiguration definieren (Transaktion SM30 mit THTTP)
- Alle Aktivitäten unter dem Stichwort "Systemadministration" sind durchzuführen.

Durch die IMG-Aktivitäten werden unter anderem auch die nachfolgend beschriebenen Maßnahmen berührt. Da diese jedoch aus Sicherheitssicht eine große Relevanz aufweisen, werden sie hier explizit aufgeführt.

Profilparameter anpassen

Über Profilparameter können grundsätzliche Funktionen eines SAP Systems konfiguriert werden. Daher müssen im Rahmen der Konfiguration auch die Profilparameter an die Bedürfnisse angepasst werden. Da Profile in mehreren Ausprägungen existieren (z. B. Start-Profil, Default-Profil, Instanz-Profil), müssen sich Administratoren mit dem Profil-Mechanismus vertraut machen.

Generell ist für jeden einzelnen Profilparameter die zu verwendende Einstellung zu definieren. Folgende Parameter verdienen dabei aus Sicherheitssicht besondere Aufmerksamkeit:

- alle Parameter mit dem Präfix "auth/"
- alle Parameter mit dem Präfix "login/"
- alle Parameter mit dem Präfix "snc/", sofern SNC eingesetzt wird
- alle Parameter mit dem Präfix "ssf/", sofern SSF eingesetzt wird

Für die Profil-Verwaltung sollte die Transaktion RZ10 verwendet werden. Das manuelle Ändern auf Dateisystemebene sollte unterbleiben. Für die Anzeige der Profilparameter kann auch der Report RSPARAM benutzt werden, der über die Transaktion SE38 aufgerufen wird. Die Profil-Dateien sind auf Betriebssystemebene vor unberechtigtem Zugriff zu schützen.

SAP Informationsquellen

Hinweise auf Detailinformationen zum Umgang mit Profilen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Systemänderbarkeit konfigurieren

Je nach Rolle eines SAP Systems muss die Systemänderbarkeit eingestellt werden. Durch die Einstellung wird bestimmt, ob Änderungen an internen System-Komponenten und Applikationskomponenten überhaupt erlaubt sind oder nicht. Dies betrifft beispielsweise den ABAP-System-Code, generell alle Objekte im Data Dictionary (DDIC) sowie den Objektnamensraum.

Für Produktiv-Systeme wird empfohlen, die Systemänderbarkeit global auf "nicht änderbar" zu setzen. Damit können Änderungen nur noch über das Transportsystem eingespielt werden. Dies ist für Produktiv-Systeme wünschenswert, damit Änderungen nur über definierte Prozeduren und Abläufe erfolgen. Wichtig ist hier, einen geordneten Änderungsmanagementprozess zu definieren und einzuhalten, siehe M 4.272 *Sichere Nutzung des SAP Transportsystems*.

Für Test- und Qualitätssicherungssysteme sollten die gleichen Einstellungen wie im Produktivsystem verwendet werden, also global "nicht änderbar". Änderungen sind im Entwicklungssystem vorzunehmen und nach dem Durchlauf des Qualitätssicherungsprozesses in das Qualitätssicherungs- und final in das Produktiv-System zu transportieren.

Für Entwicklungssysteme sollten die Komponenten, die durch die Entwicklung nicht betroffen werden, auf "nicht änderbar" gesetzt werden. Die Komponenten, in denen entwickelt wird, müssen hingegen auf "änderbar" gesetzt werden.

Die Einstellungen der Systemänderbarkeit können über die Transaktion SE06 oder SE03 erreicht werden.

SAP Informationsquellen

Hinweise auf detaillierte Informationen zum Thema finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Mandanten-Konfiguration durchführen

Neben der übergreifenden Änderbarkeit des SAP Systems können auch einzelne Mandanten gegen Veränderungen mandantenabhängiger Eigenschaften geschützt werden. Diese Einstellung ist für alle produktiven Mandanten zu benutzen. Durch die Einstellungen wird auch beeinflusst, ob Mandanten-Veränderungen automatisch aufgezeichnet werden, so dass Einstellungsveränderungen nach der Prüfung automatisch als Transportauftrag verfügbar sind und in andere Mandanten transportiert werden können, die mit den gleichen Einstellungen betrieben werden sollen.

Das Änderungsmanagement-Konzept muss festlegen, nach welchem Schema Änderungen zwischen Mandaten verteilt werden und welche Mandanten

welchen Verwendungszweck (z. B. Produktivmandant, Testmandant, Entwicklungsmandant) besitzen.

Die Einstellungen erfolgen über die Transaktion SCC4. Für die eigenen Produktivmandanten sind folgende Einstellungen empfohlen (Hinweis: Die angegebenen Bezeichnungen der Einstellungswerte finden sich so in der abgekürzten Schreibweise im SAP System.):

- Rolle des Mandanten: "Produktiv"
- Änderungen und Transporte für mandantenabhängige Objekte: "keine Änderung erlauben"
- Änderungen an mandantenübergreifenden Objekten: "keine Änderungen von Repository- und mand.unabh. Cust.-Obj."
- Schutz bzgl. Mandantenkopierer und Vergleichstool: "Schutzstufe 2: kein Überschreiben, keine ext. Verfügbarkeit"
- Einschränkungen beim Starten von CATT und eCATT: "eCATT und CATT nicht erlauben"

Entsprechende Einstellungen sollten im Test- und Akzeptanzsystem gelten. Für andere Mandanten (Entwicklung, Schulung, Demo) sind die Einstellungen geeignet zu definieren.

SAP Informationsquellen

Administratoren müssen sich mit den Auswirkungen der Mandanten-Konfiguration sehr genau vertraut machen. Hinweise auf entsprechende Detail-Dokumentation findet sich in M 2.346 *Nutzung der SAP Dokumentation*,.

Ausführbare Betriebssystemkommandos absichern

Der ABAP-Stack bietet die Möglichkeit an, Betriebssystemkommandos auszuführen. Die Kommandos werden mit den Betriebssystemrechten des technischen Betriebssystembenutzers ausgeführt, unter dem das SAP System abläuft. Dies sind in der Regel weitreichende Administratorrechte.

Der Zugriff auf diese Funktionalität muss daher abgesichert werden. Insbesondere das Anlegen oder Verändern von Kommandos muss verhindert werden. Daher sollten folgende Hinweise umgesetzt werden:

- Die Berechtigungen, externe Betriebssystemkommandos auszuführen (Berechtigung S_LOG_COM) oder zu pflegen, (Berechtigung S_RZL_ADM mit ACTVT=01) sind restriktiv zu vergeben.
- Der Zugriff auf die Transaktion SM49 "Externe Betriebssystemkommandos ausführen" ist auf die berechtigten Administratoren einzuschränken.
- Der Zugriff auf die Transaktion SM69 "Externe Betriebssystemkommandos pflegen" ist auf die berechtigten Administratoren einzuschränken.
- Für die Betriebssystemkommandos besteht die Möglichkeit, die beim Aufruf genutzten Parameterwerte vorzugeben und zu verhindern, dass zusätzliche Parameter angehängt werden können. Von dieser Möglichkeit sollte Gebrauch gemacht werden. Dies trifft insbesondere für selbst definierte Kommandos zu.

Hinweise auf Detailbeschreibungen zum Absichern der Betriebssystemkommandos finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Passwortqualität sicherstellen

Damit die Passwortqualität beim Zugang zum SAP System sichergestellt wird, sind die folgenden Hinweise zu berücksichtigen.

Es sollte eine minimale Passwortlänge definiert werden. Dazu dient der Profilparameter "login/min_password_lng". Es wird ein Wert von 8 Zeichen empfohlen. Dieser Wert stellt gleichzeitig die maximale Passwortlänge des ABAP-Stacks dar.

Für Passwörter sollten Komplexitätskriterien definiert werden. Dies sind über die folgenden Profilparameter einstellbar:

- login/min_password_diff:
  Mindestanzahl der unterschiedlichen Zeichen zwischen neuem und altem Passwort
- login/min_password_digits:
  Mindestanzahl von Ziffern im Passwort
- login/min_password_letters:
  Mindestanzahl von Buchstaben im Passwort
- login/min_password_specials:
  Mindestanzahl von Sonderzeichen im Passwort

Bei der Definition von Komplexitätskriterien ist darauf zu achten, dass konsistente Vorgaben eingestellt werden.

Für Passwörter sollte eine maximale Gültigkeitsdauer vorgegeben werden, so dass eine regelmäßige Passwortänderung erzwungen wird. Dies wird über den Profilparameter "login/password_expiration_time" konfiguriert, der die Anzahl der Tage angibt, nach denen das Passwort zu ändern ist. Empfehlenswert sind Werte zwischen 60 und 90 Tagen.

Es können verbotene Passwörter definiert werden. Diese sind in der Tabelle USR40 über die Transaktion SM31 zu pflegen. Hierüber sollten typische Trivial-Passwörter verhindert werden.

Die eingestellten Werte sind entsprechend der geltenden Passwortrichtlinie zu wählen.

Schutz vor Passwort-Attacken konfigurieren

Es wird empfohlen, das SAP System vor Passwort-Attacken zu schützen, indem nach einer Anzahl von Anmelde-Fehlversuchen die Verbindung unterbrochen wird. Die Anzahl wird durch den Profilparameter "login/fails_to_session_end" konfiguriert.

Um wiederholt angegriffene Benutzerkonten vor weiteren Angriffen zu schützen, wird empfohlen, Benutzerkonten nach einer Anzahl von Anmelde-Fehlversuchen zu sperren. Die Anzahl wird durch den Profilparameter "login/fails_to_user_lock" konfiguriert.

Es muss außerdem entschieden werden, ob gesperrte Benutzerkonten automatisch wieder um Mitternacht entsperrt werden oder ob dies manuell durch den Benutzer-Administrator erfolgen muss. Das Verhalten wird über den Profilparameter "login/failed_user_auto_unlock" gesteuert.

Die eingestellten Werte sind entsprechend der geltenden Passwortrichtlinie zu wählen.

Mehrfachanmeldungen verhindern

SAP Systeme können verhindern, dass das gleiche Benutzerkonto für mehrere parallele Anmeldungen verwendet wird. In der Regel sind in Produktiv-Systemen Mehrfachanmeldungen durch die gleiche Person nicht sinnvoll und sollten daher unterbunden werden. Das Verhalten kann für SAPGui- und RFC-Sitzungen separat gesteuert werden wird über die Profilparameter "login/disable_multi_gui_login" und "login/disable_multi_rfc_login" definiert.

Bevor Mehrfachanmeldungen über RFC unterbunden werden, muss sichergestellt sein, dass parallele Sitzungen mit demselben technischen Benutzerkonto ausgeschlossen sind.

Single Sign-On sicher konfigurieren

Werden mehrere SAP Systeme betrieben, so kann die Benutzeranmeldung über den SAP Single Sign-On (SSO) Mechanismus vereinfacht werden. Eine wiederholte Passwort-Eingabe ist dann nicht mehr notwendig, da nach einem erfolgreichen Login vom SAP System ein Single Sign-On Ticket ausgestellt wird, welches den Zugriff auf andere SAP Systeme ohne erneutes Login erlaubt. Ob und zwischen welchen SAP Systemen der Single Sign-On Mechanismus genutzt wird, muss in der Planungsphase festgelegt werden.

Folgende sicherheitsrelevante Aspekte sind zu bedenken, wenn Single Sign-On verwendet wird:

- Single Sign-On sollte nur zwischen vertrauenswürdigen Systemen konfiguriert werden. Insbesondere Single Sign-On Szenarien über Unternehmens- oder Behördengrenzen hinweg sind unter Sicherheitsgesichtspunkten zu vermeiden.
- Es empfiehlt sich, pro Szenario nur ein System für die zentrale Anmeldung einzusetzen, das SSO-Tickets ausstellt. Alle anderen Systeme sollten SSO-Tickets nur akzeptieren.
- Besonders wichtig ist, dass die Kommunikation zwischen dem Browser des Benutzers und dem SAP System verschlüsselt wird. Ansonsten besteht potentiell die Gefahr, dass Angreifer das SSO-Ticket abhören und damit ohne Anmeldung auf das SAP System zugreifen können.

Folgende Profilparameter regeln die SSO-Konfiguration für ein SAP System:

- login/accept_sso2_ticket:
  System akzeptiert SSO-Tickets.
- login/create_sso2_ticket:

System stellt SSO-Tickets aus.

- login/ticket_expiration_time:
  Gültigkeitsdauer der ausgestellten SSO-Tickets in Stunden
- login/ticket_only_by_https:
  SSO-Tickets werden nur beim Zugriff über HTTPS ausgestellt.
- login/ticket_only_to_host:
  SSO Tickets werden nur bei Zugriffen auf das ausstellende System verwendet.

Für die Konfiguration von SSO sind zusätzliche administrative Tätigkeiten durchzuführen, die über die Transaktionen SSO2, SSO2_ADMIN (SSO2_ACL) und STRUSTSSO2 gemanagt werden können. SAP empfiehlt, die Transaktion SSO2 zu nutzen.

SAP Informationsquellen

Hinweise auf Detailinformationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Neben dem SAP SSO-Mechanismus über Tickets können auch externe Systeme für SSO genutzt werden. Diese müssen dann jedoch über die SNC-Schnittstelle (Secure Network Communication) eingebunden sein. Für Windows-basierte Umgebungen (ab Windows 2000) wird auf die Möglichkeit hingewiesen, Single Sign-On über Kerberos zu nutzen. In diesem Fall erfolgt die Anmeldung nur am Windows-System. Beim Zugriff auf das SAP System ist dann keine Eingabe von Benutzername und Passwort mehr notwendig. Der verwendete Windows-Kerberos SNC-Provider ist standardmäßig und ohne Mehrkosten verfügbar. Es muss jedoch bedacht werden, dass der Windows Kerberos SNC-Provider keine Verschlüsselung der Kommunikation anbietet. Daher ist nur SNC-basierte Authentisierung verfügbar. Ab Windows 2000 besteht jedoch standardmäßig die Möglichkeit, IPSec zwischen Rechnern einzusetzen und so eine generelle Verschlüsselung der Kommunikation zu erreichen. Ob dies eine mögliche Variante ist, um Single Sign-On in einem Unternehmen oder einer Behörde umzusetzen, muss jeweils entscheiden werden.

SAP Informationsquellen

Weitere Maßnahmen zu SNC finden sich in M 5.125 *Absicherung der Kommunikation von und zu SAP Systemen*, SAP Informationsquellen in M 2.346 *Nutzung der SAP Dokumentation*.

Ergänzende Kontrollfragen:

- Wurden alle geplanten IMG-Aktivitäten durchgeführt?
- Ist die Systemänderbarkeit für Produktiv-Systeme deaktiviert?
- Sind die Profil-Parameter entsprechend der Planung angepasst worden?
- Ist die Qualität der Passwörter sichergestellt?
- Sind Mehrfachanmeldungen durch Dialog-Benutzer unterbunden?
- Wird Single Sign-On sicher und wie geplant eingesetzt?

M 4.259 Sicherer Einsatz der ABAP-Stack Benutzerverwaltung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der sichere Einsatz der ABAP-Stack Benutzerverwaltung ist Vorraussetzung für die Systemsicherheit, da damit bestimmt wird, wer prinzipiell Zugriff auf ein SAP System hat. Folgende Aspekte sind beim Einsatz der Benutzerverwaltung mindestens zu bedenken. Je nach Einsatzszenario müssen auch weitere Themen berücksichtigt werden, die durch die spezifischen Anforderungen im Unternehmen oder der Behörde bestimmt werden. Dabei sind auch Anforderungen zu beachten, die sich aus rechtlichen Bestimmungen ergeben.

SAP Informationsquellen

Hinweise auf SAP Dokumente zur Benutzerverwaltung in SAP Systemen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Namenskonvention für Benutzer

Benutzernamen müssen eindeutig sein. Daher ist eine Namenskonvention festzulegen, die dies auch dann garantiert, wenn Personen den gleichen Namen besitzen. In der Regel bestehen im Unternehmen oder der Behörde schon eindeutige Identifikationen für Mitarbeiter, etwa in Form der Personalnummer, die dazu benutzt werden können.

Es ist sinnvoll, Klassen von Benutzern zu bilden (z. B. Interne, Externe, Partner, technische Benutzer) und diese Klassen auch in den Benutzernamen zu kodieren.

Eindeutige Benutzerzuordnung

Durch das Benutzerverwaltungskonzept ist sicherzustellen, dass derselbe Benutzernamen in unterschiedlichen Systemen immer dieselbe Person bezeichnet.

Es ist durch geeignete organisatorische Maßnahmen auszuschließen, dass ein Benutzerkonto durch mehrere Personen genutzt wird (Account-Sharing).

Einrichten eines Notfalladministrators

Für Notfälle sollte ein SAP Konto eingerichtet werden, dass für die Notfalladministration verwendet wird. Es empfiehlt sich, dieses mit einer normalen Bezeichnung zu versehen, damit keine gezielten Angriffe auf dieses Benutzerkonto provoziert werden. Das Konto SAP* darf nicht zur Administration oder Notfalladministration verwendet werden.

Der Notfalladministrator ist in der Regel mit weitreichenden Berechtigungen ausgestattet und ist daher mit einem sicheren Passwort zu versehen. Im Rahmen der Notfallplanung sind Prozeduren zu definieren, wie das Konto zu benutzen ist (siehe M 2.341 *Planung des SAP Einsatzes* und M 6.97 *Notfallvorsorge für SAP Systeme*). Das Passwort des Notfalladministrators sollte an einem sicheren Ort (z. B. Safe) aufbewahrt werden. Der Zugriff auf das Passwort sollte im 4-Augen Prinzip erfolgen.

Absichern der Standardbenutzer

In einem SAP System sind mehrere Standardbenutzer verfügbar, die abgesichert werden müssen. Betroffen sind die Benutzer:

- SAP*
- DDIC
- EARLYWATCH
- SAPCPIC
- TMSADM
- SAPSYS
- WF-BATCH (wird erst durch das automatische Workflow-Customizing erstellt)

Zur Absicherung gehören folgende Aktionen:

- Ändern des Passwortes (siehe auch unten)
- Deaktivieren der Benutzerkennung
- Die Benutzerkennungen sollten nur für kurze Zeit aktiviert werden, um bestimmte Aktivitäten (z. B. System-Update) durchzuführen. Für das geregelte Vorgehen, sind entsprechende Prozesse notwendig. Diese müssen sicherstellen, dass die Benutzerkennungen nach Abschluss der Arbeiten wieder deaktiviert werden.
- Zuordnung der Benutzer zur Gruppe SUPER.

Nachdem Benutzerkennungen deaktiviert wurden, kann es zu Funktionseinbußen kommen. Ob eine zeitweise oder doch dauerhafte Aktivierung notwendig ist, hängt vom Verwendungszweck des Systems ab und muss im Einzelfall entschieden werden. Das zusätzliche Risiko durch einen aktivierten Standardbenutzer mit unter Umständen bekanntem Standardpasswort ist dabei zu berücksichtigen.

Das Löschen der Benutzer SAP* und DDIC wird nicht empfohlen, da diese automatisch z. B. beim Anlegen eines neuen Mandaten neu erzeugt werden. Für den Benutzer SAP* kann dieses Verhalten durch den Profilparameter "logon/no_automatic_user_sapstar" beeinflusst werden. Es wird empfohlen, den Parameter zu aktivieren.

Bevor der Benutzer SAP* deaktiviert wird, muss ein alternatives Benutzerkonto für die Notfalladministration erfolgreich eingerichtet sein.

Bei der Installation neuer Komponenten können zusätzliche Standardbenutzer angelegt werden. Diese sind dann nach der Installation entsprechend abzusichern.

SAP Informationsquellen

Hinweise auf SAP Dokumentationen zum Umgang mit Standardbenutzern in SAP Systemen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Ändern von Standardpasswörtern

Die Standardbenutzer (siehe oben) sind mit Standardpasswörtern ausgestattet. Diese sind zu ändern, um zu verhindern, dass die Benutzerkennungen unbefugt genutzt werden.

Nach der Passwortänderung kann es jedoch dazu kommen, dass Systemfunktionen nicht mehr oder nicht mehr korrekt ausgeführt werden können. Dies ist beispielsweise für die Benutzer TMSADM (siehe auch SAP Hinweis 139854) und SAPCPIC der Fall. Wird die betroffene Systemfunktion häufig genutzt, so muss der Standardbenutzer unter Umständen mit dem Standardpasswort betrieben werden. Dies ist im Rahmen der Risikobewertung zu berücksichtigen.

Für die Benutzer SAP* und DDIC ist zu berücksichtigen, dass diese z. B. beim Erzeugen neuer Mandanten automatisch neu angelegt werden, falls diese Benutzerkennungen gelöscht wurden. Dabei werden die neuen Benutzerkennungen mit den Standardpasswörtern ausgestattet.

Der Report RSUSR003 kann über die Transaktion SE38 dazu genutzt werden, um in allen Mandanten eine Prüfung auf die Existenz, den Sperrstatus und auf Standardpasswörter für die Benutzer SAP*, DDIC, SAPCPIC und EARLYWATCH durchzuführen.

Verwaltungsverfahren

Bei der Benutzerverwaltung ist zu berücksichtigen, welches Verwaltungsverfahren eingesetzt wird. Wird die zentrale Benutzerverwaltung eingesetzt, so sollten Benutzerkennungen nicht lokal angelegt werden.

Die geplanten Prozesse und Verfahren (siehe M 2.341 *Planung des SAP Einsatzes*) für die dezentrale oder zentrale Benutzerverwaltung müssen umgesetzt und eingehalten werden. Die Prozesse sollten dabei auch Regelungen zur Behandlung von Ausnahmen enthalten.

Folgende Aspekte sind für das eingesetzte Verwaltungsverfahren zu berücksichtigen:

- Für die Basis-Administration muss ein spezielles Rollenkonzept entwickelt werden.
- Im Rahmen der Planung des Verwaltungskonzeptes müssen Prozessbeschreibungen zum Änderungsmanagement von Rollen und Berechtigungen erstellt werden. Dabei ist zu berücksichtigen:
  - Die jeweiligen Verantwortlichen für die Geschäftsprozesse müssen in den Zustimmungsprozess für Rollenänderungen und Rollenzuordnungen einbezogen werden.
  - Mit dem SAP Werkzeug "Compliance Calibrator" können Geschäftsprozessrisiken analysiert werden, die möglicherweise dadurch entstehen, dass Rollen verändert werden oder dass Benutzern neue Rollen zugeordnet werden.

Ergänzende Kontrollfragen:

- Wurden die Standardbenutzer abgesichert?
- Wurden die Standardpasswörter verändert?
- Ist die eindeutige Zuordnung zwischen Personen und Benutzerkonten sichergestellt?

M 4.260 Berechtigungsverwaltung für SAP Systeme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Sicherheit der in einem SAP System verarbeiteten Geschäftsdaten wird sehr stark durch die eingestellten Berechtigungen für Benutzer und Administratoren bestimmt. Diese legen fest, welche Funktionen (im SAP Jargon auch Transaktionen genannt) von einem bestimmten Benutzer aufgerufen und damit, welche Daten eingesehen bzw. verändert werden können. Daher sind die konfigurierten Berechtigungen und deren Verwaltung ein sehr wichtiger Bestandteil der Systemsicherheit, vor allem vor dem Hintergrund möglicher Betrugshandlungen durch interne Mitarbeiter.

Das SAP Berechtigungssystem ist sehr flexibel, dadurch aber auch komplex in der Konfiguration. Im Gegensatz zu Betriebssystemen, in denen Berechtigungen direkt auf Objekten (z. B. Dateien) vergeben werden, arbeiten SAP Systeme nach dem Ausweisprinzip: Beim Zugriff auf Funktionen wird geprüft, ob der Benutzer Berechtigungen eines bestimmten Typs besitzt. Ist dies der Fall, wird geprüft, ob die eingetragenen Werte den Anforderungen entsprechen, die zum Ausführen der aufgerufenen Funktion notwendig sind. Die geprüften Berechtigungstypen und Werte werden dabei durch den Programmierer der Funktion bestimmt und können auch die Daten berücksichtigen, die beim aktuellen Aufruf an die Funktion übergeben wurden. Zusätzlich entscheidet zum Schluss der Programmierer einer Funktion, ob er eine eigentlich notwendige Berechtigungsprüfung implementiert oder nicht.

Für die Verwaltung von Berechtigungen sollten die folgenden Empfehlungen berücksichtigt werden. Die Liste ist an die lokalen Bedürfnisse und Anforderungen anzupassen und zu erweitern.

Schulung

Administratoren die für die Verwaltung von Benutzerkennungen, Rollen, Profilen oder Berechtigungen verantwortlich sind, müssen zwingend Schulungen zum SAP Berechtigungskonzept und zur Berechtigungsverwaltung (Vorgehen, Werkzeuge, richtige Verwendung) erhalten oder das entsprechende Verständnis nachweisen. Nur so wird erreicht, dass die Berechtigungsverwaltung versiert durchgeführt werden kann.

Trennen der Verantwortlichkeiten (Vier-Augen-Prinzip)

Das Verwaltungskonzept muss so ausgelegt sein, dass die Verantwortlichkeiten möglichst getrennt werden. Folgendes sollte dabei beachtet werden:

- Es sollte ein Benutzeradministrator vorgesehen werden. Dieser sollte Benutzerkennungen anlegen, verändern und Rollen zuordnen können. Das Anlegen oder Verändern von Rollen oder Profilen darf dem Administrator nicht erlaubt sein. SAP bietet hierzu die Vorlage SAP_ADM_US an.
- Es sollte ein Rollenadministrator vorgesehen werden, der Rollen anlegen und verändern kann, der jedoch keine Benutzer oder Profile anlegen oder verändern darf. SAP bietet hierzu die Vorlage SAP_ADM_AU an.

- Es sollte ein Profiladministrator vorgesehen werden. Dieser darf für vorhandene Rollen Profile generieren, die keine kritischen Systemberechtigungen enthalten (etwa S_USER*), da diese zur Benutzer- und Rollenverwaltung berechtigen. SAP bietet hierzu die Vorlage SAP_ADM_PR an.
- Diese Administratoren sind der Gruppe SUPER zuzuordnen.
- Es sollte ein Administrator-Administrator definiert werden. Dieser verwaltet die Benutzer-, Rollen-, und Profil-Administratoren. Der Administrator-Administrator sollte dem Profil S_A.SYSTEM zugeordnet werden, das zur Verwaltung von Benutzern in der Gruppe SUPER benötigt wird. Der Administrator-Administrator sollte nur im Vier-Augen-Prinzip genutzt werden. Er kann beispielsweise durch den Benutzer-Administrator gesperrt und bei Bedarf für die Dauer der Nutzung entsperrt werden.

Durch die Trennung (sofern technisch richtig umgesetzt) wird erreicht, dass sich die Administratoren nicht selbst Berechtigungen zuordnen können und für sie auf diese Weise nur die ihnen zugeordneten Aufgaben ausführbar sind.

In kleineren Unternehmen oder Behörden kann es aufgrund eingeschränkter Personalverfügbarkeit vorkommen, dass keine Trennung vorgenommen werden kann und alle Aufgaben durch eine Person ausgeführt werden. Alle Daten im SAP System können dann durch den Administrator unbemerkt eingesehen und verändert werden. Generell ist dies als sicherheitskritisch zu bewerten, so dass zusätzliche Kontrollen notwendig sind. Gleiches gilt allgemein auch im Kontext wichtiger finanz- und bilanzrelevanter Prozesse sowie bei der Verarbeitung personenbezogener Daten, wo beispielsweise eine entsprechende Funktionstrennung vorhanden sein muss. Kann diese nicht erreicht werden, müssen geeignete Kontrollen auf organisatorischer Ebene definiert und deren Durchführung sichergestellt werden. Entsprechende Prüfungen auf das Vorhandensein von Kontrollen finden beispielsweise auch im Kontext von Sarbanes Oxley Act bezogenen Prüfungen statt.

Die von SAP vorgegebenen und ausgelieferten Rollen sind sorgfältig gegen die eigenen Anforderungen zu prüfen und anzupassen.

SAP Informationsquellen

Hinweise auf SAP Dokumentationen zum Aufbau der Berechtigungsverwaltung und zu relevanten Berechtigungen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Werkzeuge zur Berechtigungsverwaltung

Berechtigungen, Profile und Rollen können auch manuell verwaltet werden. Von diesem Vorgehen wird jedoch aus Sicherheitsgründen dringend abgeraten, da aufgrund der zu verwaltenden Objektmengen bei manueller Pflege immer Berechtigungsprobleme entstehen. Der Einsatz des Profilgenerators (Transaktion PFCG) wird daher dringend empfohlen. Insbesondere dürfen dann keine manuellen Veränderungen an den Profilen erfolgen.

Administratoren müssen sich mit den Mechanismen und Verfahren beim Einsatz des Profilgenerators vertraut machen, damit eine korrekte Berechtigungsvergabe erfolgt. So muss beispielsweise der Profilgenerator zunächst über die Transaktion SU25 initialisiert werden. Insbesondere die

Verwendung und Pflege von Prüfkennzeichen (Transaktion SU24) muss bekannt sein. In Testläufen können fehlende Berechtigungen (diese sind beispielsweise über die Transaktion SU53 oder über Berechtigungstraces mit ST01 feststellbar) erkannt werden.

Neben den systeminternen Werkzeugen zur Berechtigungsverwaltung werden von Drittherstellern auch externe Werkzeuge zur Benutzer- und Berechtigungsverwaltung angeboten. Diese sind in der Regel mit einer komfortableren Benutzungsschnittstelle ausgestattet, da diese direkt auf dem Betriebssystem ablaufen. Ob solche Werkzeuge als Alternative zu den systeminternen Werkzeugen genutzt werden, ist jeweils im Einzelfall unter Kosten/Nutzen-Aspekten zu entscheiden.

SAP Informationsquellen

Hinweise auf SAP Dokumentationen zur Berechtigungsverwaltung mit dem Profilgenerator finden sich in M 2.346 *Nutzung der SAP Dokumentation.*

Applikationsspezifische Berechtigungsverwaltung

Einige Produkte und Applikationen nutzen zusätzlich zum SAP Standardberechtigungskonzept auch noch eigene Berechtigungskonzepte und -verwaltungswerkzeuge (z. B. das SAP Customer Relationship Management, mySAP CRM oder das Modul Human Capital Management, HCM). Dies ist bei der Verwaltung auch zu berücksichtigen, da zusätzliche Verwaltungsschritte und -arbeiten notwendig sind. Insbesondere muss bedacht werden, dass das Produkt oder die Applikation nur dann sicher betrieben werden kann, wenn auch die applikationsspezifischen Berechtigungen über die applikationsspezifischen Verwaltungswerkzeuge sicher konfiguriert wurden. Generell ist dabei auch auf minimale Berechtigungen, Rollentrennung und auf Trennung von Aufgaben und Verantwortlichkeiten zu achten. So darf beispielsweise in einem CRM-System ein Warenbestellkorb nicht durch die gleiche Person zur Bestellung freigegeben werden, die den Warenkorb erzeugt hat.

Generell spielt auf Applikationsebene das Thema Geschäftsrisikomanagement eine wichtige Rolle: Bei der Vergabe von Berechtigungen definiert unter anderem auch das Risikomanagement die Kriterien für die Vergabe von Berechtigungen.

Ergänzende Kontrollfragen:

- Ist ein Vier-Augen-Prinzip für die Berechtigungsverwaltung umgesetzt?
- Wird der Profilgenerator zur Berechtigungsvergabe richtig genutzt?
- Wurden applikationsspezifische Berechtigungsmechanismen berücksichtigt und sicher konfiguriert?

M 4.261 Sicherer Umgang mit kritischen SAP Berechtigungen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Berechtigungen, die im Sinne der Sicherheit oder aus rechtlicher oder betriebswirtschaftlicher Sicht kritische Operationen erlauben, werden von SAP "kritische Berechtigung" genannt. Betroffen sind z. B. Operationen, die zu Betrug führen können oder über die wichtige Daten und Konfigurationen gelesen oder modifiziert werden können.

Die Vergabe von kritischen SAP Berechtigungen muss generell mit besonderer Sorgfalt erfolgen. Der Umgang mit kritischen SAP Berechtigungen ist daher im Vorfeld zu planen. Organisatorische und technische Maßnahmen sowie Prozesse müssen dann sicherstellen, dass das gewünschte Sicherheitsniveau umgesetzt wird. Im Folgenden wird bewusst keine Liste mit kritischen SAP Berechtigungen angegeben, da diese immer unvollständig wäre und damit Administratoren in falscher Sicherheit wiegt. In der Regel wird dann darauf verzichtet, die Liste zu prüfen und zu erweitern. Die Identifikation kritischer SAP Berechtigungen für den konkreten Einsatz eines SAP Systems ist jedoch ein wichtiger Schritt, der auf jeden Fall durchgeführt werden muss.

Kritische SAP Berechtigungen, Profile, Rollen identifizieren

Kritische SAP Berechtigungen hängen aufgrund des SAP Berechtigungskonzeptes auch von den Feldern und Feldwerten von Berechtigungsobjekten ab. Dies gilt insbesondere für Berechtigungen, die in Applikationen oder Modulen zum Einsatz kommen und damit aus betriebswirtschaftlicher Sicht als kritisch zu betrachten sind. Es wird daher empfohlen, kritische Felder in Berechtigungsobjekten zu identifizieren, um so die betroffenen Berechtigungsobjekte zu identifizieren. Nur so kann überhaupt eine spätere Prüfung erfolgen, und nur bei Kenntnis der Berechtigungsobjekte kann die Prüfung automatisiert werden. Beispiele für kritische Felder in Berechtigungsobjekten sind Felder für Kosten-Center, Buchungskreis, Profit-Center oder Werk.

Kritische SAP Berechtigungen sind auch alle Berechtigungen, die im Rahmen der SAP System-Administration verwendet werden. Dies sind alle Berechtigungen die von Berechtigungsobjekten abgeleitet sind und mit dem Präfix "S_" beginnen.

Neben Berechtigungen lassen sich auch kritische Profile und Rollen identifizieren, die bereits im Auslieferungszustand enthalten sind. Alle Profile, die auf "_ALL" enden, sind als kritisch anzusehen, da damit in der Regel alle Berechtigungen erteilt werden, die für einen Teilbereich im System, einer Applikation oder eines Moduls relevant sind. Alle Rollen, die die Zeichenkette "ADM" enthalten, sind als kritisch anzusehen, da diese in der Regel administrative Rollen bezeichnen.

Bei der Identifikation kritischer SAP Berechtigungen, Profile und Rollen ist zu bedenken, dass SAP für Namen zwar ein Konzept vorschlägt, dies aber

durch Applikationen oder eigene Entwicklungen nicht immer berücksichtigt wird. Daher können auch kritische Berechtigungen, Profile und Rollen bestehen, die nicht in das vorgenannte Namensschema passen.

Manuell ist die Identifikation kritischer SAP Berechtigungen insgesamt schwierig. Es sind jedoch von SAP und Drittherstellern Werkzeuge verfügbar, die automatisiert auf kritische Berechtigungen prüfen können. Dabei sind die kritischen SAP Berechtigungen in der Regel durch den Hersteller der Prüfsoftware vordefiniert.

SAP Informationsquellen

Hinweise auf SAP Dokumentationen zu Berechtigungsprüfungen finden sich in M 2.346 *Nutzung der SAP Dokumentation*. Bei der Identifikation kritischer Berechtigungen ist entsprechendes Wissen über die zugrunde liegenden Berechtigungsprüfungen notwendig.

Anpassen kritischer SAP Berechtigungen, Profile, Rollen

Sind die kritischen SAP Berechtigungen, Profile und Rollen identifiziert, so sollten diese gemäß der Berechtigungsplanung angepasst werden. Insbesondere bei der Anpassung von Profilen und Rollen zur Systemverwaltung müssen die damit verbundenen Effekte für Systemfunktionen berücksichtigt werden. Nach der Anpassung ist daher zu prüfen, ob das gewünschte Systemverhalten erreicht wurde oder ob es zu Fehlfunktionen kommt. Dieser Anpassungsprozess kann bei stärkeren Veränderungen an den vorgegeben Berechtigungen, Profilen oder Rollen aufwendig und zeitintensiv sein und sollte nicht im Produktivsystem durchgeführt werden.

Verwendung kritischer SAP Systemberechtigungen einschränken

Im Rahmen der Berechtigungsplanung müssen die Regeln für den Umgang mit kritischen SAP Berechtigungen, Profilen und Rollen festgelegt werden. Folgende Empfehlungen sind dabei zu berücksichtigen:

- Die Profile SAP_ALL, SAP_NEW* und S_DEVELOP* dürfen in einem Produktivsystem nicht genutzt werden.
- Administrative Berechtigungen, Profile und Rollen dürfen entsprechend der Berechtigungsplanung (siehe M 2.342 *Planung von SAP Berechtigungen*) nur an administrative Benutzer vergeben werden. Auf ausreichende Rollentrennung ist dabei zu achten.

SAP Informationsquellen

Hinweise auf weitere Informationen dazu finden sich in, M 2.346 *Nutzung der SAP Dokumentation*.

Liste mit kritischen SAP Berechtigungen pflegen

Sind die kritischen SAP Berechtigungen identifiziert, so empfiehlt es sich, diese Liste im SAP System zu pflegen. Dann kann automatisiert geprüft werden, welchen Benutzern kritische SAP Berechtigungen zugeordnet wurden. Die Pflege der Liste kritischer SAP Berechtigungen erfolgt über die Transaktion SU96. Über den Report "RSUSR009" lassen sich die Benutzer anzeigen, die eine der kritischen SAP Berechtigungen besitzen.

Auch bestimmte Kombinationen von unkritischen SAP Berechtigungen können kritisch sein, da sie beispielsweise in der Kombination ermöglichen, dass eine oder mehrere als kritisch eingestufte Transaktionen aufgerufen werden können. Ein SAP System bietet hier die Möglichkeit an, automatisiert nach Benutzern zu suchen, die die Berechtigungen besitzen, bestimmte Kombinationen von Transaktionen aufzurufen. Dazu ist über die Transaktion SU98 (Pflege der Tabelle SUKRI) eine Liste der kritischen Kombinationen zu pflegen. Über den Report "RSUSR008" lassen sich dann die Benutzer identifizieren, die die kritischen SAP Berechtigungskombinationen besitzen.

In neueren SAP Systemen (ab Version 6.20) sollte der Report RSUSR008_009_new genutzt werden, der die Funktionen der Reports RSUSR008 und RSUSR009 ersetzt.

Die im Auslieferungszustand eines SAP Systems enthaltenen Listen für die kritischen SAP Berechtigungen und Transaktionskombinationen sind nur als Beispiel anzusehen und sollten nicht für die Überprüfungen genutzt werden. Die Listen müssen selbst aufgebaut und gepflegt werden. Diese können beispielsweise auch bei Sarbanes Oxley Act bezogenen Prüfungen begutachtet werden.

In diesem Kontext bietet SAP für die NetWeaver Plattform mit dem Compliance Calibrator kostenpflichtig ein entsprechendes Zusatz-Prüfwerkzeug an, so dass entsprechende Risiken automatisiert erkannt werden können. Prüfwerkzeuge sind auch von Drittherstellern erhältlich.

Ergänzende Kontrollfragen:

- Wurden kritische SAP Berechtigungen, Profile und Rollen identifiziert?
- Wurde ein Konzept für den Umgang mit kritischen SAP Berechtigungen erstellt?
- Werden die Tabellen mit kritischen SAP Berechtigungen und kritischen Kombinationen von Transaktionen sinnvoll gepflegt?

M 4.262 Konfiguration zusätzlicher SAP Berechtigungsprüfungen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Ein SAP System erlaubt es, die vorkonfigurierten Berechtigungsprüfungen (siehe dazu M 2.342 *Planung von SAP Berechtigungen*) zu verändern. Berechtigungsprüfungen können deaktiviert werden. Es können auch zusätzliche Berechtigungsprüfungen erfolgen. Im Rahmen der Berechtigungsplanung ist diese Möglichkeit zu berücksichtigen. Generell ist bei Veränderungen an den Berechtigungsprüfungen Folgendes zu bedenken:

Deaktivieren von Berechtigungsprüfungen

Werden vorhandene Berechtigungsprüfungen deaktiviert, so kann dies die Sicherheit des SAP Systems gefährden, da damit Zugriffskontrollen abgeschaltet werden. Bevor Prüfungen deaktiviert werden, müssen die Auswirkungen auf die Sicherheit sorgfältig geprüft werden.

SAP Informationsquellen

Hinweise auf weitere Informationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Erzeugen von Transaktionen für den Start von Programmen oder Reports

Programme und Reports können beispielsweise über die Transaktion SE38 (ABAP Editor) gestartet werden. Nicht jedem Programm oder Report ist jedoch ein Transaktionscode zugeordnet. Sollen bestimmte Programme oder Reports Benutzern verfügbar gemacht werden, so empfiehlt sich, diese über eine Transaktion verfügbar zu machen. Dies hat den Vorteil, dass der Zugriff auf die Transaktion und damit das Programm oder den Report über Berechtigungen vom Typ S_TCODE geschützt werden können. Zusätzlich kann der Zugriff auf die Transaktion SE38 gesperrt werden, da damit prinzipiell beliebiger Code ausgeführt werden kann.

Auch bei diesem Vorgehen ist zu beachten, dass weiterhin die durch den Profilgenerator erzeugten Berechtigungen zum Aufruf von Programmen oder Reports gepflegt werden müssen. Dazu sind die vom Berechtigungsobjekt S_PROGRAM abgeleiteten Berechtigungen in den Rollen-Berechtigungsprofilen entsprechend der Berechtigungsplanung zu modifizieren.

Einsatz von Parametertransaktionen

Über neu angelegte Parametertransaktionen können für Transaktionen Werte oder Wertebereiche für die Aufrufparameter vorgegeben werden. Die neu angelegten Parametertransaktionen (Transaktion SU93) können dann über eigene Berechtigungen (Berechtigungsobjekt S_TCODE) zugriffsbeschränkt werden.

Es ist in diesem Zusammenhang wichtig zu berücksichtigen, dass der Einsatz von Parametertransaktionen nicht als Sicherheitsverfahren geeignet ist, um den Zugriff auf Funktionen der Transaktion oder auf Daten zu beschränken. Generell muss der Zugriff, beispielsweise auf Programme, Reports oder

Tabellen, immer über die entsprechenden Berechtigungsobjekte (S_PROGRAM für Programme und Reports, S_TABU_DIS für Tabellen) eingeschränkt werden.

Anpassen der ABAP-Berechtigungsgruppen

Für Programme, Reports und Tabellen können so genannte Berechtigungsgruppen definiert werden. Damit kann eine Gruppierung erfolgen, so dass der Zugriff auf die Programme, Reports oder Tabellen einer Gruppe über ein Berechtigungsobjekt gesteuert werden kann.

Folgendes ist beim Einsatz von ABAP-Berechtigungsgruppen zu beachten:

- Der Zugriff wird immer auf alle Objekte einer Gruppe reglementiert.
- Die Berechtigungsgruppe stellt eine zusätzliche Prüfung dar. Die normalen Berechtigungsprüfungen, die das Programm oder der Report durchführt, werden davon nicht berührt.
- Werden Berechtigungsgruppen genutzt, so kann in der Planung mit einer groben Gruppierung, etwa bezüglich einzelner Applikationen oder Module, begonnen werden. Diese können dann entsprechend dem gewünschten Schutzbedarf weiter verfeinert werden.
- Die genaue Funktionsweise von Berechtigungsgruppen und deren Verwaltung muss Planern und durchführenden Administratoren bekannt sein.

SAP Informationsquellen

Hinweise auf weitere Informationen zur Konfiguration von Berechtigungsgruppen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Eigene zusätzliche Berechtigungsobjekte

Werden im Unternehmen oder der Behörde eigene (ABAP-) Programme entwickelt oder der Programm-Code vorhandener Programme modifiziert, so können auch Berechtigungsprüfungen für neue, selbst definierte Berechtigungsobjekte eingebaut werden. Damit diese durch den Profilgenerator berücksichtigt werden, müssen die Prüfkennzeichen über die Transaktion SU24 definiert und entsprechend angepasst werden. Dies ist im Rahmen der Change-Management Prozesse zu umzusetzen.

Veränderungen dokumentieren

Alle Veränderungen an der Berechtigungsprüfung sind zu dokumentieren.

Ergänzende Kontrollfragen:

- Werden Berechtigungsprüfungen nur nach sorgfältiger Prüfung deaktiviert?
- Werden für Programme und Reports Transaktionen erzeugt und die Zugriffsberechtigungen restriktiv vergeben?
- Werden ABAP-Berechtigungsgruppen sinnvoll eingesetzt?

M 4.263 Absicherung von SAP Destinationen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Ein SAP System kann neben der Server-Rolle, in der es seine Funktionen zum Zugriff anbietet, auch die Client-Rolle annehmen, in der es auf Funktionen anderer SAP Systeme zugreift. Destinationen beschreiben dabei die unterschiedlichen Zielsysteme und enthalten alle zum Zugriff notwendigen Informationen. Generell sind dies der Rechnername oder die IP-Adresse, das zu verwendende Protokoll und Nummer des Kommunikationsports, die die Netzverbindung zum Zielsystem beschreiben.

Für Destinationen können aber auch Authentisierungsinformationen hinterlegt werden. Beim Zugriff auf die Destination werden diese dann zur Anmeldung am Zielsystem genutzt. Sind keine Authentisierungsinformationen hinterlegt, so müssen diese durch den aufrufenden Benutzer angegeben werden. Die entfernte Ausführung erfolgt dann unter den Berechtigungen des angegebenen Benutzers. In diesem Zusammenhang werden im Kontext von Destinationen, auf die über RFC (Remote Function Call) zugegriffen wird, üblicherweise folgende Begrifflichkeiten verwendet:

- RFC-Benutzer: Der Benutzer, der im Server-System aktiv ist und bestimmte Berechtigungen besitzt.
- RFC-Service-Benutzer: Ein RFC-Benutzer wird dann Service-Benutzer genannt, wenn die Anmeldedaten (Benutzer und Kennwort) beim Client gespeichert sind.

Destinationen werden in einer mandantenunabhängigen Tabelle gehalten, daher hat jeder Benutzer Zugriff auf alle Destinationen im SAP System. Somit muss der Zugriff auf die Destinationen abgesichert werden. Folgende Empfehlungen sind für Destinationen zu berücksichtigen:

Speichern von Authentisierungsinformationen

Authentisierungsinformationen sollten nur dann hinterlegt werden, wenn dies nicht zu vermeiden ist. Es ist dabei abzuwägen, ob der Schutz des benutzten Passwortes oder der Schutz des Zielsystems vor unberechtigten Zugriffen überwiegt. Es ist zu beachten, dass für RFC-Destinationen, die aus Programmen heraus genutzt werden, die Authentisierungsinformationen hinterlegt werden müssen, sofern das Server-System nicht für die so genannte Trusted-RFC-Kommunikation konfiguriert ist, so dass generell alle RFC-Aufrufe aus den vertrauten SAP System ohne Authentisierung erfolgen können.

Werden Authentisierungsinformationen hinterlegt, so sollte ausschließlich ein Benutzer vom Typ Kommunikation gewählt werden. Insbesondere sollten keine Dialog-Benutzer eingetragen werden, da sonst über die Destination eine interaktive Anmeldung ohne Passworteingabe möglich ist.

Die Möglichkeit, Passwörter unverschlüsselt zu speichern, sollte nicht benutzt werden.

Zugriff auf Destinationen

Der Zugriff auf Destinationen muss eingeschränkt werden, so dass nur berechtigte Benutzer darauf zugreifen können.

Der Zugriff auf Destinationen kann über das Berechtigungsobjekt S_ICF gesteuert werden. Folgende Berechtigungsfelder sind für das Berechtigungsobjekt definiert, die für die Zugriffssteuerung benutzt werden:

- ICF_FIELD: Typ des zu schützenden Objekts
  Dieses Feld kann folgende Werte beinhalten:
  - SERVICE: für Verwendung von ICF-Services
  - DEST: für Verwendung von RFC-Destinationen (ab 6.20)
- ICF_VALUE: Wert des zu schützenden ICF-Objektes
  Dieses Feld enthält den Wert des entsprechenden Objektes. Die Werte, die geschützt werden sollen, werden in der Transaktion SICF für ICF-Services und in der Transaktion SM59 für RFC-Destinationen gepflegt.

Folgendes ist dabei zu beachten:

- Destinationen müssen nach Einsatzszenarien gruppiert werden. Benutzern kann dann der Zugriff auf alle im Szenario benötigten Destinationen erlaubt werden. Probleme treten jedoch dann auf, wenn Destinationen in mehreren Szenarien eingesetzt werden, da pro Destination nur eine Zuordnung zu genau einer Gruppe möglich ist. In diesem Fall muss eine weitere Unterteilung erfolgen.
- Der Zugriff auf Destinationen mit unterschiedlichem Schadenspotential muss über getrennte Berechtigungen gesteuert werden.

Es ist zu bedenken, dass eine Destination für viele Zwecke genutzt werden kann. Der Zugriffsschutz kann daher nur als Einstiegshürde dienen. Schlussendlich muss der Schutz des Zielsystems durch die aufgerufenen Funktionen selbst und die Berechtigungsvergabe im Zielsystem erfolgen.

Dies gilt insbesondere für Destinationen, auf die über Trusted-RFC zugegriffen wird (dann auch "Trusted Destination" genannt). In diesem Fall werden die Berechtigungen über die Berechtigungsobjekte S_RFC und S_RFCACL gesteuert.

SAP Informationsquellen

Hinweise auf Detailinformationen zur Zugriffssteuerung auf Destinationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Unbenutzte Destinationen absichern

Für nicht benutzte Destinationen muss entschieden werden, ob diese nur vorübergehend oder gar nicht mehr genutzt werden. Im ersten Fall sind die Destinationen zu deaktivieren, im zweiten Fall sind die Destinationen zu löschen.

Übertragen von Destinationen in andere Systeme

Werden Destinationen von einem System in ein anderes System übertragen, so werden auch die in Destinationen gespeicherten Authentisierungsdaten übertragen. Diese Destinationen können dann im System, in das sie importiert wurden, sofort zum erfolgreichen Zugriff auf das in der Destination angegebene Zielsystem benutzt werden. Dies ist beim Übertragen von Destinationen (z. B. bei Systemkopien) zu berücksichtigen.

Zugriff auf Destinationspflege und -tabelle einschränken

Die Pflege von Destinationen erfolgt über die Transaktion SM59. Es wird empfohlen, den Zugriff auf diese Transaktion auf die berechtigten Administratoren einzuschränken (Berechtigungsobjekt S_TCODE).

Es ist zu bedenken, dass die RFC-Destinationsdaten in der Tabelle RFCDES abgelegt werden. Hinterlegte Passwörter sind dabei kodiert gespeichert, im SAP System sind jedoch alle Informationen vorhanden, um die Passwörter zu dekodieren. Der direkte Tabellenzugriff ist daher ebenso einzuschränken (siehe M 4.264 *Einschränkung von direkten Tabellenveränderungen in SAP Systemen*).

THOST Tabelle absichern

In der Tabelle THOST werden symbolische Rechnernamen (SAP Name), die innerhalb des SAP Systems verwendet werden, auf DNS-Rechnernamen (Netz-Name) abgebildet. Der Zugriff auf die Tabellenpflege (Transaktion SM55 oder über SE16) muss daher auf die berechtigten Administratoren eingeschränkt werden (Berechtigungsobjekt S_TCODE).

Auf die Konsistenz der SAP Namen mit den Netz-Namen ist zu achten, damit auf die jeweils richtigen IT-Systeme zugegriffen wird.

Ergänzende Kontrollfragen:

- Werden Benutzer-Anmeldeinformationen für Destinationen nur dann gespeichert, wenn andere Lösungen nicht in Frage kommen?
- Sind alle gespeicherten Benutzer für Destinationen Service-Benutzer im Zielsystem?
- Ist der Zugriff auf Destinationen auf die berechtigten Benutzer eingeschränkt?
- Ist der Zugriff auf die Destinationspflege eingeschränkt?

M 4.264 Einschränkung von direkten Tabellenveränderungen in SAP Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Alle Daten eines SAP Systems werden in den Tabellen der Datenbank des SAP Systems gehalten. Bei der Nutzung erfolgen die Tabellenveränderungen z. B. durch die aufgerufenen Transaktionen, Programme oder RFC-Bausteine.

Berechtigungen auf Tabellen-Zugriffstransaktionen einschränken

Im SAP System besteht die Möglichkeit, auch direkt auf die Inhalte von Tabellen lesend oder verändernd zuzugreifen. Der Zugriff auf Tabellen und Tabelleninhalte kann durch unterschiedliche Transaktionen erfolgen. Dies sind beispielsweise SE16 Data Browser, SE80 Workbench, SE84 Repository Browser, SM30 Pflege Tabellensichten, SM31 Pflege Tabellen, SE11 Data Dictionary, SQVI Quick Viewer.

Je nach Version des SAP Systems und je nachdem, welche Applikationen und Module installiert sind, können auch zusätzliche Transaktionen oder Reports existieren, die direkte Tabellenzugriffe erlauben.

Der Zugriff auf die oben genannten Transaktionen sollte mindestens eingeschränkt werden, so dass nur die berechtigten Administratoren oder Benutzer diese aufrufen können. Die Liste der Transaktionen, die aus diesem Grund zugriffsbeschränkt werden sollten, muss entsprechend der lokalen Systemausprägung erweitert werden. Der Zugriff wird über das Berechtigungsobjekt S_TCODE konfiguriert.

Es wird empfohlen, regelmäßig zu prüfen, welche Benutzer auf die in diesem Sinne kritischen Transaktionen zugreifen können. Dazu kann beispielsweise das Benutzer-Informationssystem (Transaktion SUIM) genutzt werden, über das Benutzer nach unterschiedlichen Suchkriterien aufgelistet werden können.

Über die Transaktion S_BCE_68001398 können direkt die Benutzer aufgelistet werden, die auf eine bestimmte Transaktion Zugriff besitzen. Diese Transaktion kann für Einzeltests benutzt werden.

Berechtigungen für den Tabellenzugriff konfigurieren

Können die Transaktionen für den direkten Tabellenzugriff nicht beschränkt werden, so besteht die Möglichkeit, Tabellenzugriffe über direkte Berechtigungen auf Tabellen zu steuern. Die dabei benutzten Berechtigungsobjekte sind S_TABU_DIS, S_TABU_CLI und S_TABU_LIN. Über das Berechtigungsobjekt S_TABU_DIS können Berechtigungen auf mandantenbezogene Tabellen-Gruppen vergeben werden. Diese werden in der Tabelle TBRG definiert und fassen einzelne Tabellen zu Gruppen zusammen. Für jede Tabellen-Gruppe wird über die Tabelle TDDAT eine zugehörige Berechtigungsgruppe definiert. Für die Zugriffssteuerung werden die Namen der Tabellen-Berechtigungsgruppen als Werte in den Parameter DIBERCLS aufgenommen. Die erlaubten Operationen werden über den Parameter ACTVT gesteuert. Über das Berechtigungsobjekt S_TABU_CLI können analog Berechtigungen auf mandantenunabhängige Tabellen-Gruppen vergeben werden.

Es ist unbedingt notwendig, Berechtigungsobjekte S_TABU_DIS und S_TABU_CLI für die Zugriffskontrolle auf Tabellen einzusetzen, wenn der Zugriff auf Transaktionen, die direkten Tabellenzugriff erlauben, nicht ausgeschlossen ist.

Mittels S_TABU_LIN lassen sich Berechtigungen auf einzelne Tabellenzeilen vergeben. Dieser Mechanismus erfordert jedoch zusätzliche Customizing-Einstellungen. Hierzu müssen so genannte Organisationskriterien definiert und aktiviert werden. Auf Grund der Komplexität der Definition der Autorisierungsreichweiten wird dieses Objekt in der Praxis eher selten verwendet.

Parametertransaktionen

Eine häufig genutzte Variante, den Zugriff auf bestimmte Tabellen zuzulassen, ist die Definition von Parametertransaktionen. Dadurch werden Transaktionen definiert, die andere Transaktionen mit vordefinierten Werten aufrufen. Im vorliegenden Fall wird dann die Transaktion SE16 direkt mit dem gewünschten Tabellennamen aufgerufen. Der Tabellenname wird dann als Wert für den Parameter "DATABROWSE-TABLENAME" in den Vorschlagswerten definiert. Parametertransaktionen werden über die Transaktion SE93 definiert. Bei diesem Vorgehen ist zu beachten, dass trotzdem die Zugriffsberechtigungen für Tabellen über S_TABU_DIS vergeben werden müssen, da Parametertransaktionen nicht zur Zugriffssteuerung geeignet sind.

SAP Informationsquellen

Hinweise auf SAP Dokumentationen dazu finden sich in M 2.346 *Nutzung der SAP Dokumentation.*

Ergänzende Kontrollfragen:

- Sind die Berechtigungen für den direkten Tabellenzugriff eingeschränkt?

M 4.265 Sichere Konfiguration der Batch-Verarbeitung im SAP System

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Im Rahmen der Hintergrundverarbeitung (Batch-Verarbeitung) werden in der Regel Abläufe (Batch-Jobs) automatisiert durchgeführt. Zusätzlich können Arbeiten zeitgesteuert ausgeführt werden. Folgendes ist bei der Konfiguration zu bedenken:

- Batch-Jobs werden über die Transaktion SM36 gesteuert. Auf diese Transaktion sollten nur berechtigte Batch-Administratoren Zugriff besitzen.
- Über die folgenden Berechtigungsobjekte erfolgt die Verwaltung der Batch-Verarbeitung. Die Vergabe der Berechtigungen ist generell über das Berechtigungskonzept zu regeln.
  - Die Ausprägung des Berechtigungsobjektes S_BTCH_ADM mit Wert "Y" ermöglicht Vollzugriff auf die Batch-Administration.
    Es ist zu beachten, dass keine weiteren Einschränkungen erfolgen können. Ein Benutzer mit dieser Berechtigung kann immer alle Verwaltungsoperationen ausführen und darf nur an wenige Administratoren (z. B. Batch-Verwalter, Stellvertreter) vergeben werden.
  - Die Ausprägung des Berechtigungsobjektes S_BTCH_JOB mit Wert "LIST" ermöglicht es einem Batch-Verwalter, die von Batch-Jobs erzeugten Spool-Aufträge anzuzeigen. Da darin die Ausgabedaten des Batch-Jobs enthalten sind, muss im Rahmen des Berechtigungskonzeptes entschieden werden, unter welchen Umständen und durch wen diese Berechtigung verwendet werden darf.
  - Benutzer können immer - ohne besondere Berechtigungen besitzen zu müssen - eigene Jobs erzeugen und verwalten. Folgende Berechtigungsobjekte können für spezielle Operationen verwendet werden, die ohne die Berechtigung nicht möglich sind:
    - S_BTCH_JOB: Erlaubt je nach Wert-Einstellung Folgendes:
      - Wert "DELE": Jobs anderer Benutzer löschen
      - Wert "LIST": Spool-Aufträge anzeigen
      - Wert "PROT": Job-Protokolle ansehen, auch für andere Benutzer
      - Wert "SHOW": Job-Details anzeigen
      - Wert "RELE": Jobs anderer Benutzer freigeben

      Da es sich bei den betroffenen Operationen um kritische Operationen handelt, muss die Verwendung sorgfältig geplant werden. In der Regel dürfen diese Berechtigungen nicht an normale Benutzer vergeben werden.

  - S_BTCH_NAM: Ein Benutzer kann Batch-Jobs unter den Berechtigungen eines anderen Benutzers ausführen. Die Benutzer, unter denen der Batch-Job ausgeführt werden kann, sind in der Berechtigung anzugeben. Die Vergabe der Berechtigung ist unter Sicherheitsgesichtspunkten als kritisch zu betrachten und nur für Batch-Administratoren sinnvoll, um beispielsweise Batch-Jobs unter technischen Benutzern ablaufen zu lassen.

- Da die Batch-Verarbeitung im Hintergrund und automatisiert erfolgt, findet sie in der Regel unbemerkt statt. Auswirkungen, hervorgerufen durch unautorisierte Veränderungen an der Batch-Verarbeitung, können daher längere Zeit unbemerkt bleiben. Eine restriktive Berechtigungsvergabe ist daher notwendig.
- Die Hintergrund-Verarbeitung wird in der Regel unter den Berechtigungen des Benutzers durchgeführt, der einen Batch-Job erzeugt. Insofern greifen die konfigurierten Berechtigungen des Benutzers.
- Werden Batch-Jobs unter den Berechtigungen technischer Benutzer ausgeführt, so sind die Berechtigungen der technischen Benutzer zu beschränken. Es empfiehlt sich nicht, einen technischen Batch-Benutzer mit dem Profil SAP_ALL auszustatten.
- Der Zugriff auf die Verwaltung der Batch-Verarbeitung sollte nur für die berechtigten Administratoren möglich sein.
- Durch die Batch-Verarbeitung kann Last auf einem SAP System erzeugt werden. Es muss daher entschieden werden, ob normale Benutzer Batch-Jobs starten dürfen oder ob diese durch den Batch-Administrator freigegeben und eingeplant werden, nachdem der Batch-Job vom Benutzer erzeugt wurde.

SAP Informationsquellen

Hinweise zu SAP Dokumentationen zur Batch-Verarbeitung finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Ergänzende Kontrollfragen:

- Ist die Batch-Job-Verwaltung nur für berechtigte Administratoren möglich?
- Haben nur berechtigte Benutzer die Berechtigung, auf Batch-Jobs anderer Benutzer zuzugreifen?

M 4.266 Sichere Konfiguration des SAP Java-Stacks

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der Java-Stack eines SAP Systems erlaubt es, Java-basierte Technologien einzusetzen. Diese werden vornehmlich in Web-basierten Szenarien genutzt. Im Gegensatz zum ABAP-Stack ist der Java-Stack relativ neu und dessen Funktionen finden sich weniger häufig im Einsatz. Die neuen Java-basierten Technologien ergänzen jedoch die ABAP-Welt, so dass die Bedeutung des Java-Stacks in Zukunft weiter zunehmen wird. Zwar werden viele geschäftsrelevante Funktionen weiterhin im ABAP-Stack ablaufen, aber die Frontend-Komponenten werden in Java implementiert sein. Der Java-Stack wird durch einen Applikationsserver gebildet, der die J2EE (Java 2 Enterprise Edition) Spezifikation umsetzt.

Da Java- und ABAP-Stack im NetWeaver ApplicationServer integriert sind und miteinander über den JavaConnector (JCo) kommunizieren können, muss ein installierter Java-Stack abgesichert werden. Dabei kommen jedoch im Vergleich zum ABAP-Stack völlig unterschiedliche Sicherheitsmechanismen und -konzepte zum Einsatz.

Im Folgenden werden die aus Sicherheitssicht wichtigsten Schritte aufgezeigt, die bei der initialen Konfiguration des Java-Stacks durchzuführen sind. Die Darstellung beschränkt sich auf die Konfiguration des Applikationsservers und geht damit nicht auf sonstige installierte Applikationen ein.

Java-Stack Installation

Der Java-Stack sollte für SAP System Versionen, die eine separate Installation erlauben (Versionen bis 6.40), nur dann installiert werden, wenn Java-basierte Produkte oder Applikationen zum Einsatz kommen.

Kann der Java-Stack nicht separat installiert werden und wird nicht genutzt, so muss die Konfiguration so erfolgen, dass kein Zugriff auf den Java-Stack möglich ist. Dazu sollten alle Dienste des Java-Stacks deaktiviert werden.

Schulung zum Java-Stack

Administratoren, die den Java-Stack administrieren, müssen Kenntnisse in der Architektur und den Sicherheitskonzepten der J2EE-Architektur besitzen. Hier sind insbesondere Kenntnisse bezüglich der statischen Konfiguration der Sicherheit für J2EE-konforme Objekte notwendig, die über das Administrationswerkzeug durch den Administrator durchgeführt wird. Es kommt dabei ein rollenbasiertes Sicherheitskonzept zum Einsatz. Zu beachten ist, dass SAP den J2EE Java Authentication and Authorization Service (JAAS) mit den SAP spezifischen User Management Engine (UME) Funktionalitäten erweitert hat. Damit wurde die statische Konfiguration der Sicherheitseinstellungen um eine dynamische Konfigurationsmöglichkeit durch den Programmcode erweitert, die über die UME steuerbar ist. In der UME können daher beispielsweise erlaubte Aktionen in den Programmen zu Rollen zusammengefasst werden. Benutzern kann dann diese Rolle zugeordnet werden, so dass sie damit die benötigten Berechtigungen erhalten.

Administratoren muss zudem bewusst sein, dass der Java-Stack mit einer separaten Benutzer- und Berechtigungsverwaltung ausgestattet ist, so dass hier immer administrative Aufgaben durchgeführt werden müssen. Empfohlen ist hier der Einsatz der UME (siehe auch M 2.341 *Planung des SAP Einsatzes*), da damit die administrativen Tätigkeiten verringert werden.

Nicht benötigte Dienste abschalten

Der Java-Stack bietet eine Fülle von Diensten an. Nicht alle werden zum Betrieb in jedem Szenario benötigt. Daher sollten aus Sicherheitsgründen alle nicht benötigten Dienste deaktiviert werden. Problematisch dabei ist, dass Dienste voneinander abhängig sein können. Es kann zudem zwischen System-Diensten und Nicht-System-Diensten unterschieden werden. Die Verwaltung des Java-Stacks erfolgt über ein eigenes Werkzeug, den so genannten "Visual Administrator". Hier können auch die einzelnen Dienste verwaltet werden. Die Dienste finden sich dabei im "Server"-Abschnitt des Objekt-Baumes, der als Navigationshilfe im Visual Administrator dient. Die Detailinformationen zu einem Dienst werden angezeigt, sobald er selektiert wird.

Folgendes Vorgehen wird empfohlen:

- Zunächst wird der Dienst festgestellt, der die Technologie zum Ausführen der benötigten Applikation anbietet (z. B. Dienst servlet_jsp für Servlet-basierte Applikationen).
- Dann müssen die Abhängigkeiten des Dienstes festgestellt werden. Es muss dazu geklärt werden, welche anderen Dienste aktiviert sein müssen, damit der betrachtete Dienst ausgeführt werden kann. Dies ist aus der Registerkarte "Abhängigkeiten" in den Diensteigenschaften zu ersehen. In der Regel werden nur die Dienste mit starkem Abhängigkeitsverhältnis benötigt.
- Für die gefundenen Dienste muss nach gleichem Verfahren vorgegangen werden, bis sich die Liste der Dienste nicht mehr erweitert.
- Die Dienste, die nicht in der Liste erscheinen, können deaktiviert werden. Es ist zu beachten, dass bestimmte Dienste für den Betrieb des Java-Stacks benötigt werden.
- Nicht benötigte Applikationen können gestoppt oder deinstalliert werden. Dies erfolgt über den Dienst "deploy".
- Nicht benötigte Applikations-"Aliase", die über den Dienst "http" verwaltet werden, können deaktiviert werden.
- Nachdem Dienste oder Applikationen deaktiviert wurden, ist zu prüfen, ob die benötigten Dienste oder Applikation noch lauffähig sind.
- Falls die Applikation oder der Java-Stack nicht mehr lauffähig ist, sollten die Java-Stack Protokolle analysiert werden. In der Regel finden sich Fehlermeldungen, die auf den benötigten, aber deaktivierten Dienst hindeuten. Ansonsten kann nur durch Versuche die benötigte Kombination herausgefunden werden.
- Für Systemdienste muss das Startverhalten "always" über die XML-Konfigurationsdatei "runtime.xml" im Betriebssystem im jeweiligen

Dienstverzeichnis oder das GUI-basierte "Configurations"-Werkzeug verändert werden (Wert: "never" oder "manual").

Da sich der Java-Stack mit jeder Version verändert und insbesondere Unterschiede in der Dienstanzahl und -funktion bestehen, kann an dieser Stelle keine verbindliche Liste angegeben werden.

SAP Informationsquellen

Hinweise auf SAP Dokumentationen zu den Diensten und deren Funktion finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Standardinhalte entfernen

Alle Standardinhalte wie Dokumentationen (etwa Dienst deploy: sap.com/...docs.examples), Beispielprogramme (etwa Dienst deploy: sap.com/...htmlb.ear) oder statische HTML-Seiten sollten deinstalliert werden.

HTTP-Dienst absichern

Der HTTP-Dienst sollte abgesichert werden, wozu unter anderem die folgenden Punkte gehören:

- Verzeichnisanzeige nicht zulassen
- nicht benötigte Aliase deaktivieren
- HTTP PUT (Hochladen von Daten) nicht erlauben

SAP Informationsquellen

SAP Dokumentationen dazu werden in M 2.346 *Nutzung der SAP Dokumentation*.

Kryptographische Funktionsbibliothek installieren

Damit für den Java-Stack starke kryptographische Verfahren genutzt werden können, sollte eine kryptographische Funktionsbibliothek installiert werden, die starke Verfahren anbietet. Hier kann auch auf freie Implementierungen aus dem Java-Umfeld zurückgegriffen werden. Generell ist beim Einsatz von kryptographischen Funktionsbibliotheken auf die Kompatibilität mit dem Java-Stack und auf die Lizenzbestimmungen des Anbieters zu achten.

Auch Java-Stack-Komponenten wie der Secure-Storage, der zur sicheren Ablage von Daten durch System-Dienste und Applikationen dient, benötigen kryptographische Verfahren. Daher kann eine adäquate Sicherheit nur nach der Installation der kryptographischen Funktionsbibliothek erreicht werden.

Authentisierungsmodule konfigurieren

Für die Authentisierung beim Zugriff auf den Java-Stack können mehrere Authentisierungsverfahren eingesetzt werden. So sind neben dem Benutzernamen und Passwort-Verfahren auch Zertifikate oder Single Sign-On Tickets für die Authentisierung konfigurierbar. Dabei kann die Reihenfolge der verwendeten Verfahren bestimmt werden und ob ein bestimmtes Verfahren zur alleinigen Authentisierung ausreichend ist.

Im Rahmen des Berechtigungskonzeptes ist daher zu entscheiden, welche Verfahren wie einzusetzen sind. Falls notwendig, können weitere Verfahren über zusätzliche Bibliotheken von Drittherstellern eingebunden werden. Dabei wird die durch den Java-Standard spezifizierte JAAS-Schnittstelle genutzt.

Zugriff auf Systemressourcen beschränken

Durch das Berechtigungskonzept muss bestimmt werden, welche Benutzer oder Gruppen auf die Systemressourcen des Java-Stacks zugreifen dürfen und welche Zugriffsoperationen (z. B. Lesen, Schreiben, Auflisten) erlaubt werden sollen. Die konfigurierbaren Operationen hängen dabei vom Typ der Ressource ab. Es empfiehlt sich daher, die Detail-Planung anhand eines konkreten Java-Stacks - etwa nach der Installation - durchzuführen. Weitere Informationen finden sich in M 4.268 *Sichere Konfiguration der SAP Java-Stack Berechtigungen*.

Zugriff auf die Administrationsschnittstelle einschränken

Der Java-Stack wird über mehrere Schnittstellen administriert:

- Visual-Administrator
  Der Visual-Administrator kommuniziert über die P4-Schnittstelle mit dem Java-Stack. Der Zugriff auf die P4-Schnittstelle (standardmäßig Port 50004 für die Instanz 00) muss daher vor unberechtigten Zugriffen durch eine Firewall geschützt werden. Da das P4-Protokoll auch über HTTP getunnelt werden kann (standardmäßig Port 50001 für die Instanz 00), ist auch dieser Port zu schützen.
- Telnet-Dienst des Java-Stacks (standardmäßig Port 50008 für die Instanz 00)
  Wird dieser kommandozeilenbasierte Zugriff nicht genutzt, so sollte der Telnet-Dienst deaktiviert werden. Kommt Telnet zum Einsatz, so dürfen nur berechtigte Administratoren auf den Dienst zugreifen. Die Telnet-Ressource (security-Dienst, Resources, root/system/telnet) ist daher so zu konfigurieren, dass als "GrantedUsers" nur die Gruppe der berechtigten Administratoren eingetragen ist.
- Dateisystem, in dem Konfigurationsdateien abgelegt werden
  Die Verzeichnisse und Dateien der Java-Stack-Installation sind mit restriktiven Zugriffsbeschränkungen auszustatten. (Hinweis: Je nach Java-Stack-Version finden sich unterschiedliche Datei-System-Layouts. Die Entwicklung geht dahin, die Konfigurationen des Java-Stacks nur noch in der Datenbank zu halten.)

Der Zugriff auf die Administrationswerkzeuge (Visual Administrator, Configtool) ist auf die berechtigten Administratoren einzuschränken. Es ist jedoch zu bedenken, dass die Werkzeuge über das Netz arbeiten, so dass Angreifer eigene Programminstallationen nutzen können. Es empfiehlt sich daher, die Beschränkung auf Netzebene so zu konfigurieren, dass auf die administrativen Ports (siehe oben) nur von bestimmten Rechnern aus zugegriffen werden kann. Dies schließt zwar einen Angriff nicht vollständig aus, erschwert ihn jedoch.

Passwortqualität sicherstellen

Für die Benutzer des Java-Stacks sollten starke Passwörter konfiguriert werden. Die Möglichkeiten, die Passwortqualität sicherzustellen, unterscheiden sich in den einzelnen Java-Stack Versionen.

Als Mindestanforderung ist die minimale Passwortlänge auf einen Wert einzustellen, der durch die Passwortrichtlinie vorgegeben wird. Die Passwortlänge sollte mindestens 8 Zeichen betragen (Konfiguration für alle Benutzer über "Set Filter").

Auch ein maximales Alter für Passwörter sollte eingestellt werden, das den Vorgaben der Passwortrichtlinie entspricht. Dies wird über die Eigenschaften von Benutzern konfiguriert. Hier sind 90 Tage zu empfehlen.

Java-Stack Single Sign-On sicher konfigurieren

Damit auf den Java-Stack über Single Sign-On zugegriffen werden kann, müssen die Zertifikate der Systeme importiert werden, von denen Single Sign-On Tickets akzeptiert werden sollen. Dabei ist darauf zu achten, dass Single Sign-On Tickets nur von vertrauenswürdigen Systemen akzeptiert werden (siehe auch M 4.258 *Sichere Konfiguration des SAP ABAP-Stacks*).

Ergänzende Kontrollfragen:

- Sind die Standardinhalte für Produktivsysteme entfernt worden?
- Ist eine kryptographische Funktionsbibliothek installiert, die starke Verfahren anbietet?
- Sind nur die benötigten Dienste aktiviert?
- Ist der Zugriff auf administrative Schnittstellen eingeschränkt?

M 4.267 Sicherer Einsatz der SAP Java-Stack Benutzerverwaltung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der SAP Java-Stack besitzt eine eigene Benutzerverwaltung, die unabhängig vom ABAP-Stack eingesetzt werden kann. Folgendes ist dabei zu beachten:

Benutzer-Speicher konfigurieren

Der Java-Stack verwaltet seine Benutzer in einem Benutzer-Speicher, der ab Version 6.30 konfiguriert werden kann. Zur Auswahl stehen im Wesentlichen die Java-Stack Datenbank oder die User Management Engine (UME). Wird die UME eingesetzt, kann als Benutzer-Speicher auch ein LDAP-Verzeichnis oder ein ABAP-Stack genutzt werden.

In der Regel empfiehlt es sich, als Benutzer-Speicher den ABAP-Stack über die UME zu nutzen. Auf diese Weise können die Benutzer im ABAP-Stack verwaltet werden. Der Zugriff auf den ABAP-Stack erfolgt über den JavaConnector (JCo) unter den Berechtigungen des ABAP-Stack-Benutzers SAPJSF.

Im Rahmen der Einsatz-Planung ist zu entscheiden, welcher Benutzer-Speicher zum Einsatz kommen soll.

Notfall-Administrator anlegen

Wie für den ABAP-Stack muss auch für den Java-Stack ein Notfall-Administrator angelegt werden. Für diesen müssen die gleichen organisatorischen Schutzmechanismen gelten wie für den Notfall-Administrator des ABAP-Stack (siehe M 4.259 *Sicherer Einsatz der ABAP-Stack Benutzerverwaltung*).

Standardbenutzer absichern

Die Java-Stack Standardbenutzer Administrator, System und Guest müssen wie folgt abgesichert werden:

- Es muss ein sicheres Passwort gewählt werden. Je nach Version erfolgt dies während der Installation oder muss manuell nach der Installation vergeben werden.
- Das Gast-Konto (Benutzer Guest) muss deaktiviert sein.

Konzeption zur Benutzerverwaltung

Im Rahmen der Planung ist ein Konzept zur Benutzerverwaltung zu erstellen, das auch den Java-Stack berücksichtigt. Dabei ist unter anderem zu bedenken, dass die Benutzer in der Regel nur über das Werkzeug Visual-Admin verwaltet werden. Standardmäßig muss dabei die Anmeldung unter Administrator-Rechten (Mitgliedschaft in der Gruppe "Administrators") erfolgen. Dies bedeutet, dass sich beispielsweise Help-Desk-Mitarbeiter unter administrativen Berechtigungen verbinden. Dies kann zwar durch Rekonfiguration der internen Berechtigungsstrukturen eingeschränkt werden, diese ist jedoch aufwendig und verhindert nicht alle administrativen Tätigkeiten.

Alternativ kann die Benutzerverwaltung auch über die Web-Schnittstelle der UME erfolgen, falls diese zum Einsatz kommt.

Der Java-Stack erlaubt es, dass sich unbekannte Benutzer selbst registrieren können. Im Rahmen der Konzeption ist zu entscheiden, ob diese Funktion eingesetzt werden soll. Dabei ist eine sorgfältige Risikobetrachtung durchzuführen, da sich selbstregistrierte Benutzer nach der Registrierung gegenüber dem Java-Stack authentisieren können. Zwar besitzen die Benutzer dann in der Regel noch keine weiteren Berechtigungen, sind jedoch Applikationen mit Sicherheitsschwächen installiert (z. B. keine Berechtigungsprüfung beim Zugriff über bestimmte URLs), so können diese unter Umständen durch selbstregistrierte Benutzer ausgenutzt werden. Insbesondere im Internet-Einsatz ist diese Funktion kritisch zu bewerten. Um die Selbstregistrierung zu unterbinden, muss die UME Eigenschaft "ume.logon.selfreg" auf den Wert "FALSE" gesetzt werden. Die Konfiguration erfolgt über die Properties-Datei im Dateisystem oder über das Java Stack Werkzeug "Configtool". Generell muss der Einsatz der Selbstregistrierung sorgfältig geplant werden, von einer standardmäßigen Nutzung muss daher abgesehen werden. Es wird empfohlen, dass der Einsatz der Selbstregistrierung durch das Sicherheitsmanagement genehmigt werden muss.

Zugriff auf UME Web-Schnittstelle

Die UME Web-Schnittstelle erlaubt die Benutzerverwaltung über einen Browser. Wird diese Funktion eingesetzt, ist Folgendes zu berücksichtigen:

- Standardmäßig können Benutzer und Administratoren auf die UME Web-Schnittstelle zugreifen. Für normale Benutzer ist dann die Verwaltung des eigenen Benutzerkontos möglich (z. B. Passwortänderung). Für Benutzer der Gruppe "Administrators" ist die Verwaltung von Benutzern möglich (z. B. Benutzer anlegen).
- Auf die UME Web-Schnittstelle zur Benutzerverwaltung sollten nur berechtigte Administratoren zugreifen können. Dies kann durch entsprechende Authentisierungsanforderungen auf die Zugriffs-URL realisiert werden.
- Es sollte überlegt werden, ob die UME Web-Schnittstelle nur von Client-Rechnern berechtigter Administratoren zugreifbar sein sollte.
- Nutzen Applikationen die UME zum Speichern von benutzerbezogenen Eigenschaften (UME-Properties), so ist zu bedenken, dass diese durch die Benutzer selbst verändert werden können, wenn ihnen der Zugriff auf die UME Web-Schnittstelle gewährt wird.

Ob und unter welchen sicherheitsrelevanten Randbedingungen die UME Web-Schnittstelle eingesetzt werden soll, ist in der Planungsphase zu entscheiden.

Ergänzende Kontrollfragen:

- Wurde der gewünschte Benutzer-Speicher festgelegt?
- Ist ein Notfall-Administrator angelegt worden?
- Sind die Standardbenutzer abgesichert worden?

- Liegt ein Konzept zur sicheren Benutzerverwaltung vor?
- Wird die UME Web-Schnittstelle sicher verwendet, falls diese eingesetzt wird?

M 4.268 Sichere Konfiguration der SAP Java-Stack Berechtigungen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Bei der Planung und Konfiguration der SAP Java-Stack Berechtigungen ist Folgendes zu berücksichtigen:

- Das SAP Java-Stack Berechtigungskonzept unterscheidet sich fundamental vom Berechtigungskonzept des ABAP-Stacks, da hier die Konzepte der Java Spezifikation J2EE umgesetzt sind.
- Für die korrekte und sichere Konfiguration sind detaillierte Kenntnisse des J2EE-Sicherheitsmodells und der -Sicherheitskonzepte notwendig. Daher sollte die Konfiguration nur durch geschulte Administratoren erfolgen.
- Die Konfiguration der Zugriffbeschränkungen auf Ressourcen und für Java Protection Domains (Code Security) erfolgt über den "security" Service.
- Zugriffsbeschränkungen auf die JNDI-Objekte (Java Objekt Registratur und Namensdienst) erfolgen über den "naming" Dienst.
- Zugriffsbeschränkungen auf Java Bean-Methoden erfolgen über den "ejb" Dienst jeweils in den Eigenschaften der einzelnen Bean-Objekte auf der Registrierkarte "Security".
- Die jeweils verfügbaren Objekte hängen von den installierten Applikationen ab.
- Die Gruppe "root", die in Versionen vor 6.40 verfügbar ist, bezeichnet nicht eine Gruppe von Administratoren, sondern alle Benutzer. Die Gruppe entspricht daher eher der vergleichbaren Windows-Gruppe "Jeder/Everyone".
- Nach der Installation müssen die voreingestellten Berechtigungen geprüft und unter Umständen entsprechend dem erstellten Berechtigungskonzept abgeändert werden.

Generell sind die Berechtigungen restriktiv zu vergeben. Im Rahmen der Berechtigungsplanung muss jeweils entschieden werden, welcher Benutzer welche Berechtigung auf welche Objekte besitzt.

Ergänzende Kontrollfragen:

- Sind die Berechtigungen des SAP Java-Stacks restriktiv vergeben?

M 4.269 Sichere Konfiguration der SAP System Datenbank

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die von einem SAP System zur Speicherung genutzte Datenbank enthält alle Informationen eines SAP Systems. Die Kommunikation zwischen SAP System und Datenbank erfolgt über SQL-Anfragen, die über das lokale Netz übertragen werden, sofern Datenbank und die SAP Systemkomponenten nicht auf demselben Rechner installiert werden. Daher muss die Datenbank möglichst gut geschützt werden. Folgendes ist zu beachten:

- Die gemeinsame Installation von SAP System und Datenbank auf einem Rechner ist allgemein nur für kleine Unternehmen und Behörden sinnvoll. Für größere Institutionen ist die getrennte Installation vorzuziehen, da der Datenbankrechner so optimal auf die Last- und Performanzanforderungen separat ausgelegt werden kann.
- Kein Datenbank-Administrator darf Zugriff auf die Tabellen des SAP Systems besitzen. Die Datenbank-Berechtigungen sind zu prüfen und entsprechend anzupassen. Es ist dabei zu berücksichtigen, dass es typischerweise immer einen Datenbank-Administrator gibt, der Vollzugriff auf alle Datenbanken in der Institution und damit Tabellen besitzt.
- Auf die Datenbank darf nur vom SAP System selbst zugegriffen werden. Dies bedeutet insbesondere:
  - Direkte Datenbankverbindungen von anderen Systemen oder Clients sind durch eine Firewall zu unterbinden.
  - Die Datenbank sollte vom SAP System exklusiv genutzt werden. Andere Applikationen dürfen hier keine eigenen Tabellen erzeugen. Insbesondere sind Datenbank-Verknüpfungen zwischen der Datenbank und den Tabellen des SAP Systems und anderen Datenbanken auszuschließen.
- Auf dem Datenbank-Rechner für das SAP System dürfen keine anderen Dienste oder Applikationen ablaufen. Ausnahmen bilden hier Werkzeuge zur Betriebssystemüberwachung. Werden diese eingesetzt, so ist sicherzustellen, dass Verbindungsversuche nur authentisiert und von bestimmten Rechnern (Administrations-Server, Administrator-Client) erfolgen.
- Das vom SAP System genutzte Datenbank-Konto ist mit einem sicheren Passwort zu versehen.
- Das verwendete Datenbank-Produkt ist sicher zu konfigurieren.
  - Nicht benötigte Funktionen und Dienste sind abzuschalten. Dies betrifft insbesondere HTTP-basierte Zugriffsschnittstellen wie Applikationsserver, die die Datenbanken zum Zugriff über eine Web-Schnittstelle anbieten. In der Regel werden hier auch administrative Möglichkeiten angeboten.

- Standardbenutzer sind zu deaktivieren oder zu löschen, sofern diese nicht für administrative Operationen benötigt werden.
- Alle Passwörter von Standardbenutzern sind zu ändern, auch wenn diese Konten deaktiviert wurden.

In Abhängigkeit vom Einsatzszenario können noch weitere Maßnahmen notwendig sein. Die Liste ist daher geeignet zu erweitern.

SAP Informationsquellen

Es wird empfohlen, die Empfehlungen von SAP zur Absicherung der Datenbank umzusetzen. Details dazu finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Ergänzende Kontrollfragen:

- Ist die Datenbank des SAP Systems durch eine Firewall vor direkten Zugriffen Dritter geschützt?
- Wurden die Empfehlungen von SAP für das eingesetzte Datenbank-Produkt umgesetzt?

M 4.270 SAP Protokollierung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Damit die Systemfunktionen und die Systemsicherheit eines SAP Systems überwacht werden können, müssen Ereignisse protokolliert werden. Ein SAP System bietet dazu viele Möglichkeiten an. Es ist zu beachten, dass sich die vorliegende Maßnahme mit der Protokollierung im Sinne von "Monitoring des SAP Basissystems unter dem Gesichtspunkt der IT Sicherheit" beschäftigt. Betriebswirtschaftliche Prüfungen (Audits) sind nicht Gegenstand der Maßnahme.

SAP Informationsquellen

SAP Dokumentationen mit Detailbeschreibungen zu den Systemüberwachungsfunktionen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Generell ist für die Protokollierung Folgendes zu beachten.

Protokollierungskonzept

Es muss ein Protokollierungskonzept erstellt werden. Das Konzept muss den ABAP- und Java-Stack berücksichtigen. Im Konzept ist festzulegen, welche Protokolldaten im SAP System gesammelt werden. Da bei der Protokollierung auch personenbezogene Daten anfallen können, sind der Datenschutzbeauftragte und der Personal- oder Betriebsrat in die Planung einzubeziehen.

Sicherheit der Protokolldaten

Die protokollierten Daten können wichtige Systeminformationen und personenbezogene Daten enthalten. Der Zugriff auf die Protokolldaten muss daher eingeschränkt werden. Dies kann Einstellungen sowohl innerhalb des SAP Systems als auch außerhalb des SAP Systems (z. B. auf Dateiebene) notwendig machen.

Wichtige Systemereignisse auswerten

Wichtige Systemereignisse werden im Systemlog protokolliert. Die Ereignisse sollten regelmäßig ausgewertet werden. Dazu kann die Transaktion SM21 genutzt werden. Es ist zu bedenken, dass über diese Transaktion auch auf Systemlogs entfernter SAP Systeme zugegriffen werden kann, sofern die Berechtigung dazu besteht. Der Zugriff auf die Transaktion SM21 ist daher auf die berechtigten Administratoren zu beschränken.

Beim Betrieb mehrerer SAP Systeme empfiehlt es sich, eine zentrale Protokollierung einzusetzen, so dass die Auswertung auf einem System erfolgen kann.

Verwendung von Traces einschränken

Traces erlauben es, Systemaktivitäten bei einem Zugriff genau zu protokollieren. Dabei können unter Umständen auch die verarbeiteten Daten - etwa über das Protokollieren der SQL-Anfragen an die Datenbank oder die über die ALE-Schnittstelle übergebenen Dokumente - eingesehen werden.

Für produktive Systeme dürfen Traces daher nicht genutzt werden. Fehleranalysen sollten im Test- oder Entwicklungssystem erfolgen. Müssen Traces in einem Produktivsystem eingesetzt werden, so ist dies über ein entsprechendes Ausnahmeverfahren zu regeln.

Der Zugriff auf die Trace-Transaktionen - darunter fallen die meisten Transaktionen mit dem Präfix "ST" (die Liste dieser Transaktionen mit Kurzbeschreibung kann über die Transaktion SE93 angezeigt werden) - ist daher einzuschränken (Berechtigungsobjekt S_TCODE).

Aktivieren der Änderungsverfolgung für Tabellen

Die Datenbank-Tabellen des SAP Systems halten alle System- und Geschäftsdaten. Im Rahmen des Protokoll- und Audit-Konzeptes ist daher festzulegen, für welche Tabellen eine Änderungsverfolgung aktiviert werden soll. In der Regel protokollieren die SAP Anwendungen alle für eine Nachvollziehbarkeit notwendigen Daten. Für die SAP Basis gilt: Customizing-Tabellen, also Tabellen, die durch den Kunden verändert werden können, werden mit aktivierter Änderungsverfolgung ausgeliefert. Dadurch können die Änderungen an den Tabellen nachvollzogen werden. Dies ist auch für Unternehmen wichtig, die dem Sarbanes Oxley Act unterliegen, da so im Rahmen von Kontrollen geprüft werden kann, welche Benutzer welche Veränderungen durchgeführt haben.

Es ist dabei zu bedenken, dass die Änderungsverfolgung nur für Tabellen aktiviert werden kann, für die der Entwickler dies vorgesehen hat. Das Aktivieren erfolgt im Data Dictionary (DDIC), wo für die betroffene Tabelle die Option "Datenänderungen protokollieren" einzustellen ist (Transaktion SE13). Zusätzlich muss die Protokollierung im Systemprofil aktiviert werden. Dazu ist der Parameter "rec/client" zu konfigurieren, über den eingestellt wird, für welche Mandanten die Änderungsverfolgung aktiviert wird (Einstellmöglichkeiten: OFF / mmm/ nnn,mmm,... / ALL).

Die Änderungsverfolgung wird für Produktiv- und Customizing-Mandanten empfohlen. Die Einstellung "ALL" ist nicht sinnvoll. Dies führt beispielsweise bei Updates zu Performanzeinbußen, da auch der Mandant 000 und mögliche Test-Mandaten betroffen sind.

SAP Informationsquellen

Hinweise auf weitere Informationen zur Änderungsverfolgung sind in M 2.346 *Nutzung der SAP Dokumentation*.

Zugriff auf die Monitoring-Werkzeuge einschränken

Der Zugriff auf die durch das SAP System angebotenen Monitoring-Werkzeuge ist auf die berechtigten Administratoren einzuschränken. In der Regel kann dies über die Beschränkung des Zugriffs auf die Transaktionen und die Berechtigungseinstellungen erfolgen.

Es ist zu beachten, dass einige Monitoring-Werkzeuge auch Web-Schnittstellen zum Zugriff anbieten, wie etwa der ABAP-Stack Message-Server Monitor oder die Monitore des Java-Stacks (z. B. SQL-Trace, Systeminfo).

Einsatz des SAP Security Audit Log

Das SAP Security Audit Log zeichnet wichtige sicherheitsrelevante Systemereignisse auf. Der Einsatz ist daher sicherzustellen. Die Konfiguration erfolgt über die Transaktion SM19. Die Transaktion SM18 dient zum Löschen alter Log-Dateien, die Transaktionen SM20 und SM20N dienen zur Auswertung. Das Security Audit Log erlaubt so genannte dynamische Konfigurationen, deren Einstellungen zur Laufzeit verändert werden können und so genannte statische Konfigurationen, für die bei Einstellungsänderungen ein System-Neustart durchgeführt werden muss.

Für die Konfiguration der zu protokollierenden Ereignisse sollte Folgendes beachtet werden:

- Alle Ereignisse der Klasse "kritisch" sollten aktiviert werden.
- Alle Ereignisse der Klasse "schwerwiegend" sollten aktiviert werden.
- Für die Ereignisse der Klasse "unkritisch" muss entschieden werden, ob diese protokolliert werden sollen. Dabei ist zu bedenken, dass darunter auch Ereignisse sind, die sehr viele Protokolleinträge erzeugen. Ist das Security Audit Log voll, werden keine Einträge mehr protokolliert.

Der Zugriff auf die Transaktionen SM18, SM19, SM20 und SM20N sollte auf die berechtigten Administratoren eingeschränkt sein. Das Security Audit Log muss regelmäßig ausgewertet werden.

Ergänzende Kontrollfragen:

- Wurde ein sinnvolles Protokollierungskonzept erstellt?
- Werden die Protokolle regelmäßig ausgewertet?
- Ist der Zugriff auf die administrativen Funktionen und die Protokolldaten auf die berechtigten Administratoren eingeschränkt?

M 4.271 Virenschutz für SAP Systeme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Leiter Entwicklung

Verantwortlich für Umsetzung: Administrator, Entwickler

Mit der Version SAP NetWeaver 04 wurde die Möglichkeit geschaffen, ein externes Anti-Viren-Programm an SAP Systeme anzuschließen. Damit ist es allen Anwendungen im ABAP- und Java-Stack möglich, die verarbeiteten Daten auf Computer-Viren scannen zu lassen. Dazu wurde die "Viren Scanner Schnittstelle" für Anti-Viren-Programme definiert, die jedoch durch die jeweiligen Programme explizit angesprochen werden muss.

Bei Eigenentwicklungen oder bei Zusatzsoftware von Drittherstellern für SAP Systeme sollte darauf geachtet werden, dass die Schnittstelle für Anti-Viren-Programme unterstützt wird. Dies gilt für den Einsatz in Szenarien, in denen Daten in ein SAP System geladen und anderen Benutzern zum Herunterladen angeboten werden. Es wird empfohlen, in die Beschaffungskriterien für Software von Drittherstellern für SAP Systeme eine Prüfung aufzunehmen, ob diese die Schnittstelle für Anti-Viren-Programm unterstützen.

Der Einsatz der Anti-Viren-Programme im SAP Umfeld ist mit dem behörden- oder unternehmensweiten Computer-Viren-Schutzkonzept abzustimmen.

SAP Informationsquellen

Hinweise auf Dokumentationen zur Schnittstelle für Anti-Viren-Programme finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Ergänzende Kontrollfragen:

- Wird die Schnittstelle für Anti-Viren-Programme in Eigenentwicklungen unterstützt?
- Ist die Unterstützung der SAP Schnittstelle für Anti-Viren-Programme eines der Beschaffungskriterien für Software für SAP Systeme?

M 4.272 Sichere Nutzung des SAP Transportsystems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Über das SAP Transportsystem (Transport Management System, TMS) erfolgt das Einspielen neuer Funktionalitäten oder veränderter Objekte in den ABAP-Stack. Da dies grundsätzlich ein Risiko darstellt, muss das Transportsystem möglichst sicher konfiguriert und benutzt werden. Folgende Aspekte sind daher für das Transportmanagementsystem zu berücksichtigen:

Generell müssen Personen, die Transporte erstellen, prüfen und durchführen, mit den Konzepten und Verfahren des SAP Transportmechanismus (Transport Organizer, Transport Management System) vertraut sein.

Berechtigungen im Transportsystem

Über den Schutz der Transaktionen, die für das Transportsystem genutzt werden, und durch Berechtigungen ist sicherzustellen, dass nur die berechtigten Personen auf das Transportsystem zugreifen können. Unter anderem sind folgende Transaktionen betroffen: SE01, SE03, SE06, SE09, SE10, STMS*

Transportverzeichnis schützen

Die zu transportierenden Daten werden als Dateien im Transportverzeichnis im Dateisystem abgelegt. Der Zugriff auf das Transportverzeichnis muss daher auf Betriebssystem- und Netzebene eingeschränkt werden, so dass nur berechtigte Personen und nur berechtigte entfernte Instanzen Zugriff besitzen. Es ist dabei zu beachten, dass alle Instanzen einer Transportdomäne Zugriff auf das gleiche Transportverzeichnis haben müssen.

Es ist zu bedenken, dass unberechtigte Veränderungen an den Transportdateien zu Fehlfunktionen beim Import oder auch zu weiteren Sicherheitsproblemen führen können.

Sichere Übertragung von Transporten

Transporte werden aus dem Dateisystem in ein SAP System geladen. Dabei kann ein zentrales Transportverzeichnis, auf das über das lokale Netz zugegriffen wird, genutzt werden. Alternativ ist es auch möglich, Transportdateien über Dateitransfermechanismen (z. B. ftp, sfpt, scp) manuell oder zeitgesteuert zu übertragen.

Da Transportdateien vor unberechtigter Kenntnisnahme und Veränderungen geschützt werden müssen, sollte der eingesetzte Übertragungsmechanismus die Sicherheit der Daten beispielsweise durch Verschlüsselung gewährleisten.

SAP Informationsquellen

Hinweise auf Dokumentationen zum Transportmanagementsystem finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Ergänzende Kontrollfragen:

- Sind die relevanten Transaktionen des Transportsystems geschützt?
- Werden die Transportdaten auf Betriebssystem- und Netz-Ebene geschützt?

M 4.273 Sichere Nutzung der SAP Java-Stack Software-Verteilung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der Java-Stack nutzt ein eigenes Software-Verteilungsverfahren, das sich vom ABAP-Stack Transportsystem unterscheidet. Der so genannte Software Deployment Manager (SDM) dient dazu, neue Software in den JAVA-Stack einzuspielen. Der SDM ist Client-/Server-basiert aufgebaut, so dass Änderungen auch aus der Entfernung eingespielt werden können. Neben den allgemeinen Anforderungen (siehe M 2.221 *Änderungsmanagement*) ist Folgendes im Kontext der Software-Verteilung (Deployment) unter Sicherheitsgesichtpunkten zu bedenken:

- Es muss ein Konzept für die SAP Software-Verteilung geplant und erstellt worden sein. Das Software-Verteilungskonzept muss auf die Java-Besonderheiten abgestimmt sein, da hier im Vergleich zum ABAP-Stack unterschiedliche Verfahren und Werkzeuge eingesetzt werden müssen.
- Für den Test-, Validierungs- und Abnahmeprozess sind die Verantwortlichkeiten zu definieren.
- Durch Entwickler oder andere Personen dürfen keine Software-Verteilungen direkt aus den Entwicklungsumgebungen in Produktivsysteme erfolgen. Es ist zu bedenken, dass die SAP Entwicklungsumgebung Software direkt in den Java-Stack laden kann. Dies ist durch technische Maßnahmen (z. B. Firewall) auszuschließen.
- Der für die Software-Verteilung eingesetzte Software Deployment Manager (SDM) Dienst muss sicher betrieben werden. Ältere Versionen des SDM bieten nur eine schwache Absicherung, da nur ein Benutzer unterstützt wird und keine weiteren Berechtigungen vergeben werden können.
- Die SDM-Server-Komponente sollte nicht permanent laufen, sondern nur bei Bedarf gestartet werden.

SAP Informationsquellen

Quellen für SAP Dokumentationen finden sich in M 2.341 *Planung des SAP Einsatzes*.

Ergänzende Kontrollfragen:

- Ist das Software-Verteilungskonzept auf die Java-Besonderheiten abgestimmt?
- Sind Prozesse etabliert, die die Sicherheit bei der Software-Verteilung so weit wie möglich garantieren?
- Ist das direkte Einspielen von Software in den Java-Stack durch Entwickler ausgeschlossen?

M 4.274 Sichere Grundkonfiguration von Speichersystemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Sämtliche Konfigurationsarbeiten an Speichersystemen müssen entsprechend der erstellten Sicherheitsrichtlinie (siehe M 2.352 *Erstellung einer Sicherheitsrichtlinie für NAS-Systeme*, M 2.353 *Erstellung einer Sicherheitsrichtlinie für SAN-Systeme*) durchgeführt werden und wie in M 2.358 *Dokumentation der Systemeinstellungen von Speichersystemen* beschrieben dokumentiert und kommentiert werden.

Betriebssystem

Speichersysteme, die als NAS-Systeme betrieben werden können, sind spezialisierte Server, die intern von einem Betriebssystem verwaltet werden. Dieses Betriebssystem ist üblicherweise eine eingeschränkte und leistungsgesteigerte Version eines Standard-Betriebssystems.

Auch bei SAN-Systemen, die aus einer Vielzahl von Einzelkomponenten bestehen können, werden gegebenenfalls einzelne Komponenten durch Standard-nahe Systeme verwaltet.

Vor allem bei diesen Betriebssystemen aber auch bei herstellerspezifischen "unbekannten" Systemen muss vor Inbetriebnahme sichergestellt sein, dass ein aktueller Stand aller Software- und Firmwarekomponenten hergestellt wird, um bestmögliche Stabilität des Systems und auch Schutz gegen Angriffe wie z. B. durch Wurmprogramme sicherzustellen.

Grundkonfiguration

Vorsicht bei Default-Einstellungen

Bevor ein Speichersystem in die IT-Produktion integriert wird, muss eine sichere Grundkonfiguration hergestellt werden. Viele Geräte werden vom Hersteller mit einer Default-Konfiguration ausgeliefert, die vor allem auf eine schnelle Inbetriebnahme mit möglichst umfassender Funktionalität ausgerichtet ist und in der so gut wie keine Sicherheitsmechanismen aktiv sind. Daher muss die Überprüfung der Default-Einstellungen und die Grundkonfiguration offline, in einem eigens dafür eingerichteten und besonders gesicherten Testnetz oder über das Administrationsnetz, erfolgen.

Bei der Konfiguration muss beachtet werden, dass unter Umständen nicht jedes Administrations- oder Konfigurationswerkzeug (Konsole, Webschnittstelle, externes Konfigurationsprogramm) alle relevanten Informationen anzeigt.

Daher ist es wichtig, anhand der vorhandenen Dokumentation nachzuvollziehen, dass auch alle relevanten Einstellungen vorgenommen wurden. Es ist wünschenswert, wenn Konfigurationswerkzeuge alle Konfigurationsschritte am Speichergerät mindestens in lokalen Logdateien, besser noch auf einem zentralen Logging-System auswertbar dokumentieren.

Es bietet sich an, die Grundkonfiguration in folgende Schritte zu unterteilen:

- Lokale Konfiguration: Überprüfung und Anpassung der Konfigurationsparameter, die sich auf das Gerät selbst beziehen (beispielsweise

Einstellung von RAID-Levels, Zuordnung von Festplatten zu Volumes, Zuordnung von Backup Geräten zu Speichergeräten), Einstellungen zur Protokollierung, Einstellungen für Konsolenzugang etc.

- Netzkonfiguration: Überprüfung und Anpassung der Konfigurationsparameter, die sich auf die Einbindung des Geräts in das lokale Netz, das Administrationsnetz und das Speichernetz beziehen. Dienste zur Administration wie telnet, tftp, oder http, bei denen Anmeldung und alle Informationen im Klartext und ausgetauscht werden, sollten durch die verschlüsselten Äquivalente ssh, sftp und https ersetzt werden.
- Bei SAN-Systemen muss die interne Segmentierung des Netzes durch Zoning und Port-Binding vorgenommen werden. Den angeschlossenen Servern sollten nur die tatsächlich benötigten Ressourcen des SAN zugeordnet werden.
- Die Administration der Speichersysteme sollte in die zentrale Rechteverwaltung eingebunden werden (z. B. Active Directory, LDAP, Radius,...).

Benutzerkonten und Passwörter

Die Möglichkeiten für die Einrichtung von Benutzern und Rollen und das Zuweisen von Berechtigungen unterscheiden sich von Hersteller zu Hersteller teilweise erheblich. Daher ist es empfehlenswert, entsprechend dem vorgegebenen Rechte- und Rollenkonzept für die Administration der Speichergeräte ein detailliertes Konzept für die jeweiligen Geräte zu erstellen.

Oft sind ein oder mehrere Administrationszugänge mit allgemein bekannten Standardnamen und Passwort oder sogar ohne Passwort vorkonfiguriert. Auf einschlägigen Internet-Seiten können Listen mit herstellerspezifischen Standard-Accounts und Passwörtern heruntergeladen werden.

Standardnamen ändern

Bei der Inbetriebnahme des Geräts müssen diese Standard-Benutzerkonten, falls möglich, geändert werden. In jedem Fall müssen aber die Passwörter der Standard-Accounts geändert werden. Nicht benutzte Benutzerkonten müssen deaktiviert werden.

Entsprechend dem Rechte- und Rollenkonzept müssen anschließend die vorgesehenen Benutzerkonten und -rollen eingerichtet werden.

Gesicherte Speicherung der Konfiguration

Konfigurationsdateien müssen vor unbefugtem Zugriff besonders geschützt werden. Auch wenn z. B. eine verschlüsselte Speicherung von Passwörtern sichergestellt ist, müssen solche Dateien vor unberechtigtem Lesen geschützt werden, da sie geschäftskritische Informationen enthalten und auch verschlüsselte Passwörter häufig in recht kurzer Zeit durch passende Programme entschlüsselt werden könnten.

Passwortrichtlinien der Institution bezüglich Länge, Stärke und Änderungshäufigkeit sind also unbedingt zu beachten.

Login-Banner

Jenseits des Administrationsnetzes sollten keinesfalls Login-Nachrichten eines Speichersystems sichtbar werden. In diesen Login-Nachrichten sind oft Informationen (beispielsweise Modell- oder Versionsnummer, Software-

Release-Stand oder Patchlevel) enthalten, die einem potentiellen Angreifer von Nutzen sein können.

Sollte es sich nicht vermeiden lassen, dass auch im Intranet der Institution ein Login möglich ist, sollte die Standard-Loginnachricht durch eine angepasste Version ersetzt werden, die keine internen Informationen enthält. Die Modell- und Versionsnummer des Geräts und die Version des Betriebssystems darf unter keinen Umständen vom Login-Banner verraten werden. Stattdessen sollten folgende Informationen bei einer Anmeldung am Gerät angezeigt werden:

- Jeglicher Zugriff darf nur durch autorisiertes Personal erfolgen.
- Alle Arbeiten sind entsprechend der Sicherheitsrichtlinie durchzuführen.
- Das Gerät ist in zentrale Kontrollmechanismen, wie beispielsweise in ein Netzmanagementsystem (NMS) zur Protokollierung und Erkennung von Verstößen gegen die Sicherheitsrichtlinie eingebunden.
- Verstöße gegen die Sicherheitsrichtlinie werden disziplinarisch / strafrechtlich verfolgt.

Protokollierung

Die interne Protokollierung auf dem Speichersystem muss so konfiguriert werden, dass vor allem Informationen, die zur Früherkennung von Problemen benötigt werden, leicht sichtbar werden.

Das Speichersystem und die zur Administration und Protokollierung genutzten Rechner sollten durch Nutzung eines NTP-Servers zeitlich synchronisiert werden..

Es ist generell ratsam, alle IT-Systeme der Institution per NTP auf eine einheitliche Zeit zu synchronisieren.

Schnittstellen

Nicht genutzte Schnittstellen auf Speichersystemen sind zu deaktivieren. Das bedeutet, dass nicht genutzte Anschlüsse (z. B. eine serielle Schnittstelle zum Anschluss eines Terminals) nicht verkabelt und Dienste, die nicht genutzt werden sollen, explizit deaktiviert werden sollten.

Test der Konfiguration

Zum Abschluss des Testbetriebes sollten Standardsysteme und auch die Absicherung des Administrationsnetzes durch einen Sicherheitscheck geprüft werden.

Backup der Konfiguration

Die Konfigurationsdateien der Grundkonfiguration bilden die Basis für die weitere Konfiguration. Es müssen sowohl von der mit dem Gerät ausgelieferten Default-Konfiguration als auch von den Daten, die das Ergebnis der Grundkonfiguration darstellen, Sicherungskopien hergestellt und geschützt aufbewahrt werden.

Diese bilden die Grundlage für einen Wiederanlauf nach gravierenden Störungen (siehe M 6.98 *Notfallvorsorge für Speichersysteme*).

Ergänzende Kontrollfragen:

- Wurde die Einrichtung anhand der Sicherheitsrichtlinie durchgeführt?
- Wie ist die Abbildung des allgemeinen Rollenkonzepts für die Administration auf die Administratorkonten des Speichersystems.?
- Wurden alle nicht benötigten Standard-Benutzerkonten deaktiviert und alle Standard-Passwörter geändert?
- Wie wird sichergestellt, dass nach einer Konfigurationsänderung, oder Neuinstallation des Systems, die Passwörter nicht auf den Standard-Wert gesetzt und die Standard-Benutzerkonten nicht wieder aktiviert werden?
- Ist das Login-Banner für normale Anwender unsichtbar?
- Sind alle relevanten Angaben zur Konfiguration dokumentiert worden?

M 4.275 Sicherer Betrieb eines Speichersystems

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator

Ein Speichersystem läuft im Normalfall weitgehend autonom ohne Eingriffe durch das Bedienungspersonal. Zur Absicherung des Betriebes gibt es jedoch einige Maßnahmen, die ergriffen werden müssen, wenn die Funktionalitäten eines Speichersystems ohne Probleme zur Verfügung stehen sollen. Realisiert wird die Überwachung des Betriebs durch ein Managementsystem (siehe M 2.359 *Überwachung und Verwaltung von Speichersystemen*) .

Überwachung

- **Anwendungen, Systemprogramme**

  Es muss sichergestellt werden, dass Dienstprogramme wie Scheduler, die die automatische Datensicherung steuern oder auch Anti-Virensoftware störungsfrei laufen.

- **Kapazitätskontrolle und System-Auslastung**

  Es muss sichergestellt werden, dass Kapazitätsgrenzen von Speichergeräten nicht überschritten werden und Engpässe auf Speichersystemen oder im Speichernetz so rechtzeitig erkannt werden, dass Gegenmaßnahmen getroffen werden können.

- **Überwachung kritischer Ereignisse**

  Die Integrität sicherheitskritischer Einstellungen und die Beachtung von Sicherheitsvorgaben muss überwacht werden. Ereignisse, die gegen wesentliche Sicherheitsregeln verstoßen, müssen unübersehbar gemeldet werden.

- **Reduzieren der Systemnachrichten**

  Systemnachrichten sollten so reduziert werden, dass nur wirklich wichtige Nachrichten dargestellt werden.

Nachrichten nur, wenn wichtig

Organisatorische Maßnahmen

Um Änderungen und Wartungsarbeiten an einem Speichersystem durchführen zu können, die eine Betriebsunterbrechung zur Folge haben, sind Wartungsfenster zu definieren.

An einem laufenden Speichersystem dürfen keine die Produktion beeinflussenden Wartungsarbeiten und Änderungen außerhalb des Wartungsfensters durchgeführt werden. Alle Änderungen, ob geplant oder ungeplant, müssen über ein Änderungsmanagement-Verfahren mit allen beteiligten Fachverantwortlichen abgestimmt werden. Der Änderungsplan sollte zur Nachverfolgbarkeit archiviert werden.

Keine Wartungsarbeiten außerhalb des Wartungsfensters

Insbesondere Updates von Firmware oder Betriebssystem von Speichersystemen und Netzkomponenten eines SANs dürfen nur innerhalb eines Wartungsfensters durchgeführt werden.

Relevante Änderungen an der Konfiguration oder an interner Software des Speichersystems müssen unbedingt aktuell dokumentiert werden. Diese

Dokumentation muss vor allem für die Behandlung von Störungen und in Notfallsituationen eindeutig und leicht verfügbar sein.

Insbesondere nach Änderungen der Systemkonfiguration sind die Logdateien von Komponenten zur Datensicherung und Archivierung zu kontrollieren. Es sind außerplanmäßige Test vorzunehmen, ob Daten vom Backup wiederhergestellt werden können (siehe dazu auch M 6.22 *Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen*).

Absicherung der Systemverwaltung

Das Managementsystem für das Speichersystem ist selbst so abzusichern, dass ein Zugriff unberechtigter Anwender nicht möglich ist.

Ergänzende Kontrollfragen:

- Wird die Verfügbarkeit aller internen Anwendungen des Speichersystems kontrolliert?
- Wird die Systemauslastung kontrolliert?
- Werden Änderungen nur über das Änderungsmanagement aktiviert?
- Werden Wartungsarbeiten, wie Updates, nur während der dafür vorgesehenen Zeitfenster durchgeführt?

M 4.276 Planung des Einsatzes von Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Vor der Einführung von Windows Server 2003 sind umfangreiche Planungen durchzuführen, damit eine geregelte und auch sichere Einführung sowie in Folge ein sicherer Betrieb ermöglicht wird. Dabei ist zu gewährleisten, dass die festgelegten Sicherheitsrichtlinien (siehe M 2.316 *Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server*) eingehalten werden und so eine richtlinienkonforme Umsetzung erfolgt. Hierbei ist zu beachten, dass Windows Server 2003 in der Standardinstallation ohne bereits vorinstallierte Softwarekomponenten zur Verfügung steht, um den Betrieb später nicht benötigter Komponenten zu vermeiden. In Abhängigkeit des Einsatzszenarios ist zu definieren, für welche Serverrolle Windows Server 2003 geplant wird und welche Softwarekomponenten hierfür gegebenenfalls zusätzlich installiert werden müssen.

Die im Zusammenhang mit der Einführung bzw. dem Betrieb von Active Directory stehenden Fragestellungen bzw. Planungsschritte werden hier nur ansatzweise berücksichtigt.

Grobkonzept

Die Planung eines Windows Server 2003 erfolgt in mehreren Schritten. Ein definierter Anforderungskatalog gemäß M 2.80 *Erstellung eines Anforderungskatalogs für Standardsoftware* erleichtert die Planung erheblich und ist zu empfehlen.

Typische Fragestellungen

Die konkrete Planung kann nach dem Prinzip des Top-Down-Entwurfes erfolgen: Ausgehend von einem Grobkonzept für das Gesamtsystem werden konkrete Planungen für Teilkomponenten in spezifischen Teilkonzepten festgelegt. Im Grobkonzept werden beispielsweise folgende typische Fragestellungen behandelt:

- Wird ein neues Netz aufgebaut oder wird ein bestehendes Netz migriert?
- Soll ein existierendes Windows-Netz (z. B. basierend auf Windows 2000 Server) vollständig oder nur teilweise nach Windows Server 2003 migriert werden?
- Handelt es sich um einen zusätzlichen einzuführenden Server oder um das Upgrade eines existierenden Servers (siehe M 4.283 *Sichere Migration von Windows NT 4 Server und Windows 2000 Server auf Windows Server 2003*)?
- Welche Komponenten, z. B. Dateiserver, Druckserver, DNS-Server, werden ersetzt, welche bleiben erhalten?
- Müssen existierende Verfahren oder Komponenten, wie z. B. ein bestehendes Kerberos-System oder auch eine bestehende PKI, in Windows Server 2003 integriert werden? Hier sind u. a. die Interoperabilität mit anderen IT-Systemen sowie der angebotene Funktionsumfang zu berücksichtigen.

- Wird die geplante Konfiguration des Servers der zu erwartenden Datenmenge und Spitzenlast gerecht?
- Ist das Lizenzierungsmodell ausreichend und geeignet für das Bereitstellungskonzept und das Notfallkonzept?
- Ist ein Mischbetrieb von Windows Server 2003 und anderen Betriebssystemen, wie Windows 2000, Windows 95, Novell oder Unix, notwendig? Ist dies der Fall, so hat dies u. a. Einfluss auf die im System verwendeten Authentisierungsverfahren, die abhängig von den anderen eingesetzten Betriebssystemen auch Schwachstellen aufweisen und damit die Sicherheit der Windows-Server-2003 Umgebung insgesamt herabsetzen können. Der Sicherheitsstandard in der Mischumgebung sollte in einer IT-Sicherheitsrichtlinie festgelegt sein.

Rollenplanung

Serverrollen planen

Im Rahmen der Erstellung von Teilkonzepten sollten die Serverrollen festgelegt werden. Das Bedienkonzept von Windows Server 2003 definiert mittels verschiedener Konfigurations-Assistenten konkrete Rollen, welche zunächst als Ausgangsbasis für die Planung berücksichtigt werden sollten. Die Rollen sind in Abhängigkeit des Einsatzszenarios und der Anforderungsdefinition zu planen. In Teilkonzepten für die einzelnen Rollen müssen die spezifischen Anforderungen berücksichtigt werden, wie z. B. die zu erwartende Datenmenge und Last, Kommunikationsprotokolle und -schnittstellen, Zugriffskonzept, Konfiguration der jeweiligen Betriebssystemkomponenten usw.

Rollen (Auswahl)

Serverrolle	Server-konfigurations-Assistent	Manuelle Konfigu-ration	Sicherheits-konfigurations-Assistent
Dateiserver	x		x
Druckserver	x		x
Anwendungsserver	x		x
Mailserver	x		
Terminalserver	x		x
RAS/VPN-Server	x		x
Domänencontroller	x		x
DNS-Server	x		x
DHCP-Server	x		x
Streaming Media-Server	x		x
WINS-Server	x		x
Web-Server		x	x

Remote Installations-Server		x	x
Bastion-Host		x	
Zertifikatsserver		x	x

Der Sicherheitskonfigurations-Assistent unterstützt eine große Zahl weiterer Serverrollen von Microsoft-Produkten, z. B. die Rolle des Datenbankservers.

Sicherheits-konfigurations-Assistent

- **Kombination von Serverrollen**

  Rollen können kombiniert werden, um sowohl Beschaffungskosten als auch den Administrationsaufwand zu verringern. Kombinationsmöglichkeiten sind hauptsächlich durch folgende Aspekte beschränkt:

  Kombination von Serverrollen

  - Sicherheit/Schutzbedarf des IT-Systems
  - designbedingte Beschränkungen von Windows Server 2003
  - Skalierbarkeitsanforderungen

  Nachfolgende Möglichkeiten der Rollenverteilung sind Empfehlungen. In jedem Fall sind die geplanten Rollenkombinationen zu testen.

  Rollenverteilung

  Anwendungsserver, Zertifikatsserver, Webserver, RAS/VPN-Server:

  Diese Rollen sollten hauptsächlich aus Gründen der Sicherheit jeweils getrennt von anderen Rollen verwendet werden.

  Terminalserver, Druckserver:

  Diese Rollen sind hauptsächlich aus Design- und Skalierbarkeitsgründen von anderen Rollen zu trennen. Zum Beispiel werden auf Druckservern Treiber von anderen Herstellern installiert, die die Verfügbarkeit des Servers beeinträchtigen können.

  Bastion Host:

  Ein Bastion-Host ist ein abzusichernder Computer, der direkt mit dem Internet verbunden ist. Bastion-Hosts werden in der Regel als Webserver, DNS-Server, FTP-Server, SMTP-Server und als NNTP-Server eingesetzt. Die Rolle des Bastion-Hosts eignet sich für Server im exponierten Bereich und sollte nicht mit anderen Serverrollen kombiniert werden.

- **Kombinationen**

  Infrastrukturdienste können gemeinsam auf einem Server betrieben werden. Kommt Active Directory zum Einsatz, empfiehlt sich die Integration von DNS auf den Domänencontrollern. Bei erhöhten Sicherheitsanforderungen in mittleren und großen Umgebungen sollte WINS nicht auf dem Domänencontroller integriert werden.

  Kombinationen von Rollen

  In vielen Fällen bietet es sich an, einem Dateiserver weitere Rollen hinzuzufügen, z. B. Infrastrukturdienste. Auch die Rolle des Streaming-Media-Servers könnte von einem Dateiserver übernommen werden.

Die Verwendung von Remoteinstallationsdiensten (RIS) ist auf einem Dateiserver möglich, zum Beispiel im Rahmen von Helpdesk-Szenarien. Hierbei kann jedoch die Sicherheit des Servers durch die Remoteinstallationsdienste beeinträchtigt werden.

Die Dienste der Mailserverrolle können für bestimmte administrative oder infrastrukturelle Einsatzzwecke mit anderen Rollen kombiniert werden. Hier sollte seitens der Anforderungsdefinition klar von der Rolle des Bastion-Hosts unterschieden werden.

- **Weitere Serverapplikationen und -dienste**

  Weitere Serverapplikationen und -dienste

  Die Internet Information Services (IIS) enthalten Basisdienste für verschiedene Serverrollen (z. B. Webserver) und stellen selbst keine eigene Serverrolle dar. Bei der Planung sollte unter Sicherheitsgesichtspunkten zwischen statischen und dynamischen IIS-Komponenten unterschieden werden.

  Weitere Software

  Weitere Serverrollen können durch Zusatzsoftware bereitgestellt werden. Die Verträglichkeit mit den Standardrollen ist im Einzelfall abzuwägen, dabei sind die bei den oben zur Kombination von Rollen beschriebenen möglichen Konflikte zu berücksichtigen. Die Planung sollte auf Basis der Ergebnisse des Software-Auswahlprozesses (siehe B 1.10 *Standardsoftware*) erfolgen.

  16-bit-Anwendungen und sonstige veraltete Software, die keine Sicherheitsmechanismen auf Anwendungsebene bieten bzw. die Mechanismen von Windows Server 2003 nicht unterstützen, stellen ein erhöhtes Sicherheitsrisiko für den Server dar. Daher sind besondere Anforderungen der Absicherung auf Daten- und Netzwerkebene bei der Planung der Windows Server 2003 Umgebung zu berücksichtigen. Dies ist sowohl technisch als auch organisatorisch relevant.

- **Rollen in heterogenen Umgebungen**

  Bei heterogenen Serverumgebungen Voraussetzungen beachten

  Heterogene Serverumgebungen mit vorhandenen Diensten und Rollen beeinflussen ebenfalls die Rollenplanung, vor allem wenn vorhandene Dienste in Windows Server 2003 überführt, konsolidiert oder wenn bestimmte Rollen parallel auf verschiedenen Plattformen realisiert werden sollen (das klassische Beispiel hierfür ist DNS). Letztlich ist die Rollenplanung auch vom Format und den Migrationsmöglichkeiten vorhandener Datenbestände und Produktionssysteme und der damit verbundenen mittel- und langfristigen Strategie abhängig.

Überlegungen zur Konfiguration des Servers

Die Dimensionierung der Hardware erfolgt unter den Gesichtspunkten Performance, Verfügbarkeit und Serverrolle.

Performance

Für die Performance sollten die Mindestanforderungen des Herstellers sowie der Anforderungskatalog berücksichtigt werden. Lastsimulationstools von der Microsoft-Website oder von Serverherstellern ermöglichen eine Vorhersage des Lastverhaltens von Windows Server 2003 Komponenten. Insbesondere die Maximalzahl gleichzeitiger Benutzer ist sorgfältig und prognostisch einzuschätzen. Bei hoher Benutzerzahl bzw. Nutzungsintensität ist die

Zusammenfassung mehrerer Server zu einem Cluster zu erwägen.

voraussichtliche Last und zu erwartende Datenmenge

Die geplanten Serverrollen und Serverapplikationen, die voraussichtliche Last sowie die zu erwartende Datenmenge entscheiden über weitere Parameter der Hardwarekonfiguration. Wichtige Parameter sind z. B. die Aufteilung von Festplatten-Arrays und das Partitionslayout. Die Einrichtung unabhängiger Festplatten-Arrays (RAID-Level) ist aus Performance- und Verfügbarkeitsgründen für bestimmte Serverrollen zu empfehlen, z. B. Dateiserver oder Datenbankserver. Die Software-RAID-Varianten von Windows Server 2003 ermöglichen es, kurzfristig und kostengünstig eine Datenredundanz zu konfigurieren. Sie eignen sich jedoch nicht für Performance-Steigerung und können auch einen Plattenausfall im laufenden Betrieb meist nicht kompensieren. Hardware-RAID-Level sind bei der Planung in jedem Fall zu bevorzugen.

Partitionslayout

Die Planung des Partitionslayouts sollte sich am zu erwartenden Datenaufkommen und an der logischen Trennung verschiedener Datenarten orientieren. Z. B. ist eine Partition sinnvoll, die nur das Betriebssystem und Programmdateien enthält. Nutzdaten oder temporäre Daten sollten auf separate Partitionen, die sich gegebenenfalls auf anderen Disk Arrays befinden, verteilt werden. Bei Windows Server 2003 mit Service Pack 1 oder früher sind Datenträgerkontingente nur auf Partitions- bzw. Volumeebene konfigurierbar.

Netzanbindung

Geeignete Netz-Anbindung

Im Rahmen der Einsatzplanung von Windows Server 2003 ist es notwendig, in Abhängigkeit der gewählten Serverrolle eine geeignete Netzanbindung zu berücksichtigen. Die benötigten Kommunikationsprotokolle können aus der Serverrolle(n) abgeleitet werden. Hier ist zu prüfen, ob die Kommunikationsprotokolle mit dem Netzkonzept, den Sicherheitsrichtlinien für die Kommunikationsprotokolle und gegebenenfalls dem Konzept für die Sicherheitsgateways in Konflikt stehen. Der Datendurchsatz am Server kann aufgrund des zu erwartenden Zugriffsaufkommens durch Clients dimensioniert werden. Im Fall von verschlüsselten Zugriffen sind die Performanceeinbußen zu berücksichtigen. Entsprechend sollte die Leistungsfähigkeit skaliert werden, z. B. durch schnellere Prozessoren und Netzwerkadapter oder softwareseitig mit Hilfe des Netzlastenausgleichs in einem Cluster unter Windows Server 2003. Sowohl die Kommunikationsprotokolle als auch der Datendurchsatz sind wesentliche Merkmale der Verfügbarkeit und müssen sorgfältig geplant werden.

Erhöhte Sicherheitsanforderungen für Server in exponierter Lage

Bei der Planung eines Servers, auf den über unsichere Netze zugegriffen werden kann oder der sich in einer besonders exponierten Lage befindet, zum Beispiel Webserver mit Anbindung zum Internet, müssen erhöhte Sicherheitsanforderungen beachtet werden. Bei der Planung für Server in exponierter Lage kann prinzipiell analog zur Planung von Servern im geschützten Bereich vorgegangen werden, jedoch ist bei allen Planungsaspekten von einer stark erhöhten Bedrohung durch Einbruchsversuche, Denial-of-Service-Attacken oder sonstigen Kompromittierungsversuchen auszugehen. Außerdem muss konzeptionell festgelegt werden, wie der oder die Server vom lokalen Netz isoliert werden und wie gegebenenfalls

die Kommunikation mit dem lokalen Netz abgesichert werden kann. Als Beispiel sind Sicherheitsgateways und DMZ-Anordnung zu nennen.

Einsatz von Mitgliedsservern

Grundsätzlich nicht empfehlenswert ist der Einsatz von Mitgliedsservern einer geschützten Active-Directory-Umgebung in exponierter Lage oder DMZ. Die Sicherheitskontexte sollten entsprechend getrennt werden.

Möglichkeiten des Zugriffs

Zugriffswege planen

Bei der Einsatzplanung ist auch zu berücksichtigen, welche Zugriffswege ermöglicht werden müssen bzw. sollen (NetBIOS-Freigaben, WebDAV, DFS usw.). Hinsichtlich der Absicherung der Kommunikation sind gegebenenfalls die Maßnahmen M 4.277 *Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows Server 2003* und M 5.132 *Sicherer Einsatz von WebDAV unter Windows Server 2003* zu berücksichtigen. Die Notwendigkeit jedes zugelassenen Zugriffswegs ist zu begründen.

Überlegungen zur Administration des Servers

Weiterführende Aspekte

Im Rahmen der Planung des Einsatzes sollten folgende weiterführende Aspekte berücksichtigt werden. Eigene Teilkonzepte hierfür sind zu empfehlen, vorhandene Konzepte sollten ergänzt werden.

- Planung der Administration (M 2.364 *Planung der Administration für Windows Server 2003*), dies beinhaltet auch eventuell erforderliche Zusatzsoftware für die Administration
- Überwachung (Monitoring, Protokollierung, Auswertung), siehe M 2.365 *Planung der Systemüberwachung unter Windows Server 2003*
- Patchmanagement, Updates
- Bereitstellung (M 4.281 *Sichere Installation und Bereitstellung von Windows Server 2003*, M 4.283 *Sichere Migration von Windows NT 4 Server und Windows 2000 Server auf Windows Server 2003)*
- Übernahme bestehender Daten

Festlegungen zu diesen Aspekten sollten in der Sicherheitsrichtlinie für Windows Server 2003 getroffen und bei der weiteren Planung berücksichtigt werden. Vor dem produktiven Einsatz sollte die Richtlinie in verbindlicher Form vorliegen.

Lizenzmodell

Geeignete Lizenzmodelle sind abhängig vom Einsatz der Windows-Systeme. Für die Lizenzkontrolle wird Windows Server 2003 vom Hersteller mit Produktschlüssel und Produktaktivierung ausgeliefert. Es ist darauf zu achten, dass der betrachtete IT-Verbund ausreichend lizenziert ist und das für das einzelne Windows Server 2003 System eine aktivierbare oder aktivierungsfreie Installationsquelle und Lizenz verfügbar ist. Dies ist gegebenenfalls im Bereitstellungskonzept und im Notfallkonzept zu berücksichtigen.

Ergänzende Kontrollfragen:

- Sind die benötigten Serverrollen identifiziert und auf Verträglichkeit überprüft worden?

- Ist die benötigte Interoperabilität mit anderen IT-Systemen gegeben?
- Entspricht die Netzanbindung hinsichtlich Kapazität und Sicherheit den Anforderungen?

M 4.277 Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Grundlegende Protokolle für netzinterne Kommunikation

Die grundlegenden Protokolle für die netzinterne Kommunikation zwischen Windows-Servern und Clients sind SMB, RPC und LDAP. Diese Protokolle sind eng mit der Sicherheitsarchitektur von Windows Server 2003 verzahnt und profitieren von den integrierten Technologien, um eine sichere Kommunikation zu gewährleisten.

Anmeldung verschlüsseln

Grundsätzlich muss die Verwendung der Klartextanmeldung, unter Windows Standardauthentisierung genannt, unterbunden werden. Gleiches gilt für einige andere Anmeldeverfahren mit schwacher Verschlüsselung, die mit allgemein verfügbaren Auditwerkzeugen leicht kompromittiert werden können. Die Anmeldung muss also hinreichend stark verschlüsselt sein, sowohl bei der Kommunikation innerhalb einer Windows-Umgebung als auch zwischen Windows und anderen IT-Systemen wie z. B. Samba oder MacOS.

Bei der Planung muss berücksichtigt werden, dass einige Sicherheitseinstellungen für SMB, RPC und LDAP nach einer Standardinstallation nicht gesetzt sind. Hinweise zu den Einstellungen sind unter den Hilfsmitteln zum IT-Grundschutz zu finden (siehe *RPC, SMB und LDAP unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*). Die Sicherheitseinstellungen sollten überprüft und gegebenenfalls angepasst werden.

Neben den dort genannten Einstellungen sollten mindestens die Standard-Sicherheitseinstellungen von Windows Server 2003 mit Service Pack 1 aktiv sein (siehe *Windows Default Security and Services Configuration.xls* aus dem *Microsoft Security Guide* "*Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*" Version 2.0 vom 27. Dezember 2005).

Kompatibilität

Kompatibilität in heterogenen Netzwerken

Die nach einer Standardinstallation vorzunehmenden Sicherheitseinstellungen sind mit den in G 2.114 *Uneinheitliche Windows-Server-2003-Sicherheitseinstellungen bei SMB, RPC und LDAP* beschriebenen Gefahren verbunden. In einem heterogenen Netz sollten diese Einstellungen erst durch das Änderungsmanagement freigegeben werden, nachdem die Verträglichkeit mit allen beteiligten Systemtypen erfolgreich in einem isolierten Testsystem erprobt wurde. Im Test sollte auch die Verfügbarkeit bei hoher Last erprobt werden. Mit Systemtypen sind hier Clients und Server unterschiedlicher Windows-Versionen und Service Packs sowie unterschiedlicher Betriebssystem-Plattformen gemeint. Ausführliche Kompatibilitätshinweise sind im *Microsoft Knowledge Base Artikel 823659* Revision 11 vom 9. Februar 2006 (oder einer späteren Revision) dokumentiert. Die deutsche Revision 3.3 ist veraltet, enthält missverständliche Übersetzungen und sollte daher nicht als Referenz verwendet werden.

Einige grundlegende Kompatibilitätshinweise, geeignete Werkzeuge sowie Hinweise zur Vorgehensweise bei der Aktivierung sind in den Hilfsmitteln zum IT-Grundschutz zu finden (siehe *RPC, SMB und LDAP unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Werkzeuge

Sicherheitsvorlage

Die Einstellungen sind in einer Sicherheitsvorlage für diesen Server einzustellen, siehe dazu M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003*.

Dokumentation

Eine minimale Dokumentation muss die wirksame Sicherheitsvorlage für jeden Server und deren Inhalt enthalten. Falls einzelne Einstellungen nicht flächendeckend übernommen werden, so sind die jeweiligen Bereiche abzugrenzen, zu begründen und auf alternative Sicherheitsmaßnahmen zu verweisen, z. B. eine stärkere Isolierung des oder der Server oder die Aktivierung von IPSec (siehe M 5.90 *Einsatz von IPSec unter Windows 2000/XP*).

Zumindest die wirksame Sicherheitsvorlage für jeden Server dokumentieren

Ergänzende Kontrollfragen:

- Wurden die Standard-Sicherheitseinstellungen zur Kommunikation innerhalb einer Windows-Umgebung gemäß den Empfehlungen dieser Maßnahme angepasst und getestet?
- Werden Authentisierungsvorgänge durch die Kommunikationsprotokolle angemessen abgesichert?
- Wurden bei heterogenen Netzen Kompatibilität und Lastverhalten berücksichtigt und in einer isolierten Testumgebung getestet?

M 4.278 Sichere Nutzung von EFS unter Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Vertraulichkeit für dedizierte lokale Daten

Das verschlüsselnde Dateisystem (Encrypting File System, EFS) von Windows Server 2003/XP ist für Benutzer ein einfach zu bedienendes Mittel zum anwendungsunabhängigen Arbeiten mit verschlüsselten Dateien. Es eignet sich am besten für einzelne Benutzer und exponierte Client-Computer, die zeitweise außerhalb der geschützten IT-Umgebung zum Einsatz kommen. Die Hauptintention ist das Herstellen von Vertraulichkeit für dedizierte lokale Daten. Grundlagen sind M 4.147 *Sichere Nutzung von EFS unter Windows 2000/XP* zu entnehmen.

Weniger geeignet ist EFS für die großflächige Verschlüsselung von zentralisierten Benutzerdaten auf Remote-Servern, beispielsweise Dateiservern. Dies ist nur mit spezieller Planung der Schlüsselverwaltung zu realisieren. Einen erheblichen Aufwand für die Sicherung und den Schutz großer Datenmengen und einer Vielzahl von Benutzerschlüsseln muss in Kauf genommen werden.

Unterschiede bei der Implementierung

Zu Beginn der Planung sollte klar unterschieden werden, ob mit EFS die Verschlüsselung von servergespeicherten Dateien im Netz angeboten werden soll oder ob es nur darum geht, Sitzungsdaten und vertrauliche administrative Daten lokal auf dem Server zu verschlüsseln. In letzterem Fall funktioniert der Server wie ein Client-Computer mit aktiviertem EFS und es sollte die Maßnahme M 4.147 *Sichere Nutzung von EFS unter Windows 2000/XP* umgesetzt werden. Es sollte jedoch mit der Verschlüsselung von Statusinformationen des Systems (z. B. DNS-Zonendateien, Druckerwarteschlange auf Druckservern), Protokolldateien (z. B. IIS-Protokoll) und den gemeinsamen temporären Ordnern (*C:\WINDOWS\Temp*) äußerst sparsam umgegangen werden. Hier sind Tests unter lastähnlichen Bedingungen zu empfehlen, bevor die Verschlüsselung für solche kritischen Dateien eingeschaltet wird, sonst kann durch G 4.54 *Verlust des Schutzes durch das verschlüsselnde Dateisystem EFS* der gesamte Server gestört werden.

Verschlüsseln von Sitzungs- und vertraulichen Arbeitsdaten

Eine Möglichkeit, mit EFS die Sicherheit von administrativen Sitzungen auf dem Server zu erhöhen, stellt das Verschlüsseln von Sitzungsdaten (z. B. temporäre Verzeichnisse, Desktop-Ordner, *Eigene Dateien*, Druckerwarteschlange) und vertraulichen Arbeitsdaten wie zum Beispiel Dokumentationsunterlagen dar. Dies ist weniger kritisch, da im Zweifel nur das Profil nicht mehr funktioniert und zentrale Dienste unberührt bleiben. Anwendungen erstellen regelmäßig zur Laufzeit temporäre Kopien von Dateien. Es ist zu prüfen, welche Ordner von Anwendungen für temporäre Dateien verwendet werden. Für diese Ordner kann EFS aktiviert werden, damit diese Daten nicht während der Bearbeitung von unberechtigten Dritten eingesehen werden können.

EFS als Verschlüsselungsdienst für Remote-Dateien (servergespeicherte Dateien im Netz) sollte nur aktiviert werden, wenn ein sehr hoher Schutzbedarf hinsichtlich der Vertraulichkeit von Daten auf dem Server erforderlich ist und die zusätzlichen Risiken und der Aufwand dafür gerechtfertigt sind. Dies ist in einer Richtlinie für die IT-Umgebung festzuschreiben. Der Einsatzbereich für EFS ist genau zu definieren. Hierzu ist auch die Gefährdung G 4.54 *Verlust des Schutzes durch das verschlüsselnde Dateisystem EFS* zu beachten.

Deaktivieren von EFS nach Standardinstallation

Wird EFS im Zusammenhang mit WebDAV-Freigaben verwendet, findet die Verschlüsselung einer Datei nicht auf dem Server, sondern auf dem Client statt. Die verschlüsselte Datei kann dann auf der WebDAV-Freigabe per HTTP-Transfer abgelegt werden. EFS braucht dazu nicht auf dem Server aktiviert zu werden. Für den Benutzer bestehen dann die gleichen Risiken wie bei der lokalen Verschlüsselung von Daten auf seinem Client. In der oben genannten Richtlinie muss festgehalten werden, in wie weit der Administrator zentrale Mittel zur Wartung, Sicherung und Wiederherstellung solcher Daten bei Schlüsselverlust bereitstellen soll. Je weitgehender dies gefordert wird, desto höher sind die Anforderungen und der Aufwand für das zentrale Schlüsselmanagement.

Die Aktivierung von EFS im Behörden- oder Unternehmensumfeld ist nur mit der gleichzeitigen Nutzung einer Public Key Infrastructure (PKI) und der Konfiguration von Wiederherstellungsagenten zu empfehlen.

EFS deaktivieren

EFS auf Server deaktivieren

Nach einer Standardinstallation von Windows Server 2003 ist EFS aktiv. Ein Wiederherstellungsagent ist nicht konfiguriert. EFS sollte für den normalen Betrieb in der Sicherheitsrichtlinie des Servers deaktiviert werden:

> *Start* | *Systemsteuerung* | *Verwaltung* | *Lokale Sicherheitsrichtlinie* | *Richtlinien öffentlicher Schlüssel* | Eigenschaften von *Verschlüsselndes Dateisystem* | *Benutzer dürfen das Verschlüsselnde Dateisystem verwenden* deaktivieren

Active-Directory

In einer Active-Directory-Umgebung sollte diese Einstellung durch eine Gruppenrichtlinie für alle Server- und Clientcomputer vorgegeben werden.

Wenn EFS nachträglich auf einem laufenden System deaktiviert wird, empfiehlt es sich, das System nach noch verschlüsselten Datenbeständen zu durchsuchen. Dies kann z. B. mit dem Programm *EFSinfo.exe* aus den *Support Tools* für Windows Server 2003 durchgeführt werden.

Beispiel für Befehl an der Kommandozeile: efsinfo /s:c:\

Rollentrennung für den DRA

Datenwiederherstellungsagent

Eine geeignete Rollentrennung verhindert, dass Administratoren uneingeschränkt auf verschlüsselte Daten zugreifen können. Eine kritische Rolle spielt der Datenwiederherstellungsagent (Data Recovery Agent, DRA), mit dem Daten zentral und unabhängig von den verschlüsselnden Benutzern wiederhergestellt werden können. Datenwiederherstellungsagenten werden in Form spezieller Sicherheitszertifikate erzeugt. Folgende Bedingungen sollten für einen DRA eingehalten werden:

- Das vordefinierte Administratorkonto darf nicht mit einem DRA-Zertifikat versehen werden
- Benutzerkonten, die die Rolle eines DRA übernehmen, sollten generell keine Administratorrechte besitzen
- Es sind so wenige Datenwiederherstellungsagenten wie möglich zu erstellen
- Es ist stets ein separates Konto für den Einsatz als DRA zu verwenden

Der private Schlüssel des DRA sollte kennwortgeschützt auf einen externen Datenträger exportiert und vom System gelöscht werden. Der Datenträger mit der Sicherung des privaten Schlüssels ist in einem Bereich mit geschütztem Zugang (Tresor) zu verwahren. Zur Erhöhung der Sicherheit können die Kennwörter getrennt von den Datenträgern aufbewahrt werden.

Es sollte erwogen werden, ein Hardware-Sicherheitsmodul (HSM, siehe B 1.7 *Kryptokonzept*) einzusetzen, um die Sicherheit des privaten Schlüssels eines DRA zu erhöhen.

Datensicherung

Das Dienstkonto für die Datensicherung sollte keinerlei EFS- oder Wiederherstellungszertifikat besitzen und somit Daten nur verschlüsselt lesen und auf das Sicherungsmedium schreiben können.

Abgelaufene DRA-Zertifikate

Abgelaufene DRA-Zertifikate ermöglichen Zugriff und Wiederherstellung

Abgelaufene DRA-Zertifikate bleiben weiterhin sicherheitskritisch, weil sie

- Zugriff auf alle bisher verschlüsselten Daten ermöglichen (gefährdete Vertraulichkeit).
- die einzige Wiederherstellungsmöglichkeit für den bisher verschlüsselten Datenbestand auf dem Server sind (gefährdete Verfügbarkeit).

Rechtzeitig neue DRA-Zertifikate anlegen

Vor Ablauf des alten DRA-Zertifikats muss ein neues hinzugefügt werden, da unmittelbar nach Ablauf die Verschlüsselung nicht mehr funktioniert. Für den neuen DRA müssen die gleichen Sicherheitsmaßnahmen umgesetzt werden (siehe oben). Dies ist bei Planung und Betrieb zu berücksichtigen.

Löschen alter DRA-Zertifikate

Die Entsorgung eines alten DRA-Zertifikats ist nur ratsam, nachdem der gesamte Datenbestand entschlüsselt und mit einem neuen DRA wieder verschlüsselt wurde. Dies kann, abhängig von der Datenmenge und -organisation, einen erheblichen Aufwand und ein erhebliches Risiko für die Verfügbarkeit und Integrität der Daten mit sich bringen und sollte nur in Ausnahmefällen durchgeführt werden, z. B. wenn die Schlüsselstärke des bisherigen DRA-Zertifikats als nicht mehr ausreichend erachtet wird.

Zentrales Schlüsselmanagement

Problem: selbst signierte Zertifikate

EFS erfordert ein definiertes zentrales Schlüsselmanagement. Der Einsatz einer Public Key Infrastructure (PKI) ist dringend empfohlen, damit nicht selbst signierte Zertifikate des lokalen Servers oder Clients benutzt werden. Weitere Informationen zu diesem Thema sind unter den Hilfsmitteln zum IT-Grundschutz zu finden (siehe *Schutz der Zertifikatsdienste unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Es ist außerdem empfehlenswert, das automatische Verlängern der EFS-Zertifikate zu erlauben, da nach deren Ablauf sonst auf selbst signierte Zertifikate zurückgegriffen wird.

Wiederherstellungsagent

Es ist notwendig, einen Wiederherstellungsagenten festzulegen, um Gefahren wie G 4.55 *Datenverlust beim Zurücksetzen des Kennworts in Windows Server 2003 und Windows XP* vorzubeugen. Der Assistent hierfür ist unter

> *Start* | *Systemsteuerung* | *Verwaltung* | *Lokale Sicherheitsrichtlinie* | *Richtlinien öffentlicher Schlüssel* | *Verschlüsselndes Dateisystem* | Menüpunkt *Aktion* | *Datenwiederherstellungs-Agenten erstellen...*

aufzurufen.

Archivierung privater Schlüssel

Das Risiko des Verlusts der Benutzerschlüssel kann weiter verringert werden, indem die Archivierung der privaten Schlüssel auf der Zertifizierungsstelle zugelassen wird, welche die EFS-Zertifikate ausstellt. Allerdings können die Schlüssel durch die zentrale Speicherung einem erhöhten Missbrauchsrisiko ausgesetzt sein. Dadurch entsteht ein deutlich höherer organisatorischer und administrativer Aufwand für die Zertifizierungsdienste, insbesondere für Schlüsselwiederherstellungsagenten, Rollentrennung und Schutz der Zertifizierungsstelle insgesamt.

Wiederherstellungsstation

Für größere IT-Verbundsysteme empfehlenswert

In größeren IT-Verbünden sollte die Einrichtung einer Wiederherstellungsstation erwogen werden, welche in einem Bereich mit gesicherter Zugangskontrolle verwahrt und nur im Bedarfsfall aktiviert wird. Die zu entschlüsselnden Dateien können mit einem Sicherungswerkzeug wie *ntbackup* auf die Wiederherstellungsstation übertragen und dort mit dem Schlüssel des DRA wiederhergestellt werden. Der DRA-Schlüssel kann auf der Wiederherstellungsstation verbleiben. Ein weiterer Vorteil der Verwendung einer Wiederherstellungsstation ist, dass der Schlüssel auf der Wiederherstellungsstation nicht durch nicht vertrauenswürdige Software gefährdet werden kann.

Für die Wiederherstellungsstation kann Virtualisierungstechnologie eingesetzt werden. Das heißt, das gesamte Betriebssystem wird in einer simulierten Hardware-Umgebung installiert. Diese virtuelle Umgebung kann leicht auf einem Wechseldatenträger gespeichert und sicher verwahrt werden.

Schulung

Zur Funktion und den Risiken von EFS muss der Benutzer geschult werden. Mit geschulten Benutzern und einem Schlüsselmanagement kann durch die Nutzung von EFS ein Sicherheitsgewinn erzielt werden.

Ergänzende Kontrollfragen:

- Wird EFS nur bei hohem Schutzbedarf hinsichtlich der Vertraulichkeit eingesetzt?
- Ist der Einsatzbereich (z. B. Verschlüsselung der Sitzungsdaten auf dem Server) definiert und sind alle Nutzer angemessen geschult?
- Erfolgt der Einsatz von Datenwiederherstellungsagenten (DRA) restriktiv?

- Werden abgelaufene DRA-Zertifikate sicher aufbewahrt?
- Besitzt das Dienstkonto für die Datensicherung keine EFS- oder Wiederherstellungszertifikate?
- Existiert ein zentrales Schlüsselmanagement in Form einer Public Key Infrastructure (PKI)?
- Wird eine Wiederherstellungsstation eingesetzt?

M 4.279 Erweiterte Sicherheitsaspekte für Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Für IT-Verbünde mit erhöhtem Schutzbedarf, in denen Windows Server 2003 eingesetzt wird, sind zusätzliche Maßnahmen zur Erreichung eines solchen Schutzniveaus erforderlich. Damit ist nicht nur die Erhöhung der Verfügbarkeit des Systems insgesamt gemeint (Redundanz, Hochverfügbarkeitscluster), sondern auch gezielte Maßnahmen zum erhöhten Schutz der Vertraulichkeit und Integrität von Anwendungen, Daten und Datenverkehr im Netz. Die Maßnahmen können unter Umständen eine Einschränkung von Funktionalität oder Interoperabilität bedeuten. Deshalb sollte auf jeden Fall eine Testumgebung zur Verfügung stehen, um die gewünschte Funktionalität sicherzustellen.

Die nachfolgend erläuterten Aspekte sind bereichsübergreifend und keinesfalls erschöpfend. Je nach Rolle des Servers, Einsatzszenario und entsprechender Gefährdungslage sind weitere Vorkehrungen zu treffen. In den spezifischen Maßnahmen für Windows Server 2003 werden dazu weitere Anhaltspunkte genannt.

Produktaktivierung

Die Online-Produktaktivierung benötigt eine aktive Internetverbindung und das HTTP-Protokoll. Während der Installationsphase sollte diese Verbindung nur über ein Sicherheits-Gateway mit Proxyserver realisiert werden, d. h. die Option *AutoActivate* darf ausschließlich gemeinsam mit der Option *ActivateProxy* verwendet werden. Dazu muss die Antwortdatei manuell editiert werden. Die Aktivierung kann auch später skriptgesteuert (z. B. im Post-Installationsskript) oder manuell ausgelöst werden.

Telefonische Produktaktivierung

Bei hohem Schutzbedarf des Servers kann auf die telefonische Aktivierung ausgewichen werden.

Verschlüsselung

IPSec

Durch *IPSec* können alle IP-basierten Kommunikationsverbindungen von und zu einem Client abgesichert werden. Dabei ist es möglich, die Endpunkte der Kommunikation zu authentisieren und die Datenpakete signiert und verschlüsselt zu übertragen, so dass die Integrität und Vertraulichkeit der Daten bei erhöhten Anforderungen an die Sicherheit gewährleistet werden kann. Das Teilkonzept für eine IPSec-Infrastruktur sollte den erhöhten Administrationsaufwand berücksichtigen und setzt eine Verträglichkeitsprüfung mit den beteiligten Systemen in einer Testumgebung voraus.

FIPS-konforme Verschlüsselung

Falls Verschlüsselung gemäß den Richtlinien FIPS (Federal Information Processing Standard) der US-amerikanischen Behörde NIST (National Institute of Standards and Technology) für das *SSL/TLS-Protokoll* und für das *Encrypting File System* (EFS) benötigt wird, kann dies unter

Konsole *Lokale Sicherheitsrichtlinie | Lokale Richtlinien Sicherheitsoptionen | Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden*

eingestellt werden. Die Aktivierung bedeutet sichere Verschlüsselung (z. B. 3DES), aber nicht unbedingt immer höchstmögliche Schlüssellänge. Beispielsweise wird AES (beim EFS) nicht berücksichtigt.

Erhöhter Rechenaufwand

Generell darf der erhöhte Rechenaufwand und der mögliche Einfluss auf das Lastverhalten des Servers nicht vernachlässigt werden.

Weiterhin sollte *Systemkryptografie: Starken Schlüsselschutz für auf dem Computer gespeicherte Benutzerschlüssel erzwingen* mindestens auf *Benutzer wird zur Eingabe aufgefordert, wenn der Schlüssel zum ersten mal verwendet wird* setzen. Dadurch wird bei Zugriff auf den privaten Schlüssel eines Sicherheitszertifikats die Kennworteingabe erzwungen.

Hochverfügbarkeit

Bei hohen Verfügbarkeitsanforderungen kann es erforderlich sein, nicht nur Teile der Serverhardware, sondern den gesamten Server redundant auszulegen und in einem Hochverfügbarkeits-Cluster zusammenzufassen. Windows Server 2003 Enterprise Edition unterstützt mittels des *Clusterdienstes* acht Knoten in einem Cluster, die je nach Anforderung für Hochverfügbarkeit und Lastverteilung optimiert werden können. Jeder der redundanten Server sollte einheitlichen Hardwareanforderungen gerecht werden. Die Planung des Clusters muss bei der Rollenplanung berücksichtigt werden, da bestimmte Dienste nur eingeschränkt clusterfähig sind.

Der *Netzwerklastenausgleich* wird nicht nur von der Enterprise Edition, sondern auch von der Web Edition und der Standard Edition unterstützt.

Denial-of-Service

Um sich gegen DoS-Attacken abzusichern, sollten die TCP/IP-Einstellungen des Servers (siehe Hilfsmittel zum IT-Grundschutz, *Absichern von IP-Protokollen unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*) überprüft und gegebenenfalls gesetzt werden. Zum Setzen der Registrierungsschlüssel wird die Verwendung von administrativen Vorlagen empfohlen (siehe M 2.368 *Umgang mit administrativen Vorlagen unter Windows Server 2003*). Diese Vorkehrungen sollten auf jeden Fall ausgeführt werden, wenn der Server in einer exponierten Umgebung eingesetzt wird, z. B. als Sicherheits-Gateway oder in einer Demilitarized Zone (DMZ). Innerhalb einer geschützten IT-Umgebung sind sie optional.

Spezifische Schutzmaßnahmen für Webserver oder Bastion Host

Der Einsatz als Webserver oder als sogenannter *Bastion Host* (öffentlich erreichbarer Computer des Unternehmensnetzes) erfordert weitere spezifische Schutzmaßnahmen, die z. B. im Baustein B 5.10 *Internet Information Server* beschrieben sind.

Plug and Play

Automatische Hardwareerkennung

Ein weiteres Gefahrenpotential stellt die automatische Hardware-Erkennung (*Plug and Play*) dar, falls der Server nicht hineichend vor unbefugtem Zugang geschützt ist. Im Normalfall genügt es, alle nicht benötigten Anschlüsse zu deaktivieren (z. B. im *BIOS* und im Windows-*Gerätemanager*). Laufwerke für

Wechseldatenträger sollten entfernt oder verschlossen werden oder durch Software-Werkzeuge von Drittherstellern kontrolliert werden. Windows Server 2003 stellt entsprechende Funktionalitäten nur sehr eingeschränkt zu Verfügung.

Die vollständige Umgehung von *Plug and Play* ist in Windows Server 2003 nicht vorgesehen und beeinträchtigt die Systemstabilität. Der Testaufwand und das Risiko sind nur bei besonders hohen Sicherheitsanforderungen gerechtfertigt.

Ressourcenberechtigungen

Systemhärtung

Die standardmäßigen Ressourcenberechtigungen in den Systemordnern und an Systemobjekten sind restriktiv, sollten aber bei sehr hohem Schutzbedarf gehärtet werden. Hierzu werden die Berechtigungen für bestimmte Standardgruppen entzogen und explizit an bestimmte Benutzerkonten vergeben.

Die Einstellung in der Konsole *Lokale Sicherheitsrichtlinie* | *Lokale Richtlinien Sicherheitsoptionen* | *Systemobjekte: Standardbesitzer für Objekte, die von Mitgliedern der Administratorengruppe erstellt werden* steht standardmäßig auf *Administratorgruppe*. Besitzer haben immer besondere Berechtigungen auf ihr Objekt. Außerdem kann die Überwachung von Gruppen als Besitzer von Objekten nicht optimal gelöst werden. Die Einstellung *Administratorengruppe* sollte durch *Objektersteller* ersetzt werden. Dies verschlechtert jedoch die Administrierbarkeit des Servers erheblich.

M 4.280 Sichere Basiskonfiguration von Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Sichere Konfiguration bedeutet die Umsetzung von Einstellungen, die sich aus den Sicherheitsrichtlinien und -vorgaben, den Rollen des Servers und der IT-Umgebung ergeben. Eine Reihe von Einstellungen findet sich bei vielen Rollen und Szenarien wieder.

Regelmäßig überprüfen

Die sichere Basiskonfiguration muss während der Bereitstellung des Servers, bei Änderungen der Serverkonfiguration und bei Änderungen von Vorgaben und Richtlinien durchgeführt werden. Außerdem empfiehlt es sich, die Durchsetzung der Einstellungen turnusmäßig zu überprüfen, um Fehleinstellungen durch alltägliche Administrationsarbeiten oder sonstige Einflüsse zu vermeiden.

Checkliste

Die notwendigen Einstellungen sind zu identifizieren, z. B. in Form einer Checkliste. In der Liste sollten die bei der Grundschutzmodellierung gefundenen Maßnahmen berücksichtigt werden.

Ein Beispiel für eine Liste ist unter den Hilfsmitteln zum IT-Grundschutz zu finden (siehe *Sichere Basiskonfiguration von Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Standard-Sicherheitseinstellungen und Sicherheitsvorlagen

Quellenangaben zu den Einstellungen
Vorlagen verwenden

Für die gefundenen Einstellungen sollten nach Möglichkeit Sicherheitsvorlagen und administrative Vorlagen (M 2.368 *Umgang mit administrativen Vorlagen unter Windows Server 2003*) erstellt werden. Dadurch wird der Grad an Standardisierung und Automatisierung der Basiskonfiguration erhöht, die Einstellungen können später leichter überprüft und revisioniert werden. Die Basiskonfiguration kann mit relativ wenig Aufwand dokumentiert werden, indem die Vorlagen exportiert und der Dokumentation beigefügt werden. Darauf aufbauend kann ein Freigabeprozess für die Basiskonfiguration im IT-Änderungsmanagement (M 2.221 *Änderungsmanagement*) etabliert werden.

Sichere Standardeinstellungen nicht grundlos ändern

Die genannten Aspekte setzen voraus, dass die Standardeinstellungen von Windows Server 2003 nicht willkürlich manipuliert werden. Standard-Gruppenmitgliedschaften sollten belassen, Basisrechte für systeminterne Konten (z. B. *NT-Autorität*) sollten nicht manipuliert werden. Standardberechtigungen in Subkomponenten wie z. B. *WMI* und den Komponentendiensten sollten erhalten bleiben. Abweichungen sollten in Form von Checklisten und Vorlagen geplant, begründet und durchgeführt werden, insbesondere wenn die Abweichung eine Verschlechterung des Sicherheitsstandards bewirken könnte. Als Referenz für Standardeinstellungen dienen die mitgelieferten Sicherheitsvorlagen, hauptsächlich *defltsv.inf* (für Server) und *defltdc.inf* (für Domänencontroller) im Ordner *C:\WINDOWS\inf*. In der Vorlage *setup security.inf* (Ordner *C:\WINDOWS\security\templates*) sind alle Einstellungen nach Abschluss des Setup-Programms festgehalten.

Weitere Informationen sind in M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003* zu finden.

Weitere Referenzen sind die Konfigurationsvorlagen des Sicherheitskonfigurations-Assitenten (ab Service Pack 1), die Tabelle *Windows Default Security and Services Configuration.xls* (aus der Herstellerdokumentation "*Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*" Version 2.0 vom 27. Dezember 2005 oder später), die Maßnahmen des IT-Grundschutzes sowie sonstige Dokumentationsunterlagen des Herstellers.

In den weiteren Abschnitten dieser Maßnahme werden einige Einstellungen und Vorgaben aufgezählt. Sie sind nicht in anderen Maßnahmen für Windows Server 2003 enthalten, beeinflussen aber die Sicherheit der Basiskonfiguration. Sie sollten beim Erstellen der Checkliste ebenfalls berücksichtigt werden.

Wichtige sicherheitsrelevante Funktionen

NTFS verwenden

Festplattenpartitionen sollten bei der ersten Formatierung ausschließlich mit NTFS formatiert werden. Das Setup-Programm von Windows Server 2003 nimmt während der Installation u. U. eine Konvertierung der Systempartition vor. Auf einem produktiven System sollte das nachträgliche Konvertieren von FAT32-Partitionen jedoch vermieden und gleich NTFS gewählt werden.

Auslagerungsdatei löschen

Aus der Auslagerungsdatei des Arbeitsspeichers können unverschlüsselte Daten extrahiert werden. Die Auslagerungsdatei sollte bei jedem Herunterfahren automatisch gelöscht werden:

> *Start* | *Systemsteuerung* | *Verwaltung* | Konsole *Lokale Sicherheitsrichtlinie* öffnen | auswählen des Knotens *Lokale Richtlinien* | *Sicherheitsoptionen* | *Herunterfahren: Auslagerungsdatei des Virtuellen Arbeitsspeichers löschen*

Plug and Play

Ein weiteres Gefahrenpotential stellen die automatische Hardware-Erkennung (*Plug and Play*) sowie *Autorun*-Funktionen (Automatisches Starten von Programmen) dar, falls der Server nicht hinreichend vor unbefugtem Zugang geschützt ist. Alle nicht benötigten Anschlüsse sollten deaktiviert werden (z. B. im *BIOS* und im Windows-*Gerätemanager*). Es ist auch zu überlegen, ob Laufwerke für Wechseldatenträger entfernt oder physikalisch verschlossen werden können. Alternativ kann die Verwendung von Wechselmedien durch Software-Werkzeuge von Drittherstellern kontrolliert werden. Windows bietet hierfür keine eigenen ausreichenden Mittel.

Systemzeit synchronisieren

Der sichere Betrieb von mehreren Servern setzt eine synchrone Systemzeit voraus. Hierfür kann der im System vorhandene Client für das Network Time Protocol (NTP) genutzt werden

Gruppen als Besitzer von Objekten

Besitzer haben immer besondere Berechtigungen auf ihre Objekte. Erstellt ein administrativer Benutzer ein Objekt, ist standardmäßig die lokale Sicherheitsgruppe *Administratoren* der Besitzer. Für Gruppen als Besitzer von Objekten kann die Überwachung nicht optimal gelöst werden. Datenträgerkontingente werden ebenfalls anhand des Dateibesitzes diskreter Benutzer gesteuert. Durch Gruppen als Besitzer von Dateien kommen irreführende Kontingenteinträge und Screeningergebnisse (ab Windows

Server 2003 R2) zustande. Diese Problematik sollte in erster Linie durch geeignete Konzepte gelöst werden, welche sich mit den Bereichen Überwachungseinstellungen, Berechtigungen (z. B. Berechtigungskonzept) und Datenträgerkontingente (z. B. Teilkonzept für einen Dateiserver) befassen.

Anonyme Aufzählung von Freigaben

Wenn keine Kompatibilität zu Windows NT 4.0, Windows ME/98 oder früher benötigt wird, sollte überlegt werden, die anonyme Aufzählung von Freigaben zu deaktivieren:

Start | *Systemsteuerung* | *Verwaltung* | Konsole *Lokale Sicherheitsrichtlinie* öffnen | auswählen des Knotens *Lokale Richtlinien* | *Sicherheitsoptionen* | *Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten und Freigaben nicht erlauben* setzen auf *Aktiviert*

Weitere Sicherheitskomponenten

Wiederherstellungs-konsole

Auf unveränderten Windows-Server-2003-Installationsdatenträgern befindet sich eine eingeschränkte Kommandozeilenumgebung (*Wiederherstellungs-konsole*), die auf dem Server alternativ zum Betriebssystem gestartet werden kann. Damit kann die Konfiguration des installierten Windows-Betriebsystems manipuliert werden. Für die Authentisierung wird das Kennwort des in der Windows-Server-2003-Installation standardmäßig vordefinierten Administratorkontos abgefragt. Dies funktioniert unabhängig davon, ob das Konto umbenannt oder deaktiviert wurde. Die Wieder-herstellungskonsole kann auch direkt auf die Festplatte installiert werden und verhält sich wie ein zusätzlich installiertes Betriebssystem. In beiden Fällen stellt dies einen Eingriff in den Bootvorgang dar, wodurch dieser weniger geschützt ist. Die Installation der Wiederherstellungskonsole sollte daher nicht willkürlich erfolgen, sondern in einer Richtlinie geregelt werden. Die Sicherheitseinstellungen nach einer Standardinstallation (*Start* | *Systemsteuerung* | *Verwaltung* | Konsole *Lokale Sicherheitsrichtlinie* öffnen | auswählen des Knotens *Lokale Richtlinien* | *Sicherheitsoptionen* | *Wiederherstellungskonsole*) sollten beibehalten werden.

Verstärkte Sicherheitskonfiguration für Internetexplorer

Nach einer Standardinstallation ist die *Verstärkte Sicherheitskonfiguration für Internetexplorer* aktiv (*Systemsteuerung* | *Software* | *Windows-Komponenten*). Diese Komponente sollte nur deaktiviert werden, falls eine Internet-Explorer-basierte Applikation (eines Drittherstellers), die auf dem Server benötigt wird, nicht damit kompatibel ist.

Windows-Firewall, Schutz des Bootvorgangs

Die Windows-Firewall wird ab Windows Server 2003 mit Service Pack 1 beim Boot-Vorgang gemeinsam mit dem TCP/IP-Protokoll geladen und aktiviert, wodurch das TCP/IP-Protokoll bereits während des Bootvorgangs besser geschützt wird. Der Dienst *Windows-Firewall/Gemeinsame Nutzung der Internetverbindung* muss dafür auf *Automatisch* gesetzt sein.

Nach dem Bootvorgang ist die Firewallfunktionalität (nicht der Dienst selbst) standardmäßig wieder inaktiv. Bei Sicherheitsvorfällen im lokalen Netz (sich ausbreitende Schadprogramme oder Angriffe von innen) ist der Server ungeschützt. Daher sollte überlegt werden, die Aktivierung der Windows-Firewall bei einer sicheren Basiskonfiguration zu berücksichtigen.

Hierzu können gezielt die typischen Dienste und Funktionen in der lokalen Gruppenrichtlinie (*Start* | *Ausführen...* | *gpedit.msc*) freigeschaltet werden (*Computerkonfiguration* | *Administrative Vorlagen* | *Netzwerk* | *Netzwerkverbindungen* | *Windows Firewall*) oder die Konfiguration mittels des SCW durchgeführt werden. Die Windows-Firewall unterstützt RPC-Dienste, welche über die vordefinierten Konten *Lokales System*, *Lokaler Dienst* und *Netzwerkdienst* laufen, beispielsweise für die Remote-Administration. Zusatzsoftware mit RPC-Diensten muss vorher getestet werden.

Nicht benötigte Funktionen abschalten

Nicht benötigte Basis- und Hilfsfunktionen abschalten

Auf einem Windows Server 2003 System sind häufig Basis- und Hilfsfunktionen aktiv, die nicht in jedem Fall benötigt werden. Es gilt das Prinzip: deaktivieren, um die Angriffsfläche und unnötige Risiken zu minimieren. Möglicherweise sinkt dadurch die Flexibilität von Windows Server 2003 und der Administrationsaufwand steigt. Aus Sicherheitsgründen sollten deaktivierte Funktionen trotzdem nur mit entsprechender Begründung bzw. Dokumentation wieder aktiviert werden.

Nur erforderliche Funktionen aktivieren

Es sollte genau überlegt werden, welche Funktionen für den konkreten Einsatz eines Windows Servers 2003 benötigt werden, so dass nur diese aktiviert werden. Unter den Hilfsmitteln zum IT-Grundschutz ist eine Tabelle mit einer Auswahl an Funktionen und Empfehlungen enthalten, die in der oben genannten Checkliste berücksichtigt werden können (siehe *Sichere Basiskonfiguration von Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*). Von Funktionen ohne konkrete Empfehlung ist im Einzelfall nur ein geringes Bedrohungspotential zu erwarten. Sofern sie nicht benötigt werden, sollten sie deaktiviert werden bzw. bleiben.

Die darin nicht genannten Dienste aus der Konsole *Dienste* sollten auf die Standardeinstellung von Windows Server 2003 (mit Service Pack 1) gesetzt werden (siehe die in der Herstellerdokumentation "*Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*" Version 2.0 vom 27. Dezember 2005 oder später erwähnte Excel-Datei *Windows Default Security and Services Configuration.xls*).

Hinweis: Durch zu restriktives Abschalten von Diensten kann das System in einen nicht lauffähigen Zustand geraten. Zum Erhalt der Verfügbarkeit des Systems ist ein entsprechender Testaufwand zu betreiben.

Dokumentation

Die Dokumentation der Basiskonfiguration sollte den Anforderungen des Änderungsmanagements entsprechen. Sie sollte alle verwendeten Vorlagen mit Versionsnummer und Beschreibung enthalten. Für jeden Server sollte ersichtlich sein, welche Vorlagen bei ihm wirken.

Ergänzende Kontrollfragen:

- Ist die Windows-Firewall aktiviert und konfiguriert?
- Sind die notwendigen Einstellungen für die Basiskonfiguration dokumentiert, z. B. in Form einer Checkliste?

- Wurden für die Einstellungen Sicherheitsvorlagen und administrative Vorlagen erstellt?
- Falls die Standardeinstellungen verändert wurden, ist dies anhand von Checklisten und Vorlagen geplant, begründet und durchgeführt worden?
- Sind nicht benötigte Basis- und Hilfsfunktionen abgeschaltet?

M 4.281 Sichere Installation und Bereitstellung von Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Installationskonzept, Bereitstellungskonzept

Die Bereitstellung umfasst die Schritte nach Planung und Beschaffung des Servers oder einer Gruppe von Servern bis zur Aufnahme des produktiven Betriebs. Besonders kritisch ist die Installation des Betriebssystems. Während dieser Phase greifen die Schutzmechanismen von Windows Server 2003 nicht. Viele Vorgaben aus IT-Sicherheitsrichtlinien können erst auf einem installierten Server durchgesetzt werden. Andererseits werden wichtige Parameter für den späteren Betrieb schon durch die Installation festgelegt. Daher muss ein Installationskonzept gemäß M 2.318 *Sichere Installation eines Servers* erstellt werden, das dem spezifischen Verhalten von Windows Server 2003 Rechnung trägt. Bei einer Gruppe von Servern oder bei wiederkehrenden Installationen gewinnt die Automatisierung und Standardisierung von Installationen an Bedeutung, außerdem haben die vorhandene IT-Umgebung und eventuell vorhandene Software-Management-Systeme Einfluss auf die Installation und Bereitstellung. Solche Betrachtungen sprengen oft den Rahmen eines Installationskonzepts für den einzelnen Server. Daher ist die Erstellung eines umfassenderen, wiederverwendbaren Bereitstellungskonzepts zu empfehlen, welches die bestehenden Installationskonzepte berücksichtigt. Die Konzepte für Installation und Bereitstellung sollten so angelegt sein, dass dem Administrator eine konkrete Handlungsanweisung für seinen jeweiligen Installationsauftrag zur Verfügung steht.

Bereitstellungsvarianten

Neben der manuellen Installation von einem unveränderten Windows-Server-2003-Datenträger sind zwei grundlegende Bereitstellungsvarianten zu unterscheiden: Festplattenabbild (Image) und Installation von einer Installationsquelle mittels Setup-Programm. Mit beiden Varianten ist eine Automatisierung und Standardisierung auf unterschiedliche Art und Weise möglich.

In der Abbildung werden für die weiteren Betrachtungen diese Bereitstellungsvarianten exemplarisch als zwei mögliche Pfade zugrunde gelegt:

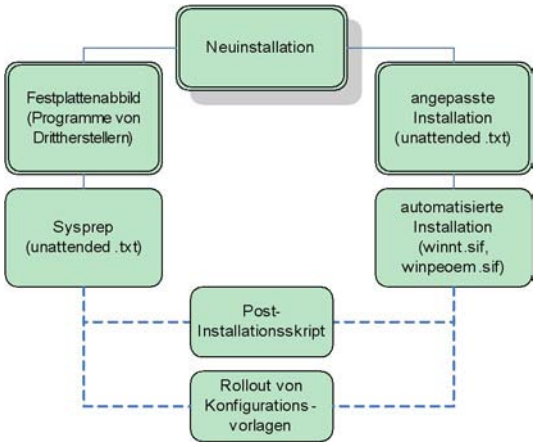


Abbildung: Bereitstellungspfade

Aus der Abbildung können die grundlegenden Mittel für die Bereitstellung und die Reihenfolge abgeleitet werden, in welcher die Mittel vorbereitet werden. Das Szenario kann variiert und durch Zusatz-Software ergänzt werden. Der Administrator sollte zumindest in der Anwendung der hier gezeigten Mittel geschult sein, da sie fast allen Verfahren zugrunde liegen.

Für das Installationskonzept zu berücksichtigende Aspekte

Im Installationskonzept für den einzelnen Server müssen eine Reihe von Faktoren berücksichtigt werden:

- Bootvorgang und Initiierung der Installation
- Treiber für Massenspeichergeräte und gegebenenfalls Netzwerktreiber müssen beim Bootvorgang zur Verfügung gestellt werden
- Art der Installationsquelle (Datenträger, Netzwerk)
- Service Packs in die Installationsquelle integrieren (sog. *slipstreamed*)
- Bereitstellung des Produktschlüssels
- Hardware-Treiber zur Verfügung stellen
- Einspielen von Produktaktualisierungen (Patches)
- gegebenenfalls Domänenbeitritt
- Serverrollen konfigurieren
- sicherheitsrelevanten Einstellungen vornehmen, gemäß Sicherheitsrichtlinien
- Produktaktivierung von Windows Server 2003

Für ein Bereitstellungskonzept werden diese und weitere Aspekte systemübergreifend betrachtet. Eine Orientierungshilfe findet sich unter den Hilfsmitteln zum IT-Grundschutz (siehe *Bereitstellungskonzept von Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Die gängigen Produkte für Softwaremanagement und -verteilung integrieren und automatisieren einige Basismechanismen von Windows Server 2003, z. B. Antwortdateien oder Treiberbereitstellung. Nachfolgend werden daher einige allgemeingültige Sicherheitsaspekte erläutert.

Sicherheitsaspekte

Festplattenabbild

Ein Festplattenabbild wird von einem vollständig installierten lauffähigen Server gezogen und auf einen anderen Server gespiegelt. Ein Manko dieses Verfahrens ist die identische Sicherheitskennung (SID) von gespiegelten Systemen. Für Authentisierungsvorgänge in einer Windows-Umgebung sind eindeutige SIDs zwingend erforderlich. Das Verfahren zur nachträglichen Änderung der SID (*Sysprep* oder Programme von Drittanbietern) greift tief in das System ein und berührt sämtliche sicherheitskritischen Objekte. Außerdem ist ein Festplattenabbild unflexibel gegenüber Änderungen der Hard- und Softwarekonfiguration. Gespiegelte Systeme müssen aktiviert werden, daher sind Mehrfach- oder Volumenlizenzprogramme zu empfehlen. In geeigneten Testverfahren sollte der zuverlässige Betrieb der gespiegelten Systeme nachgewiesen werden.

Abbilder ermöglichen einen hohen Grad an Standardisierung sowie Schutz vor Installationsproblemen. Sie können leicht verwaltet und archiviert werden. Softwaremanagementprogramme können bei der Aufspielung von Festplattenabbildern gewisse Systemparameter anpassen, weitere Anpassung erfolgen durch *Sysprep* (mit Antwortdatei) und Post-Installationsskripte. Die Vorteile dieses Konzeptes kommen bei einer großen Anzahl von Abbildern mit jeweils geringem Anpassungsbedarf zum Tragen.

Angepasste Installation

Automatisierte angepasste Installationen basieren auf einer Antwortdatei für den Installationsvorgang. Sie bieten hohe Flexibilität und Modularität für Hard- und Softwarekonfiguration und sind mit geringem Aufwand anzupassen. Der Installationsverlauf ist anfälliger für Fehler oder Kompromittierungsversuche, allerdings wird für jede Installation ein individuelles Protokoll generiert. Für vollständige Automation sind Lizenzprogramme mit einheitlichem Produktschlüssel zu empfehlen.

Installationsprotokolle aufheben

Am Ende der Installation sollten die Installationsprotokolle gesichert werden. Dies sind *setuplog.txt* und alle Dateien mit der Erweiterung *.log*, im Systemstammverzeichnis (meist *C:\WINDOWS*), sowie alle *.log*-Dateien in *C:\WINDOWS\security\logs*. Die Datei *setuperr.log* muss immer ausgewertet werden.

Antwortdateien verwalten

Antwortdateien (*unattended.txt*, *winnt.sif, winpeoem.sif, ini*-Dateien usw.) enthalten kritische Konfigurationsinformationen, die von unbefugten Personen für Einbruchsversuche missbraucht werden können. Installationsmedien oder Installationsquellen mit angepassten Antwortdateien sollten daher immer vor unbefugtem Zugriff geschützt aufbewahrt bzw. mit eingeschränkten Berechtigungen versehen werden. Zum Erstellen der Antwortdateien dient der Setup Manager (Datei *SetupMgr.exe* auf der Installations-CD bzw. CD1 bei Windows Server 2003 R2 in *\SUPPORT\TOOLS\DEPLOY.CAB*). Der Zugriff sollte auf Administratoren beschränkt werden sowie einer Versionskontrolle unterliegen.

Installationskonten schützen

Besonders wichtig ist Planung der Installationskonten, die während der Bereitstellungsphase verwendet werden sollen. Diese sind ähnlich kritisch wie administrative Konten und sollten entsprechend überwacht werden. Sie sollten mit minimalen Berechtigungen versehen werden, die Möglichkeiten der Anmeldung sollten eingeschränkt sein.

Windows Update

Das Laden von Produktaktualisierungen schon während des Installationsprozesses erhöht die Sicherheit. Dennoch sollten die Aktualisierungen nicht direkt aus dem Internet (*Windows Update*) geladen werden. Vorzugsweise sollte *Dynamic Update* verwendet werden, welches auf eine lokale Quelle zugreift und die individuelle und bewusste Freigabe von Aktualisierungen ermöglicht. Dazu muss die Option *DUShare* manuell in die Antwortdatei eingetragen werden. *DUShare* verweist auf einen Ordner der Installationsquelle, der Update-Pakete in Form von *.cab*-Dateien enthält.

Alternativ zu diesem Verfahren können Produktaktualisierungen nach der Installation mit Hilfe von *Windows Update* und Post-Installationsskripten von einem lokalen Update-Server eingespielt werden. Eines der beiden beschriebenen Verfahren sollte im Bereitstellungskonzept definiert werden.

Hinweis: Die Herstellerdokumentation zum Thema Antwortdateien ist in den Dateien *ref.chm* und *deploy.chm* auf der Installations-CD bzw. CD1 bei Windows Server 2003 R2 in *\SUPPORT\TOOLS\DEPLOY.CAB* zu finden.

Ab Windows Server 2003 mit Service Pack 1 ist während und nach der Installation die lokale Firewall solange aktiv und restriktiv eingestellt, bis der Aktualisierungsprozess einmal durchlaufen wurde. Erst danach ist die volle Konnektivität gegeben. Dieser Modus schützt den Server, wenn Produktaktivierung und -aktualisierung direkt über das Internet vorgenommen werden. Für geringen Schutzbedarf genügt dieses Szenario, jedoch ersetzt es nicht ein isoliertes Installationsnetz.

Konformität mit Sicherheitsrichtlinien

Die Konformität mit den aktuellen Sicherheitsrichtlinien bei Aufnahme des produktiven Betriebs muss durch den Bereitstellungsvorgang gewährleistet werden. Sicherheitsvorlagen werden meist durch Gruppenrichtlinien und Active Directory auf den Server übertragen und aktiviert. Alternativ oder zusätzlich können die Vorlagen mit Hilfe von Post-Installationsskripten eingespielt werden. Die fertige Installation muss mit den aktuellen Vorlagen und den sonstigen aktuellen Sicherheitsvorgaben getestet werden. Das Durchsetzen der Vorlagen und Einstellungen sollte Teil des Installations- bzw. Bereitstellungskonzeptes sein.

Dokumentation

Das Bereitstellungskonzept ist ausführlich und verständlich zu dokumentieren. Es sollte für jeden Server eine aktuelle Installationsanweisung geben.

Ergänzende Kontrollfragen:

- Ist aufgrund der Vielzahl von Servern im IT-Verbund ein Bereitstellungskonzept nötig?
- Ist ein Bereitstellungskonzept erstellt worden, das die Installation per Image bzw. per Antwortdatei berücksichtigt?
- Enthalten die Antwortdateien keine Klartextkennwörter aus der Produktivumgebung?
- Könnten die verwendeten Installationskonten kompromittiert und missbraucht werden?

M 4.282 Sichere Konfiguration der IIS-Basis-Komponente unter Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

IIS als Teilkomponente des Anwendungsservers

Die Internet Information Services (IIS) 6.0 sind eine wichtige Komponente von Windows Server 2003, ohne die viele wichtige Funktionen des Betriebssystems nicht oder nur eingeschränkt zur Verfügung stehen. Die IIS wurden seit Version 5 um neue Technologien erweitert, modularisiert und größtenteils aus dem Betriebsystemkern ausgegliedert. Dieses neue Systemdesign macht die IIS robuster und das Betriebssystem weniger anfällig. Die IIS sind in Windows Server 2003 im Kontext eines Anwendungsservers für Web-basierte Anwendungen integriert. Dementsprechend heißt die Komponente in Windows Server 2003 *Anwendungsserver*. Die IIS sind eine Teilkomponente des Anwendungsservers. Die Komponente *Anwendungsserver* ist nach einer Standardinstallation des Betriebssystems vollständig deaktiviert.

Empfehlungen für Windows-Server-2003-Komponenten oder zusätzliche Applikationen, die IIS benötigen

Die im Folgenden beschriebenen Empfehlungen gehen nicht näher auf die sichere Installation eines Anwendungsservers oder Intranet/Internet-Servers (siehe hierzu B 5.10 *Internet Information Server*) ein. Sie sollten stattdessen immer dann angewendet werden, wenn eine andere Windows Server 2003 Komponente oder eine zusätzliche Applikation die Installation der IIS als Hilfsdienst anfordert. Diese Maßnahme weist auf die einzelnen Punkte hin, die bei einer sicheren Konfiguration der IIS-Basis-Komponente beachtet werden müssen. Konkrete Einstellungen zu den hier aufgeführten Hinweisen sind unter den Hilfsmitteln zum IT-Grundschutz (siehe *Absichern der IIS-Basis-Komponente unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*) zu finden.

Welche Komponenten können installiert werden?

Auf dem Server sollten nur der *COM+-Netzwerkzugriff* sowie die *Internetinformationsdienste* (IIS) aktiviert sein. Für letztere ist die Aktivierung auf *Gemeinsame Dateien*, *Informationsdienste-Manager* und *WWW-Dienst* einzuschränken; optional darf lediglich noch *Internetdrucken* verwendet werden.

Weitere IIS-Dienste neben dem HTTP-Server

Weitere Werkzeuge und Serveranwendungen

Unter *Anwendungsserver* sind die verbreiteten Protokolle SMTP, NNTP und FTP sowie der Message-Queuing-Dienst aufgelistet. Einige Werkzeuge und Serveranwendungen fordern deren Installation an. Mit diesen Protokollen und Diensten sind weitere Gefährdungen verbunden, so dass neben den hier genannten Empfehlungen noch weitere Maßnahmen gemäß den Ergebnissen der Modellierung nach IT-Grundschutz umzusetzen sind (siehe auch M 5.131 *Absicherung von IP-Protokollen unter Windows Server 2003*).

Auf einem Domänencontroller für Active Directory sollten nur die notwendigen IIS-Dienste und -Protokolle installiert sein.

Absichern der Basiskonfiguration

Ordner schützen

Die Installationsroutine der IIS legt im Stammverzeichnis des Systemlaufwerks die Verzeichnisse *C:\Inetpub* und *C:\Inetpub\wwwroot* an. Beide Ordner sollten umbenannt werden. Die Sicherheitsgruppe *Benutzer* ist aus den Sicherheitseinstellungen von *C:\Inetpub\wwwroot* und allen darunter liegenden Ordnern zu entfernen. Der Ordner *AdminScripts* sollte in ein benutzerdefiniertes Verzeichnis verschoben werden. Generell ist auf alle Beispiel- und Testskripte auf dem produktiven Server zu verzichten, egal ob sie aus eigener Feder, aus dem Internet oder aus Softwareentwicklungspaketen stammen.

Dieselben Vorkehrungen gelten auch für folgende Ordner, sofern diese vorhanden sind:

- *C:\inetpub\ftproot* (FTP-Server)
- *C:\inetpub\mailroot* (SMTP-Server)
- *C:\inetpub\nntpfile* (NNTP-Server)

Standardobjekte deaktivieren

Alle virtuellen Standardserver, die Standardwebsite und die Standard-FTP-Site sind zu beenden, wenn sie nicht benötigt werden. Es ist zu empfehlen, die Standardwebsite grundsätzlich deaktiviert zu lassen und neue Websites nur für klar definierte Einsatzzwecke hinzuzufügen, z. B. für WebDAV-Freigaben.

Virtuelle Verzeichnisse

Viele virtuelle Verzeichnisse im Internetinformationsdienste-Manager verweisen auf Funktionen des Betriebssystems, beispielsweise Internetdrucken oder Zertifikatsdienste. Die Basisverzeichnisse sind daher meist Systemordnern des Betriebsystems zugeordnet. Daher sollte generell die Sicherheitsgruppe *Benutzer* aus den Sicherheitseinstellungen der jeweiligen Basisverzeichnisse entfernt werden. Wenn bestimmte Ressourcen auch für Benutzer zur Verfügung stehen sollen, z. B. Internetdrucken oder das IIS-basierte Ändern des Benutzerkennworts, so ist ein entsprechendes Berechtigungskonzept zu planen und umzusetzen. Allgemeines zu Berechtigungen im IIS wird in M 4.185 *Absichern von virtuellen Verzeichnissen und Web-Anwendungen beim IIS-Einsatz* beschrieben.

Umgang mit dynamischen Inhalten

ASP nur für administrative und infrastrukturelle Zwecke aktivieren

Die Zertifizierungsdienste und andere Windows-Komponenten enthalten z. T. grafische Benutzeroberflächen, die mit ASP laufen. Es ist daher nicht immer möglich, ASP zu deaktivieren. In Windows Server 2003 sind die Einflussmöglichkeiten von ASP auf das Betriebssystem standardmäßig stark eingeschränkt (aktiviertes *IISLockdown*). Unter kontrollierten Bedingungen ist daher ohne größeren Aufwand ein sicherer Betrieb dieser Komponenten möglich. Dies bedeutet vor allem, dass ASP ausschließlich für administrative und infrastrukturelle Zwecke aktiviert wird. Zudem existieren ein geeignetes Administrationskonzept und eine entsprechende Sicherheitsrichtlinie. Der Zugriff auf Benutzerebene wird eingeschränkt, protokolliert und kontrolliert. Ansonsten ergeben sich weitere Risiken, für die entsprechende Maßnahmen umgesetzt werden müssen (siehe B 5.10 *Internet Information Server*). Zum ausführen von dynamische Inhalte startet IIS eigenständige Prozesse. Mehrere Anwendungen sollten durch ein geeignete Prozessmanagement isoliert voneinander betrieben werden.

Zugriff einschränken und absichern

Restriktive Einstellungen nötig

Der Zugriff auf die virtuellen Server und Verzeichnisse ist standardmäßig nicht eingeschränkt, obwohl die IIS-Dienste nur vom lokalen Computer oder von bestimmten Clients im Netz abgefragt werden. Außerdem wird die Klartextübermittlung von Kennwörtern nicht verhindert. Daher sollten restriktivere Einstellungen als Grundeinstellung vorgegeben werden.

Authentisierungsmethoden

Integrierte Windows-Authentifizierung

Im LAN stellt die *Integrierte Windows-Authentifizierung* die sicherste und komfortabelste Methode dar. Sie funktioniert mit den meisten gängigen Browsern, z. B. Internet Explorer und Firefox. Ist ein Teil des LAN durch einen Sicherheits-Gateway abgeschirmt, so muss die Unterstützung für die *Integrierte Windows-Authentifizierung* überprüft werden.

Digest-Authentifizierung

Sofern die IT-Sicherheitsrichtlinie es zulässt und Gefährdungen (siehe G 5.133 *Unautorisierte Benutzung web-basierter Administrationswerkzeuge*) ausreichend berücksichtigt werden, kann in bestimmten Bereichen auf *Digest-Authentifizierung* (verschlüsseltes Senden der Anmeldeinformationen nach RFC 2617 unter Verwendung von Domänencontrollern) ausgewichen werden. Ist dies nicht möglich, muss die gesamte Verbindung über einen verschlüsselten Kanal aufgebaut werden (siehe unten).

Voraussetzungen für *Digest-Authentifizierung* sind

- Active Directory mit der Windows-Server-2003-Schemaerweiterung
- Windows Server 2003 auf allen Domänencontrollern der lokalen Active-Directory-Site
- HTTP-1.1-Unterstützung auf Clients (z. B. MS Internet Explorer ab Version 5)
- HTTP-1.1-Unterstützung auf Sicherheits-Gateways

In Windows Server 2003 wurde Digest als Security Service Provider Interface (SSPI) integriert (*erweiterte Digest-Authentifizierung*). Voraussetzung ist, dass sowohl IIS als auch Domänencontroller unter Windows Server 2003 laufen. Auf dem Server mit IIS muss das SSPI für Digest mit Hilfe eines Skriptes erzwungen werden, da Windows Server 2003 auf das ältere Digest-Modul von Windows 2000 zurückschaltet oder die Authentisierung ganz fehlschlägt, sobald die Konfiguration der Windows-Domäne nicht homogen ist.

Der Aufruf auf der Kommandozeile lautet:

cscript adsutil.vbs SET W3SVC/UseDigestSSP wahr

Das Konfigurationsskript *adsutil.vbs* befindet sich im Verzeichnis *AdminScripts*. Informationen zum Verwenden von Skripten sind in M 2.367 *Einsatz von Kommandos und Skripten unter Windows Server 2003* zu finden.

Verschlüsselung in einem sicherem Kanal (SSL/TLS)

Der sichere Kanal ist oft der einzige Weg, um bei Administrationswerkzeugen von Drittherstellern eine verschlüsselte Kennwortübertragung zu erreichen.

Jede Webseite, nachfolgend virtueller Server genannt, muss mit einem gültigen Zertifikat ausgestattet sein und die verschlüsselte Kommunikation über einen sicheren Kanal ermöglichen.

Für Server mit hohem oder sehr hohem Schutzbedarf kann die Anforderung von Clientzertifikaten aktiviert werden. Mit Hilfe weiterer Systeme wie z. B. Chipkarten besteht damit die Möglichkeit, eine zwei-Faktor-Authentisierung zu realisieren.

Überwachung

Protokollierung und Metabase-Überwachung

Auf allen virtuellen Servern und Webseiten muss im Eigenschaften-Dialogfenster die Protokollierung aktiviert werden. Die Standardeinstellung von einer Protokolldatei pro Tag sollte belassen werden, sofern die IT-Sicherheitsrichtlinie für den Server keine längerfristigen Protokolle vorschreibt. Ab Windows Server 2003 mit Service Pack 1 sollte zudem die Metabase-Überwachung eingestellt werden. Dazu dient das Konfigurationsskript *iiscnfg.vbs*.

Der Kommandozeilenaufruf

iiscnfg.vbs /enableaudit W3SVC/<Bezeichner>/ROOT

aktiviert die Überwachung auf der Webseite-Konfiguration und den untergeordneten virtuellen Verzeichnissen. Der <*Bezeichner*> ist die Nummer des virtuellen Servers. Diese ist im Internetinformationsdienste-Manager unter dem Knoten *Websites* neben den aufgelisteten Websites dokumentiert. Schließlich muss die Gruppenrichtlinie für die Objektüberwachung auf dem Server aktiviert bzw. wirksam sein (siehe auch M 2.365 *Planung der Systemüberwachung unter Windows Server 2003*).

Dokumentation

Es sollte mindestens dokumentiert werden, welcher Server Zugriffspunkt für welches administrative Werkzeug ist, welche Authentisierungsmethoden dafür eingestellt sind und auf welche weiteren Ressourcen das Werkzeug gegebenenfalls Zugriff benötigt. Abweichungen von den genannten Grundeinstellungen bzw. vom Installationsstandard sollten dokumentiert und begründet werden.

Ergänzende Kontrollfragen:

- Sind nur die notwendigen IIS-Dienste und -Protokolle installiert?
- Wurde die Basiskonfiguration abgesichert und der Zugriff auf die virtuellen Server und Verzeichnisse eingeschränkt?
- Wird nur Windows-integrierte oder erweiterte Digest-Authentifizierung verwendet?
- Wurde die Protokollierung auf allen virtuellen Servern und Webseite aktiviert?
- Wurde eine Konfigurationsdokumentation (Abweichungen vom Installationsstandard) erstellt?

M 4.283 Sichere Migration von Windows NT 4 Server und Windows 2000 Server auf Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Aktualisierung einer Vorgängerversion auf Windows Server 2003 hat meist verschiedene Gründe und verfolgt mehrere Ziele. Die Ausgangspositionen sind dabei organisatorisch und technisch sehr vielfältig. Deshalb ist die umfassende und sorgfältige Planung einer Serveraktualisierung unter Berücksichtigung der zu erreichenden Ziele unerlässlich. Die Forderungen in M 2.315 *Planung des Servereinsatzes* und M 2.319 *Migration eines Servers* sind zu beachten. Für die Migration eines Windows NT-Servers gelten grundsätzlich auch die Festlegungen aus M 2.233 *Planung der Migration von Windows NT auf Windows 2000*.

Vor- und Nachteile verschiedener Migrationspfade

Unterschiedliche Sicherheitsstandards zwischen aktualisierten Server und Neuinstallation beachten

Bei der Entscheidung für einen Migrationspfad sind besonders die Vor- und Nachteile der Aktualisierung eines bestehenden Servers (In-place Upgrade) gegen die einer Neuinstallation sorgfältig abzuwägen. So weicht unter Umständen ein aktualisierter Server auf Grund übernommener "Altlasten" oder alter Konzepte erheblich von den Sicherheitsstandards eines neu installierten Windows Server 2003 Systems ab. Maßgeblich ist auch die Ausgangsversion des aktualisierten Servers. Die Standardsicherheitseinstellungen eines aktualisierten Windows Server 2003 entsprechen nicht den Standardeinstellungen der Neuinstallation. Die Einstellungen werden vom Setup-Programm je nach Ausgangsversion und Service Pack unterschiedlich gesetzt. Wird also Windows NT 4.0 Server auf Windows Server 2003 aktualisiert, dann unterscheiden sich die resultierenden Einstellungen von denen eines von Windows 2000 Server aus aktualisierten Windows-Server-2003-Systems.

Für die Durchsetzung einer homogenen IT-Sicherheitsrichtlinie müssen abhängig von der Ausgangssituation (Version, Rolle, Konfiguration) die Sicherheitskonfigurationen angepasst werden.

Die Aktualisierung eines bestehenden Servers erfordert im Allgemeinen weniger Aufwand, da die vorhandenen Benutzer, Gruppen und Rechte beibehalten werden. Dateien und Anwendungen müssen nicht neu installiert werden.

Eine Neuinstallation mit frisch formatierten Festplatten ist hingegen leistungsfähiger. Die Datenträgerpartitionen können den aktuellen Bedürfnissen angepasst werden. Für Server, bei denen die Verfügbarkeitsanforderungen sehr hoch sind, ist eine Neuinstallation zu empfehlen. Anderenfalls sollte nach vorheriger Datensicherung auf jeden Fall eine komplette Defragmentierung der Partitionen erfolgen.

Vorbereitungen

Dokumentation, Upgrade-Fähigkeit des Betriebssystems und notwendige Treiber berücksichtigen

Die Herstellerinformationen, insbesondere die mitgelieferten Dokumentationen auf den Installationsmedien (z. B. Verzeichnis *\DOC* auf dem Windows Server 2003 Installationsmedium) sind zu beachten. Vor einer Aktualisierung muss geprüft werden, ob die Voraussetzungen dafür erfüllt sind. Dazu gehört die Upgrade-Fähigkeit der unterschiedlichen Versionen der Betriebssysteme. Die Systemanforderungen und Hardwarekompatibilität sind beim Hersteller nachzulesen oder mittels *Setup* vom Windows Server 2003 Installationsmedium mit *Systemkompatibilität prüfen* zu kontrollieren. Neben diesen empfohlenen Herstelleranforderungen sind die produktiv benötigten Kapazitäten (Festplatte, Arbeitsspeicher usw.) zu berücksichtigen. Informationen über die vorhandenen Geräte und Treiber helfen unter Umständen bei erforderlichen manuellen Eingriffen. Es wird empfohlen, ein Inventarverzeichnis für den Server anzulegen, in dem Angaben zu dessen Komponenten (wie Bezeichnung, Typ, Anzahl, IRQ, E/A-Adresse, etc.) dokumentiert sind. Sofern Treiber für diese Komponenten vom Hersteller angeboten werden, sollten diese vorab beschafft werden.

Der Einsatz von Windows Server 2003 erfordert gegebenenfalls den Einsatz neuer Treiber, die möglicherweise nur mit neueren BIOS-Versionen lauffähig sind, wodurch ein Update des BIOS notwendig wird. Dies sollte jedoch erst geschehen, nachdem recherchiert wurde, welche Treiberversionen welche BIOS-Stände benötigen.

Befinden sich auf dem zu aktualisierenden Server

- Cluster,
- Volumensätze,
- Spiegelsätze,
- Stripesets oder
- FAT/FAT32-Partitionen

bedürfen diese der besonderen Berücksichtigung, wobei die Nutzung von FAT grundsätzlich nicht zu empfehlen ist.

Upgrade-Fähigkeit der Software

Software, welche auf dem aktualisierten Server weiter betrieben werden soll, ist vorab auf ihre Kompatibilität zu testen. Dazu gehören u.a. Virenschutzprogramme, Backup- und Managementsysteme sowie Verschlüsselungsanwendungen.

Namenskonventionen

Die Namen, Namensdienste und Netzwerkeinstellungen der zu migrierenden Server sind so zu wählen, dass in allen Phasen keine Konflikte oder zusätzliche Gefährdungen auftreten.

Hinweise hierzu finden sich unter den Hilfsmitteln zum IT-Grundschutz (siehe *DNS/WINS/DHCP als Infrastrukturdienste unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Ein produktiver Windows Server 2003 sollte (abgesehen von der Wiederherstellungskonsole) grundsätzlich nur eine Betriebssysteminstallation beherbergen und ausschließlich NTFS-Partitionen besitzen.

Prüfliste

Es sollte überlegt werden, aus den Erkenntnissen und Anforderungen der Planungsphase eine Prüfliste zu erstellen, welche in einer Testmigration und vor allem nach der durchgeführten Migration dem dokumentierten Funktionsnachweis dient.

Durchführung

Installation und Datensicherung

Nach dem erfolgreichen Abschluss aller Tests sollte die Migration eines produktiven Servers mit dem Geschäftsbetrieb abgestimmt werden. Zum angekündigten Termin ist der Server für den Installationsvorgang aus dem Produktivbetrieb zu entfernen. Für eine aktuelle vollständige Datensicherung ist zu sorgen.

Bereitstellung von Software

Für die Installation darf nur Software aus sicheren Quellen verwendet werden (M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*). Aktuelle Servicepacks, Sicherheitspatches und Treiber müssen zur Verfügung stehen. Deren Bereitstellung auf geeigneten Wechselmedien wie CD oder DVD ist am sichersten und auch später nachvollziehbar.

Aktiver Netzwerkanschluss nötig

Während der Installation ist ein aktiver Netzwerkanschluss am Server notwendig. Der serielle Anschluss einer evtl. vorhandenen unterbrechungsfreien Stromversorgung ist wegen möglicher Komplikationen bei der Schnittstellenerkennung vorsorglich zu trennen.

Dynamische Updates vermeiden

Die Option eines *dynamischen Updates* über das Internet sowie eine unbeaufsichtigte Aktualisierung sind zu vermeiden, denn beim Aktualisieren von produktiv genutzten Servern sind meist Besonderheiten zu berücksichtigen, die individuelle Entscheidungen und Eingriffe erfordern. Internetverbindungen während einer Serverinstallation erfordern zusätzliche Sicherheitsmaßnahmen und schaffen vermeidbare Gefährdungen. Außerdem kann ihre Verfügbarkeit nicht garantiert werden.

Hilfsmittel

Werkzeuge von Microsoft

Die Servermigration auf neue Hardware wird durch Werkzeuge von Microsoft unterstützt. Vor dem Einsatz von diesen Tools und Werkzeugen ist mit dem Hersteller die Unterstützung bei Problemen zu klären Sie sind besonders sorgfältig auszuwählen und vor ihrer Anwendung zu testen. Es können ebenso Werkzeuge von Drittanbietern einbezogen werden.

- Das *File Server Migration Toolkit* (FSMT) dient zur Migration und Konsolidierung der Daten älterer Dateiserver. Neben den Daten werden mit *FSMT* auch die Berechtigungen auf NTFS- und Freigabe-Ebene übertragen.
- Der *Microsoft Print Migrator* überträgt Druckertreiber und deren Konfiguration jedoch ohne Sicherheitsberechtigungen.

- Für die Migration und Konsolidierung von Domänen steht das *Active Directory Migration Tool* (ADMT) zur Verfügung.
- Für die Migration eines Betriebssystems und der installierten Anwendungen eines physischen Servers in eine virtuelle Maschine unter MS Virtual Server 2005 kann das Tool *Virtual Server Migration Toolkit* (VSMT) genutzt werden.

Nacharbeiten

Nach Abschluss wesentlicher Arbeitsschritte, z. B. nach einem Neustart des Windows Server 2003, sind die Ereignisanzeigen auf kritische Fehler und Hinweise zu prüfen.

Abhängig von der Produktversion und den Lizenzbedingungen ist gegebenenfalls eine Produktaktivierung erforderlich. Hinweise hierzu finden sich unter den Hilfsmitteln zum IT-Grundschutz (siehe *Auswahl geeigneter Lizenzierungsmethoden für Windows XP/Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Sicherheitskonfiguration

Richtlinien und Vorlagen definieren

Die Sicherheitskonfiguration unter Windows Server 2003 wird mit verschiedenen Werkzeugen durchgeführt, deren Konfigurationsbereiche sich teilweise überschneiden. Es können eigene Richtlinien und Vorlagen definiert werden.

- Nach einer Aktualisierung ist mit Hilfe des *Sicherheitskonfigurations-Assistenten* (SCW) eine vorbereitete Sicherheitskonfiguration auf den Server anzuwenden. Die Rolle des betroffenen Servers muss zu diesem Zeitpunkt definiert sein.
- Mit der *Microsoft Management Console* (MMC) werden mittels *Sicherheitskonfiguration und -Analyse* bzw. *Sicherheitsvorlagen* Vorlagen für Sicherheitseinstellungen erstellt und gegebenenfalls angewendet. Die Anwendung dieser Vorlagen ist auch über Gruppenrichtlinien möglich. Im *Sicherheitshandbuch für Windows Server 2003* (online beim Hersteller verfügbar) stehen empfohlene Sicherheitsvorlagen, Beschreibungen und Dokumentationsvorlagen zur Verfügung. Diese Vorschläge müssen jedoch in jedem Fall an die spezifischen Anforderungen angepasst werden. Hilfestellung hierzu bieten die Maßnahmen M 4.280 *Sichere Basiskonfiguration von Windows Server 2003* und M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003*.

Nach jeder Sicherheitskonfiguration sind die Ereignisanzeigen zu kontrollieren.

Internet-Explorer

Unter Windows Server 2003 ist der Internet-Explorer standardmäßig auf erhöhte Sicherheit eingestellt. Die daraus resultierenden Einschränkungen können durch Übernahme von Internetadressen in die Zone *vertrauenswürdige Sites* bzw. der UNC-Pfade in die Zone *Lokales Intranet* aufgehoben werden. Der Benutzer muss dafür die erforderlichen Berechtigungen für die Konfiguration des Internet-Explorers besitzen.

Zusätzliche lokale Gruppen und Benutzer

Unter Windows Server 2003 wurden zusätzliche lokale Gruppen und Benutzer, z. B. *Remotedesktopbenutzer*, *Netzwerkkonfigurations-Operatoren*,

Support_388945a0 (deaktiviert), eingerichtet, welche beachtet und berücksichtigt werden müssen.

Der Verzeichnispfad für Benutzerprofile hat sich gegenüber Windows NT 4.0 verändert. Vorhandene Skripte und Verfahren sind gegebenenfalls diesbezüglich anzupassen.

Ergänzende Kontrollfragen:

- Gibt es eine Migrationsplanung?
- Stehen sichere Installationsmedien zur Verfügung?
- Wurde das Setup vom Windows-Server-2003-Installationsmedium mit der Option *Systemkompatibilität prüfen* durchgeführt?
- Wurde eine Sicherheitskonfiguration durchgeführt und dokumentiert?

M 4.284 Umgang mit Diensten unter Windows Server 2003

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Administrator

Dienste werden unter dem Sicherheitskontext bestimmter Konten ausgeführt (so genannte Dienstkonten). Zugriffe auf Ressourcen erfolgen mittels des Dienstkontos, ähnlich wie bei einem Benutzer mit Benutzerkonto. Einmal gestartet bleiben Dienste prinzipiell aktiv, also bleibt auch das zugehörige Dienstkonto dauerhaft angemeldet bzw. es wird die Anmeldung regelmäßig durch die zentrale Dienstesteuerung erneuert. Außerdem handelt es sich auf Servern meist um betriebskritische zentrale Dienste. Dienstkonten sind daher exponierter als normale Benutzerkonten. Sofern Abhängigkeiten zwischen Diensten existieren, kann auch ein kompromittierter, scheinbar weniger wichtiger Dienst einen betriebskritischen Dienst zum Absturz bringen. Aus diesen Gründen sollten Dienste und Dienstkonten unter Beachtung spezieller Regeln administriert werden.

1. Für Dienstkonten sollte niemals das vordefinierte Administratorkonto verwendet werden.

   Built-in-Administrator nicht verwenden

2. Jeder Dienst sollte mit einem eigenen Dienstkonto laufen.

   Separate Dienstkonten

   Ein kompromittiertes Dienstkonto mit hohem Berechtigungsniveau kann leichter isoliert werden, wenn es nicht für mehrere Dienste verwendet wird. In der Praxis betreiben Serverapplikationen möglicherweise eine Gruppe von Diensten im Kontext desselben Kontos. Hier muss im Einzelfall abgewogen werden, ob dies mit dem Schutzbedarf des Systems vereinbar ist und inwieweit unterschiedliche Dienstkonten zugewiesen werden können, ohne die gewünschte Funktionalität zu beeinträchtigen.

   Eine Ausnahme bilden die speziellen, vordefinierten Konten *NT AUTHORITY\LocalService, NT AUTHORITY\NetworkService.* Sie werden von der internen Dienstesteuerung verwaltet und stellen jedem Dienst einen isolierten Sicherheitskontext zur Verfügung. Die Authentisierung wird systemintern durch die Dienstesteuerung geregelt. Kennworteintragungen werden ignoriert.

3. Jedes Dienstkonto sollte nur mit den minimal erforderlichen Berechtigungen ausgestattet sein.

   NetworkService

   Deshalb sind vorrangig die vordefinierten Konten *NT AUTHORITY\LocalService* für lokal agierende Dienste und *NT AUTHORITY\NetworkService* für Dienste mit Netzwerkzugriff in Betracht zu ziehen. Sie haben standardmäßig die gleichen Berechtigungen wie die vordefinierte Gruppe *Authentifizierte Benutzer* (normale Benutzer).

Lokale Konten sind Domänenkonten vorzuziehen. Werden Domänenkonten verwendet, sollten sie mit so wenigen Domänenberechtigungen wie möglich ausgestattet werden, und es sollte für eine entsprechende Verfügbarkeit von Domänencontrollern gesorgt werden. Dienstkonten sollte die lokale Anmeldung verweigert werden (*Start* | *Systemsteuerung* | *Verwaltung* | *Lokale Sicherheitsrichtlinie* |

Lokale Richtlinien | Zuweisen von Benutzerrechten | Lokal anmelden verweigern oder in einer Domänengruppenrichtlinie).

4. Als Faustregel gilt, dass Applikationen mit Diensten auf Administrator-Niveau auf einem eigenen Server zu betreiben sind. Je höher die Anzahl solcher Applikationen auf einem Server ist, desto geringer ist das erreichbare Sicherheitsniveau. Als Beispiel sind Backup-Server oder Domänencontroller zu nennen, welche ihre Kerndienste nur mit vollen administrativen Berechtigungen ausüben können.

Separate Server

5. Die voreingestellten Konten für die in Windows enthaltenen Dienste sollten nicht verändert werden.

Windows-Standards für Dienste belassen

6. Unnötige oder potenziell gefährliche Dienste sollten deaktiviert werden.
7. Viele Skripte und sonstige ausführbare Dateien können als Dienst installiert und ausgeführt werden. Dies ist im Normalfall kein empfohlenes Vorgehen.

   Im Einzelfall muss geklärt werden, wie das Verhalten von als Dienst ausgeführten Prozessen (d. h. Skripte oder Programme) die Systemstabilität und -sicherheit beeinflusst. Beispielsweise kann *Dienst beenden* oder *Dienst neu starten* zu korrupten Daten führen, weil der Prozess auf solche Ereignisse nicht selbst reagieren kann, sondern einfach gelöscht wird. Auch hier gilt: kleinstmöglicher Sicherheitskontext verringert das Risiko. Der Einsatz eines solchen Verfahrens sollte in einer Testumgebung erprobt worden sein. Es sollte erwogen werden, starke Überwachungseinstellungen (*System Access Control List*, SACL) für die Dienstkonten zu setzen, um unvorhergesehenes Verhalten erkennen zu können.

Prozesse zu Diensten erheben

8. Für Kennwörter von Dienstkonten sind die üblichen Festlegungen für Benutzerkennwörter teilweise ungeeignet. Die folgende Tabelle zeigt beispielhaft die Standardeinstellungen nach der Installation.

Kennwortrichtlinie	Standard-einstellung auf Domänencontrollern	Tauglichkeit für Dienstkonten
Kennwortchronik	24	ja
Maximales Kennwortalter (in Tagen)	42	ungeeignet
Minimales Kennwortalter (in Tagen)	1	ja
Minimale Kennwortlänge	7	nicht ausreichend
Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert	ja
Kennwörter mit umkehrbarer Verschlüsselung speichern	Deaktiviert	ja

Das Kennwort sollte eine zweistellige Kennwortlänge (bis 127 Zeichen möglich) besitzen. Es darf nicht automatisch ablaufen (Option *Kennwort läuft nie ab* in den Eigenschaften des Kontos), sondern sollte während regelmäßiger Wartungszyklen geändert werden. Die Kennwörter sind sicher zu hinterlegen, siehe hierzu M 2.22 *Hinterlegen des Passwortes*. Bei einer größeren Anzahl von Diensten und Servern kann das Hinterlegen

und Ändern der Kennwörter (inklusive Funktionstest der Dienste) sehr aufwendig werden, so dass der Sicherheitsgewinn unter Umständen nicht mehr gegeben ist. Hilfsprogramme für die Kennwortverwaltung von Dienstkonten können hier eine wertvolle Hilfe sein, stellen aber wiederum ihrerseits ein Risiko dar. Das Alter von Kennwörtern und das Verfahren für deren Verwaltung sollte in Abhängigkeit des Schutzbedarfs und des Aufwandes festgelegt sowie in einer Richtlinie dokumentiert werden.

Dokumentation

Zu allen Diensten, die nicht mit einem vordefinierten Konto laufen, sind die Dienstkonten sowie deren Berechtigungen zu vermerken.

Ergänzende Kontrollfragen:

- Werden vordefinierte Konten mit administrativen Berechtigungen verwendet?
- Haben alle Dienstkonten nur die minimal benötigten Rechte?
- Wurde ein Verfahren zum Ändern der Kennwörter der Dienstkonten definiert?

M 4.285 Deinstallation nicht benötigter Client-Funktionen von Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Clientzubehör deinstallieren oder deaktivieren

Die Standardinstallation von Windows Server 2003 enthält verschiedene Funktionen, die als Clientzubehör von Windows XP bekannt sind. Auf einem Server werden sie nicht benötigt und sollten deinstalliert oder, falls Deinstallation nicht möglich, zumindest deaktiviert werden, um die Angriffsfläche zu verringern und die damit verbundenen unnötigen Risiken zu reduzieren.

Deinstallieren von Programmen unter Zubehör

Deinstallieren von Programmen unter *Start* | *Alle Programme* | *Zubehör*

1. Als Administrator am Server anmelden
2. Sicherheitskopie der Datei *C:\WINDOWS\inf\sysoc.inf* anlegen, z. B. als *Kopie von sysoc.inf*
3. Folgende Zeilen in *C:\WINDOWS\inf\sysoc.inf* ändern und abspeichern:

   OEAccess=ocgen.dll,OcEntry,oeaccess.inf,hide,7

   ändern in

   OEAccess=ocgen.dll,OcEntry,oeaccess.inf,,7

   und

   MultiM=ocgen.dll,OcEntry,multimed.inf,HIDE,7

   ändern in

   MultiM=ocgen.dll,OcEntry,multimed.inf,,7
4. Zu *Start* | *Systemsteuerung* | *Software* | *Windowskomponenten hinzufügen/entfernen* wechseln und folgende Checkboxen deaktivieren:
   - Outlook Express
   - Zubehör und Dienstprogramme / Multimedia / Audiorecorder
   - Zubehör und Dienstprogramme / Multimedia / Mediaplayer
   - Zubehör und Dienstprogramme / Kommunikation / Telefon

Hinweis: Durch die Schritte 1 bis 3 werden die Software-Optionen in Schritt 4 erst sichtbar gemacht.

Deaktivieren von Mediaplayer, Outlook Express und Netmeeting

Deaktivieren von Mediaplayer, Outlook Express und Netmeeting

Die Deinstallationsroutinen der integrierten Komponenten Mediaplayer, Outlook Express und Netmeeting entfernen die Programme nicht vollständig, das ungewollte Ausführen ist weiterhin möglich. Deshalb sollten diese Programme mit Hilfe der Richtlinien für Softwareeinschränkungen (siehe M 4.286 *Verwendung der Softwareeinschränkungsrichtlinie unter Windows Server 2003*) deaktiviert werden. Werden Active Directory und Gruppenrichtlinien verwendet, so muss die Wirksamkeit der Einstellungen auf dem einzelnen Server durch korrekte Konfiguration der Gruppenrichtlinien

sichergestellt sein (siehe M 2.231 *Planung der Gruppenrichtlinien unter Windows 2000*).

Anpassen der lokalen Softwareeinschränkungsrichtlinie:

1. Die lokale Sicherheitsrichtlinie über *Start* | *Systemsteuerung* | *Verwaltung* | *Lokale Sicherheitsrichtlinie* öffnen
2. In den Zweig *Richtlinien für Softwareeinschränkungen* | *Zusätzliche Regeln* wechseln
3. Neue Pfadregeln mit der Sicherheitsstufe *Nicht erlaubt* für folgende Pfade *hinzufügen:*

   %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%\NetMeeting

   %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%\Outlook Express

   %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%\Windows Media Player

Falls eines der deaktivierten Programme bisher beim Start des Betriebssystems automatisch geladen wurde, können Fehlermeldungen auftreten. Die entsprechenden Autostart-Funktionen sollten vor der Aktivierung der Richtlinie abgeschaltet werden, z. B. mit *msconfig.exe*.

Weiterhin sollte die Internetkommunikation für Windows-Client-Komponenten eingeschränkt werden. Dazu ist in der lokalen Gruppenrichtlinie (*Start* | *Ausführen...* | *gpedit.msc*) der Zweig *Computerkonfiguration* | *Administrative Vorlagen* | *System* | *Internetkommunikationsverwaltung* | *Internetkommunikationseinstellungen* auszuwählen. Hier sollten alle Funktionen deaktiviert werden. Nur *Automatische Aktualisierung von Stammzertifikaten* und *Windows Update* sollten aktiviert bleiben, solange hierfür kein alternatives Verfahren für den Server festgelegt wurde.

Wenn weitere nicht benötigte Client-Anwendungen und -Funktionen auf dem Server aktiv sind, dann sind auch diese zu deinstallieren bzw. zu deaktivieren..

Ergänzende Kontrollfragen:

- Enthält der Server überflüssige Client-Funktionen?

M 4.286 Verwendung der Softwareeinschränkungsrichtlinie unter Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Schutz gegen Schadprogramme

Bedingt unter anderem durch die intensive Nutzung des Internets (WWW, E-Mail usw.) werden Benutzer häufig mit unbekannter Software konfrontiert. Dabei müssen die Benutzer entscheiden, ob sie diese Software einsetzen möchten. Schadprogramme z. B. tarnen sich häufig als so genannte Trojanische Pferde, um Benutzer dazu zu verführen, diese zu installieren und auszuführen. Für den einzelnen Benutzer ist es oft schwierig zu entscheiden, welche Software er ausführen kann und soll. Durch Softwareeinschränkungsrichtlinien kann die IT-Umgebung vor nicht erwünschter oder nicht vertrauenswürdiger Software geschützt werden.

Lokale Softwareeinschränkungsrichtlinie als Mindestvoraussetzung

Nach einer Standardinstallation von Windows Server 2003 sollte zumindest eine lokale Softwareeinschränkungsrichtlinie erzeugt werden:

> *Start* | *Systemsteuerung* | *Verwaltung* | *Lokale Sicherheitsrichtlinie* | im Kontextmenü von *Richtlinien für Softwareeinschränkung* die Option *Neue Richtlinien für Softwareeinschränkungen erstellen* auswählen

Einstellungen unter *Vertrauenswürdige Herausgeber*:

- *Administratoren des lokalen Computers* aktivieren
- *Herausgeber* und *Zeitstempel* aktivieren

Designierte Dateitypen sind die Dateitypen, auf die die Softwareeinschränkungsrichtlinien Wirkung haben. Deshalb sollte die Liste *designierte Dateitypen* regelmäßig aktualisiert werden. Als Referenz kann zum Beispiel die Virenschutz-Richtlinie des IT-Verbunds dienen, in welcher kritische Dateierweiterungen definiert sind.

Die anderen Einstellungen sollten im Normalfall auf den Standardwerten belassen werden. Insbesondere die vordefinierten Regeln sollten nicht verändert werden, da das System sonst in einen unbenutzbaren Zustand versetzt werden kann. Die Richtlinien sollten immer für alle Benutzer gelten, die Administratoren eingeschlossen.

Arten zusätzlicher Regeln

Regeltyp	Erklärung	Zuverlässigkeit der Sicherheits-maßnahme
Hashregel	Bei Zugriff auf eine Datei wird ihr Hashwert berechnet und mit einem zuvor hinterlegten Hashwert verglichen.	mittel

	Die Regel greift bei identischen Hashwerten. Wird der Dateiinhalt allerdings zwischendurch manipuliert, ändert sich auch der Hashwert, und die Regel greift nicht mehr!	
Zertifikatsregel	Die Zertifikatsregel identifiziert Software anhand eines Authenticode-Zertifikats des Softwareherausgebers und lässt die Ausführung in Abhängigkeit der Sicherheitsstufe auch in geschützten Bereichen des Servers zu.	mittel
Pfadregel	Die Pfadregel identifiziert Software über einen angegebenen Dateipfad. Durch Verschieben des Programms verliert die Regel ihre Gültigkeit.	gering
Internetzonenregel	Zonenregeln gelten nur für .msi-Dateien (Windows Installer-Pakete)	gering

Einsatz der Softwareeinschränkungsrichtlinie

Planung und Tests erforderlich

Die Richtlinie zur Softwareeinschränkung erfordert eine ausführliche Planung sowie hinreichende Tests in einer Testumgebung, vor allem, wenn die Sicherheitsebene *Nicht erlaubt* als Standard gesetzt wird. Bei der Umsetzung sollte bevorzugt mit Hash- und Zertifikatsregeln gearbeitet werden, da die Pfad- und Internetzonenregeln nur einen geringen Schutz vor Ausführung von Programmen und Programmbibliotheken geben. Außerdem sollte die *Microsoft Knowledge Base* hinzugezogen werden, um dort dokumentierte unerwartete und unerwünschte Effekte bei der Anwendung von Hashregeln ausschließen zu können.

In der Softwareeinschränkungsrichtlinie können die DLL-Bibliotheken von vorn herein mit blockiert werden. In diesem Fall müssen eine hohe Zahl von Regeln für ausdrücklich zugelassene Bibliotheken definiert werden. Zugriffe auf DLL-Bibliotheken treten während der Programmausführung häufig auf, und jedes Mal muss die komplette Liste abgearbeitet werden. Performance-Auswirkungen sollten daher ebenfalls berücksichtigt werden.

Die Anwendung der Richtlinie sollte vornehmlich auf exponierten Servern mit hohen Sicherheitsanforderungen wie so genannten *Bastion Hosts* (öffentlich erreichbare Computer des Unternehmensnetzes) durchgeführt werden, um die Angriffsmöglichkeiten durch Schadprogramme zu minimieren. Die aktivierte Richtlinie mit entsprechend eingerichteten Regeln kann Virenschutzprogramme nicht ersetzen. Zur Abwehr von Sicherheitsvorfällen, z. B. im Zusammenhang mit Schadprogrammen, kann die Richtlinie zur

Softwareeinschränkung als vorsorgliche Schutzmaßnahme oder Notfallmaßnahme angewendet werden.

Wenn eine Softwareeinschränkungsrichtlinie mittels Gruppenrichtlinien des Active Directory verteilt wird, sollte hierfür ein separates Gruppenrichtlinien-Objekt erstellt werden. Die Regeln in den Standardgruppenrichtlinien sollten nicht verändert werden. Wenn sich unerwartete und unerwünschte Effekte im laufenden Betrieb herausstellen, kann das separate Gruppenrichtlinien-Objekt problemlos deaktiviert werden, und es greifen die Standardregeln.

Dokumentation

Dokumentation

Alle Regeln außer den vordefinierten sollten dokumentiert werden. Der jeweilige Zweck sollte ebenfalls dokumentiert werden.

Ergänzende Kontrollfragen:

- Wird die Liste der designierten Dateitypen regelmäßig aktualisiert?
- Wird eine Softwareeinschränkungsrichtlinie mit Hash- oder Zertifikatsregeln auf dem Windows Server 2003 genutzt und sind diese dokumentiert?

M 4.287 Sichere Administration der VoIP-Middleware

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Bei VoIP-Middleware handelt es sich grundsätzlich um Server-Systeme, die mit den gleichen Sicherheitsmaßnahmen zu schützen sind, wie sie auch für andere Serversysteme eingesetzt werden. Darüber hinaus sind weitere Sicherheitsmaßnahmen anzuwenden, die den besonderen Bedrohungen bei VoIP-Systemen gerecht werden.

Vor der Inbetriebnahme müssen die VoIP-Komponenten sicher konfiguriert werden. Das Vorgehen bei der Erstinstallation ist zu dokumentieren. Im Folgenden werden einige Punkte vorgestellt, die für eine sichere Konfiguration und Administration berücksichtigt werden müssen.

Leistungsmerkmale

VoIP-Systeme bieten, wie auch traditionelle TK-Systeme, eine Vielzahl verschiedener Leistungsmerkmale. Es sollte vor Inbetriebnahme eines VoIP-Systems geklärt sein, welche Leistungsmerkmale und Funktionalitäten vorhanden sind und welche benötigt werden (siehe M 2.372 *Planung des VoIP-Einsatzes*). Die nicht benötigten sowie die sicherheitskritischen Leistungsmerkmale müssen deaktiviert werden. Zu den sicherheitskritischen Leistungsmerkmalen gehören beispielsweise das Aufschalten auf ein bestehendes Gespräch, Raumüberwachungsfunktionen und Wechselsprechen.

Administration und Zugänge

Administration und Konfiguration der Middleware ist immer an der Konsole oder über gesicherte Verbindungen durchzuführen. Die Administration kann beispielsweise über eine Secure Shell (SSH) oder eine verschlüsselte VPN-Verbindung erfolgen.

Viele VoIP-Systeme ermöglichen eine Konfiguration über eine Web-Oberfläche. Der dabei installierte Web-Server kann ein zusätzliches Sicherheitsrisiko darstellen. Daher ist es empfehlenswert, den Web-Server für eine mögliche Web-basierte Konfigurationsoberfläche nicht auf der kritischen Middleware, wie Gateways und Gatekeeper zu betreiben. Eine Web-basierte Konfiguration sollte immer gesichert erfolgen, beispielsweise durch den Einsatz von SSL oder TLS.

Bei der Planung des Administrationskonzeptes sollte ein Rollenkonzept vorgesehen sein, das verschiedene Berechtigungsstufen umfasst. Jeder Rolle sollten im Sinne einer Vertretungsregelung mindestens zwei Personen zugeordnet werden.

Sehr oft bietet es sich an, die VoIP-Komponenten, wie Softphones oder Middleware-Applikationen, auf Standard-PCs mit allgemein verbreiteten Betriebssystemen zu installieren. Die Administration der Betriebssysteme ist, wenn möglich, von der Administration der VoIP-Applikationen personell zu trennen.

Konfigurationsänderungen sollten durch das System so protokolliert werden, dass Manipulationen zeitnah nachvollzogen werden können. Die Protokolldaten selber müssen so abgesichert werden, dass Manipulationen an

ihnen ausgeschlossen sind. Hierauf sollten auch Administratoren möglichst keine Zugriffsmöglichkeiten haben. Zum Schutz der Protokolldaten können diese z. B. auf WORM-Medien gespeichert werden oder der Zugriff kann auf Revisoren beschränkt werden.

Backup

Ein umfassendes Datensicherungskonzept ist eine zentrale Anforderung zur Sicherstellung bzw. zur raschen Wiederherstellung der Verfügbarkeit, aber auch, um die Integrität jederzeit überprüfen zu können. Dabei ist darauf zu achten, dass bei der Sicherung personenbezogener Daten, wie beispielsweise privater Verbindungsdaten, diese so abgelegt werden, dass sie vor unbefugtem Zugriff geschützt sind, also beispielsweise verschlüsselt.

Sicherheit der Software

Es ist darauf zu achten, dass die eingesetzte Software immer auf einem aktuellen Stand ist und etwaige sicherheitsrelevante Patches unverzüglich aufgespielt werden. Dies gilt insbesondere auch für das eingesetzte Betriebssystem.

Es muss gewährleistet werden, dass nur Original-Updates und -Patches eingespielt werden. Dies gilt sowohl für die Beschaffung, beispielsweise von den Internetseiten eines Herstellers, als auch für die Übertragung auf die VoIP-Komponenten. Durch folgende Maßnahmen können die Manipulationen bei der Übertragung erschwert beziehungsweise entdeckt werden:

- Vergleich von Prüfsummen
- Nutzung von sicheren Kommunikationswegen
- Verwendung von Zertifikaten

Für die Verlässlichkeit des Gesamtsystems ist eine korrekt implementierte Software von großer Bedeutung. Insbesondere die vitalen Funktionen des Telefoniesystems, wie die einfache Vermittlung von Gesprächen und die Gateway-Funktion in das digitale Fernsprechnetz, sollten daher einem besonderen Evaluierungsprozess unterzogen werden.

Wünschenswert ist es deshalb, dass die Software für die Basisfunktionen des Telefoniesystems, wie die einfache Vermittlung von Gesprächen und die Gateway-Funktion in das digitale Fernsprechnetz, nach einem bewährten Modell entwickelt und möglichst auch von einer unabhängigen Instanz überprüft wurde.

Betriebssystemsicherheit

Die VoIP-Komponenten sollten so konzipiert werden, dass verschiedene Dienste auf verschiedenen Servern betrieben werden (siehe auch M 4.97 *Ein Dienst pro Server*). Allerdings ist insbesondere bei kompakten Stand-alone-Systemen, die meist nur aus einer Hardware-Komponente bestehen, die vollständige Trennung von Diensten nicht immer möglich.

Das eingesetzte Betriebsystem sollte als minimales Betriebssystem (siehe M 4.95 *Minimales Betriebssystem*) ausgelegt sein und die Anzahl der auf der Middleware ausgeführten Applikationen so klein wie möglich gehalten werden. Jede zusätzliche Applikation kann Schwachstellen enthalten, die für Angriffe ausgenutzt werden können. Daher ist genau zu prüfen, welche Appli-

kationen benötigt werden. Nicht benötigte Anwendungen sind zu deinstallieren. Software, die nur zur Installation benötigt wird, sollte im Anschluss gelöscht werden (beispielsweise Compiler). Nicht benötigte Netzdienste sind ebenfalls zu deaktivieren und der Zugriff auf die verbleibenden Netzdienste ist durch lokale Paketfilter zu beschränken.

Ergänzende Kontrollfragen:

- Ist sichergestellt, dass Updates und Patches weder bei der Übertragung zwischen Hersteller und Kunden noch innerhalb des lokalen Datennetzes manipuliert werden können?
- Wurden alle Dienste auf den IT-Systemen deaktiviert, die nicht für den VoIP-Betrieb benötigt werden?
- Werden alle relevanten Informationen bei der Datensicherung berücksichtigt?

M 4.288 Sichere Administration von VoIP-Endgeräten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Wie die VoIP-Middleware müssen auch die VoIP-Endgeräte zahlreiche Sicherheitsvorgaben erfüllen. Ein Unterschied zwischen den Sicherheitsmaßnahmen der Middleware besteht darin, wie diese sicher konfiguriert werden.

Vertrauenswürdige Firmware-Updates

Viele VoIP-Endgeräte bieten die Möglichkeit zum automatischen Update ihrer Firmware. Es muss sichergestellt werden, dass neue Firmware nur nach erfolgreicher Überprüfung der Authentizität und Integrität des Codes auf die Endgeräte aufgespielt wird. Falls der Hersteller für die Updates Prüfsummen zur Verfügung stellt oder die Update-Pakete digital signiert, müssen die Prüfsummen oder Signaturen vor der Installation überprüft werden. Stellt der Hersteller keine Prüfsummen bereit, muss sichergestellt sein, dass Updates nur über vertrauenswürdige Quellen bezogen werden.

Vertrauenswürdiges Konfigurieren und Digitale Zertifikate

Die meisten VoIP-Endgeräte bieten verschiedene Möglichkeiten zur Konfiguration. Beispiele hierfür sind die lokale Konfiguration am Endgerät, die Web-basierte Konfiguration durch Zugriff auf einen im Endgerät integrierten Webserver sowie die automatische Konfiguration durch "Ziehen" (Pull) der Konfiguration von einem http(s)- oder TFTP-Server.

Die lokale Konfiguration wird in der Praxis selten eingesetzt. Sie sollte mit einem Passwort geschützt sein. Falls sie nicht genutzt werden soll, sollte sie deaktiviert werden. Der Zugang zur Web-basierten Konfiguration sollte ebenfalls nur mit einem Passwort möglich sein und über eine gesicherte Verbindung, beispielsweise über SSL oder TLS, erfolgen. Ein zusätzlicher Schutz wird durch die Verwendung eines Client-Zertifikats zur Authentisierung der Clients erreicht.

Die automatische Konfiguration über einen TFTP-Server sollte nicht gewählt und stattdessen deaktiviert werden, da sie nicht ausreichend sicher ist. Insbesondere die automatische Auswahl eines TFTP-Servers während des DHCP-Bootvorganges bietet zahlreiche Angriffsmöglichkeiten.

Eine automatische Konfiguration sollte grundsätzlich über einen https-Server erfolgen. Der https-Server sollte sich mit einem Zertifikat authentisieren, das vom Endgerät vor dem Laden der Konfiguration überprüft werden kann. Üblicherweise wird das Server-Zertifikat bei der Erstinbetriebnahme manuell auf die Endgeräte installiert.

Sicherheitsfunktionalität

Viele VoIP-Telefone bieten die Möglichkeit zur passwortbasierten ein- oder mehrstufigen Zugangskontrolle (z. B. personenbezogenes Login oder Passwort für Amtsberechtigung). Es ist zu entscheiden, ob die Benutzer nur mit einer vorherigen Anmeldung das Telefon benutzen dürfen. Bei aktiviertem Passwortschutz sollten dann nur Notrufdienste zur Verfügung stehen. Um eine Nutzung durch unautorisierte Personen zu verhindern, müssen die Benutzer dann auch bei kurzfristiger Abwesenheit das Telefon sperren.

Sicherheitsfunktionalitäten, wie beispielsweise Anmeldepasswörter oder Passwörter für Amtsberechtigungen, müssen vor dem Produktiveinsatz ausführlich getestet werden, ob sie auch korrekt implementiert sind. Diese Authentisierungsmechanismen sollten von den Benutzern verwendet werden. Allerdings müssen sie über die Schwächen informiert werden. Anderenfalls besteht die Gefahr, dass nur eine Scheinsicherheit besteht.

Softphones werden in der Regel auf einem Standard-PC, der weitere Aufgaben erfüllt, betrieben. Dieser muss ebenfalls so administriert werden, dass er ein angemessenes IT-Sicherheitsniveau erreicht. Hierzu gehören beispielsweise auch Maßnahmen, dass das Mikrofon nicht durch Dritte aktiviert werden kann. Wird diese Anforderung nicht umgesetzt, könnte das Mikrofon durch einen Angreifer zum Abhören missbraucht werden.

Durch die umfangreiche Angriffsfläche, die komplexe Arbeitsplatzsysteme bieten können, dürfen bei einem hohen oder sehr hohen Schutzbedarf keine Softphones eingesetzt werden.

In der Dokumentation der Komponenten sind oft Informationen zu finden, welche weiteren Sicherheitsfunktionen unterstützt werden. Es ist zu dokumentieren, welche Sicherheitsfunktionen aktiviert wurden.

Ergänzende Kontrollfragen:

- Ist sichergestellt, dass Updates und Patches weder bei der Übertragung zwischen Hersteller und Kunden noch innerhalb des lokalen Datennetzes manipuliert werden können?
- Wurde, wenn möglich, überprüft, dass das Mikrofon bei einem Softphone nicht von Dritten aktiviert werden kann?
- Ist dokumentiert worden, welche Sicherheitsfunktionen die Endgeräte bieten und welche davon genutzt werden?

M 4.289 Einschränkung der Erreichbarkeit über VoIP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

In den wenigsten Fällen ist es ratsam, dass direkt aus dem Internet auf die VoIP-Komponenten einer Behörde beziehungsweise eines Unternehmens zugegriffen werden kann. Ein direkter Zugriff, beispielsweise durch den Verbindungsaufbau auf eine interne IP-Adresse, kann einem Angreifer zahlreiche Möglichkeiten eröffnen. Daher ist zu entscheiden, wie externen Gesprächspartnern die Kontaktaufnahme über die VoIP-Architektur ermöglicht werden soll.

Zunächst ist zu prüfen, ob überhaupt der direkte Aufbau einer VoIP-Verbindung von außerhalb unterstützt werden soll. Oft ist es ausreichend, dass die Kontaktaufnahme über ein leitungsvermittelndes Telefonnetz stattfindet. In diesem Fall dürfen keine internen VoIP-Komponenten aus dem öffentlichen Datennetz erreichbar sein. Auf das Gateway, das zwischen dem öffentlichen, leitungsvermittelnden Telefonnetz und dem lokalen VoIP-Netz betrieben wird, sollte vom öffentlichen Datennetz ebenfalls kein Zugriff möglich sein. Bei einem generellen Verzicht auf die Erreichbarkeit über VoIP von außen ergeben sich aber Nachteile für externe Gesprächspartner. Besitzen diese einen Anschluss an ein öffentliches Datennetz, müssen sie dennoch über das öffentliche, leitungsvermittelnde Telefonnetz eine Verbindung aufbauen. Die hierfür anfallenden Kosten sind in der Regel höher als die für ein direkter Verbindungsaufbau zu einer VoIP-Adresse, wie einer SIP-URL. Da diesem Nachteil jedoch viele Vorteile, besonders bei sicherheitskritischen Anwendungsfällen, gegenüberstehen, sollte die Erreichbarkeit über VoIP von außen kritisch betrachtet werden.

Werden Verbindungen von außen nur über das öffentliche, leitungsvermittelnde Telefonnetz zugelassen, so kann auch SPIT (Spam over IP-Telephone) vermieden werden. Da SPIT dann nicht kostengünstig über das Datennetz übermittelt werden kann, fallen die gleichen Kosten wie bei einem Anruf bei einem Benutzer an, der nicht VoIP einsetzt.

Soll dennoch ein Verbindungsaufbau von oder in das öffentliche Datennetz gewünscht werden, ist die Entscheidung inklusive der Restrisiken zu dokumentieren. Außerdem müssen entsprechende Sicherheitsmaßnahmen ergriffen werden. Beispielsweise kann der gesamte Datenverkehr über einen Konzentrator geleitet werden, der wie ein Proxy-Server Verbindungsanfragen annimmt und an das nächste System, wie beispielsweise einen weiteren Server oder direkt an ein Endgerät, weiterleitet. Bei dem Einsatz eines Konzentrators sollten folgende Punkte beachtet werden:

- Sowohl die Signalisierungs- als auch die Sprachinformationen zwischen dem öffentlichen und privaten Datennetz müssen über den Konzentrator geleitet werden. Der Aufbau von individuellen Verbindungen sollte unterbunden werden. Die Paketfilter und Sicherheitsgateways müssen dementsprechend konfiguriert werden, so dass die VoIP-Kommunikation mit externen Kommunikationspartnern nur über einen Konzentrator stattfinden kann. Beispielsweise kann der Konzentrator innerhalb der demilitarisierten Zone (DMZ) des Sicherheitsgateways betrieben werden. Auf diese Weise

könnte der direkte Verbindungsaufbau aus dem lokalen Netz ins öffentliche Netz beziehungsweise aus dem öffentlichen Netz ins lokale Netz vermieden werden.

- Wegen eines fehlenden Signalisierungsstandards empfiehlt es sich, so viele Signalisierungsprotokolle wie möglich nach außen zu unterstützen. Daher sollte der Konzentrator als Gateway zwischen den im lokalen Datennetz verwendeten Protokoll und den Protokollen, die für externe Benutzer zur Verfügung stehenden, betrieben werden können.
- Um einem Missbrauch entgegenzuwirken, sollte ein Gesprächsaufbau aus dem internen in das externe Datennetz nur nach einer Authentisierung am Konzentrator möglich sein.
- Bei Verbindungen innerhalb des lokalen Datennetzes sollte der Konzentrator nicht beteiligt werden.
- Es muss festgelegt werden, welche Funktionen neben der Sprachkommunikation externen Teilnehmern angeboten werden sollen.
- Der Konzentrator sollte Signalisierungs- und Sprachpakete, die nicht protokollkonform (Beispiele sind zu große Datenpakete) sind, erkennen und abweisen.
- Da direkt auf den Konzentrator aus dem öffentlichen Datennetz zugegriffen werden kann, sollte die sicherheitskritische Konfiguration im Vordergrund stehen.
- Gesprächsteilnehmer aus dem öffentlichen Datennetz müssen die IP-Adresse des Konzentrators kennen, um eine Verbindung zu ihm aufbauen zu können. Daher bietet es sich an, die Adresse des Konzentrators durch einen entsprechenden Eintrag im DNS-Server der Behörde beziehungsweise des Unternehmens zu veröffentlichen.
- Der Empfang, die Bearbeitung und die Weiterleitung der Sprach- und Signalisierungsinformationen können hohe Ressourcen beanspruchen. Daher sollte sowohl die Netzanbindung als auch die Systemressourcen ausreichend dimensioniert werden.
- Werden hohe Anforderungen an die Verfügbarkeit der Erreichbarkeit gestellt, sollte der Konzentrator redundant ausgelegt werden können. Bei einer redundanten Auslegung zur Lastverteilung müssen die verbleibenden Systeme genügend Ressourcen bereitstellen, um einen möglichen Ausfall ausgleichen zu können.

Viele Hersteller bieten hierfür teilweise proprietäre Systeme an. Als Alternative im Open-Source-Umfeld erfüllt die Software-Telefonanlage Asterisk, die als Appliance betrieben kann, viele diese Anforderungen. Ein weiterer Vorteil beim Einsatz eines Konzentrators ist die Vermeidung der Probleme, die bei der Verwendung von NAT (Network Adress Translation) auftreten.

M 4.290 Anforderungen an ein Sicherheitsgateway für den Einsatz von VoIP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Wird ein IP-Datennetz für VoIP genutzt, ergeben sich zusätzliche Anforderungen, insbesondere auch an die Sicherheit des Netzes. Oftmals ist die strikte Trennung von Sprach- und Datennetzen nicht möglich, da beispielsweise Softphones von Arbeitsplatzrechnern aus dem Datennetz auf den VoIP-Server im Sprachnetz zugreifen, Groupware-Clients das direkte Wählen von Rufnummern gespeicherter Kontakte aus der Applikation ermöglichen oder VoIP-Server mit Verzeichnisdiensten, wie LDAP (Lightweight Directory Access Protocol) gekoppelt werden. Hinzu kommt eventuell die Vernetzung geografisch getrennter Behörden-, Unternehmens- bzw. Organisationsstandorte, die beispielsweise einen zentralen VoIP-Server für die organisationsweite Kommunikation verwenden und gleichzeitig diese Verbindung für den Austausch von Daten nutzen.

Ein Sicherheitsgateway soll ein internes, sicheres System vor unberechtigten Zugriffen aus einem unsicheren Netz schützen und gleichzeitig berechtigte Zugriffe zu den geschützten Bereichen zulassen. Was als sicheres bzw. unsicheres Netz gilt, welche Ressourcen schützenswert sind und wie sie zu schützen sind, wird in den Sicherheitsrichtlinien der Organisation festgelegt (siehe hierzu auch B 3.301 *Sicherheitsgateway (Firewall*).

Bei der Planung der VoIP-Nutzung sollte überprüft werden, ob das bestehende Sicherheitsgateway für den Einsatz von VoIP angepasst werden kann. Anderenfalls muss ein zusätzliches Sicherheitsgateway hierfür beschafft und installiert werden.

Auswahl und Anforderungen an ein Sicherheitsgateway

Die Leistungsfähigkeit des eingesetzten Sicherheitsgateways bei der Nutzung von VoIP beeinflusst nicht nur den Schutz, sondern auch die Qualität der übertragenen Sprache. Durch die Verarbeitung vieler kleiner Datenpakete, die bei VoIP üblich sind, wird das Sicherheitsgateway stark belastet, wodurch Delay und Jitter der übertragenen Sprachsignale direkt beeinflusst werden.

Werden Signalisierungs- und Sprachdaten über das Sicherheitsgateway hinaus geleitet, sollte ein VoIP-fähiges Sicherheitsgateway verwendet werden, das in der Lage ist, die verwendeten Signalisierungsprotokolle mit dem gesamten Rufauf- und -abbau zu analysieren und die jeweiligen Zustände zu speichern. Anhand der Protokolldaten (z. B. die zu verwendenden UDP-Ports für die mit RTP übertragenen Sprachdaten) werden die benötigten Ports für die Dauer der Kommunikation geöffnet.

Im Weiterem hängt die Auswahl des richtigen Systems von den folgenden Faktoren ab:

- Wie groß ist das Netz?
- Welche Systemkomponenten stehen zur Verfügung? Ermöglichen bestehende Switches eine VLAN-Trennung von Sprach- und Datennetzen? Un-

terstützen bestehende Router Zugriffslisten (ACLs) oder Funktionalitäten von Sicherheitsgateways?

- Welche Sicherheitsgateways werden bereits im Datennetz eingesetzt?
- Ist nur eine auf das LAN begrenzte IP-Telefonie oder auch die Internet-Telefonie geplant?
- Wie umfassend sind die Kenntnisse des betreuenden IT-Personals?
- Welche VoIP-Systemkomponenten werden eingesetzt?
- Welcher finanzielle Rahmen steht für die Umsetzung der Sicherheitsziele zur Verfügung?

Konzeption eines Sicherheitsgateways

Unabhängig davon, ob ein bestehendes Sicherheitsgateway für die Nutzung von VoIP verändert oder ob ein neues System beschafft werden soll, kann es aus folgenden Komponenten bestehen:

- **Zustandsloser Paketfilter (Stateless Packet Filter)**

  Einfache Paketfilter können auf Routern, Layer-3-Switches bzw. Sicherheitsgateways zur Trennung von Daten- und Sprachnetz eingesetzt werden, wobei ihre Filterfunktionalität gegenüber zustandsbasierenden Filtern bzw. Application Level Gateways deutlich eingeschränkt ist.

- **Zustandsbasierende Filterung (stateful packet inspection)**

  Zustandsbasierende Paketfilter können die für eine Kommunikation benötigten Rückpakete dynamisch durchlassen und so ein erhöhtes Maß an Sicherheit für ein Netz bereitstellen. Sie speichern Zustände einer Verbindung ab und können so Rückpakete, die zu einer bestehenden Verbindung gehören, durchlassen, ohne das dafür explizite Zugriffslisten konfiguriert werden müssen.

- **Application Level Gateway (ALG)**

  Ein Application Level Gateway kann im Gegensatz zu den vorgenannten Systemen nicht nur auf IP-Adressen und Ports, sondern auch auf der Applikationsebene filtern. Der Vorteil eines Application Level Gateways macht sich gerade bei der Übertragung von RTP-Paketen bemerkbar. Die für die RTP-Übertragung zu verwendenden UDP-Ports werden im Rahmen der Signalisierung (mittels SDP) zwischen den Endpunkten ausgetauscht. Diese Ports variieren in der Regel bei jedem neuen Gespräch und müssen an dem Sicherheitsgateway freigegeben werden. Da das ALG den Austausch der Protokollnachrichten verfolgt, in denen die IP-Adressen und die zu verwendenden UDP-Ports vereinbart werden, kann es dynamisch Filter anpassen, die den betreffenden RTP-Strom passieren lassen.

Vergleicht man zustandslose Paketfilter, zustandsorientierte Paketfilter und ALGs miteinander, so empfiehlt es sich aufgrund der Vorteile möglichst ein ALG einzusetzen. Um eingehenden RTP-Verkehr zu ermöglichen, müssen zustandslose und zustandsorientierte Sicherheitsgateways große Portbereiche dauerhaft öffnen, damit RTP-Pakete mit Sprachdaten durchgelassen werden können. Eine solche Konfiguration stellt ein erhebliches Sicherheitsrisiko dar.

Application Level Gateways hingegen öffnen nur die tatsächlich benötigten Ports für die Dauer der Kommunikation und bieten daher weniger potentielle Angriffsmöglichkeiten.

Die Verwendung von Protokollen wie IAX (InterAsterisk eXchange) erleichtert die Konzeption des Sicherheitsgateways. Da hierbei sowohl die Signalisierungs- und die Medientransportinformationen über einen Nachrichtenstrom übertragen werden, wird nur ein festgelegter Port benötigt. Aufgrund der fehlenden Portaushandlung müssen keine dynamischen Portfilterungen durchgeführt werden.

Konfiguration eines Sicherheitsgateways

Die bei der Nutzung von VoIP eingesetzten Sicherheitsgateways unterscheiden sich kaum von klassischen Sicherheitsgateways. Für deren Aufbau und sicheren Betrieb sind die im Baustein B 3.301 *Sicherheitsgateway (Firewall)* beschriebenen Maßnahmen umzusetzen.

Die VoIP-spezifischen Einstellungen müssen analog zu den Maßnahmen aus diesem Baustein vorgenommen werden, wie diese konkret umzusetzen sind, ist der Dokumentation des eingesetzten Produktes zu entnehmen.

Ergänzende Kontrollfragen:

- Ist das Sicherheitsgateway für den Einsatz von VoIP angepasst worden?

M 4.291 Sichere Konfiguration der VoIP-Middleware

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Funktion und die Sicherheit der VoIP-Middleware wird wesentlich durch die eingestellten Konfigurationsparameter bestimmt. Sehr oft werden mehrere unabhängige VoIP-Komponenten, wie Gatekeeper und Gateways, benötigt. Das nicht abgestimmte Ändern eines Konfigurationsparameters bei einer Komponente kann daher im Zusammenspiel mit den anderen Komponenten zu Fehlfunktionen führen.

Die für die VoIP-Komponenten zuständigen Administratoren müssen nach der Inbetriebnahme zahlreiche weitere Änderungen vornehmen können. Verlassen Mitarbeiter die Behörde oder das Unternehmen oder kommen neue hinzu, müssen Änderungen vorgenommen werden. Auch bei einem Wechsel in ein anderes Netzsegment, beispielsweise durch einen Umzug in ein anderes Gebäude, müssen Anpassungen durchgeführt werden können. Daher sollte eine Konfigurationsoberfläche gewählt werden, über die die Administratoren diese Anpassungen effizient vornehmen können.

In der Regel werden den Mitarbeitern jeweils ein Benutzername und ein Passwort für die VoIP-Nutzung zugewiesen. Bei der Nutzung von VoiceMails kann an dieser Stelle eine E-Mail-Adresse eingetragen werden. Es ist darauf zu achten, dass die Benutzer Passwörter auswählen, die nicht zu kurz oder leicht zu erraten sind. Einstellungen, die nur sichere Passwörter akzeptieren, sollten aktiviert werden. Benutzer, die nur stationäre Geräte mit einer gleichbleibenden IP-Adresse besitzen, sollten sich nur mit dem Gerät, dem diese IP-Adresse zugewiesen wurde, anmelden dürfen.

Bei der Zuordnung zwischen Benutzernamen und Telefonnummer müssen eventuell vorhandene interne Vorgaben beachtet werden. Die Vergabe von Telefonnummern, die keinem Benutzer zugeordnet werden, spielt eine weitere Rolle. Ein Beispiel hierfür sind für Besucher frei zugängliche Telefone in Konferenzräumen. Prinzipiell sollten diese Telefonanschlüsse so wenig Privilegien wie möglich erhalten. In der Regel ist die Beschränkung, dass nur interne Gesprächsteilnehmer angerufen werden können, akzeptabel und ausreichend.

Oft kann festgelegt werden, welcher Benutzer welche Signalisierungsprotokolle verwenden darf. Wenn es möglich ist, sollten alle Benutzer nur ein Protokoll verwenden dürfen, da dies den Administrationsaufwand verringert. Unterstützen die Endgeräte verschlüsselte Signalisierungsprotokolle, sollte darauf geachtet werden, dass eine unverschlüsselte Anmeldung nicht möglich ist.

Den Benutzern des TK-Systems können bestimmte Rechte (Privilegien) zugeordnet oder entzogen werden. Beispielsweise kann das recht eingeschränkt werden, ins Ausland oder kostenpflichtige Service-Rufnummern anzurufen. Bei der Konfiguration muss das Ziel verfolgt werden, dass jeder Benutzer nur die Privilegien erhält, die für ihn vorgesehen sind.

Kleine, selbstentwickelte und den Gegebenheiten angepasste Makros können den Administratoren die Konfiguration erleichtern. Diese Makros sind aus-

führlich zu dokumentieren. Bei dem Einsatz der Makros ist darauf zu achten, dass sie vor dem Einsatz einer ausführlichen Qualitätssicherung unterzogen und gründlich getestet wurden. Anderenfalls besteht beispielsweise die Gefahr, dass solche Makros schwer auffindbare Konfigurationsmängel erzeugen oder unerwünschte Seiteneffekte mit sich bringen.

Während der Konfiguration muss darauf geachtet werden, dass zusätzliche und nicht zwingend benötigte Dienste deaktiviert werden beziehungsweise bleiben. Anderenfalls besteht die Gefahr, dass diese Dienste für Angriffe ausgenutzt werden.

Zahlreiche Ereignisse können protokolliert werden. Über die Signalisierungsinformationen kann beispielsweise ausgewertet werden, welcher Benutzer wie lange mit wem telefoniert hat. Werden die Medieninformationen nicht direkt zwischen den Endgeräten, sondern über die Middleware ausgetauscht, ist eine zentrale Auswertung der Gesprächsinhalte grundsätzlich möglich. Einerseits können Protokollierungsfunktionen zur Nachvollziehbarkeit des VoIP-Betriebs beitragen. Andererseits muss verhindert werden, dass Protokollierungsfunktionen für Verletzungen der IT-Sicherheit oder des Datenschutzes missbraucht werden.

Es muss deshalb systematisch und verbindlich festgelegt werden, welche Informationen protokolliert werden und wie die regelmäßige Auswertung der Protokolldaten erfolgt. Dabei ist in jedem Fall der Datenschutzbeauftragte und der Personal- beziehungsweise Betriebsrat zu beteiligen. Treten bei der Auswertung Unstimmigkeiten auf, müssen diese näher beleuchtet und die Ursachen gegebenenfalls beseitigt werden.

Alle Einstellungen sind durch eine regelmäßige Revision zu überprüfen.

Ergänzende Kontrollfragen:

- Wird regelmäßig überprüft, ob alle Benutzereintragungen aktuell sind?
- Ist sichergestellt, dass jeder Benutzer nur die Privilegien erhält, die für ihn vorgesehen sind?

M 4.292 Protokollierung bei VoIP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Bei einer Kommunikation über VoIP können zahlreiche Informationen protokolliert werden. Meist müssen bestimmte Statusinformationen der VoIP-Middleware protokolliert werden, um für einen reibungslosen Betrieb zu sorgen. Erst die regelmäßige Auswertung dieser Protokolldaten ermöglicht es, die korrekte Funktion der Geräte zu beurteilen und Angriffsversuche zu erkennen. Mit Hilfe der Protokolldaten kann oft auch die Art eines Angriffsversuches nachvollzogen und die Konfiguration entsprechend angepasst werden.

Die sorgfältige Konfiguration der Protokollierungsfunktionen ist besonders wichtig, da nur eine sinnvollen Filterung aus der Vielzahl von Informationen die relevanten Daten extrahiert.

Je nach Art der protokollierten Ereignisse kann es erforderlich sein, schnellstmöglich einzugreifen. Daher müssen die Protokolldaten regelmäßig ausgewertet werden.

Einerseits können Protokollierungsfunktionen zur Nachvollziehbarkeit des VoIP-Betriebs beitragen. Andererseits besteht die Gefahr, dass Protokollierungsfunktionen für Verletzungen der IT-Sicherheit oder des Datenschutzes missbraucht werden. Es muss deshalb verbindlich festgelegt und dokumentiert werden, welche Informationen protokolliert werden und wie die regelmäßige Auswertung der Protokolldaten erfolgt. Dabei ist in jedem Fall der Datenschutzbeauftragte und der Personal- beziehungsweise Betriebsrat zu beteiligen (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*). Der Umfang der Protokollierung und die Kriterien für deren Auswertung sollten dokumentiert und innerhalb der Institution abgestimmt werden. Gegebenenfalls sollten frühzeitig die jeweiligen Mitbestimmungsgremien beteiligt werden.

Protokollierung der Signalisierung

Durch die Auswertung der Signalisierung können zahlreiche Informationen ermittelt werden. An einem Sip-Proxy, Gatekeeper oder Gateway sollten folgende Daten aufgezeichnet werden:

- wer mit wem telefoniert hat,
- wie lange telefoniert wurde,
- ob der Empfänger das Gespräch entgegen genommen hat,
- von welchem Netz und welcher IP-Adresse aus das Gespräch geführt wurde,
- welche Medientransportprotokolle und welcher Codec ausgehandelt wurden.

Diese Informationen können beispielsweise für eine Kostenabrechnung oder für eine Optimierung der VoIP-Infrastruktur genutzt werden.

Protokollierung des Medientransports

Durch die Protokollierung an einer geeigneten Stelle im Netz können unter bestimmten Bedingungen die eigentlichen Gesprächsinhalte aufgezeichnet

werden. Bei Gesprächen, die das Netz über eine definierte Stelle verlassen, wie beispielsweise über einen Proxy, könnte die Protokollierung direkt an dieser Stelle vorgenommen werden.

Bei internen Gesprächen ist häufig kein Proxy erforderlich. Auch in diesem Fall ist eine Aufzeichnung der Gesprächsinhalte in der Regel möglich, beispielsweise an den beteiligten Endgeräten oder Routern.

Werden die kryptographischen Schlüssel bei einem wirksam verschlüsselten Medientransport direkt von den beteiligten Gesprächsteilnehmern ausgehandelt, können weniger Informationen an zentraler Stelle erfasst werden.

Protokollierung der Systemstatusinformationen

Neben den oben genannten Punkten sollten folgende Informationen nach Möglichkeit an der VoIP-Middleware protokolliert werden:

- Alle direkten Anmeldungen auf der Appliance beziehungsweise auf dem IT-System,
- Veränderungen der Konfiguration,
- Fehlerhafte Anmeldungen am VoIP-Dienst,
- Systemfehler,
- Auslastung,
- Änderungen an der Benutzerverwaltung (Anlegen oder Löschen von Benutzern, Änderungen der Zuordnung zwischen Benutzer und Telefonnummer, etc.),
- Hardware-Fehlfunktionen, die zu einem Ausfall eines IT-Systems führen können und
- wichtige Systemereignisse des IT-Systems, auf dem die VoIP-Applikation betrieben wird. Weitere Informationen hierzu sind dem entsprechenden IT-Grundschutz-Baustein zum Betriebssystem entnehmen.

Zentrale Verwaltung der Protokolldaten

Es ist zu empfehlen, die Protokolldaten über das Netz auf einen eigenen syslog-Server zu übertragen. Dies dient der zentralen Sammlung, Archivierung und Auswertung der Protokolldaten, da auf den VoIP-Applicances oft keine ausreichenden Betriebsmittel dafür vorhanden sind. Außerdem bietet dies den Vorteil, dass bei einer Kompromittierung eines Gerätes die bereits übertragenen Protokolldaten vom Angreifer nicht direkt verändert oder gelöscht werden können.

Falls die Übertragung zum syslog-Server unverschlüsselt erfolgt, ist ein Mithören auf dem Übertragungsweg möglich. Daher sollten die Protokolldaten entweder nur am Server selber gespeichert werden, oder verschlüsselt oder über ein eigenes Netz (Administrationsnetz) übertragen werden.

Zeitsynchronisation

Alle Protokolldaten sollten möglichst mit einem korrekten Zeitstempel versehen sein. Nur so ist eine effektive Auswertung dieser Daten, insbesondere bei der Analyse von versuchten oder erfolgten Angriffen, möglich. Des-

halb sollten im internen Netz entsprechende Server eingerichtet werden, die allen Systemen die korrekte Zeit bereitstellen. Dies kann beispielsweise auf Basis des NTP-Dienstes geschehen (siehe M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*).

Ergänzende Kontrollfragen:

- Werden bei der Protokollierung und Auswertung Datenschutzaspekte berücksichtigt?
- Wie wird sichergestellt, dass alle Geräte eine korrekte Systemzeit haben?

M 4.293 Sicherer Betrieb von Hotspots

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter IT

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement, Administrator

Zweck eines Hotspots ist im Allgemeinen (fremden) Benutzern einen einfachen Zugang zum Internet zu erlauben. Um einen Hotspot dauerhaft und sicher betreiben zu können, ist eine erfolgreiche Authentisierung aller Benutzer am Hotspot erforderlich. Gebräuchliche und ansatzweise sichere Verfahren sind beispielsweise:

- Webauthentisierung

  Hierbei gibt der Benutzer über eine Webschnittstelle seine Zugangsdaten (IP-Adresse, Benutzername, Passwort etc.) ein. Dies sollte natürlich über SSL/TLS verschlüsselt erfolgen. Nach einer erfolgreichen Anmeldung wird der Zugang für den Client freigeschaltet.

- PPTP (Point to Point Tunnel Protocol)

  PPTP ist ein typisches Tunneling-Protokoll für VPNs, also Protokollen, die verwendet werden, um Daten bei der Übertragung zu verschlüsseln, durch den Tunnel zu übertragen und die Verbindung zu verwalten. Als kryptographische Verfahren stehen bei PPTP RC4 mit 40 oder 128 Bit zur Verschlüsselung sowie PAP oder CHAP zur Authentisierung zur Auswahl. Aufgrund von Sicherheitsproblemen in der ersten Version sollte nur PPTPv2 zum Einsatz kommen sowie ein Verschlüsselungsverfahren mit ausreichender Schlüssellänge.

- IPSec

  IPSec bietet starke kryptographische Verfahren und eine gegenseitige Authentisierung der Kommunikationspartner. Diese sollte sinnvollerweise auf Zertifikaten basieren. Deren Verwendung ist aber einerseits noch nicht in allen IPsec-Implementationen vorgesehen, zum anderen müssen diese erst geeignet generiert und verteilt werden (typisches PKI-Problem).

- WLAN-spezifische Sicherheitsmechanismen wie WEP, IEEE 802.1X, WPA, WPA2, TKIP, IEEE 802.11i

  Bei allen WLAN-spezifischen Sicherheitsmechanismen soll für Sicherheit auf der Funkstrecke gesorgt werden. Diese müssen geeignet kombiniert werden. Aufgrund der Entwicklung in diesen Bereichen (siehe oben) sind aufgrund des Verbreitungsgrads bzw. der Sicherheitsmängel dieser Verfahren nicht alle für die Verwendung bei Hotspots geeignet.

Beim Betrieb von Hotspots sollten außerdem folgende Sicherheitsmaßnahmen umgesetzt werden:

- Access Points, die als Hotspot betrieben werden sollen, dürfen nicht direkt mit einem LAN verbunden werden, sondern nur über ein Sicherheitsgateway.
- Die Kommunikation von WLAN-Clients untereinander, die sogenannte Inter-Client-Kommunikation, sollte komplett unterbunden werden.

- Die Funkschnittstelle sollte mit Funk-Analyse-Systemen überwacht werden, um fremde Access Points und Hotspots zu erkennen.
- Die Authentisierungsdaten sollten über die Funkstrecke, also zwischen WLAN-Client und Access Point immer verschlüsselt übertragen werden. Bei der weiteren Übertragung der Daten von einem Hotspot-Access Point zu den Authentisierungssystemen (beispielsweise einem RADIUS-Server) sind geeignete Verschlüsselungsverfahren wie SSL oder IPSec anzuwenden, vor allem bei der Nutzung öffentlicher Netze.
- Falls für die Authentisierung Zertifikate verwendet werden, sollten diese von einer geeigneten Zertifizierungsinstanz signiert sein. Außerdem sollte der Fingerprint des Serverzertifikats veröffentlicht werden, damit Benutzer die Echtheit überprüfen können.
- Jeder Betreiber eines Hotspots sollte mindestens ein geeignetes Verfahren zur Verschlüsselung der Funkstrecke anbieten, damit die Benutzer ihre Daten vor unbefugtem Mitlesen schützen können. Nicht alle Benutzer haben allerdings ein ausgeprägtes Interesse am Schutz ihrer Daten und Systeme. Es können auch die technischen Voraussetzungen für die Nutzung von angebotenen Verschlüsselungsverfahren fehlen. Daher sollte deren Nutzung optional sein. Die Benutzer sollten aber unbedingt auf die Möglichkeit und die Vorteile der verschlüsselten Übertragung hingewiesen werden.
- Viele Benutzer wollen über einen Hotspot per Remote Access auf das Netz der eigenen Institution zugreifen. Hierfür müssen diese die organisationseigenen Sicherheitsvorgaben umsetzen können. Daher sollte die technische Ausgestaltung des Hotspots die Nutzung typischer Sicherheitsmaßnahmen wie IPsec ermöglichen.

Außerdem sollten Hotspot-Betreiber regelmäßig die Protokolle daraufhin überprüfen, ob hier Unregelmäßigkeiten zu erkennen sind, also beispielsweise die Zahl der Benutzer die der angemeldeten Gäste übersteigt.

Anbieter von öffentlichen Hotspots haben darüber hinaus die jeweiligen gesetzlichen und regulatorischen Vorgaben zu beachten. In Deutschland gehören hierzu die Vorgaben der Bundesnetzagentur für die Bereitstellung von Internetzugängen.

Die Sicherheitsrichtlinien, die Hotspot-Benutzer beachten sollten, sind in M 2.389 *Sichere Nutzung von Hotspots* beschrieben.

Ergänzende Kontrollfragen:

- Sind die Nutzungsbedingung für den Hotspot für jeden Benutzer transparent?
- Wurden ausreichende Maßnahmen getroffen, um die Funkstrecke abzusichern?

M 4.294 Sichere Konfiguration der Access Points

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Keinesfalls dürfen Access Points in der Konfiguration des Lieferzustandes verwendet oder mit Einstellungen z. B. für SSID (Service Set Identifier), Zugangskennwörter oder kryptographischen Schlüssel versehen werden, die in den Handbüchern des Produktes genannt werden.

Folgende Einstellung sollten vorgenommen bzw. auf individuelle, sichere Werte geändert werden:

- Soweit möglich, sollte ein administrativer Zugriff auf die Access Points über die Luftschnittstelle generell deaktiviert werden.
- Alle Administrationspasswörter sollten möglichst komplex sein und regelmäßig gewechselt werden.
- Unsichere Administrationszugänge (z. B. über Telnet, HTTP) sollten möglichst abgeschaltet werden. Ein administrativer Zugriff muss in jedem Fall über eine verschlüsselte Verbindung erfolgen (z. B. über SSL oder SSH).

Deaktivierung unsicherer Administrationszugänge

- Die voreingestellte SSIDs, kryptographische Schlüssel oder Passwörter müssen gleich nach Inbetriebnahme geändert werden.
- Die SSID sollte keinen Hinweis auf den Inhaber oder den Zweck eines WLAN geben. Ebenso sollte die SSID nicht auf "Any" gesetzt sein, da sonst jede beliebige WLAN-Komponente an der Kommunikation teilnehmen kann.
- Der SSID-Broadcast sollte deaktiviert werden, damit die Existenz des WLAN nicht unnötig mitgeteilt wird. Ferner sollte die Assoziation via SSID-Broadcast deaktiviert sein, damit der Client explizit die gewünschte SSID bei der Assoziierung angeben muss.
- Es müssen geeignete Verschlüsselungsmechanismen aktiviert werden. Gleichzeitig muss sichergestellt sein, dass alle Komponenten im WLAN diese unterstützen. Es darf nicht möglich sein, mit WLAN-Komponenten Verbindungen aufzubauen, die keine oder nur unzureichende Verschlüsselungsmechanismen besitzen.
- Kryptographische Schlüssel sollten möglichst zufällig gewählt und regelmäßig gewechselt werden. Es sollte ein komplexer Pre-Shared Key (PSK) bei der Nutzung von WPA-PSK bzw. WPA2-PSK verwendet werden. Falls kryptographische Schlüssel wie der PSK über ein Passwort generiert wird, so sollte hierfür ein Passwort hoher Komplexität mit mindestens 20 Zeichen gewählt werden.
- Zur Einschränkung der zugelassenen Kommunikationspartner eines Access Point sollten Access Control Lists (ACLs) auf MAC-Adress-Ebene verwendet werden. Dies ist insbesondere bei kleinen bis sehr kleinen WLAN-Installationen hilfreich. Als alleiniges Instrument kann sie aber besonders im WLAN (durch die leichte Abhörbarkeit) im Allgemeinen nicht für ein ausreichendes Maß an Sicherheit sorgen, da MAC-Adressen einfach geändert werden können. ACLs im WLAN können daher nur als eine

Access Control Lists

schwache, ergänzende Zusatzmaßnahme gesehen werden, deren Einsatz vor allem in speziellen Situationen sinnvoll ist. Da der Sicherheitsgewinn begrenzt ist, sollte in größeren Netzen abgewogen werden, ob der Sicherheitsgewinn den entstehenen Administrationsaufwand rechtfertigt.

- Der DHCP (Dynamic Host Configuration Protocol) Server im Access Point sollte, falls vorhanden und technisch möglich, abgeschaltet werden, d. h. es sollten statische IP-Adressen vergeben und der zulässige IP-Adressraum möglichst klein gehalten werden. Der DHCP Server wird einem Eindringling andernfalls automatisch eine gültige IP-Adresse zuweisen.
- Beim Einsatz mehrerer Access-Points sind die benutzten Frequenzkanäle benachbarter Access-Points möglichst überlappungsfrei zu wählen.
- Änderungen an der Systemkonfiguration müssen getestet und dokumentiert werden.
- Es muss regelmäßig überprüft werden, ob alle sicherheitsrelevanten Updates und Patches eingespielt worden sind. Auch für die zugehörigen Gerätetreiber der WLAN-Hardware auf den WLAN-Clients ist dies zu berücksichtigen. Eine neue Software-Version oder ein Patch sollte erst nach einem angemessenen Test im WLAN eingespielt werden. Es ist in der Praxis schon vorgekommen, dass nach einen Software-Update die WLAN-Kommunikation nur noch eingeschränkt oder sogar gar nicht mehr möglich war.

  Es sollten Melde- und Informationsprozeduren im Änderungsmanagement spezifiziert werden, die beschreiben, wer und wie bei derartigen Änderungen zu informieren ist. Ebenso ist die Dokumentation der WLAN-Infrastruktur anzupassen.
- Wenn WLAN-Komponenten längere Zeit nicht benutzt werden, sollten sie abgeschaltet werden. Access Points sollten außerhalb der Arbeitszeiten (beispielsweise nachts und am Wochenende) automatisch deaktiviert werden.

Diese Aufgaben können durch den Einsatz einer WLAN-Management-Software und durch Einbindung in ein zentrales Netz-Management sinnvoll unterstützt und überwacht werden.

Ergänzende Kontrollfragen:

- Auf welchen Wegen wird zur Administration auf das System zugegriffen?
- Wie werden Konfigurationsänderungen getestet und dokumentiert?
- Ist sichergestellt, dass Patches und Updates gegen bekannt gewordene Sicherheitslücken zeitnah installiert werden?
- Ist sichergestellt, dass WLAN-Komponenten auch tatsächlich abgeschaltet werden, wenn sie länger nicht benutzt werden?

M 4.295 Sichere Konfiguration der WLAN-Clients

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Damit WLANs sicher betrieben werden können, müssen auch alle damit gekoppelten Clients sicher konfiguriert sein. Geeignete IT-Sicherheitsempfehlungen für Clients sind in den Bausteinen der Schicht 3 *IT-Systeme* beschrieben. Zusätzlich sollten folgende WLAN-spezifischen Sicherheitsmaßnahmen ergriffen werden:

- Voreingestellte SSIDs, kryptographische Schlüssel und Passwörter müssen direkt nach Inbetriebnahme geändert werden. Passwörter sollten so gewählt werden, dass sie nur schwer zu erraten sind.
- Der Ad-hoc-Modus sollte abgeschaltet werden, damit Clients nur über einen Access Point miteinander kommunizieren können, nicht direkt untereinander.
- Schutzbedürftige Daten auf mobilen Endgeräten sollten verschlüsselt werden. Hierfür gibt es eine Vielzahl hardware- oder softwarebasierender Produkte, die es erlauben, einzelne Dateien, bestimmte Bereiche oder die ganze Festplatte zu verschlüsseln, so dass nur diejenigen, die über eine Zugriffsberechtigung verfügen, die Daten entschlüsseln können.
- Die WLAN-Schnittstellen von Clients sollten generell deaktiviert sein, solange diese nicht tatsächlich genutzt werden. Vor allem sollte dies immer dann erfolgen, wenn die Clients in einem kabelgebundenen LAN angemeldet sind. Der Zugriff von einem Client auf das hausinterne LAN über die üblichen internen Anbindungen sollte also nur dann möglich sein, wenn keine WLAN-Aktivitäten erfolgen. Ansonsten bietet dies Angreifern die Möglichkeit, über die WLAN-Schnittstelle auf eventuell ins Hausnetz bestehende (und authentisierte) Verbindungen zuzugreifen.
- Beim Aufbau von VPN-Verbindungen sollte diverse Sicherheitsvoraussetzungen auf Client-Seite erfüllt sein. So sollte es nicht möglich sein, neben einer VPN-Verbindung andere Kommunikationsschnittstellen parallel zu nutzen, damit nicht über unsichere Kanäle die als sicher betrachtete VPN-Anbindungen ausgehöhlt wird. Außerdem ist es empfehlenswert, gewisse Mindest-Sicherheitsmaßnahmen bei den Clients nicht nur vorauszusetzen, sondern sie besser auch noch zu überprüfen, bevor ein Zugriff über VPN gestattet wird. Dafür empfehlen sich Tools, die die Einhaltung der Sicherheitsrichtlinien auf den Clients überprüfen, bevor der Server weitere Kommunikation erlaubt.
- Es muss regelmäßig überprüft werden, ob alle sicherheitsrelevanten Updates und Patches eingespielt worden sind. Das Einspielen eines größeren Software-Updates auf WLAN-Clients über das WLAN kann problematisch sein, da die Bandbreite im WLAN im Vergleich zum kabelbasierten LAN deutlich geringer ist. Die Installation eines Updates dauert damit nicht nur erheblich länger, sondern auch andere Nutzer des WLANs können spürbar behindert werden, da WLAN ein Shared Medium ist. Wenn möglich, sollte daher ein Client für die Installation eines größeren Software-Update an ein kabelbasiertes LAN angeschlossen werden. Ergänzend kann die

Übertragung von Software Updates auf der Luftschnittstelle niedriger priorisiert werden, sofern die hierdurch verlängerte Installationszeit praktikabel ist. Auf diese Weise werden andere WLAN-Anwendung nicht mehr signifikant durch das Software-Update gestört.

Es sollte regelmäßig kontrolliert werden, dass sicherheitsrelevante Einstellungen nicht geändert worden sind.

Es muss klar geregelt werden, ob und unter welchen Rahmenbedingungen WLAN-Clients an fremden Netzen angemeldet werden dürfen (siehe M 4.251 *Arbeiten mit fremden IT-Systemen*), vor allem wenn diese Zugriff auf die Produktivumgebung haben oder auf diesen vertrauliche Informationen gespeichert sind.

WLAN-Clients sollten grundsätzlich nicht in unsicheren Umgebungen, wie z. B. öffentliche Hotspots oder nur durch WEP gesicherte WLANs, betrieben werden. WLAN-Clients, die Daten hohen Schutzbedarfs verarbeiten, dürfen nur in WLANs eingesetzt werden, die vollständig unter eigener Kontrolle betrieben werden und entsprechend sicher konfiguriert wurden. Die Nutzung in anderen WLANs ist zu untersagen.

Alle Benutzer von WLAN-Komponenten sollten über potentielle Risiken und Probleme bei der Nutzung sowie über den Nutzen, aber auch die Grenzen der eingesetzten Sicherheitsmaßnahmen informiert sein. Alle Benutzer müssen die Sicherheitsrichtlinie zur WLAN-Nutzung kennen (siehe M 2.382 *Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung*). Niemand sollte auf ein internes WLAN zugreifen dürfen, der nicht vorher den in der WLAN-Sicherheitsrichtlinie festgehaltenen Nutzungsbedingungen schriftlich zugestimmt hat.

Ergänzende Kontrollfragen:

- Sind die Benutzer darüber informiert, welche Sicherheitsaspekte sie bei der WLAN-Nutzung zu beachten haben?
- Ist sichergestellt, dass Patches und Updates gegen bekannt gewordene Sicherheitslücken zeitnah installiert werden?
- Werden die WLAN-Schnittstellen von Clients ausgeschaltet, wenn sie nicht genutzt werden?

M 4.296 Einsatz einer geeigneten WLAN-Management-Lösung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Damit bei allen WLAN-Komponenten eine aus Sicherheitssicht optimale Konfiguration gewährleistet ist, sollten diese sorgfältig administriert werden. Da die Administration bei großen WLANs aufwendig und komplex sein kann, ist der Einsatz von WLAN-Systemmanagement-Tools sinnvoll. Diese sollten möglichst auch in vorhandene IT- und Netzmanagement-Tools integriert werden können.

Generell ist die Realisierung einer Management-Lösung zu empfehlen, die neben einer Überwachung des WLAN auch eine Online-Dokumentation ermöglichen kann. Je nach Leistungsumfang sollte es folgende Möglichkeiten bieten:

- Dokumentation der Firmware-Stände der Access Points
- Dokumentation der Firmware-Stände und Treiber der WLAN-Adapter der WLAN-Clients
- Dokumentation der Sicherheitskonfigurationen
- Dokumentation von ortsspezifischen Konfigurationen
- Historienverwaltung von Konfigurationsänderungen

Damit die Administratoren einen Überblick über alle stationären und mobilen Systeme und Anwendungen erhalten, und dies möglichst einfach, sollte eine Systemmanagement-Lösung mobile Endgeräte und deren Anwendungen automatisch inventarisieren können. Jedes Endgerät sollte von der Management-Software in die Konfigurations- und Kontrollprozesse einbezogen werden, sobald es am Netz angemeldet wird.

Die Nutzung dieser Funktionen richtet sich nach den Festlegungen im Betriebshandbuch.

Das Management-System sollte darüber hinaus über eine Alarm- und Fehlerbehandlung verfügen. Hierbei sollten folgende Aufgaben durch die Administratoren durchgeführt werden können:

- Auswertung und Bewertung von Alarmen, z. B. eine Häufung von fehlgeschlagenen Authentisierungsversuchen an einem Access Point
- Auswertung von Statistiken zur Fehlersuche
- Auslösung von Maßnahmen bei einem vermuteten Sicherheitsvorfall
- Anpassung von Schwellwerten zur Alarmauslösung an eine geänderte WLAN-Nutzung

Es sollte ein geeignetes Netzmanagement-Protokoll ausgewählt werden, beispielsweise SNMPv3 (siehe auch M 2.144 *Geeignete Auswahl eines Netzmanagement-Protokolls*).

Die aufgezeichneten Protokolldaten sollten regelmäßig, spätestens einmal monatlich, ausgewertet werden. Der Umfang der Protokollierung ist mit der

Personalvertretung und dem Datenschutzbeauftragten abzustimmen. Die WLAN-Management-Software bzw. die allgemeine Netz-Management-Lösung sollte Filtermöglichkeiten bieten, um die Protokolldaten besser auswerten zu können.

Ergänzende Kontrollfragen:

- Wann wurden die aufgezeichneten Protokolldaten zuletzt ausgewertet?
- Wurden alle WLAN-Komponenten inventarisiert?

M 4.297 Sicherer Betrieb der WLAN-Komponenten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

WLANs sind attraktive Ziele für Angreifer und müssen daher sehr sorgfältig konfiguriert werden, damit sie sicher betrieben werden können. Alle WLAN-Komponenten müssen so konfiguriert sein, dass sie so gut wie möglich gegen Angriffe geschützt sind. Solange WLAN-Komponenten nicht entsprechend konfiguriert sind, dürfen sie nicht aktiviert bzw. mit der Produktivumgebung gekoppelt werden.

Abzusichernde WLAN-Komponenten sind unter anderem die Access Points, das Distribution System, die WLAN-Clients, die Betriebssysteme, auf denen die WLAN-Komponenten betrieben werden, und die verwendeten Protokolle. Insbesondere sind folgende Punkte zu beachten:

- Für die Administration der verschiedenen WLAN-Komponenten müssen Verantwortliche benannt werden.
- Nach der Installation und Inbetriebnahme von WLAN-Komponenten müssen alle erforderlichen Sicherheitsmechanismen aktiviert werden.
- Die Administration der WLAN-Komponenten darf nur über eine sichere Verbindung erfolgen, d. h. die Administration sollte an der Konsole direkt, nach starker Authentisierung (bei Zugriff aus dem LAN) oder über eine verschlüsselte Verbindung (bei Zugriff aus dem Internet) erfolgen.
- Es muss die Regel "Alles was nicht ausdrücklich erlaubt ist, ist verboten" realisiert sein. So darf z. B. kein Benutzer, der nicht in einer Access-Liste eingetragen ist, auf das WLAN zugreifen. Die Vergabe von Zugriffsrechten auf Verzeichnisse und Dateien sollte so restriktiv wie möglich erfolgen.
- Es ist darauf zu achten, dass die eingesetzte Software immer auf einem aktuellen Stand ist und etwaige sicherheitsrelevante Patches unverzüglich aufgespielt werden.
- Konfigurationsänderungen sollten durch das System so protokolliert werden, dass Manipulationen zeitnah nachvollzogen werden können. Die Protokolldaten selber müssen so abgesichert werden, dass Manipulationen an ihnen ausgeschlossen sind.
- Es sollten alle sicherheitsrelevanten Ereignisse protokolliert werden. Dazu gehören z. B. Versuche von unberechtigten Zugriffen und Daten zur Netzauslastung und -überlastung. Die aufgezeichneten Protokolldaten müssen regelmäßig ausgewertet werden. Der Umfang der Protokollierung ist mit der Personalvertretung und dem Datenschutzbeauftragten abzustimmen.
- Die WLAN-Komponenten müssen in das Datensicherungskonzept einbezogen werden. Beim Wiedereinspielen von gesicherten Datenbeständen muss darauf geachtet werden, dass für den sicheren WLAN-Betrieb relevante Dateien wie Access-Listen, Passwortdateien oder Filterregeln auf dem aktuellsten Stand sind.

Es sollte möglichst eine Standard-Konfiguration für die eingesetzten WLAN-Komponenten ausgearbeitet werden, die die Vorgaben aus der WLAN-Sicherheitsrichtlinie wiederspiegelt. Dies erleichert bei einer Vielzahl zu betreuender Geräte außerdem das Einspielen von Änderungen. Ebenso lassen sich hierüber Abweichungen von der Soll-Konfiguration schneller feststellen.

Sinnvoll ist der Einsatz einer WLAN-Management-Lösung, die für eine effiziente Konfiguration der Access Points sorgt. Access Points und die aktiven Komponenten des Distribution System sollten weiterhin in das Netz-Management-System eingebunden und überwacht werden können. Schließlich sollte auch die Verfügbarkeit der Authentisierungsserver über das Management-System geprüft werden können. Gegebenenfalls bietet sich die Erweiterung eines bereits genutzten Netz-Management-Systems um ein WLAN-Management-Modul an.

Der Anschluss von fremden Access Points oder Manipulationen an den Switches des Distribution Systems sollte durch das WLAN-Management-System erkannt werden. Der betroffene Netz-Port des Distribution Switch sollte in einem solchen Fall umgehend gesperrt werden.

Ebenso sollte die Konfiguration der Access Points und des Distribution Systems regelmäßig geprüft werden. Hierzu muss die aktuell vorgefundene Systemkonfiguration gegen eine dokumentierte und validierte Konfiguration geprüft werden. Bei nicht bestätigten Änderungen müssen die Systeme untersucht und gegebenenfalls sogar abgeschaltet und geprüft werden, ob ein Angriff vorliegt.

Für den sicheren Betrieb der WLAN-Komponenten ist sowohl die Grund-Konfiguration, die aufbauend auf der WLAN-Sicherheitsrichtlinie festgelegt wurde, als auch alle durchgeführten Änderungen sorgfältig zu dokumentieren, um diese jederzeit nachvollziehbar zu machen. Neben der Dokumentation der Sicherheitskonfigurationen gehört auch die Dokumentation der Firmware-Stände der Access Points und die Dokumentation von ortsspezifischen Konfigurationen.

Ergänzende Kontrollfragen

- Ist sichergestellt, dass auf allen WLAN-Komponenten die erforderlichen Sicherheitsmechanismen aktiviert sind?
- Wie wird sichergestellt, dass die Betriebssysteme und Programme, die auf den WLAN-Komponenten eingesetzt werden, stets auf einem sicheren Patch-Stand sind?
- Auf welchem Weg greifen Administratoren oder Revisoren auf das Sicherheitsgateway bzw. die Komponenten zu?
- Werden alle relevanten Informationen auf WLAN-Komponenten bei der Datensicherung berücksichtigt?

M 4.298 Regelmäßige Audits der WLAN-Komponenten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Bei allen Komponenten der WLAN-Infrastruktur muss regelmäßig überprüft werden, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt und ob diese korrekt konfiguriert sind. Neben den Access Points zählen hierzu die Komponenten des Distribution Systems, die Elemente der Sicherheitsinfrastruktur (inklusive der Authentisierungsserver) und die Elemente des WLAN-Management-Systems. Das WLAN-Management-System sollte je nach bereitgestelltem Funktionsumfang nicht nur die aktuelle Konfigurationen der Access Points, sondern auch die der Komponenten des Distribution Systems verwalten und über eine Historienverwaltung auch vorhergehende Konfigurationen führen (siehe M 4.296 *Einsatz einer geeigneten WLAN-Management-Lösung*). Ebenso sollten zentrale Sicherheitssysteme, wie der Authentisierungsserver oder das Koppelelement am Übergangspunkt zwischen Distribution System und LAN, regelmäßigen Sicherheitsüberprüfungen unterzogen werden.

Insbesondere für Installationen in öffentlich zugänglichen Bereichen sollte eine stichprobenartige Prüfung im Hinblick auf gewaltsame Öffnungsversuche oder Manipulationsversuche (speziell für Access Points) durchgeführt werden. Ein Indiz für eine Kompromittierung des WLAN ist zum Beispiel ein zwischen Access Point und Distribution Switch geschalteter Hub. Derartige zu Diagnosezwecken erfolgte Aufbauten dürfen nur autorisiertem Personal zugänglich sein und sind nach Ende der Messungen umgehend zu entfernen.

Weiterhin müssen die WLAN-Clients regelmäßig überprüft werden. Bei einer größeren Anzahl sollte dies zumindest stichprobenweise geschehen. Zu prüfen ist zunächst die Konfiguration von WLAN-Adapter und IEEE 802.1X Supplicant (bzw. VPN-Client, falls im WLAN genutzt). Weiterhin ist systemabhängig auch der Patch Level der Betriebssysteme, die Aktualität der Treibers für die WLAN-Adapter der Clients, die Regelbasis der Personal Firewalls, die Aktualität des verwendeten Virenschutzes sowie die Sicherheitseinstellungen der über das WLAN genutzten Anwendungen zu.

Falls Unregelmäßigkeiten oder Schwachstellen festgestellt werden, müssen diese dokumentiert werden, hierbei muss auch festgehalten werden, wie diese verfolgt werden.

Neben den regelmäßigen Audits der einzelnen WLAN-Komponenten sollte auch regelmäßig eine Revision der WLAN-Sicherheitsrichtlinie durchgeführt werden. Insbesondere sollte eine Bewertung erfolgen, ob die ergriffenen Maßnahmen zur Absicherung des WLANs noch dem Stand der Technik entsprechen und ob der zu Grunde gelegte Schutzbedarf nach wie vor gültig ist.

Außerdem sollte immer wieder hinterfragt werden, ob alle Benutzer über die erforderlichen WLAN-Sicherheitsmaßnahmen informiert sind und diese umsetzen.

Ergänzende Kontrollfragen:

- Werden regelmäßig Sicherheitsaudits durchgeführt?
- Wie werden festgestellte Unregelmäßigkeiten dokumentiert und verfolgt?

M 5 Maßnahmenkatalog Kommunikation

M 5.29	Gelegentliche Kontrolle programmierter Zieladressen und Protokolle	
M 5.30	Aktivierung einer vorhandenen Callback-Option	
M 5.31	Geeignete Modem-Konfiguration	
M 5.32	Sicherer Einsatz von Kommunikationssoftware	
M 5.33	Absicherung der per Modem durchgeführten Fernwartung	
M 5.34	Einsatz von Einmalpasswörtern	
M 5.35	Einsatz der Sicherheitsmechanismen von UUCP	
M 5.36	Verschlüsselung unter Unix und Windows NT	
M 5.37	Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz	
M 5.38	Sichere Einbindung von DOS-PCs in ein Unix-Netz	**entfallen**
M 5.39	Sicherer Einsatz der Protokolle und Dienste	
M 5.40	Sichere Einbindung von DOS-PCs in ein Windows NT Netz	**entfallen**
M 5.41	Sichere Konfiguration des Fernzugriffs unter Windows NT	
M 5.42	Sichere Konfiguration der TCP/IP-Netzverwaltung unter Windows NT	
M 5.43	Sichere Konfiguration der TCP/IP-Netzdienste unter Windows NT	
M 5.44	Einseitiger Verbindungsaufbau	
M 5.45	Sicherheit von WWW-Browsern	
M 5.46	Einsatz von Stand-alone-Systemen zur Nutzung des Internets	
M 5.47	Einrichten einer Closed User Group	
M 5.48	Authentisierung mittels CLIP/COLP	
M 5.49	Callback basierend auf CLIP/COLP	
M 5.50	Authentisierung mittels PAP/CHAP	
M 5.51	Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution	
M 5.52	Sicherheitstechnische Anforderungen an den Kommunikationsrechner	
M 5.53	Schutz vor Mailbomben	
M 5.54	Schutz vor Mailüberlastung und Spam	

M 5.55	Kontrolle von Alias-Dateien und Verteilerlisten	
M 5.56	Sicherer Betrieb eines Mailservers	
M 5.57	Sichere Konfiguration der Mail-Clients	
M 5.58	Auswahl und Installation von Datenbankschnittstellen-Treibern	
M 5.59	Schutz vor DNS-Spoofing	
M 5.60	Auswahl einer geeigneten Backbone-Technologie	
M 5.61	Geeignete physikalische Segmentierung	
M 5.62	Geeignete logische Segmentierung	
M 5.63	Einsatz von GnuPG oder PGP	
M 5.64	Secure Shell	
M 5.65	Einsatz von S-HTTP	**entfallen**
M 5.66	Verwendung von SSL	
M 5.67	Verwendung eines Zeitstempel-Dienstes	
M 5.68	Einsatz von Verschlüsselungsverfahren zur Netzkommunikation	
M 5.69	Schutz vor aktiven Inhalten	
M 5.70	Adreßumsetzung - NAT (Network Address Translation)	
M 5.71	Intrusion Detection und Intrusion Response Systeme	
M 5.72	Deaktivieren nicht benötigter Netzdienste	
M 5.73	Sicherer Betrieb eines Faxservers	
M 5.74	Pflege der Faxserver-Adressbücher und der Verteillisten	
M 5.75	Schutz vor Überlastung des Faxservers	
M 5.76	Einsatz geeigneter Tunnel-Protokolle für die RAS-Kommunikation	
M 5.77	Bildung von Teilnetzen	
M 5.78	Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung	
M 5.79	Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung	
M 5.80	Schutz vor Abhören der Raumgespräche über Mobiltelefone	
M 5.81	Sichere Datenübertragung über Mobiltelefone	
M 5.82	Sicherer Einsatz von SAMBA	

M 5.135 Sicherer Medientransport mit SRTP

M 5.136 Dienstgüte und Netzmanagement bei VoIP

M 5.137 Einsatz von NAT für VoIP

M 5.138 Einsatz von RADIUS-Servern

M 5.139 Sichere Anbindung eines WLANs an ein LAN

M 5.140 Aufbau eines Distribution Systems

M 5.141 Regelmäßige Sicherheitschecks in WLANs

M 5.1 Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen

Verantwortlich für Initiierung: Leiter Haustechnik

Verantwortlich für Umsetzung: Administrator, Haustechnik

Nicht benötigte Leitungen sollten nach Möglichkeit entfernt werden. Ist dies aufgrund der damit verbundenen Beeinträchtigung des Dienstbetriebes (Öffnen von Decken, Fensterbank- und Fußbodenkanälen) nicht möglich oder werden für zukünftige Netzerweiterungen Reserven vorgehalten, sind folgende Maßnahmen sinnvoll:

- Kennzeichnen der nicht benötigten Leitungen in der Revisions-Dokumentation und Löschen der Eintragungen in der im Verteiler befindlichen Dokumentation,
- Auftrennen aller Rangierungen und Verbindungen der freien Leitungen in den Verteilern (soweit möglich),
- Kurzschließen der freien Leitungen an beiden Kabelenden und in allen berührten Verteilern,
- Auflegen der freien Leitungen auf Erde (Masse) an beiden Kabelenden und in allen berührten Verteilern; bei dadurch entstehenden Masse-Brumm-Schleifen ist nur einseitig zu erden,
- Gewährleisten, dass nicht benötigte Leitungen bei ohnehin anstehenden Arbeiten im Netz entfernt werden.

Alle hier genannten Arbeiten im Netz müssen revisionsfähig dokumentiert und in sinnvollen Zeitabständen und in jedem Fall nach Leitungsarbeiten durch Dritte fachkundig geprüft werden. Diese Prüfungen sind zu protokollieren.

Ergänzende Kontrollfragen:

- Wer entscheidet über die Notwendigkeiten von Leitungen und über die Größe von Reserven?
- Wer prüft das ordnungsgemäße Kurzschließen und Erden?

M 5.2 Auswahl einer geeigneten Netz-Topographie

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Planer, Leiter Haustechnik

Unter der Topographie eines Netzes wird die rein physikalische Struktur eines Netzes in Form der Kabelführung verstanden. Im Gegensatz dazu handelt es sich bei der Netztopologie um die logische Struktur eines Netzes. Die Topographie und Topologie eines Netzes sind nicht notwendig identisch. Die Topographie orientiert sich naturgemäß fast immer an den räumlichen Verhältnissen, unter denen das Netz aufgebaut wird. Dies sind u. a.:

- Standorte der Netzteilnehmer,
- verfügbarer Platz für Trassen und Kabel (M 1.21 *Ausreichende Trassendimensionierung*),
- erforderliche Kabeltypen (M 1.20 *Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht*),
- Anforderungen an den Schutz von Kabeln (M 1.22 *Materielle Sicherung von Leitungen und Verteilern*).

Nachfolgend werden die Vor- und Nachteile möglicher Topographien aufgeführt. Weitere denkbare Topographien, die an dieser Stelle nicht genannt sind, können als Spezialfall der betrachteten Strukturen aufgefasst werden.

Im Allgemeinen können zwei Grundformen unterschieden werden: der Stern und der Bus. Daraus lassen sich als Erweiterungen aus dem Stern eine baumförmige Struktur und aus dem Bus eine ringförmige Struktur ableiten. Diese vier Formen werden im Folgenden kurz dargestellt:

Stern

Bei einem Stern sind alle Teilnehmer des Netzes über eine dedizierte Leitung mit einem zentralen Knoten verbunden. Die häufig anzutreffende Token-Ring-Architektur wird topographisch als Stern verkabelt, bildet topologisch jedoch einen Ring.

Die Vorteile:

- Die Beschädigung einer Leitung beeinträchtigt nur den Betrieb des daran angeschlossenen Systems.
- Änderungen der Zuordnung von Netzteilnehmern zum Anschlusspunkt am zentralen Knoten sowie Trennungen einzelner Teilnehmer lassen sich zentral durchführen.
- Mit einer Sternverkabelung können alle denkbaren logischen Topologien nachgebildet werden.

Die Nachteile:

- Bei einem Ausfall des zentralen Knotens fallen alle angeschlossenen IT-Systeme aus.

- Durch die Einzelanbindung jedes Teilnehmers an den zentralen Knoten ist ein hoher Kabelaufwand erforderlich.
- Mit zunehmender Zahl individueller Leitungen wächst die Gefahr des Übersprechens.
- Durch die sternförmige Verkabelung können Reichweitenprobleme in Abhängigkeit vom verwendeten Kabeltyp und vom eingesetzten Protokoll auftreten (siehe M 5.3 *Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht*). In diesem Fall können Verstärker (Repeater) eingesetzt werden, was jedoch u. U. bei einer hohen Zahl von Leitungen sehr kostenintensiv ist. Hinzu kommt, dass nicht beliebig viele Verstärker in eine Leitung geschaltet werden dürfen. Dies ist ebenfalls vom verwendeten Protokoll abhängig. Eine andere Möglichkeit ist hier der Übergang zu einer baumförmigen Struktur.

Baum

Eine Baumstruktur entsteht durch die Verbindung mehrerer Sterne. In diesem Fall werden die Netzteilnehmer zu Gruppen zusammengefasst, die an dezentrale Netzknoten sternförmig angeschlossen werden. Diese dezentralen Netzknoten sind wiederum über eine Leitung oder mehrere dedizierte Leitungen miteinander verbunden. Unter Umständen werden auch alle dezentralen Netzknoten an einem zentralen Netzknoten zusammengeführt.

Die Vorteile:

- Für den Anschluss der Systeme an die dezentralen Netzknoten gelten die gleichen Vorteile wie beim Stern.
- Für neue Teilnehmer muss nur im Bereich des dezentralen Netzknotens neu verkabelt werden.
- Bei entsprechender Auslegung der dezentralen Netzknoten ist ein Datenaustausch zwischen den Teilnehmern eines solchen Knotens auch bei einem Ausfall der anderen Knoten möglich.
- Durch die Verbindung der dezentralen Knoten untereinander über eine Leitung reduziert sich der Verkabelungsaufwand.
- Zur Überwindung großer Entfernungen zwischen den Knoten reicht die Verstärkung auf einer Leitung (Kostenersparnis).
- Für die Verbindung der Knoten ist der Einsatz hochwertigerer (meist teurerer) Kabel sinnvoll, mit denen auch größere Distanzen ohne zusätzliche Verstärkung überwunden werden können. Das bringt gegenüber den sonst notwendigen Verstärkern Vorteile in Bezug auf Ausfallsicherheit und Kostenreduzierung.
- Eine Baumstruktur ermöglicht es, durch Vermaschung der einzelnen Knoten redundante Verbindungen aufzubauen.

Die Nachteile:

- Bei Störung eines Übergangs zu einem anderen dezentralen Netzknoten wird der Betrieb mit allen daran angeschlossenen Teilnehmern unterbrochen.

Bus

Bei einem Bus werden alle Netzteilnehmer an eine gemeinsame Leitung angeschlossen. Dies geschieht im Allgemeinen durch ein zentrales Kabel, an das mit Stichleitungen die einzelnen Teilnehmer angebunden werden.

Die Vorteile:

- Die Verkabelung reduziert sich auf ein Kabel, hinzu kommen evtl. notwendige Stichleitungen.
- Die Nachinstallation neuer Teilnehmer erfordert im Allgemeinen nur geringen Verkabelungsaufwand. Sie werden einfach an das vorhandene Buskabel angeschlossen.
- Der Bus ist durch den Einsatz von Verstärkern einfach verlängerbar. Dabei sind jedoch die Längenrestriktionen aufgrund des eingesetzten Kabeltyps und des verwendeten Protokolls zu beachten (siehe M 5.3 *Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht*).
- Ressourcen können an nahezu beliebigen Stellen am Bus angeschlossen werden.
- Eine Busverkabelung erfordert durch das zentrale Kabel deutlich weniger Platz als eine vergleichbare Sternverkabelung mit TP-Kabel.

Die Nachteile:

- Störungen, die auf das Kabel wirken, beeinträchtigen den gesamten Bus.
- Unterbrechungen des Buskabels bringen den gesamten Datenverkehr zum Erliegen.
- Ab einer gewissen maximalen Länge und einer bestimmten Anzahl von Teilnehmern ist keine einfache Erweiterung des Busses mehr möglich.
- Abhängig vom Kabeltyp müssen Restriktionen beim Anschluss neuer Teilnehmer beachtet werden (z. B. der Mindestabstand zwischen zwei Teilnehmern).

Ring

Der Ring ist aus topographischer Sicht ein Bus, dessen beide Enden miteinander verbunden sind. Eine Sonderform des Rings besteht in der doppelten Ausführung als Doppelring, wie sie z. B. bei FDDI Verwendung findet.

Die Vorteile:

- Der Ring kann bei einer Leitungsunterbrechung mit gewissen Beeinträchtigungen weiterarbeiten. Die Art der Beeinträchtigung hängt vom für den Ring verwendeten Netzzugangsprotokoll ab. Beeinträchtigungen können z. B. Bandbreitenverluste sein.
- Die mögliche Ausführung als Doppelring ermöglicht eine zusätzliche Redundanz bzw. Fehlertoleranz.

Die Nachteile:

- Die verfügbaren Protokolle für Ring- und Doppelringsysteme sind beschränkt, d. h. es können nicht alle Protokolle auf diesen eingesetzt werden. Dies kann sich für die zukünftige Weiterentwicklung des Netzes nachteilig auswirken.

Collapsed und Distributed Backbone

Ein **Collapsed Backbone** ist eine spezielle Ausprägung eines Netzknotens, der innerhalb seiner Backplane (eine lokale Hochgeschwindigkeitsverbindung innerhalb eines Gerätes) eine der o. g. Strukturen oder eine Mischform daraus realisiert. Bei einem Collapsed Backbone werden alle Kabel zentral zu einem Netzknoten geführt, so dass es sich im Prinzip um eine Sternverkabelung handelt. Innerhalb des Netzknotens können nun die unterschiedlichsten Strukturen unterstützt werden. So werden beispielsweise bei einer Baumstruktur die nötigen Verbindungswege zwischen den dezentralen Sternen durch sehr kurze Verbindungen innerhalb des Netzknotens realisiert.

Die Vorteile:

- Alle Kabelanschlüsse können zentral kontrolliert und verwaltet werden.
- Es werden im Allgemeinen hohe Übertragungsraten in der Backplane erreicht. Hierdurch steht, je nach Produkt, zwischen den Segmenten die volle Netzbandbreite zur Verfügung.

Die Nachteile:

- Bei einem Ausfall des Collapsed Backbones fallen alle Netzzugänge aus.

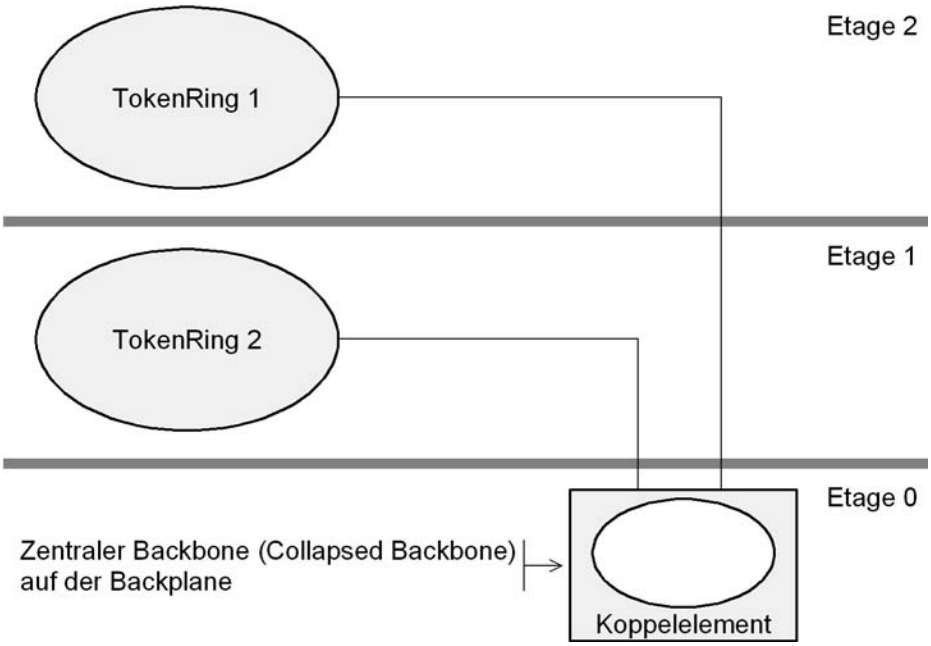


Abbildung: Collapsed Backbone

Bei einem **Distributed Backbone** sind die einzelnen Netzkomponenten, die zum Backbone gehören, räumlich verteilt und werden durch die normale Netzinfrastruktur gekoppelt. Topographische Bäume werden beispielsweise im Allgemeinen durch einen Distributed Backbone realisiert.

Bei der Auswahl einer geeigneten Netztopographie kann, wie bereits eingangs erwähnt, keine allgemein gültige Empfehlung gegeben werden. Solch eine Entscheidung wird u. a. immer stark durch bauliche Gegebenheiten beeinflusst. Allgemein üblich ist heute bei Neuinstallationen eine strukturierte Verkabelung in Stern- oder Baumform. Hierbei ist es sinnvoll, im Backbone-Bereich (Primär- und Sekundärbereich) Lichtwellenleiter und für die Etagenverkabelung (Tertiärbereich) Twisted-Pair-Kabel mind. der Kategorie 5 zu verwenden. Mit Primärbereich wird dabei der Bereich der Kabelführung, der Gebäude miteinander verbindet, bezeichnet und mit Sekundärbereich die Verkabelung zur Verbindung der aktiven Netzkomponenten einzelner Abschnitte innerhalb eines Gebäudes (z. B. zur Verbindung von Stockwerken).

Die Wahl dieser Medien für die einzelnen Bereiche gewährleistet aus heutiger Sicht eine zukunftssichere Verkabelung, die auch höheren Bandbreitenanforderungen v. a. im Backbone-Bereich gerecht wird. Im Einzelfall ist jedoch auch zu prüfen, ob es sinnvoll oder notwendig ist, eine Mischform aus Stern- und Ringverkabelung zu installieren. Hier bietet sich häufig die Möglichkeit, die Primärverkabelung zwischen Gebäuden als FDDI-Doppelring und die Sekundär- und Tertiärverkabelung wie o. g. als Stern- oder Baum auszuführen.

M 5.3 Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Planer, Leiter Haustechnik

Die Auswahl des Kabels aus kommunikationstechnischer Sicht wird u. a. durch die erforderliche Übertragungsrate (Bandbreite) und durch die Entfernungen, die ohne Verstärker zu überwinden sind, bestimmt. Bei der Auswahl sind zusätzlich die Anforderungen durch die baulichen Gegebenheiten zu beachten. Vor- und Nachteile werden nachfolgend unter IT-Sicherheitsgesichtspunkten beschrieben.

Für die kabelgebundene Kommunikation können derzeit zwei Übertragungsmedien unterschieden werden: Kommunikation über Kupferkabel oder über ein optisches Medium (Lichtwellenleiter, LWL). Bei beiden Medientypen lassen sich wiederum verschiedene Unterkategorien unterscheiden. Die wichtigsten Vertreter für das Medium Kupfer sind das Koaxialkabel (ein Mittelleiter mit einer Gesamtabschirmung) und das mehradrige Kupferkabel mit paarweise verdrillten Adern (Twisted-Pair-Kabel, TP-Kabel). Diese werden im folgenden näher erläutert.

Twisted-Pair-Kabel

Twisted-Pair-Kabel gibt es in vielen Ausführungen. Sie unterscheiden sich zum einen in der Art ihrer Abschirmung und zum anderen in der möglichen Bandbreite. An Abschirmungsklassen gibt es derzeit

- das ungeschirmte (*unshielded*, UTP),
- das ungeschirmte mit einer Gesamtabschirmung (*screened-unshielded*, S/UTP),
- das geschirmte, bei dem die einzelnen Aderpaare abgeschirmt sind (*shielded*, STP), und
- das geschirmte TP-Kabel mit einer zusätzlichen Gesamtabschirmung (*screened-shielded*, S/STP).

Zusätzlich den Bezeichnungen der Abschirmung werden TP-Kabel bezüglich der Bandbreite und anderer elektrischer Eigenschaften in Kategorien von derzeit 1 bis 5 eingeteilt. Ein Normentwurf für die neuen Kategorien 6 und 7 liegt vor. Hierbei gilt, um so höher die Kategorie umso höher ist auch die mögliche Bandbreite. Die Bandbreite bestimmt sich hierbei aus verschiedenen physikalischen Eigenschaften des Kabels. Mit den üblichen Kabeln der Kategorien 3 bis 5 in UTP oder STP-Ausführung lassen sich mit Ethernet bzw. Fast-Ethernet zwischen 10 und 100 MBit/s bei einer maximalen Länge von 100 m übertragen, mit ATM lassen sich auf Kategorie 5-Kabeln bis zu 155 MBit/s übertragen. Kabel der Kategorie 6 werden eine Bandbreite von 600 MHz besitzen und ermöglichen damit Übertragungsraten bis 1 GBit/s.

Das TP-Kabel wird heute vor allem für Sternverkabelungen und zum Teil auch für Ringverkabelungen eingesetzt.

Die Vorteile:

- TP-Kabel, insbesondere deren Konfektion, sind bei geringerem Bandbreitenbedarf im Vergleich zu LWL relativ billig.
- TP-Kabel bis zur Kategorie 5 lassen sich relativ einfach verlegen und konfektionieren.
- TP-Kabel können als Universalverkabelung angesehen werden, da andere Dienste ohne größeren technischen Aufwand hierüber genutzt werden können (z. B. Telefonie). Bei geringerem Bandbreitenbedarf können vorhandene Telefonnetze auf TP-Basis auch als Datennetze genutzt werden.
- Bestehende Installationen können messtechnisch leicht überprüft werden.

Die Nachteile:

- Je nach Ausführung des Kabels (UTP bis S/STP) wird das Kabel durch ein mehr oder weniger starkes elektrodynamisches Feld umgeben. Hierdurch besteht sowohl die Gefahr einer Wechselwirkung mit anderen Feldern (z. B. benachbartes Kabel oder von Starkstrominstallationen) als auch die Möglichkeit des Abhörens.
- Die maximale Kabellänge ist bei den heute üblichen Anforderungen auf 100 m (inklusive der notwendigen Anschluss- und Patchkabel) beschränkt (siehe unten stehende Tabelle).
- Bei ungeschirmtem Installationskabel (UTP) mit vielen Paaren kann es zum Übersprechen zwischen einzelnen Paaren kommen.

Koaxial-Kabel

Koaxialkabel werden vor allem für Busverkabelungen oder z. B. zur Verbindung der Netzknoten in Baumstrukturen eingesetzt. Durch die Gesamtabschirmung des Mittelleiters kann hier im allgemeinen von einer guten elektromagnetischen Verträglichkeit (EMV) ausgegangen werden.

Die Vorteile:

- Die Bandbreite und die unverstärkte Übertragungsstrecke sind höher als beim TP-Kabel. Für die beiden Kabeltypen, die für das Ethernet-Protokoll eingesetzt werden können, liegen die maximalen Obergrenzen je nach Kabeltyp bei 185 bzw. 500 m (Thin- bzw. Thick-Ethernetkabel).
- Die Gefahr des Übersprechens ist bei Koaxialkabeln kleiner als bei TP-Kabeln.

Die Nachteile:

- Koaxialkabel sind im allgemeinen teurer als TP-Kabel.
- Trotz der Koaxialbauweise ist das Kabel abhörbar und empfindlich gegenüber Störungen.
- Abhängig vom verwendeten Koaxialkabel haben diese relativ große Biegeradien und sind damit schwieriger zu verlegen als beispielsweise TP-Kabel.

- Für Koaxialkabel sind nur wenige Netzzugangsprotokolle definiert. Beispielsweise kann Fast-Ethernet nicht über Koaxialkabel betrieben werden.

Lichtwellenleiter (LWL)

Lichtwellenleiter verwenden Licht im sichtbaren bis zum stark infraroten Bereich zur Signalübertragung. Ein Lichtwellenleiter ist ähnlich wie ein Koaxialkabel aufgebaut. Um den eigentlichen Lichtwellenleiter in der Mitte ist ein Mantel gelegt, der andere optische Eigenschaften als der Kern hat. Um diese Gesamtheit ist ein weiterer Mantel zum Schutz vor mechanischen und optischen Einflüssen gelegt. LWL gibt es in zwei verschiedenen Ausführungen: als Multimode- und als Singlemode-LWL. Diese beiden Typen unterscheiden sich vor allem in der möglichen Bandbreite und der maximalen Länge, die ohne zusätzliche Verstärker erreicht werden können.

LWL werden im allgemeinen zur Überbrückung von großen Distanzen (z. B. Verbindungen zwischen Gebäuden oder Stockwerken) in einem Backbone und zum Teil in Doppelringsystemen eingesetzt.

Die Vorteile:

- Die Bandbreite und die unverstärkte Reichweite ist höher als bei Kupferkabel.
- Abhören ist nur mit hohem technischen Aufwand möglich.
- Unzulässige Umrangierungen sind durch verfügbare Technik einfach zu erkennen.
- LWL sind unempfindlich gegenüber allen nicht zerstörenden Umfeldbedingungen, insbesondere gegenüber elektromagnetischen Feldern.
- LWL benötigen relativ wenig Platz.
- Ein Übersprechen oder eine Beeinflussung zwischen verschiedenen LWL oder einem LWL und TP-Kabeln findet nicht statt.
- Die Brandlast ist bei LWL im Vergleich zu Kupferkabeln geringer, da sie weniger bzw. eine andere Ummantelung besitzen und in der Regel weniger Kabelmaterial auf einer Strecke benötigt wird.

Die Nachteile:

- Der Installationspreis für LWL liegt vor allem durch die notwendigen Spleißarbeiten sehr viel höher als bei Kupferkabel.
- Die Koppel-Komponenten zum Betrieb von LWL, insbesondere für Singlemode-LWL, sind teurer als solche für Kupferkabel.
- Die Verlegung und Konfektion von LWL erfordert Spezialkenntnisse, Sonderwerkzeuge und besondere zusätzliche Komponenten (z. B. Spleißboxen).
- LWL können nicht in jedem beliebigen Radius geführt werden. Hieraus kann sich eine schwierigere Installation durch Beachtung der möglichen und notwendigen Kabelführungen ergeben.

Eine Übersicht über die Längenbeschränkungen von Kabeln für einige der üblichen Protokolle (Ethernet, Fast-Ethernet, FDDI und CDDI, siehe M 5.60 *Auswahl einer geeigneten Backbone-Technologie*) gibt die folgende Tabelle:

Netzzugangs-protokoll		**Kabeltyp**	**max. Länge**
Ethernet	10Base2	Koaxial	185 m
	10Base5	Koaxial	500 m
	10Base-T	TP	100 m
	10Base-FL Monomode	LWL	2 km
	10Base-FL Singlemode	LWL	5 km
Fast Ethernet	100Base-TX	TP	100 m
	100Base-FX	LWL	412 m
FDDI	Monomode	LWL	2 km
	Singlemode	LWL	60 km
CDDI		TP	100 m

Tabelle: Auswahl einer geeigneten Backbone-Technologie

Zu beachten ist, dass hier die jeweilige maximale Länge genannt ist. Diese setzt sich häufig aus dem eigentlichen Installationskabel und den Anschlusskabeln (Patchkabeln) zusammen. Für 10Base-T sollte also z. B. die Länge des Installationskabels 90 m nicht überschreiten, um genügend Längenspielraum für Patchkabel zu haben. Bei einigen Verfahren (z. B. 100Base-FX) reduziert sich die Länge durch den Einsatz und die Art von Repeatern!

Für Neuinstallationen ist es sinnvoll, im Primär- und Sekundärbereich LWL einzusetzen, da diese durch die hohe verfügbare Bandbreite auch zukünftigen Anforderungen gerecht werden können. Für den Tertiärbereich ist zu prüfen, ob ein Einsatz von TP-Kabeln oder LWL aus technischer und sicherheitstechnischer Sicht möglich bzw. notwendig ist und jeweils auch aus wirtschaftlicher Sicht vertretbar ist (siehe auch M 5.2 *Auswahl einer geeigneten Netz-Topographie*).

M 5.4 Dokumentation und Kennzeichnung der Verkabelung

Verantwortlich für Initiierung: Leiter IT, Leiter Haustechnik

Verantwortlich für Umsetzung: Haustechnik

Für Wartung, Fehlersuche, Instandsetzung und für erfolgreiche Überprüfung der Verkabelung ist eine gute Dokumentation und eindeutige Kennzeichnung aller Kabel erforderlich. Die Güte dieser Revisions-Dokumentation ist abhängig von der Vollständigkeit, der Aktualität und der Lesbarkeit.

In dieser Dokumentation (auch Bestandsplan genannt) sind alle das Netz betreffenden Sachverhalte aufzunehmen:

- genauer Kabeltyp,
- nutzungsorientierte Kabelkennzeichnung,
- Standorte von Zentralen und Verteilern mit genauen Bezeichnungen,
- genaue Führung von Kabeln und Trassen in der Liegenschaft (Einzeichnung in bemaßte Grundriss- und Lagepläne),
- Trassendimensionierung und -belegung,
- Belegungspläne aller Rangierungen und Verteiler,
- Nutzung aller Leitungen, Nennung der daran angeschlossenen Netzteilnehmer,
- technische Daten von Anschlusspunkten,
- Gefahrenpunkte,
- vorhandene und zu prüfende Schutzmaßnahmen.

Es muss möglich sein, sich anhand dieser Dokumentation einfach und schnell ein genaues Bild über die Verkabelung zu machen.

Da es mit zunehmender Größe eines Netzes nicht möglich ist, alle Informationen in einem Plan unterzubringen, ist eine Aufteilung der Informationen sinnvoll. Tatsächliche Lageinformationen sind immer in maßstäbliche Pläne einzuzeichnen. Andere Informationen können in Tabellenform geführt werden. Wichtig dabei ist eine eindeutige Zuordnung aller Angaben untereinander.

Um die Aktualität der Dokumentation zu gewährleisten, ist sicherzustellen, dass alle Arbeiten am Netz rechtzeitig und vollständig demjenigen bekannt werden, der die Dokumentation führt. Es ist z. B. denkbar, die Ausgabe von Material, die Vergabe von Fremdaufträgen oder die Freigabe gesicherter Bereiche von der Mitzeichnung dieser Person abhängig zu machen.

Da diese Dokumentation schutzwürdige Informationen beinhaltet, ist sie sicher aufzubewahren und der Zugriff zu regeln.

Ergänzende Kontrollfragen:

- Wer ist für die Dokumentation der Verkabelung zuständig?
- Wird die Dokumentation hinreichend schnell aktualisiert?
- Wie wird die Revisions-Dokumentation vor unerlaubtem Zugriff geschützt?

M 5.5 Schadensmindernde Kabelführung

Verantwortlich für Initiierung: Planer, Leiter IT, Leiter Haustechnik

Verantwortlich für Umsetzung: Haustechnik

Bei der Planung von Kabeltrassen ist darauf zu achten, dass erkennbare Gefahrenquellen umgangen werden. Grundsätzlich sollen Trassen nur in den Bereichen verlegt werden, die ausschließlich dem Benutzer zugänglich sind. Ein übersichtlicher Aufbau der Trassen erleichtert die Kontrolle. Trassen und einzelne Kabel sollen immer so verlegt werden, dass sie vor direkten Beschädigungen durch Personen, Fahrzeuge und Maschinen geschützt sind.

Lauf- oder Fahrbereich

Der Standort von Geräten sollte so gewählt werden, dass Kabel nicht im Lauf- oder Fahrbereich liegen. Ist dies nicht zu vermeiden, sind die Kabel den zu erwartenden Belastungen entsprechend durch geeignete Kanalsysteme zu schützen.

Zugentlastung der Kabel

Grundsätzlich ist bei Geräteanschlussleitungen auf eine ausreichende Zugentlastung der Kabel in den Steckern zu achten. Bisweilen kann es sinnvoll sein, auf die vorgesehene Verschraubung von Steckern zu verzichten. Bei Zugbelastung werden nur Steckverbindungen auseinander gerissen und nicht die Stecker-Kabel- oder Stecker-Geräte-Verlötung.

Tiefgaragen stellen ein großes Problem für eine schadensmindernde Kabelführung dar. Durch die Sicherheitsschaltungen und die langen Offenzeiten von Einfahrtstoren ist der Zutritt von Fremdpersonen zu Tiefgaragen nie auszuschließen. Durch die in der Regel geringen Deckenhöhen ist es mit einfachen Mitteln möglich, sich Zugriff zu dort verlaufenden Trassen zu verschaffen. Durch Trassen im Fahrbereich kann die zulässige Fahrzeughöhe unterschritten werden. Beschädigungen oder Zerstörungen der Trassen und Kabel durch Fahrzeuge sind dann nicht auszuschließen.

Kabel durch fremdgenutzte Bereichen

Bei gemeinsam mit Dritten genutzten Gebäuden ist darauf zu achten, dass Kabel nicht in Fußbodenkanälen durch deren Bereiche führen. Fußboden- und Fensterbank-Kanalsysteme sind gegenüber den fremdgenutzten Bereichen mechanisch fest zu verschließen. Besser ist es, sie an den Bereichsgrenzen enden zu lassen.

Bereiche mit hoher Brandgefahr sind zu meiden. Ist dies nicht möglich und ist der Betriebserhalt aller auf der Trasse liegenden Kabel erforderlich, ist der entsprechende Trassenbereich mit Brandabschottung zu versehen. Ist der Betriebserhalt nur für einzelne Kabel erforderlich, ist dafür ein entsprechendes Kabel zu wählen.

In Produktionsbetrieben ist mit hohen induktiven Lasten und daraus resultierenden Störfeldern zu rechnen. Auch diese sind bei der Trassen- und Kabelverlegung zu berücksichtigen. Für den Schutz der Kabel gilt sinngemäß das gleiche wie bei der Brandabschottung.

Bei Erdtrassen ist ca. 10 cm über der Trasse ein Warnband zu verlegen. Bei einzelnen Kabeln (ohne Rohr) ist der Einbau von Kabelabdeckungen sinnvoll.

Befestigung

Leitungen müssen so verlegt sein, dass ein Sturm sie nicht bewegen kann. Beispielsweise sollte dafür Sorge getragen werden, dass Leitungen auf freien Dachflächen mindestens alle 5 m angemessen befestigt sind. Hierbei sollte berücksichtigt werden, dass bei einem Sturm starke Kräfte auf die Kabel oder Kabelstränge wirken können. Außerdem müssen Leitungen geschützt gegen mechanische Beschädigungen verlegt werden, da Gegenstände darauf fallen könnten. Leitungen auf Dachflächen oder in Bereichen, die mit Lamellenwänden verkleidet sind, sollten daher immer in Schutzrohren verlegt sein.

Ergänzende Kontrollfragen:

- Sind alle Trassen und Kabel so verlegt worden, dass sie vor direkten Beschädigungen geschützt sind?
- Sind Leitungen, die über unkontrollierte Bereiche führen, gegen Fremdzugriffe geschützt?
- Sind Leitungen, die an Außenflächen des Gebäudes verlegt sind, ausreichend gegen Sturmeinwirkungen geschützt?

M 5.6 Obligatorischer Einsatz eines Netzpasswortes

Diese Maßnahme ist mit Version 2005 entfallen.

M 5.7 Netzverwaltung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT

Netze können zentral oder lokal an den einzelnen Knoten verwaltet werden. Das ist neben den technischen Möglichkeiten davon abhängig, wer den Netzknoten administriert. In jedem Fall ist eine zentrale Koordinierung aller Netzaktivitäten einer Behörde oder eines Unternehmens notwendig, damit Redundanzen vermieden werden. Zentral gesteuert werden sollten:

- die Auswahl und Verlegung der Kabel,
- die Auswahl der eingesetzten IT-Systeme und Anwendungen, um Unverträglichkeiten zu vermeiden,
- die zentrale Vergabe von Netzadressen und Benutzer-IDs,
- die organisatorische Zuteilung von Netzkomponenten z. B. zu Abteilungen.

Die einzelnen Netzknoten und die dort angeschlossenen IT-Systeme können auch lokal verwaltet werden.

Die Aufgaben- und Verantwortungsbereiche der Systemverwalter müssen dabei klar spezifiziert und eindeutig geregelt sein (siehe auch M 2.26 *Ernennung eines Administrators und eines Vertreters*).

M 5.8 Regelmäßiger Sicherheitscheck des Netzes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der Netzadministrator sollte regelmäßig, mindestens monatlich, einen Sicherheitscheck des Netzes durchführen. Für praktisch alle Betriebssysteme sind Programme verfügbar oder bereits im Lieferumfang des Betriebssystems oder der Betriebssystem-Distribution enthalten, die entsprechende Funktionen zur Verfügung stellen.

Bei einem solchen Sicherheitscheck sollten beispielsweise folgende Punkte überprüft werden:

- Gibt es Benutzer ohne Passwort?
- Gibt es Benutzer, die längere Zeit das Netz nicht mehr benutzt haben?
- Gibt es Benutzer, deren Passwort nicht die erforderlichen Bedingungen einhält?
- Welche Benutzer besitzen die gleichen Rechte wie der Administrator?
- Sind Systemprogramme und Systemkonfiguration unverändert und konsistent?
- Entsprechen die Berechtigungen von
  - Systemprogrammen und Systemkonfiguration
  - Anwendungsprogrammen und -daten
  - Benutzerverzeichnissen und -daten

  den Vorgaben der Sicherheitsrichtlinie?
- Welche Netzdienste laufen auf den einzelnen Systemen? Sind sie den Vorgaben der Sicherheitsrichtlinie entsprechend konfiguriert?

Bei einem regelmäßigen Sicherheitscheck können auch Penetrationstests im lokalen Subnetz integriert werden. Dabei kann der "Grad" der Penetrationstests variiert werden (beispielsweise: wöchentlich einfache automatisierte Überprüfungen, monatlich gründlicherer Test mit teilweise manueller Durchführung, einmal jährlich ein grundlegender Test des gesamten Netzes).

Für Unix-Systeme werden in M 4.26 *Regelmäßiger Sicherheitscheck des Unix-Systems* verschiedene Programme beschrieben, die entsprechende Funktionen enthalten.

Bei der Durchführung des Sicherheitschecks sollte der Netzadministrator seine Schritte so dokumentieren, dass sie (beispielsweise bei einem Verdacht auf ein kompromittiertes System) nachvollzogen werden können. Die Ergebnisse des Sicherheitschecks müssen dokumentiert werden, Abweichungen vom "Sollzustand" muss nachgegangen werden.

Ergänzende Kontrollfragen:

- Werden die Durchführung und die Ergebnisse des Sicherheitschecks dokumentiert?

M 5.9 Protokollierung am Server

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

sicherheitsrelevante Ereignisse protokollieren

Die am Netz-Server mögliche Protokollierung ist in einem sinnvollen Umfang zu aktivieren. In regelmäßigen Abständen muss der Netzadministrator die Protokolldateien des Netz-Servers überprüfen. Es sollten alle sicherheitsrelevanten Ereignisse protokolliert werden. Dabei sind insbesondere folgende Vorkommnisse von Interesse:

- falsche Passworteingabe für eine Benutzer-Kennung bis hin zur Sperrung der Benutzer-Kennung bei Erreichen der Fehlversuchsgrenze,
- Versuche von unberechtigten Zugriffen,
- Stromausfall,
- Daten zur Netzauslastung und -überlastung.

Wie viele Ereignisse darüber hinaus protokolliert werden, hängt unter anderem vom Schutzbedarf der jeweiligen IT-Systeme ab. Je höher deren Schutzbedarf ist, desto mehr sollte protokolliert werden.

Da die Protokoll-Dateien mit der Zeit sehr umfangreich werden können, sollten die Auswertungsintervalle so kurz gewählt werden, dass eine sinnvolle Auswertung möglich ist. Um eine sinnvolle Auswertung zu ermöglichen, sollte jeder Protokoll-Eintrag Benutzer-Kennung bzw. Prozessnummer, Kennzeichnung des Endgeräts, Datum und Uhrzeit enthalten.

Es ist zu prüfen, welche gesetzlichen oder vertraglichen Aufbewahrungsfristen für Protokoll-Dateien beachtet werden müssen. Um die Nachvollziehbarkeit von Aktionen zu gewährleistungen, kann eine Mindestspeicherdauer vorgeschrieben sein, aus Datenschutzgründen kann es auch eine Löschungpflicht geben (siehe auch M 2.110 *Datenschutzaspekte bei der Protokollierung*).

Ergänzende Kontrollfragen:

- Wer wertet die Protokoll-Dateien in welchen Abständen aus?
- Werden die Auswertungen dokumentiert?

M 5.10 Restriktive Rechtevergabe

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Zugriffsrechte auf Dateien, die auf der Festplatte des Netz-Servers gespeichert sind, müssen restriktiv vergeben werden. Jeder Benutzer erhält nur auf die Dateien ein Zugriffsrecht, die er für seine Aufgabenerfüllung benötigt. Das Zugriffsrecht selbst wiederum wird auf die notwendige Zugriffsart beschränkt (Dazu siehe auch M 2.5 *Aufgabenverteilung und Funktionstrennung*, M 2.7 *Vergabe von Zugangsberechtigungen* und M 2.8 *Vergabe von Zugriffsrechten*). So ist es zum Beispiel in den seltensten Fällen notwendig, ein Schreibrecht auf Programmdateien zu vergeben.

Meist darf über die Vererbung von Rechten auf Dateien in Unterverzeichnissen zugegriffen werden, wenn ein Zugriffsrecht auf das übergeordnete Verzeichnis bestand. Daraus ergibt sich, dass Zugriffsrechte auf höchster Ebene (Volume-Ebene) nur sehr eingeschränkt erteilt werden sollten. Insbesondere ist bei der Installation neuer Softwareprodukte die Rechtevergabe erneut zu überprüfen.

Sind die PCs mit Diskettenlaufwerken ausgestattet, so ist auf restriktive Rechtevergabe besonderen Wert zu legen.

Sollte der Speicherplatz des Netz-Servers gering ausgelegt sein, kann eine Beschränkung der maximalen Speicherkapazität, die ein Benutzer auf dem Netz-Server belegen darf, eingestellt werden.

Ergänzende Kontrollfragen:

- Kann anhand der Dokumentation der Rechtestruktur festgestellt werden, dass nur die minimal notwendigen Rechte vergeben wurden?

M 5.11 Server-Konsole sperren

Diese Maßnahme ist mit Version 2005 entfallen.

M 5.12 Einrichtung eines zusätzlichen Netzadministrators

Diese Maßnahme ist mit Version 2005 entfallen.

M 5.13 Geeigneter Einsatz von Elementen zur Netzkopplung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Geräte zur Netzkopplung wie Router, Bridges oder Gateways verbinden nicht nur Netze, sie können auch zur physikalischen oder logischen Segmentierung von Netzen benutzt werden. Durch die Aufteilung von großen Netzen in Teilnetze kann z. B. die Verfügbarkeit verbessert werden, da ein Fehler nur einen begrenzten Bereich des Netzes betrifft und dort schneller lokalisiert werden kann. Bei zunehmender Anzahl von Netzstationen können Antwortzeiten unakzeptabel und eine Teilnetzbildung zur Lasttrennung notwendig werden. Der Schutz von sensitiven Informationen kann ein weiterer Grund zur Segmentierung von Netzen sein, so dass diese nicht auf dem Gesamtnetz verfügbar sind. Um sich vor externen Angreifern zu schützen, kann es sinnvoll sein, einen Transfer von Paketen nur vom sicheren ins unsichere Netz zuzulassen, zum Schutz von vertraulichen Daten kann es andererseits sinnvoll sein, keinen Transfer von Paketen vom sicheren ins unsichere Netz zuzulassen.

Die Aufteilung in Netzsegmente bzw. die Netzkopplung kann auf verschiedenen Schichten nach dem OSI-Modell erfolgen. Netzkoppelkomponenten auf der physikalischen Schicht (Schicht 1) des OSI-Modells sind z. B. Repeater, auf der Sicherungsschicht (Schicht 2) z. B. Bridges, auf der Vermittlungsschicht (Schicht 3) z. B. Router und auf der Anwendungsschicht (Schicht 7) im allgemeinen Gateways. Zum besseren Verständnis ist das OSI-Modell in der folgenden Abbildung dargestellt.

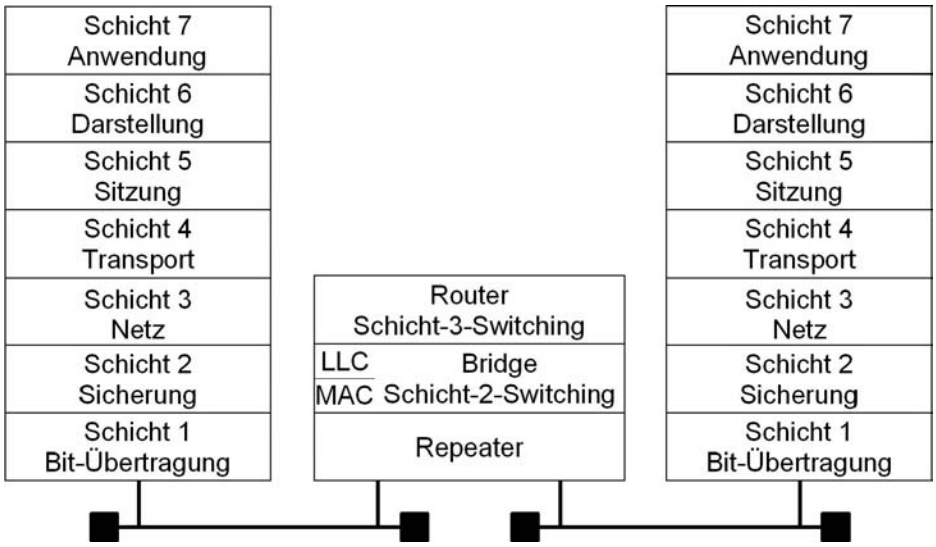


Abbildung: Das OSI/ISO Referenzmodell

Eine Verbindung mit einem anderen Netz auf einer höheren Schicht (ab Schicht 3) des OSI-Modells ermöglicht es z. B. den Datenfluss nach Sicherheitsanforderungen zu reglementieren und somit zu schützende und unsichere Netze kontrolliert zu verbinden.

Andererseits kann das Trennen von Netzen erforderlich sein, wenn diese vor Zugriffen aus dem jeweils anderen Netz geschützt werden sollen oder um die Verfügbarkeit der Netze im Fehlerfall zu erhöhen bzw. die Netzlast in den jeweiligen Netzsegmenten zu verringern.

Um Manipulationen zu verhindern, müssen alle Geräte zur Netzkopplung so aufgestellt werden, dass nur Berechtigte physikalischen Zugang haben.

Repeater

Repeater arbeiten auf der Schicht 1 des OSI-Modells und sind einfache Signalverstärker. Dadurch erlauben sie es, die maximale Kabellänge eines bestehenden Netzsegmentes zu verlängern bzw. mehrere Netzsegmente zu verbinden. Beispielsweise kann mit ihnen beim Einsatz von Ethernet auf Koaxialkabelbasis die maximale Kabellänge auf über 185 m bzw. auf über 500 m (für Thin- bzw. Thick-Ethernetkabel) verlängert werden. Zu beachten sind hierbei die Konfigurationsregeln für Repeater, die die Anzahl und Anordnung von Repeatern beschränken.

Im Fall einer Twisted-Pair-Verkabelung werden Repeater häufig als zentraler oder dezentraler Netzknoten zur Verbindung der einzelnen Netzteilnehmer eingesetzt. Da hierfür mehrere Repeater in einem Gerät miteinander verbunden werden müssen, werden diese Geräte auch Multiport-Repeater genannt. Multiport-Repeater werden häufig auch als Hubs bzw. als Mini-Hubs bezeichnet.

Durch die somit erreichte Trennung auf der Schicht 1 des Netzes werden elektrische Fehler auf ein Segment beschränkt. Dies gilt jedoch nicht für Fehler in höheren Schichten (z. B. zu häufige Kollisionen oder ein Broadcast-Sturm). Von einigen Herstellern gibt es inzwischen auch Multiport-Repeater, die Informationen aus Schicht 2 auswerten (aber noch keine Bridges sind) und dadurch z. B. die Implementation von Zugriffsbeschränkungen erlauben. Mit solchen Geräten lässt sich beispielsweise einstellen, dass nur bestimmte Netzteilnehmer Zugang zum Netz bekommen.

Bridge

Die Verbindung von Netzen auf der Ebene 2 des ISO-OSI-Referenzmodells erfolgt über Bridges. Eine Bridge verbindet zwei Netze, die in der Regel dasselbe Logical Link Control (LLC) Protokoll benutzen, aber unterschiedliche Medium Access Control (MAC) Protokolle. Eine Bridge kann z. B. ein Ethernet mit einem Token-Ring-Netz verbinden. Eine solche Bridge wird dann Translation-Bridge oder T-Bridge genannt.

Hierdurch ergeben sich drei wesentliche Vorteile:

- Die Bridge trennt Collision-Domains, d. h. performanceverringernde Kollisionen bei CSMA/CD-basierten Netzen gelangen nicht in das andere Segment.

- Eine Bridge leitet nur diejenigen Datenpakete in ein anderes Segment, die dort auch ihre Zieladresse haben. Hierdurch bleibt der Datenverkehr auf das jeweils notwendige Segment beschränkt, wodurch die Abhörsicherheit steigt.
- Schließlich steigt dadurch auch der Datendurchsatz in jedem Segment, da auf jeder Seite der Bridge unabhängig Daten übertragen werden können und somit eine Lasttrennung erfolgt.

Switch (Ethernet, Token-Ring, ATM)

Ein *Switch* ist eine Variante einer Brücke, die mehrere logische LAN-Segmente verbindet (Multiport-Brücke), arbeitet also auf Schicht 2 des OSI-Modells. Einige neuere Produkte implementieren zusätzlich auch Switching-Funktionalität auf der Schicht 3 des OSI-Modells, erlauben also hiermit auch eine Schicht 3 Segmentierung.

Ein Ethernet-Switch besteht aus mehreren Bridges, die auf geeignete Weise intern miteinander verbunden sind (z. B. über eine so genannte Switching-Matrix).

Ein Ethernet-Switch bietet die Vorteile einer Bridge für mehrere Anschlüsse (üblich sind derzeit 8 bis 32 Anschlüsse pro Switch), d. h. jeder Netzteilnehmer bzw. jedes Segment an einem Switchanschluss bildet eine eigene Collision-Domain und der Verbindungsaufbau beruht auf den tatsächlichen Erfordernissen. Damit kann jedes angeschlossene Segment mit allen anderen unbeeinflusst von dem Verkehr und der Last der anderen Segmente kommunizieren, solange das entsprechende Segment nicht bereits anderweitig belegt ist. Switches bieten sich vor allem zur Lasttrennung und als zentrale Kopplungskomponente von mehreren Teilsegmenten an. Durch die Kaskadierung von Switches, d. h. durch den Anschluss von nachgeordneten Switches an einen zentralen Switch, lassen sich bei geeigneter Wahl der logischen Netzstruktur sehr leistungsfähige Netze bilden.

Ethernet-Switches, die nach der IEEE-Norm für Bridges arbeiten, benutzen die Store-and-Forward-Technik. Bei dieser Technik wird zunächst das gesamte Ethernet-Paket des Quellports eingelesen und auf Korrektheit überprüft. Nur korrekt und vollständig empfangene Pakete werden an das Zielsegment weitergeschickt. Die Verzögerungszeit solcher Switches ist relativ hoch, sie garantieren aber auch, dass keine fehlerhaften Pakete in andere Segmente übertragen werden. Der Einsatz solcher Store-and-Forward-Switches ist dann zu empfehlen, wenn Wert auf maximale Verfügbarkeit und Integrität und nicht so sehr auf Bandbreite gelegt wird.

Im Gegensatz dazu wurden alternativ Techniken entwickelt, die den Durchsatz eines Ethernet-Switches erhöhen, also die Verzögerungszeit zu verkleinern, die ein zu verarbeitendes Datenpaket erfährt. Hierzu wird die On-the-Fly-Technik (auch Cut-Through genannt) eingesetzt, die nicht mehr das gesamte Paket einliest und überprüft, sondern lediglich die Zieladresse des Paketes auswertet und daraufhin sofort das gesamte Paket an diese Adresse schickt. On-the-Fly-Switches sind damit maximal um den Faktor 20 schneller als Store-and-Forward-Switches. Allerdings leiten sie auch fehlerhafte Pakete in das andere Segment, wodurch die Bandbreite und damit unter Umständen die

Verfügbarkeit der einzelnen Segmente beeinträchtigt werden kann. On-the-fly-Switches sollten also in Netzen eingesetzt werden, in denen wenig fehlerhafte Pakete auftreten können und in denen es auf maximalen Durchsatz ankommt. Die meisten Hersteller bieten heute Switches an, die beide Techniken beherrschen und entsprechend konfiguriert werden können.

Von einigen Produkten wird inzwischen auch ein Switching auf der Schicht 3 des OSI-Modells unterstützt. Dabei werden die Netzteilnehmer nicht mehr nach ihrer MAC-Adresse unterschieden (Layer-2-Switching), sondern nach den Adressen der Schicht 3 (für den TCP/IP-Protokollstapel ist dies die IP-Adresse). Ein Layer-3-Switching kann weitere Performancevorteile bedeuten, in diesem Fall muss aber der Switch, analog zu einem Router, die auf der Schicht 3 verwendeten Protokolle verarbeiten können.

Switches für ATM oder Token-Ring sind funktional einem Ethernet-Switch sehr ähnlich, d. h. auch ein Switch für diese Protokolle ermöglicht es, dass zwei Netzteilnehmer oder Netzbereiche unabhängig von den anderen kommunizieren können. Für ATM-Netze ist durch die zugrunde liegende Konzeption der Einsatz eines Switches sogar zwingend.

Bei der Auswahl von Switches, mit denen ein Collapsed Backbone realisiert werden soll, muss die zur Verfügung gestellte Portdichte berücksichtigt werden. Bei einem "Collapsed backbone" sollte es vermieden werden, mehrere Switches einsetzen zu müssen, die nicht über eine gemeinsame (Hochgeschwindigkeits-) Backplane verfügen (siehe M 5.2 *Auswahl einer geeigneten Netz-Topographie*).

Router

Router trennen bzw. verbinden Netze auf der Schicht 3 des OSI-Modells. Damit arbeiten Router nicht mehr protokolltransparent (wie z. B. Repeater oder Bridges), sondern müssen die im Einsatz befindlichen Protokolle auf der Vermittlungsschicht auch verarbeiten können. Dadurch verlangsamen Router den Datenverkehr zwischen zwei verbundenen Teilnetzen merklich, da der Router jedes Paket auf der Schicht 3 auswerten muss.

Aufgrund ihrer Fähigkeit, Protokolle zu verarbeiten und diese umzusetzen, werden Router vor allem zur LAN-LAN-Kopplung und zur Anbindung eines LANs an ein WAN genutzt. Ein Router kann beispielsweise zwei LANs über eine ISDN-Leitung miteinander verbinden. Hierbei wird das LAN-Protokoll unverändert in das WAN-Protokoll eingekapselt (encapsulation) und übertragen. Ein anderes Protokoll, das hier beispielsweise zum Einsatz kommen kann, ist das X.25-Protokoll. In großen Netzen, in denen viele Teilnetze durch Router verbunden sind, ist eine wesentliche Aufgabe des Routers die Wegewahl (*Routing*) zwischen den Teilnetzen. Hierbei können prinzipiell zwei Verfahren unterschieden werden:

- Das statische Routing, bei dem die Wegewahl manuell angegeben wird.
- Das dynamische Routing, bei dem die Wegewahl durch die Router bestimmt und laufend aktualisiert wird. Hierzu stehen mehrere Algorithmen bzw. Protokolle zur Verfügung, die auch den Abgleich der Router untereinander gewährleisten. Die bekanntesten Protokolle sind RIP

(Routing Information Protocol), OSPF (Open Shortest Path First) und IGRP (Interior Gateway Routing Protocol). Für die Auswahl eines geeigneten Routing-Protokolls ist auch M 4.82 *Sichere Konfiguration der aktiven Netzkomponenten* zu beachten.

Weiterhin kann durch den Einsatz von Filtern eine Zugriffskontrolle gewährleistet werden, d. h. welche Systeme mit welchen Protokollen über den Router in welche Richtung miteinander kommunizieren dürfen.

Konzentratoren und Hubs

Unter einem *Hub* wird eine Komponente verstanden, die eine oder mehrere aktive Netzkoppelkomponenten aufnimmt und eine Kommunikation dieser Komponenten untereinander über eine interne Backplane (siehe auch M 5.2 *Auswahl einer geeigneten Netz-Topographie*) ermöglicht. Hubs, die bei Bedarf mehrere Netzkoppelkomponenten aufnehmen können, werden als *modulare Hubs* bezeichnet. Entsprechend werden Hubs, die nur aus einer Koppelkomponente bestehen und nicht zur Aufnahme weiterer Komponenten bestimmt sind, als *nicht modulare Hubs* bezeichnet. Wenn es möglich ist, die Backplanes mehrerer Hubs miteinander zu verbinden, werden diese Hubs als *stackable Hubs* bezeichnet. Durch den Einsatz eines Hubs oder eines Konzentrators erfolgt die Leitungsführung zumindest zum Teil sternförmig zu den Endgeräten, aus diesem Grund werden Hubs oder Konzentratoren auch Sternkoppler genannt.

Wie bereits bei den Repeatern erwähnt ist die kleinste Form eines Konzentrators bzw. eines Hubs ein *Multiport-Repeater*. Modulare Hubs dagegen erlauben die Aufnahme verschiedener Koppelelemente, die selbst wiederum auf verschiedenen Schichten arbeiten können (z. B. Repeater, Bridges und Router). Durch diese Konzentration der Netzkoppelkomponenten an einem Ort ergeben sich Vorteile in der einfacheren Administration des Netzes, allerdings beeinflusst der Ausfall eines solchen zentralen Hubs auch das gesamte Netz. Für diesen Fall sind geeignete Vorsorge-Maßnahmen zu treffen, wie z. B. die redundante Auslegung der Netzkomponenten (siehe M 6.53 *Redundante Auslegung der Netzkomponenten*).

Gateway

Ein Gateway verbindet zwei Netze auf der Anwendungsschicht (Schicht 7) des OSI-Modells. Daher erfüllt er nicht nur die Aufgabe, ein Netzprotokoll zu konvertieren, sondern auch Daten auf Anwendungsebene zu transportieren, gegebenenfalls zu modifizieren und unter Sicherheitsgesichtspunkten auszuwerten. Ein typisches Einsatzfeld eines Gateways ist die Kommunikation von Systemen in einem TCP/IP-Netz mit einem SNA-Host. In diesem Fall besteht das Gateway aus einer Kombination von Hard- und Software. Es gibt jedoch auch Gateways, die nur durch Software realisiert sind. Dies sind z. B. Mail-Gateways, die unterschiedliche Mailformate verstehen und konvertieren können.

M 5.14 Absicherung interner Remote-Zugänge

Verantwortlich für Initiierung: TK-Anlagen-Verantwortlicher, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Remote-Zugänge bei TK-Anlagen werden für Fernwartungs-, Fernadministrations- und Netzmanagement-Aufgaben genutzt. Ferner können noch Remote-Zugänge für die Anlagennutzer (Dial-In-Optionen) existieren.

Grundsätzlich lässt sich zwischen

- einem Remote-Zugang im eigenen TK-Anlagenverbund (interner Zugang) und
- einem Remote-Zugang aus anderen Netzen (externer Zugang)

unterscheiden.

Beim internen Remote-Zugang wird die Absicherung einer Fernwartung innerhalb eines TK-Anlagenverbundes betrachtet. Unter Anlagenverbund wird hierbei eine aus mehreren separaten Anlagenteilen bestehende Gesamtanlage verstanden, welche über ein eigenes Leitungsnetz miteinander verbunden ist. Sollte diese Verbindung über öffentliche Vermittlungseinrichtungen geführt sein, so sind zusätzlich die unter M 5.15 *Absicherung externer Remote-Zugänge* beschriebenen Maßnahmen zu realisieren. Bei Vernetzung über geschlossene Benutzergruppen innerhalb öffentlicher Netze oder über virtuelle private Netze (VPN) sollten die Maßnahmen für interne Remote Zugänge **und** nach Möglichkeit die mit * gekennzeichneten Punkte aus den Maßnahmen für externe Remote-Zugänge umgesetzt werden.

Der wichtigste Aspekt bei der Absicherung des internen "Remote-Zuganges" ist der, Eindringversuche aus externen Netzen wirksam zu unterbinden und gegebenenfalls auch erkennen zu können. Des weiteren sollen die Zugänge aus dem eigenen Netz auf die berechtigten Stellen **und** Personen eingeschränkt werden können. Je nach Art der Zugangstechnik existieren hierfür unterschiedliche Methoden.

Absicherung eines internen Remote-Zuganges via Modem

Die nachfolgende Abbildung stellt ein typisches Szenario eines internen Remote-Zugangs zu einem Fernadministrationsport via Modem dar. Die TK-Anlage PBX 1 wird vom Wartungsplatz aus direkt über die V.24-Wartungsschnittstelle administriert. Die TK-Anlage PBX 2 wird vom Wartungsplatz aus über Modem 1 - PBX 1 - PBX 2 - Modem 2 - V.24-Wartungsschnittstelle administiert.

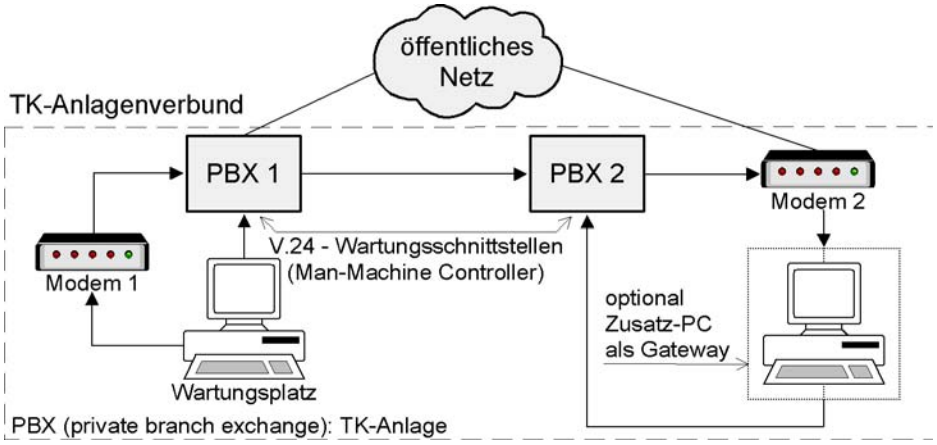


Abbildung: Aufbau einer Fernadministration via Modem

In einem solchem Fall können folgende Maßnahmen zur **Abschottung gegenüber Zugängen aus externen Netzen** ergriffen werden:

- Keine Amtsberechtigung für den Modem-Anschluss

  Der Modem-Anschluss, über den der Zugang zum Administrationsport der Anlage geführt wird, sollte in jedem Fall **nicht-amtsberechtigt** sein! Diese Minimalanforderung sollte als erstes überprüft werden. Hiermit wird vermieden, dass das Modem von außerhalb direkt angewählt werden kann.

- Geheimhaltung der Rufnummer des Wartungsports (Modem)

  Um Missbrauch von vornherein zu erschweren, sollte die Rufnummer des Wartungsapparates nicht in Telefonverzeichnissen veröffentlicht werden. Ihre Kenntnis sollte den sie unmittelbar benötigenden Personen vorbehalten bleiben.

- Verwendung von Standleitungen (optional)

  Die Verwendung von eigenen Standleitungen für die Remote-Verbindungen, die nicht über Vermittlungseinrichtungen geführt werden, ist eine der sichersten Methoden, einen externen Zugriff auf die Remote-Zugänge zu unterbinden. Da dieses Verfahren in der Regel sehr teuer ist, wird es nur in Ausnahmefällen Anwendung finden können.

Um sicherzustellen, dass **nur die berechtigten Stellen** innerhalb des eigenen Netzes auf die Remote-Zugänge zugreifen können, müssen folgende Maßnahmen umgesetzt werden:

- **Bildung geschlossener Benutzergruppen (Closed User Group, CUG)**

  In einigen TK-Anlagen lassen sich auch anlagenübergreifend CUGs einrichten. Diese geschlossenen Benutzergruppen stellen eine Art Netz im Netz dar. Alle benötigten Remote-Zugänge sollten daher mit den jeweils zugangsberechtigten Stellen in solchen CUGs zusammengefasst werden.

- **Automatischer Rückruf (Callback)**

  Die Callback-Option der Modems sollte genutzt werden (siehe M 5.30 *Aktivierung einer vorhandenen Callback-Option*). Wird ein PC-Gateway eingesetzt, so sollte das Callback von dort gestartet werden.

- **Beschränkung der Rechte des Remote-Ports (optional)**

  Sollte die TK-Anlage eine Rechteverwaltung für verschiedene Ports unterstützen, so kann diese genutzt werden, um sicherheitskritische Aktionen über Remote-Zugänge zu unterbinden und nur vor Ort zuzulassen. Viele TK-Anlagen besitzen diese Option jedoch nicht. In solchen Fällen können durch Zusatzprodukte, z. B. Portcontroller, die über einen Port ausführbaren Transaktionen beschränkt werden.

Um sicherzustellen, dass **nur die berechtigten Personen** innerhalb des eigenen Netzes auf die Remote-Zugänge zugreifen können, müssen folgende Maßnahmen umgesetzt werden:

- Identifikation und Authentisierung,
- Challenge-Response-Verfahren zur Authentikation (optional).

Absicherung eines internen Remote-Zugriffes via ISDN-Vernetzung

Aus Pratikabilitätsgründen bietet es sich teilweise an, die PCs mit Netzmanagement-Aufgaben mit ISDN-Karten auszurüsten. In einem solchen Fall sollte eine geschlossene Benutzergruppe gebildet werden. Hierzu kann die Rufnummer des rufenden Teilnehmers genutzt werden (Calling Line Identification and Presentation, CLIP). Dies könnte vom Endgerät selbst unter Zuhilfenahme der vom Netz zur Verfügung gestellten Rufnummer des anrufenden Gerätes (CLIP) realisiert werden.

Absicherung direkter Systemzugänge (Direct Inward System Access, DISA)

Direkte Systemzugänge sollten nach Möglichkeit gesperrt werden. Ist dies nicht möglich, so sollten die Berechtigungen so gesetzt werden, dass der direkte Systemzugang nur über einen dedizierten Port erfolgen kann. Auf diese Weise wird es möglich, den DISA-Zugang über ein Gateway zu führen. Ein Beispiel einer solchen Absicherung ist in der folgenden Abbildung dargestellt:

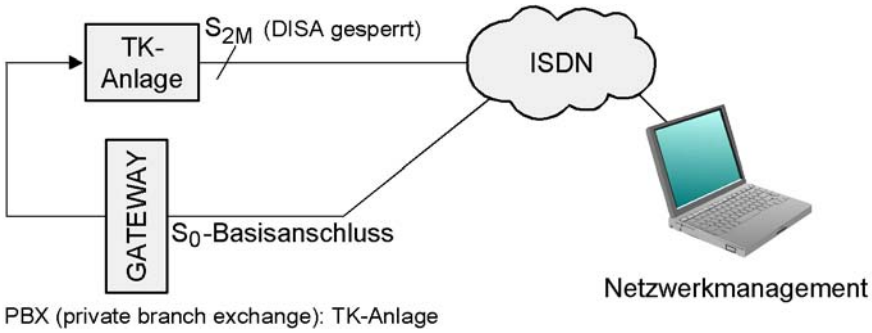


Abbildung: Absicherung eines direkten Systemzuganges

Einrichtung und Unterbringung eines Netzmanagementzentrums

Der Vorteil eines zentralen Netzmanagementes ist, neben einer komfortablen Abwicklungsmöglichkeit der Systemadministration, dass für die alltäglichen Administrationsarbeiten kein physikalischer Zutritt zu den TK-Anlagen mehr notwendig ist.

Sollte die Einrichtung eines zentralen Netzmanagementes erwogen werden, so ist dies in einem gesicherten Bereich unterzubringen. Der Zutritt zu diesem Zentrum ist durch organisatorische Maßnahmen zu regeln. Entsprechende Vorgaben können dem Baustein B 2.4 *Serverraum* entnommen werden. Die Managementrechner, von welchem die Arbeiten durchgeführt werden können, sollten auch mit geeigneten Maßnahmen abgesichert werden. Beispiele finden sich in B 3.209 *Client unter Windows XP* und B 3.204 *Client unter Unix*.

Protokollierung von Wartungsmaßnahmen

Die momentane Anlagenkonfiguration, d. h. vergebene Rufnummern und Berechtigungen, aktivierte und deaktivierte Leistungsmerkmale, eingerichtete Heranholgruppen etc., muss jederzeit nachvollziehbar sein. Hierzu ist es notwendig, vorgenommene Veränderungen zu protokollieren. Eine elegante Methode ist die Zwangsprotokollierung mit Hilfe eines PC-Gateways.

Ergänzende Kontrollfragen:

- Ist die externe Fernwartung unterbunden?
- Ist der Remote-Zugang nicht-amtsberechtigt?
- Wer kann von wo aus den Remote-Zugang anwählen?
- Wer hat Zugang zur Fernwartungszentrale?
- Befindet sich die Fernwartungszentrale in einem gesicherten Bereich?
- Werden alle Fernwartungszugriffe und Eingaben protokolliert?

M 5.15 Absicherung externer Remote-Zugänge

Verantwortlich für Initiierung: TK-Anlagen-Verantwortlicher, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Als externer Remote-Zugang wird hierbei jeder Zugriff über den Wartungseingang der TK-Anlage via öffentliche Vermittlungssysteme angesehen. Dies kann entweder dadurch notwendig werden, dass die einzelnen Anlagen des Verbundes nicht oder nicht nur (siehe Anmerkung) über Standleitungen verbunden sind oder dass auf eine schnelle Unterstützung des Herstellers in Notfällen nicht verzichtet werden kann. In diesen Fällen muss der Wartungsport (Modem) die volle Amtsberechtigung besitzen.

Die nachfolgende Abbildung stellt ein typisches Szenario eines externen Remote-Zugangs zu einem Fernadministrationsport via Modem dar. Die TK-Anlage wird vom externen Wartungsplatz aus über Modem 1 - öffentliches Netz - PBX - Modem 2 - V.24-Wartungsschnittstelle administriert.

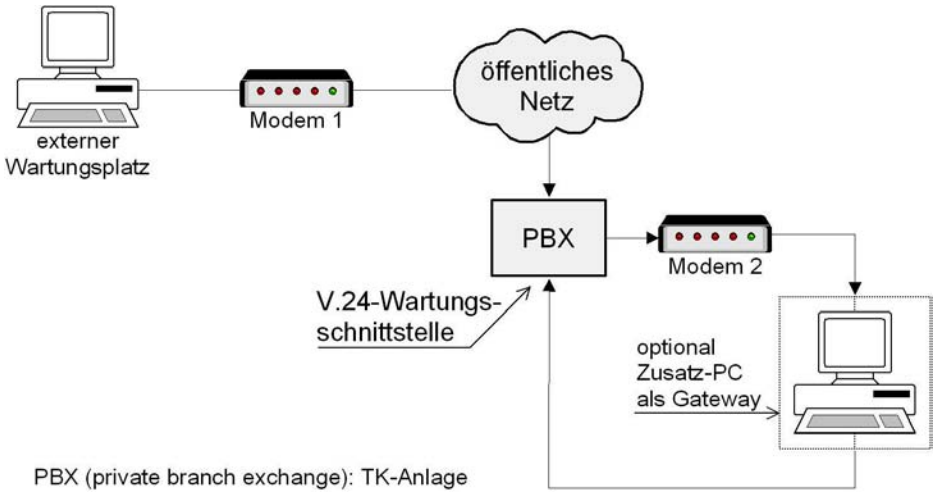


Abbildung: Aufbau einer externen Fernadministration über Modem

Aus Sicherheitsgründen ist es sinnvoll, auf externe Fernwartung zu verzichten. Ist dies nicht möglich, so sind - neben den Maßnahmen für interne Remote Zugänge - zusätzliche Sicherungsmaßnahmen unumgänglich.

Anmerkung: Einige Anlagen bieten die Möglichkeit, nur die Grundverkehrslast über Standleitungen abzuwickeln und Lastspitzen automatisch über das öffentliche Netz zu routen. Dieser Vorgang wird dem Benutzer nicht signalisiert.

PC-Gateway (siehe Anmerkung)

Zwischen Wartungsport und Modem sollte ein PC-Gateway geschaltet werden. Dieser muss die folgenden Sicherheitsfunktionen realisieren:

- Identifikation und Authentisierung des Bedieners,
- Abbruch der Verbindung bei sicherheitskritischen Ereignissen,
- Automatischer Rückruf (call back) und
- Protokollierung aller Tätigkeiten.

Darüber hinaus können noch weitere Funktionalitäten implementiert werden:

- Verhängen einer Zeitsperre bei fehlerhaften Zugangsversuchen,
- Sperren der Fernwartung im Normalbetrieb und explizite Freigabe für eine genau definierte Zeitspanne; dies ist sinnvoll, um in Notfall dem Hersteller oder einem anderen Wartungsunternehmen einen Eingriff zu ermöglichen,
- Einschränkung der Rechte des Wartungspersonals; über eine auf dem Wartungs-PC installierte Zusatzsoftware kann der Benutzer in seinem Handlungsspielraum eingeengt werden, um eine abgestufte Rechteverwaltung zu realisieren,
- "Zwangslogout" bei Leitungsunterbrechung; wird die Verbindung zwischen Fernwartungsstelle und PC-Gateway auf irgendeine Weise unterbrochen, so muss der Zugriff auf das System durch ein "Zwangslogout" beendet werden.

Physikalische Abschaltung des Fernwartungszuganges

Sollte im Normalfall keine Fernwartung benötigt und nur im Bedarfsfall eine solche ermöglicht werden, so empfiehlt sich die physikalische Abschaltung des Zuganges. Im Bedarfsfall kann dieser, eventuell nach telefonischer Rücksprache mit dem Hersteller oder der Wartungsfirma, kurzfristig aktiviert werden.

Geschlossene Benutzergruppen (Closed User Group, CUG)

In öffentlichen ISDN- und X.25-Netzen wird das Leistungsmerkmal der Bildung von CUG angeboten. Auf diese Weise wird für einen Benutzer vom Netzbetreiber ein virtuelles "Netz-im-Netz" zur Verfügung gestellt. Die geschlossenen Benutzergruppen können beim Netzbetreiber gegen entsprechende Entgelte beantragt werden.

Alternativ kann überlegt werden, die geschlossenen Benutzergruppen durch Nutzung der ISDN-Hilfsdienste Calling Line Identification and Presentation (CLIP) und Connected Line Identification and Presentation (COLP) selbst zu realisieren. Dies kann, wenn möglich, durch entsprechende Konfiguration der eigenen TK-Anlage oder aber durch entsprechende Auslegung eines PC-Gateways geschehen.

Anmerkung: Diese Maßnahme sollte auch bei interner Fernwartung über virtuelle private Netze angewandt werden.

Vermeidung bzw. Kontrolle direkter Einwahlmöglichkeiten (Dial-In)

Eine direkte Einwahlmöglichkeit, z. B. aus anderen Netzen über Nachwahl im Mehrfrequenzwahlverfahren, in die TK-Anlage sollte nach Möglichkeit unterbunden werden. Solche Verfahren werden oft für den Zugang zu Serverdiensten genutzt. Sollte ein Unterbinden aus betrieblichen Gründen nicht vermeidbar sein, so empfiehlt sich das vollständige Aktivieren der möglichen Schutzmechanismen und eine regelmäßige Kontrolle auf möglichen Missbrauch.

Ergänzende Kontrollfragen:

- Ist die Fernwartung im Normalfall physikalisch abgeschaltet?
- Von wo aus kann eine Fernwartung durchgeführt werden?
- Ist ein "Callback-Verfahren" realisiert?
- Ist ein PC-Gateway realisiert?
- Sind über Fernwartung vorgenommene Eingaben nachvollziehbar?
- Besteht über Fernwartung Zugriff auf die Protokolldateien?
- Kann der Protokolldrucker über Fernwartung deaktiviert werden?
- Werden erfolglose Login-Versuche protokolliert?
- Wird nach solchen Versuchen die Verbindung abgebrochen?
- Erfolgt ein zwangsweises Logout bei Leitungsunterbrechung?

M 5.16 Übersicht über Netzdienste

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator

Bevor unter Unix mit der Sicherheitsüberprüfung einzelner Netzdienste und -prozesse begonnen wird, sollte zunächst eine Übersicht darüber erstellt werden, welche Dienste überhaupt zur Verfügung gestellt werden müssen und welche Dienste u. U. schon installiert sind. Für letzteres ist es hilfreich, mit Hilfe des Befehls *ps* und entsprechenden Optionen eine Liste aller Netzprozesse zu erzeugen. Dann sollte man sich über die Aufgabe von jedem dieser Prozesse und darüber, wo er mit welchen Optionen gestartet wird, informieren. Häufig geschieht dies in den Dateien */etc/rc, /etc/rc.net, /etc/rc.local*, die beim Booten des Systems gelesen werden.

Besonders wichtig ist der *inetd*-Daemon, da dieser alle Prozesse, die in der Datei */etc/inetd.conf* aufgeführt sind, starten kann. Auch Konfigurationsdateien wie */etc/services, /etc/protocols, /etc/hosts, /etc/gated.conf* und andere müssen überprüft werden.

M 5.17 Einsatz der Sicherheitsmechanismen von NFS

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator

NFS (Network File System) erlaubt die gemeinsame Benutzung von Dateien auf einem Server von allen Rechnern (Clients) aus, die im selben Netz eingebunden sind und auf dem Server die Rechte dazu bekommen haben. Jeder Server lässt sich auch als Client betreiben und umgekehrt, so dass sichergestellt werden muss, dass jeder Rechner nur mit der für ihn vorgesehenen Funktionalität arbeitet. So ist es z. B. unnötig, den Mount-Daemon *mountd* oder den NFS-Daemon *nfsd* auf einem NFS-Client zu starten.

- Auf einem NFS-Server muss in einer Datei (z. B. */etc/exports* oder */etc/dfs/dfstab*) jedes Dateisystem bzw. Verzeichnis eingetragen werden, das von anderen Rechnern gemountet werden können soll. Für sie muss folgendes gelten:
  - Es sollten nur Dateisysteme exportiert werden, die unbedingt notwendig sind.
  - Mit den Schlüsselwörtern *root* und *access* lassen sich die Rechner genau spezifizieren, für die Dateisysteme zum Export freigegeben werden sollen. Fehlt die Angabe spezieller Rechner, so ist das Dateisystem für alle Rechner freigegeben, was auf keinen Fall geschehen darf!
  - Für Dateisysteme, die nur gelesen werden sollen, und hierzu gehören alle ausführbaren Dateien, sollte die Option *ro* (*read only*) benutzt werden.
  - Normalerweise wird die Benutzernummer des Systemadministrators (UID 0) bei NFS-Anfragen auf die Nummer des Benutzers *nobody* (UID -2 bzw. 65534) umgesetzt, so dass auf Dateien mit der UID 0 über NFS nicht zugegriffen werden kann. Dies gilt nicht für Dateien, die anderen privilegierten Benutzern gehören, wie z. B. *bin* oder *daemon*, was auch in Zusammenhang mit der Aufteilung der Administrationstätigkeiten (M 2.32 *Einrichtung einer eingeschränkten Benutzerumgebung*) bedacht werden muss, d. h. Dateisysteme mit Dateien dieser Benutzer dürfen nicht exportiert werden. Da jeder Rechner im Netz jede IP annehmen kann und z. B. jeder PC-Benutzer unter DOS *root*-Privilegien hat, sollte also die Umsetzung von *root* auf *nobody* nicht abgeschaltet werden, und es sollte sichergestellt werden, dass ein Eintrag *nobody:*:-2:-2:anonymous user::* in der */etc/passwd* existiert und wirksam ist. In diesem Zusammenhang muss auch beachtet werden, dass jeder Benutzer, der auf einem Netzrechner *root*-Privilegien hat (z. B. als PC-Benutzer) über NFS auch jede Gruppenkennung annehmen kann, so dass also kein exportiertes Verzeichnis und keine exportierte Datei Gruppenschreibrechte besitzen sollte und Lese- und Ausführungsrechte nur, soweit dies unumgänglich ist. Außerdem sollte beachtet werden, dass nicht nur einzelne Dateien, sondern alle darüberliegenden Verzeichnisse geschützt werden müssen!

  - Die Option *anon=-1* sollte benutzt werden, damit anonyme Anfragen verhindert werden. *anon=0* (*root*) sollte niemals benutzt werden, da hierdurch jedem Benutzer Dateizugriffe mit *root*-Rechten möglich werden.

- In Dateien wie z. B. */etc/fstab* oder */etc/vfstab* sind die Dateisysteme eingetragen, die durch einen Befehl wie z. B. *mount -a* oder *mountall* gemountet werden können. Dies kann unter Umständen auch ohne Rückfrage beim Booten geschehen. Diese Datei muss deshalb rechtzeitig auf Korrektheit überprüft werden.
- */etc/exports* und */etc/fstab* (bzw. analoge Dateien auf anderen Systemen) sind Systemdateien, auf die nur der Systemadministrator Zugriff haben darf.
- Zu exportierende Dateisysteme sollten auf einer separaten Platte oder Partition eingerichtet werden, damit z. B. das unbefugte Vollschreiben der Systemplatte durch einen Benutzer von einem anderen Rechner aus verhindert wird.
- Beim Mounten exportierter Dateisysteme muss die Option *nosuid* benutzt werden, um die Ausführung von *suid*-Programmen auf dem Client zu verhindern.
- Wenn möglich, sollte der NFS-Daemon so konfiguriert werden, dass er automatisch eine Überprüfung der Portnummern durchführt, um sicherzustellen, dass Pakete nur von den privilegierten Ports 0 - 1023 akzeptiert werden.
- Zur Kennzeichnung von Dateien werden zwischen Client und Server so genannte File-Handles benutzt, die sich sehr leicht erraten lassen. Sie sollten deshalb mit Hilfe des Programms *fsirand* randomisiert werden.
- Wenn vorhanden, sollte *SECURE-NFS* benutzt werden, so dass die Daten verschlüsselt übertragen werden. Dabei sind folgende Schritte wichtig:
  - Erzeugung von Schlüsseln für alle NFS-Benutzer,
  - Löschen des *public key* für den Benutzer *nobody,*
  - auf dem NIS-Masterserver darf *rpc.ypupdated* nicht laufen,
  - Übertragung der *public key map* auf alle Rechner, bevor *SECURE-NFS* gestartet wird,
  - Benutzung von *keylogin* und *keylogout* zur Erzeugung von *private keys* beim Ein- und Ausloggen,
  - auf jedem Client muss der *keyserv*-Daemon laufen,
  - beim Mounten muss die Option *secure* benutzt werden,
  - die Uhren auf allen Rechnern müssen synchronisiert werden, da die übertragenen Pakete mit Zeitmarken versehen werden, um das Wiedereinspielen von Nachrichten zu verhindern.

M 5.18 Einsatz der Sicherheitsmechanismen von NIS

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator

NIS (Network Information Service) lässt sich nicht ohne schwerwiegende Sicherheitslücken betreiben und sollte deshalb nur in einer sicheren Umgebung eingesetzt werden.

Für einen NIS-Server gilt folgendes:

- In der Passwortdatei */etc/passwd* darf der Eintrag *+::0:0:::* nicht enthalten sein, da sonst ein Zugang mit dem Namen "+" ohne Passwort existiert. Sollte der Eintrag notwendig sein, muss das Passwort durch ein "*" ersetzt werden (überprüfen, ob der Zugang wirklich gesperrt ist !). Trotzdem bleibt die Gefahr, dass bei einer versehentlichen Löschung der ersten Spalte (das "+") ein privilegierter Zugang ohne Passwort und ohne Benutzername möglich ist!
- Analoges gilt für die Gruppendatei */etc/group* und alle anderen sicherheitsrelevanten Dateien, die über NIS netzweit zugänglich gemacht werden sollen, wie z. B. */etc/hosts, /etc/group* oder */etc/bootparams*.
- Der Server-Prozess *ypserv* sollte nur Anfragen von vorher festgelegten Rechnern beantworten.

Für einen NIS-Client gilt folgendes:

- Der Eintrag +:*:0:0::: in der Passwortdatei */etc/passwd* sollte dokumentiert werden (siehe M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*), und es muss auf jeden Fall ein Eintrag im Passwortfeld vorhanden sein, damit nicht im Falle einer (beabsichtigten oder nicht beabsichtigten) Nichtbenutzung von NIS versehentlich ein Zugang mit dem Benutzernamen "+" ohne Passwort geschaffen wird.
- Analoges gilt für die Gruppendatei */etc/group* und alle anderen sicherheitsrelevanten Dateien, die über NIS netzweit zugänglich gemacht werden sollen.
- Der Client-Prozess *ypbind* sollte nur Daten akzeptieren, die von einem privilegierten Port kommen, da er ansonsten Daten (auch Passwörter !) von jedem beliebigen Prozess, der sich als Server ausgibt, bekommen könnte.
- Um zu verhindern, dass der NIS-Administrator auf allen NIS-Clients *root*-Rechte hat, sollte auf jedem NIS-Client ein lokaler Benutzer mit der UID 0 eingerichtet werden.
- Es muss beachtet werden, dass NIS zunächst die lokalen Dateien nach passenden Einträgen absucht, so dass z. B. die Einträge

  root::0:0:::

  +:*:0:0:::

  in der */etc/passwd* dazu führen, dass nicht das *root*-Passwort aus der NIS-Map benutzt wird, sondern der erste Eintrag ohne Passwort.

M 5.19 Einsatz der Sicherheitsmechanismen von sendmail

Verantwortlich für Initiierung: Administrator

Verantwortlich für Umsetzung: Administrator

Da die Übertragung von Mails die wohl am meisten verbreitete Anwendung in Netzen ist, sind die dafür zuständigen Prozesse von besonderer Bedeutung und einer der häufigsten Angriffspunkte in einem System. Hinzu kommt, dass diese Prozesse häufig das *suid*-Bit gesetzt haben und einem privilegierten Benutzer gehören (z. B. *root* oder *bin*). Ein Fehler in *sendmail* war z. B. einer der Wege, über die sich der Internet-Wurm ausgebreitet hat.

- Beim Starten von *sendmail* lassen sich sehr viele Optionen angeben, die zu Sicherheitsproblemen führen würden, wenn sie mit *root*-Rechten abliefen. Wenn *sendmail* von beliebigen Benutzern aufgerufen werden kann, sollte deshalb überprüft werden, ob es beim Start mit einer dieser Optionen das gesetzte *suid*-Bit ignoriert und mit der UID des Benutzers abläuft. Um Sicherheitsprobleme zu vermeiden, sollte der Administrator sicherstellen, dass *sendmail* nur mit den folgenden Optionen bei gesetztem *suid-root*-Bit von unprivilegierten Benutzern gestartet werden kann: *7, b, C, d, e, E, i, j, L, m, o, p, r, s* und *v*.
- Aufgrund der in der Vergangenheit aufgedeckten Sicherheitsdefizite des Programms *sendmail* muss stets die aktuellste Programmversion eingesetzt werden. Informationen über die aktuellen Versionen erteilen die in M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems* angegebenen Stellen wie BSI, CERT, DFN-CERT.
- Der *sendmail*-Prozess darf nicht im Debug-Modus betrieben werden können, da es sonst möglich wird, *root*-Rechte zu erlangen. Man kann dies testen, indem man den Befehl

  telnet localhost 25

  eingibt, wobei *localhost* der zu überprüfende Rechnername sein kann und *25* die Portnummer, mit der der *sendmail*-Prozess angesprochen wird. Der Rechner bzw. der *sendmail*-Prozess meldet sich dann mit

  Trying 123.45.67.8...

  Connected to xxx.yy.de.

  Escape character is '^]'.

  220 xxx Sendmail 4.1/SMI-4.1 ready at Wed, 13 Apr 94 10:04:43 +0200

  Wenn Sie nun den Befehl *debug, showq* oder bei sehr alten Versionen *wizard* eingeben, sollte dies der Prozess mit

  500 Command unrecognized

  ablehnen. Sie können dann mit dem Befehl *quit* die Verbindung wieder beenden.

- Die Befehle *vrfy* und *expn* dürfen nicht verfügbar sein, da sie zu einem Mailnamen den zugehörigen Login-Namen ausgeben, so dass sich dann durch Probieren evtl. das zugehörige Passwort herausfinden lässt. Bei Version 8 von *sendmail* lassen sich diese Befehle z. B. durch die Option *p* (privacy) beim Starten abschalten. Ob diese Befehle verfügbar sind, lässt sich wie im vorigen Punkt beschrieben feststellen, also z. B. durch Eingabe des Befehl *vrfy useralias*.
- Die Konfigurationsdatei *sendmail.cf* sollte *root* gehören und auch nur für *root* les- und schreibbar sein. Dasselbe gilt für die darüber stehenden Verzeichnisse, da sich sonst durch ein einfaches Umbenennen dieser Verzeichnisse eine neue *sendmail.cf* Datei erzeugen lässt.
- Die Angabe von ausführbaren Programmen oder von Dateien als gültige Adressen für Empfänger oder Absender muss durch die Konfiguration von *sendmail.cf* verhindert werden oder durch geeignete Maßnahmen auf bestimmte, unbedenkliche Programme und Dateien eingeschränkt werden.
- Das *F*-Kommando (also z. B. *FX/path [^#]*), mit dessen Hilfe Klassen definiert werden, sollte in der Konfigurationsdatei (*sendmail.cf*) nur benutzt werden, um Dateien zu lesen, die sowieso systemweit lesbar sind, da es sonst möglich sein kann, dass sicherheitsrelevante Informationen aus geschützten Dateien frei verfügbar werden. Die Programmform des *F*-Kommandos (z. B. *FX|/tmp/prg*) sollte nicht benutzt werden!
- Bei der Definition des Delivery Agents (z. B. *Mlocal*) dürfen nur absolute Pfade angegeben werden (z. B. *P=/bin/mail*). Außerdem sollte das Flag S (*suid*) nur gesetzt werden, wenn die damit evtl. verbundenen Sicherheitsprobleme geklärt sind.
- Jede Datei, in die *sendmail* schreiben könnte, wie z. B. *sendmail.st* für eine Statistik, sollte nur von *root* beschreibbar sein und auch nur in *root* gehörenden Verzeichnissen stehen. Dasselbe gilt für Dateien, die von *sendmail* ausgewertet werden wie z. B. *:include:* in Mailing Listen.
- Privilegierte Benutzer wie *bin* oder *root* sollten keine *.forward* Datei besitzen. Sind nämlich die Benutzer- oder Gruppenschreibrechte für diese Datei falsch gesetzt oder gelingt es einem Benutzer, in eine privilegierte Gruppe zu gelangen, kann er sich eine Shell mit der privilegierten Benutzer-Kennung erzeugen.

  Für normale Benutzer sollte die *.forward*-Datei nur von dem Besitzer beschreibbar sein und muss sich in einem Verzeichnis befinden, das dem Besitzer gehört.

  Falls ein Heimatverzeichnis systemweit beschreibbar sein muss, wie z. B. *uucp*, lässt sich auf folgende Weise verhindern, dass eine schädliche *.forward*-Datei angelegt werden kann: Es muss ein Verzeichnis mit dem Namen *.forward,* den Rechten 000 und dem Besitzer *root* angelegt werden und in diesem eine Datei ebenfalls mit den Rechten 000 und dem Besitzer *root*, so dass niemand außer *root* diese Datei verändern oder löschen kann. Das Homedirectory von *uucp* sollte dann ebenfalls *root* gehören und mit dem Sticky-Bit (*t*) versehen sein. Eine analoge Vorgehensweise empfiehlt

sich auch für andere Konfigurationsdateien (z. B. *.login, .cshrc*) in systemweit beschreibbaren Verzeichnissen.

- Aus der Alias-Datei sollte jedes ausführbare Programm entfernt werden, insbesondere auch *uudecode*. Außerdem sollte die Alias-Datei und die zugehörige Datenbank *root* gehören und auch nur für *root* beschreibbar sein.
- Es muss beachtet werden, dass jede empfangene Mail verfälscht sein kann. Dies kann entweder in der Mailqueue geschehen oder durch ein Einloggen auf Port 25. Ersteres lässt sich vermeiden, wenn das Mailqueue-Verzeichnis *root* gehört und die Rechte 0700 besitzt. Die Queue-Dateien sollten die Berechtigung 0600 haben. Die Veränderung einer Mail während ihres Transportes lässt sich nicht vermeiden, so dass die Benutzer darüber aufgeklärt werden müssen, dass z. B. eine Mail von *root*, in der sie dazu aufgefordert werden, ihr Passwort zu ändern, gefälscht sein kann.

M 5.20 Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator

Mit dem Programm *rlogin* bzw. dem zugehörigen Daemon *rlogind* ist es möglich, sich über eine Netzverbindung auf einem anderen Rechner einzuloggen, wobei allerdings nur das Passwort abgefragt wird, da der Benutzername direkt übergeben wird. Mit den Kommandos *rsh* bzw. *rcp* und dem Daemon *rshd* ist es möglich, auf einem anderen Rechner ein Kommando ausführen zu lassen. Für beide Befehle gibt es die Möglichkeit, Trusted-Hosts zu definieren und zwar entweder benutzerspezifisch im Heimatverzeichnis in der Datei *$HOME/.rhosts* oder systemweit in der Datei */etc/hosts.equiv*. Jeder Rechner, der in einer dieser Dateien eingetragen ist, wird als vertrauenswürdig angesehen, so dass ein Einloggen (mit *rlogin*) bzw. die Ausführung eines Befehles (mit *rsh*) von ihm aus ohne Angabe eines Passwortes möglich ist.

.rhost und host.equiv nicht verwenden

Da es, insbesondere von einem PC aus, sehr leicht ist, jeden beliebigen Rechnernamen vorzutäuschen, muss sichergestellt werden, dass die Dateien *$HOME/.rhosts* und */etc/hosts.equiv* **nicht** vorhanden sind oder dass sie leer sind und der Benutzer keine Zugriffsrechte auf sie hat. Hierzu sollten regelmäßig die Heimatverzeichnisse der Benutzer untersucht werden, oder es sollte verhindert werden, dass die Daemons *rlogind* und *rshd* gestartet werden können (siehe hierzu die Datei */etc/inetd.conf* und Maßnahme M 5.16 *Übersicht über Netzdienste*). Sollte die Benutzung der Datei */etc/hosts.equiv* unumgänglich sein, muss sichergestellt sein, dass kein Eintrag ‘+‘ vorhanden ist, da hierdurch jeder Rechner vertrauenswürdig würde.

Secure Shell als Ersatz nutzen

Als Ersatz für die r-Dienste kann Secure Shell (*ssh*) genutzt werden, wobei umfangreiche Funktionen zur sicheren Authentisierung und zur Wahrung von Vertraulichkeit und Integrität zum Einsatz kommen (siehe auch M 5.64 *Secure Shell*). Wenn *ssh* zum Einsatz kommt, sollten nach Möglichkeit die r-Dienste abgeschaltet werden, damit die Sicherheitsmaßnahmen nicht umgangen werden können. Dies setzt allerdings voraus, dass alle Kommunikationspartner über geeignete Implementierungen von *ssh* verfügen.

M 5.21 Sicherer Einsatz von telnet, ftp, tftp und rexec

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator

Passwörter im Klartext

Das Kommando *telnet hostname* ermöglicht es, sich nach Eingabe eines Benutzernamens und des zugehörigen Passwortes auf dem Rechner *hostname* einzuloggen. Mit *ftp* ist es möglich, größere Datenmengen zu kopieren, und *rexec* erlaubt die Ausführung von Kommandos auf einem anderen Rechner ohne ein vorhergehendes Anmelden. Bei allen drei Programmen werden die eingegebenen Benutzernamen und Passwörter unverschlüsselt über das Netz übertragen, so dass sie nur benutzt werden dürfen, wenn sichergestellt ist, dass das Netz nicht abgehört werden kann (siehe G 5.7). Alle Aufrufe von *telnet, ftp* und *rexec* sind zu protokollieren. Insbesondere ist auf fehlgeschlagene Verbindungsversuche von externen IT-Systemen zu achten.

Sicherheitslücken in ftpd

Beim Einsatz des Daemons *ftpd* muss beachtet werden, dass ähnlich wie bei *sendmail* (siehe M 5.19 *Einsatz der Sicherheitsmechanismen von sendmail*) immer wieder neue schwerwiegende Sicherheitslücken festgestellt werden, die es u. U. ermöglichen, ohne Passwort Administratorrechte zu bekommen (siehe hierzu die CERT-Mitteilung CA-94-08 vom 14.04.1994). Es sollten keine *ftp*-Versionen eingesetzt werden, die älter sind als die dort beschriebenen.

ftp-Zugang beschränken

Weiterhin sollten in die Datei */etc/ftpusers* alle Benutzernamen eingetragen werden, für die ein *ftp*-Zugang nicht erlaubt werden soll. Hierzu gehören z. B. *root, uucp* und *bin*. Bei der Einrichtung von neuen Benutzern ist darauf zu achten, diese in */etc/ftpusers* einzutragen, wenn sie gemäß ihrem Rechteprofil keinen ftp-Zugang haben dürfen (siehe auch M 2.30 *Regelung für die Einrichtung von Benutzern / Benutzergruppen*).

Mit Hilfe von *.netrc*-Dateien werden automatische FTP-Zugriffe auf entfernten IT-Systemen erlaubt. Damit dies möglich ist, enthalten *.netrc*-Dateien die benötigten Passwörter. Daher muss sichergestellt werden, dass keine *.netrc*-Dateien in den Benutzerverzeichnissen vorhanden sind oder dass sie leer sind und der Benutzer keine Zugriffsrechte auf diese hat.

eingeschränkter Dateizugriff bei tftp

Der Einsatz des Daemons *tftpd, rexd* und *rexecd* muss verhindert werden (z. B. durch Entfernen des entsprechenden Eintrags in der Datei */etc/inetd.conf*), oder es muss zumindest sichergestellt sein, dass beim Einsatz von *tftp* den Benutzern aus dem Login-Verzeichnis nur eingeschränkte Dateizugriffe möglich sind (siehe auch M 2.32 *Einrichtung einer eingeschränkten Benutzerumgebung*). Dies lässt sich überprüfen, indem man Folgendes eingibt:

```
tftp hostname
tftp>get /etc/passwd /tmp/txt
```

Meldet sich der *tftp*-Daemon nicht mit einer Fehlermeldung, muss seine Benutzung verhindert werden.

Muss für den Startvorgang von aktiven Netzkomponenten oder X-Terminals *tftp* doch eingesetzt werden, ist dies unbedingt zu dokumentieren und zu begründen. Außerdem ist beim Einsatz von *tftp* sicherzustellen, dass der *tftp*-Daemon mit der Option *-s verzeichnis* gestartet wird. Dabei ist für *verzeichnis* das ausschließlich für den Daemon sichtbare Verzeichnis einzusetzen.

Secure Shell als Ersatz verwenden

Als Ersatz für *telnet* und *rexec* kann Secure Shell (*ssh*) genutzt werden, wobei umfangreiche Funktionen zur sicheren Authentisierung und zur Wahrung von Vertraulichkeit und Integrität zum Einsatz kommen (siehe auch M 5.64 *Secure Shell*). Durch Tunneling ist es auch möglich, *ftp* mit sicherer Verschlüsselung zu betreiben. Wenn *ssh* zum Einsatz kommt, sollten daher nach Möglichkeit diese Dienste abgeschaltet werden, damit die Sicherheitsmaßnahmen nicht umgangen werden können. Dies setzt allerdings voraus, dass alle Kommunikationspartner über geeignete Implementierungen von *ssh* verfügen.

Ergänzende Kontrollfragen:

- Wird die Datei */etc/ftpusers* regelmäßig aktualisiert?
- Werden Zugriffsversuche über *telnet, ftp* und *rexec* protokolliert?
- Wird *ssh* zur Absicherung eingesetzt?
- Ist *tftp* deaktiviert?

M 5.22 Kompatibilitätsprüfung des Sender- und Empfängersystems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Verfahrensverantwortlicher

Abhängig vom Grad der Kompatibilität von Empfänger- und Sendersystem lassen sich Informationen mehr oder weniger zuverlässig per Datenträgeraustausch übertragen. Dabei sind je nach Komplexität auszutauschender Daten unterschiedliche Anforderungen an die Kompatibilität zu stellen. Vor Einrichtung eines regelmäßigen Datenträgeraustausches sollte daher die Übereinstimmung folgender Eigenschaften überprüft werden, um im Vorfeld Inkompatibilitäten festzustellen und ggf. Abhilfe zu schaffen:

- Physikalisches Lesemedium:

  Notwendige Voraussetzung ist die **Übereinstimmung der physikalischen Lesemedien** von Empfänger- und Sendersystem. Dabei reicht aber mechanische Äquivalenz noch nicht aus, denn die Nichtübereinstimmung von Parametern wie Geschwindigkeit bei Bändern oder Kapazität bei Disketten kann zu Problemen führen.

- Zeichencode (z. B. ASCII oder EBCDIC):

  Stimmen Sender- und Empfängersystem im verwendeten **Zeichencode** überein, so sind mit Hilfe des physikalischen Lesens einzelne Sektoren/Blöcke im Klartext lesbar, die unzusammenhängend auf dem Datenträger verteilt sein können. Stimmen die verwendeten Zeichencodes nicht überein, werden die übertragenen Daten falsch interpretiert.

- Formatierung des Betriebs- bzw. Dateisystem des Datenträgers:

  Verfügen beide Systeme darüber hinaus über das **gleiche Betriebs- und Dateisystem** oder sieht das Empfängerbetriebssystem vor, Formatierungen anderer Betriebssystem zu lesen (einige Unix-Betriebssysteme können DOS-Disketten einlesen), dann können alle Dateien, wie sie beim Absender vorlagen, wiederhergestellt werden. Dies ist für Informationen ausreichend, die keiner weiteren Formatierung, wie sie von den meisten Anwendungsprogrammen (z. B. Textverarbeitungsprogrammen) vorgenommen werden, unterliegen.

- Anwendungssoftware:

  Wurden Anwendungsprogramme zur Erzeugung der zu übermittelten Dateien verwendet, ist auf **Versionsgleichheit** dieser Programme zu achten, da die Dateiformate evtl. unterschiedlich sein können. Die Versionsgleichheit muss nicht bestehen, wenn die Programmversionen aufwärts- bzw. abwärtskompatibel sind.

- IT-Sicherheitssoftware und IT-Sicherheitsparameter:

  Werden darüber hinaus IT-Sicherheitsprodukte oder Schutzmechanismen bestimmter Anwendungsprogramme (siehe M 4.30 *Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen*) verwendet, so ist die Kompatibilität dieser Produkte sicherzustellen. Über die verwendeten

Schlüssel oder **Passwörter** müssen sich Absender und Empfänger auf geeignetem Wege verständigen.

Treten Inkompatibilitäten auf, so sind zusätzliche Vorkehrungen bzw. Produkte bereitzustellen, die eine entsprechende Konvertierung vorsehen, oder die Absender- und Empfängersysteme sind identisch auszustatten.

Ergänzende Kontrollfragen:

- Kommen auf Sender- und Empfängerseite die gleichen IT-Produkte (Hardware/Software) zum Einsatz?
- Sind die Versionen der Anwendungsprogramme beim Empfänger und Absender kompatibel?
- Sind dem Empfänger etwaige Schlüssel oder Passwörter zum Lesen der Information bekannt?

M 5.23 Auswahl einer geeigneten Versandart für den Datenträger

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Neben den in M 2.3 *Datenträgerverwaltung* dargestellten Umsetzungshinweisen sollte sich die Versandart der Datenträger am Gefährdungspotential orientieren. Hinsichtlich Verfügbarkeit ist die Versandart derart auszuwählen, dass eine rechtzeitige Zustellung garantiert werden kann. Je mehr Personen mit der Beförderung befasst und je länger die Zeiten sind, in denen der Datenträger unbeaufsichtigt bleibt, desto weniger kann im allgemeinen die Vertraulichkeit und Integrität garantiert werden. Dementsprechend sind angemessene Versandarten auszuwählen.

Man kann dabei z. B. zwischen folgenden Versandarten wählen:

- Post (mit verschiedenen Versandangeboten, die unterschiedliche Garantien für die Transportgeschwindigkeit und Absicherung umfassen),
- Kurierdienste,
- persönlicher Kurier und
- persönliche Übergabe.

Für eine Behörde oder ein Unternehmen empfiehlt es sich, eine Liste zu führen, in der für verschiedene Datenträger und deren Schutzbedarf angemessene Versandarten vorgeschlagen werden. Dies erleichtert den Mitarbeitern die Auswahl nicht nur in Bezug auf das bestmögliche Preis-Leistungs-Verhältnis, sondern auch auf die optimale Sicherheit. Diese Liste sollte mindestens folgende Aspekte umfassen:

- durchschnittliche Transportzeit der Versandart bzw. des Kuriers
- Vertrauenswürdigkeit der Versandart bzw. des Kuriers
- Kosten.

Ergänzende Kontrollfragen:

- Orientiert sich die Auswahl der Versandart des Datenträgers an seinem Schutzbedarf?
- Stehen vertrauenswürdige Transportunternehmen oder Kuriere zur Verfügung?

M 5.24 Nutzung eines geeigneten Faxvorblattes

Verantwortlich für Initiierung: Leiter Innerer Dienst

Verantwortlich für Umsetzung: Fax-Verantwortlicher, Benutzer

Um einen geordneten und nachvollziehbaren Fax-Austausch zu erzielen, ist die Nutzung eines standardisierten Faxvorblattes vorzusehen. Damit kann insbesondere geprüft werden, ob eine erhaltene Faxsendung vollständig empfangen und ausgedruckt wurde.

Das Faxvorblatt sollte beinhalten:

- Rufnummer des Faxgerätes,
- Name des Absenders (mit Telefonnummer und vollständiger Adresse),
- Telefonnummer eines Ansprechpartners bei Übertragungsproblemen,
- Name des Empfängers (mit Rufnummer des Faxgerätes und ggf. vollständiger Adresse),
- Seitenzahl einschließlich Faxvorblatt,
- ggf. Dringlichkeitsvermerk (evtl. gestuft) und
- Unterschrift des Absenders.

Die Bitte, fehlgeleitete Sendungen weiterzuleiten oder den Absender zu informieren, ist sinnvoll.

Ergänzende Kontrollfragen:

- Hat das Faxvorblatt alle notwendigen Bestandteile?
- Wird das Faxvorblatt konsequent genutzt?

M 5.25 Nutzung von Sende- und Empfangsprotokollen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Fax-Verantwortlicher, Fax-Poststelle

Bei der Nutzung von Fax-Diensten ist bei der Verwendung von Sende- und Empfangsprotokollen zwischen herkömmlichen Faxgeräten und Faxservern zu unterscheiden.

Einsatz eines herkömmlichen Faxgerätes

Sende- und Empfangsprotokolle regelmäßig überprüfen

Listenmäßige Protokolle von Übertragungsvorgängen, die automatisch vom Faxgerät geführt werden (Kommunikationsjournal), sind regelmäßig auszudrucken. Es bedarf einer Festlegung, wer diese Ausdrucke veranlasst, wo und wie lange sie aufbewahrt werden und in welcher Weise sie stichprobenartigen Prüfungen auf Unregelmäßigkeiten unterzogen werden. Auf die Erfordernisse des Bundesdatenschutzgesetz (BDSG) ist Rücksicht zu nehmen. Insbesondere ist der Zugriff Unbefugter zu verhindern.

Führung eines Faxtagebuchs

Es sollte zusätzlich ein Faxtagebuch geführt werden, aus dem ersichtlich wird, wer wann ein Fax an wen versandt hat. Optional kann darüber hinaus ein Faxeingangsbuch geführt werden.

Es sei darauf hingewiesen, dass eine weitere Kontrollmöglichkeit besteht, wenn das Faxgerät an eine moderne TK-Anlage angeschlossen ist. Dann ist es u. U. möglich, die Gebührendatensätze der Faxnummer in der TK-Anlage auszuwerten (siehe auch M 2.40 *Rechtzeitige Beteiligung des Personal-/Betriebsrates*).

Einsatz eines Faxservers:

Protokolldateien regelmäßig auswerten

Auch auf Faxservern ist es möglich, die Übertragungsvorgänge zu protokollieren. Diese Protokolle sollten regelmäßig ausgewertet und archiviert werden. Es bedarf insbesondere der Festlegung von Rahmenbedingungen und Zuständigkeiten für die Auswertung und Archivierung der Protokolle.

So ist z. B. denkbar, dass die Fax-Poststelle für diese Tätigkeiten zuständig ist, die Auswertung der Protokolle aber nur im Beisein eines Betriebs- oder Personalratsmitgliedes bzw. eines Angehörigen der Revision oder des Datenschutzes erfolgen darf. Auch hier gilt, dass die Erfordernisse des BDSG zu berücksichtigen sind und insbesondere der Zugriff Unbefugter zu verhindern ist.

Bei der Verwendung von Faxservern ist die manuelle Führung von Fax-Tagebüchern nicht sinnvoll. Vielmehr dürfte die lückenlose Archivierung der Sende- und Empfangsprotokolle ausreichend sein.

Teilweise besteht auch die Möglichkeit, anfallende Gebührendatensätze für abgehende Faxsendungen vom Faxserver für eine verursachungsgerechte Verrechnung zu nutzen.

Ergänzende Kontrollfragen:

- Welche Regelungen gelten für die Überprüfung der Sende- und Empfangsprotokolle?
- Wo werden die Protokolle archiviert und wer kann darauf zugreifen?

M 5.26 Telefonische Ankündigung einer Faxsendung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Vorgesetzte

Verantwortlich für Umsetzung: Benutzer

Wichtige Faxsendungen mit vertraulichen oder finanzwirksamen Inhalten (z. B. Angebote) oder termingebundene Faxsendungen sollten vor Absendung beim Empfänger (zum Beispiel per Telefon) angemeldet werden. Der Empfänger hat dann die Möglichkeit, zum entsprechenden Faxgerät zu gehen und dort das für ihn eingehende Fax direkt entgegenzunehmen, so dass kein anderer das Fax entnehmen kann.

Die Benutzer sollten von Vorgesetzten angewiesen werden, vertrauliche oder wichtige Faxsendungen anzukündigen.

Ergänzende Kontrollfragen:

- Werden wichtige Faxsendungen vorher angekündigt?
- Gibt es eine Anweisung, dies zu tun?

M 5.27 Telefonische Rückversicherung über korrekten Faxempfang

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Vorgesetzte

Verantwortlich für Umsetzung: Benutzer

Bei wichtigen Faxsendungen sollte beim Empfänger nachgefragt werden, ob die Faxsendung vollständig empfangen, ausgedruckt und ihm übergeben wurde. Die Mitarbeiter sollten hierzu angewiesen werden. Die telefonische Bestätigung kann auch auf dem Fax-Vordruck erbeten werden.

Hilfreich sind in diesem Zusammenhang die von einigen Faxgeräten als Leistungsmerkmal angebotenen Einzelsendeberichte, die Fehler beim Versand anzeigen können.

Ergänzende Kontrollfragen:

- Gibt es im Unternehmen bzw. in der Behörde Faxsendungen, deren korrekter Empfang von besonderer Wichtigkeit ist?
- Wird bei solchen Faxsendungen beim Empfänger nachgefragt?

M 5.28 Telefonische Rückversicherung über korrekten Faxabsender

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Vorgesetzte

Verantwortlich für Umsetzung: Benutzer

Bei wichtigen oder ungewöhnlichen Faxsendungen sollte in Erwägung gezogen werden, sich beim Faxabsender zu vergewissern, dass das Fax von ihm abgesandt und nicht von einem Dritten gefälscht wurde. Dies kann auf einfache Weise durch einen telefonischen Rückruf erfolgen. Die erforderliche Rufnummer ist im allgemeinen auf dem Faxvorblatt dokumentiert, sollte aber, da sie gefälscht sein könnte, verifiziert werden.

Ergänzende Kontrollfragen:

- Wird bei wichtigen oder ungewöhnlichen Faxsendungen beim Absender zurückgerufen?

M 5.29 Gelegentliche Kontrolle programmierter Zieladressen und Protokolle

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Fax-Verantwortlicher

Bei programmierbaren Kurzwahltasten oder Zieladressenspeicherung sollte gelegentlich überprüft werden, ob die gewünschte mit der einprogrammierten Faxnummer übereinstimmt und ob sie noch benötigt wird. Damit wird verhindert, dass eine von einem Unberechtigten eingegebene fremde Faxnummer längere Zeit statt der korrekten Nummer genutzt wird. Außerdem werden eventuell übersehene Änderungen der gewünschten Zielrufnummern frühzeitig entdeckt.

Ergänzende Kontrollfragen:

- Werden die gespeicherten Rufnummern sporadisch überprüft?

M 5.30 Aktivierung einer vorhandenen Callback-Option

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Benutzer, Administrator

Viele Modems bieten die Option automatischer Rückruf (Callback). Ist diese Option aktiviert, trennt das Modem, wenn es einen Anruf erhält, sofort nach dem erfolgreichen Verbindungsaufbau die Leitung und ruft eine voreingestellte Nummer zurück. Dadurch wird verhindert, dass ein nicht autorisierter Anrufer diesen Modem-Zugang missbrauchen kann, solange er nicht unter der voreingestellten Nummer erreichbar ist. Callback ist immer dann einzusetzen, wenn ein fester Kommunikationspartner sich automatisch einwählen können soll. Zu beachten ist, dass mit dem automatischen Rückruf auch die Kosten der Datenübertragung übernommen werden.

Das erforderliche Kommando ist der Bedienungsanleitung zu entnehmen, üblicherweise wird das Kommando *AT%S* benutzt. Vor der Aktivierung der Callback-Option ist festzulegen, welche Nummer zurückgerufen werden soll.

Manche Modems bieten auch die Möglichkeit, einen automatischen Rückruf mit einer Passwortabfrage zu verbinden. Das angerufene Modem fordert dabei nach dem Verbindungsaufbau das anrufende Modem zu einer Passworteingabe auf. Im angerufenen Modem wird die Gültigkeit des Passwortes überprüft. Jedem gültigen Passwort ist eine Rufnummer zugeordnet, die dann zurückgerufen wird. Dabei kann meist eine Liste von Rückrufnummern im lokalen Modem angelegt werden, so dass von verschiedenen Orten aus Verbindung mit dem lokalen Modem aufgebaut werden kann.

Es ist darauf zu achten, dass der automatische Rückruf nur auf einer Seite aktiviert ist, da der Mechanismus sonst in eine Endlosschleife führt. Callback sollte auf der passiven Seite aktiviert sein, also auf der Seite, von der Dateien abgerufen oder auf der Dateien eingespielt werden. Ein typisches Beispiel ist der Außendienstmitarbeiter, der mit einem IT-System in seiner Organisation in Verbindung treten will. Hier muss Callback auf dem organisationsinternen Modem aktiviert sein.

Es sollte sichergestellt sein, dass die voreingestellten Rufnummern des Callback sporadisch kontrolliert und aktualisiert werden.

Ein Callback kann außer durch das Modem auch von der Applikation ausgelöst werden. Wenn die eingesetzte Applikation diese Option bietet, sollte das Callback von der Applikation und nicht vom Modem ausgelöst werden. Wenn das Modem ein Callback auslöst, kann ein Angreifer versuchen, in dem Moment, wenn das Modem den Callback starten will, dieses anzuwählen und damit den Callback abzufangen. Wenn die Applikation den Callback durchführt, ist es für einen Angreifer wesentlich schwieriger, den richtigen Moment abzupassen.

Ergänzende Kontrollfragen:

- Ist die Kostenübernahme im Callback-Modus geklärt?
- Wann wurden letztmalig die voreingestellten Rufnummern überprüft?

M 5.31 Geeignete Modem-Konfiguration

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Benutzer, Administrator

Die meisten Modems arbeiten nach dem Hayes-Standard (auch AT-Standard genannt). Dies ist ein nicht normierter, herstellerabhängiger Standard. Die Basis-Befehlssätze der verschiedenen Modems stimmen größtenteils überein. Größere Abweichungen gibt es in den erweiterten Befehlssätzen. Es ist wichtig, den Befehlssatz des eingesetzten Modems daraufhin zu überprüfen, wie die im folgenden beschriebenen Funktionen umgesetzt sind und ob durch fehlerhafte Konfiguration Sicherheitslücken entstehen können.

Die gewählten Einstellungen sollten im nichtflüchtigen Speicher des Modems gespeichert werden (siehe auch M 1.38 *Geeignete Aufstellung eines Modems*). Außerdem sollten sie auf Papier ausgedruckt werden, so dass sie jederzeit mit der aktuellen Einstellung verglichen werden können.

Nachfolgend werden einige sicherheitsrelevante Konfigurationen vorgestellt:

Auto-Answer

Über das Register S0 kann eingestellt werden, dass das Modem einen ankommenden Ruf automatisch nach einer einzustellenden Anzahl von Klingelzeichen entgegennimmt. Mit der Einstellung *S0=0* wird dies verhindert und erzwungen, dass Anrufe manuell entgegengenommen werden müssen.

Diese Einstellung sollte gewählt werden, wenn verhindert werden soll, dass von außen unbemerkt eine Verbindung aufgebaut werden kann. Ansonsten ist ein Callback-Mechanismus einzusetzen (siehe M 5.30 *Aktivierung einer vorhandenen Callback-Option*).

Fernkonfiguration des Modems

Manche Modems können so eingestellt werden, dass sie von entfernten Modems fernkonfiguriert werden können. Es ist darauf zu achten, dass diese Möglichkeit ausgeschaltet ist. Zum Problem der Fernwartung über Modems siehe M 5.33 *Absicherung der per Modem durchgeführten Fernwartung*.

Passwortgeschützte Speicherung von (Rückruf-)Nummern

Bei der Speicherung von Telefonnummern oder Rückrufnummern im nichtflüchtigen Speicher des Modems können diese bei vielen Modellen durch ein Passwort geschützt werden. Wenn diese Möglichkeit vorhanden ist, sollte sie genutzt und die Passwörter entsprechend M 2.11 *Regelung des Passwortgebrauchs* gewählt werden. Bei einigen Modems wird nach Eingabe eines bestimmten Befehls eine Liste der Rufnummern **mit** den zugehörigen Passwörtern angezeigt. Daher sollte der Zugang zum Modem nur befugten Personen möglich sein (siehe M 1.38 *Geeignete Aufstellung eines Modems*).

Ergänzende Kontrollfragen:

- Ist den für das Modem verantwortlichen Mitarbeitern der komplette Befehlssatz des Modems bekannt?
- Ist die Modem-Konfiguration dokumentiert?

M 5.32 Sicherer Einsatz von Kommunikationssoftware

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Benutzer, Administrator

Die Sicherheit des Rechnerzugangs über Modem hängt entscheidend von der eingesetzten Kommunikationssoftware ab.

Fast jede Kommunikationssoftware bietet die Möglichkeit, Telefonnummern und andere Daten von Kommunikationspartnern zu speichern. Dies sind personenbezogene Daten, die entsprechend geschützt werden müssen.

Passwörter für den Zugang auf andere Rechner oder Modems sollten nicht in der Kommunikationssoftware gespeichert werden, auch wenn das komfortabel erscheinen mag. Jeder, der Zugang zum IT-System und der Kommunikationssoftware hat, kann dann unter fremdem Benutzernamen Zugang in andere Systeme erlangen (siehe auch M 1.38 *Geeignete Aufstellung eines Modems* und M 2.8 *Vergabe von Zugriffsrechten*).

Etliche Kommunikationsprogramme bieten die Möglichkeit, die Datenübertragung im Hintergrund und damit unbeobachtet laufen zu lassen, z. B. unter Windows. Dies sollte nur bei vertrauenswürdigen Kommunikationspartnern genutzt werden, da hierbei ein Kommunikationspartner die Dateiübertragung abbrechen und u. U. andere Daten als abgesprochen vom oder zum lokalen Rechner übertragen könnte. Damit könnten beispielsweise Computer-Viren auf den lokalen Rechner eingeschleust oder vertrauliche Daten kopiert werden. Es gibt außerdem auch Übertragungsprotokolle, die eine Vollduplex-Übertragung, also gleichzeitiges Senden und Empfangen zulassen. Solche Übertragungsprotokolle sollten nur mit vertrauenswürdigen Kommunikationspartnern benutzt werden, da dies einer Datenübertragung im Hintergrund entspricht.

Verfügt die Kommunikationssoftware über eine Passwortabsicherung oder über Protokollierungsfunktionen, muss sie aktiviert werden.

Ergänzende Kontrollfragen:

- Werden Passwörter in der Kommunikationssoftware gespeichert?
- Sind dem IT-Benutzer die Risiken der Datenübertragung im Hintergrund bekannt?

M 5.33 Absicherung der per Modem durchgeführten Fernwartung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Fernwartung von IT-Systemen über ein Modem birgt besondere Sicherheitsrisiken. Aus Sicherheitsgründen ist es sinnvoll, auf externe Fernwartung zu verzichten. Ist dies nicht möglich, so sind zusätzliche Sicherungsmaßnahmen unumgänglich.

Das zu wartende IT-System einschließlich des eingesetzten Modems muss die folgenden Sicherheitsfunktionen realisieren:

- Der Aufbau der Verbindung für eine Fernwartung sollte immer vom lokalen IT-System initiiert werden. Dies kann durch Anruf des zu wartenden IT-Systems bei der Fernwartungsstelle oder über einen automatischen Rückruf (Callback) realisiert werden.
- Das externe Wartungspersonal muss sich zu Beginn der Wartung authentisieren. Werden dabei Passwörter unverschlüsselt übertragen, sollten Einmalpasswörter benutzt werden (siehe M 5.34 *Einsatz von Einmalpasswörtern*).
- Alle Tätigkeiten bei der Durchführung der Fernwartung müssen auf dem zu wartenden IT-System protokolliert werden.

Darüber hinaus können am zu wartenden IT-System noch weitere Funktionalitäten implementiert werden:

- Verhängen einer Zeitsperre bei fehlerhaften Zugangsversuchen,
- Sperren der Fernwartung im Normalbetrieb und explizite Freigabe für eine genau definierte Zeitspanne,
- Einschränkung der Rechte des Wartungspersonals; das Wartungspersonal sollte nicht die vollen Administrator-Rechte besitzen; bei DOS-PCs sollte über eine Zusatzsoftware eine abgestufte Rechteverwaltung realisiert werden; bei Unix-Systemen ist außerdem M 2.33 *Aufteilung der Administrationstätigkeiten unter Unix* zu beachten, bei PC-Netzen M 2.38 *Aufteilung der Administrationstätigkeiten*

  (Das Wartungspersonal sollte nur auf die Daten und Verzeichnisse Zugriff haben, die aktuell von der Wartung betroffen sind.)
- auf dem IT-System sollte für das Wartungspersonal eine eigene Benutzer-Kennung existieren, unter der möglichst alle Wartungsarbeiten durchgeführt werden,
- wird die Verbindung zur Fernwartungsstelle auf irgendeine Weise unterbrochen, so muss der Zugriff auf das System durch einen "Zwangslogout" beendet werden.

Die Fernwartung sollte lokal durch IT-Experten beobachtet werden. Auch wenn die Fernwartung eingesetzt wird, weil intern das Know-How oder die Kapazität nicht verfügbar ist, kann das Wartungspersonal nicht unbeaufsich-

tigt gelassen werden (siehe auch M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*). Bei Unklarheiten über die Vorgänge sollte der lokale IT-Experte sofort nachfragen. Es muss jederzeit die Möglichkeit geben, die Fernwartung lokal abzubrechen.

Werden während der Wartung Daten oder Programme auf dem lokalen IT-System angelegt, so muss dies deutlich erkennbar und nachvollziehbar sein, also z. B. darf dies nur in besonders markierten Verzeichnissen oder unter bestimmten Benutzer-Kennungen erfolgen.

Entsprechend M 3.2 *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen* sind auch mit externem Wartungspersonal vertragliche Regelungen über die Geheimhaltung von Daten zu treffen. Insbesondere ist festzulegen, dass Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sorgfältig gelöscht werden. Ebenso sind die Pflichten und Kompetenzen des externen Wartungspersonals sorgfältig festzulegen.

Ergänzende Kontrollfragen:

- Von wo aus kann eine Fernwartung durchgeführt werden?
- Ist ein "Callback-Verfahren" realisiert?
- Sind die beschriebenen Sicherheitsfunktionen realisiert?
- Sind über Fernwartung vorgenommene Eingaben nachvollziehbar?
- Besteht über Fernwartung Zugriff auf die Protokolldateien?
- Werden erfolglose Login-Versuche protokolliert?
- Wird nach solchen Versuchen die Verbindung abgebrochen?
- Erfolgt ein zwangsweises Logout bei Leitungsunterbrechung?

M 5.34 Einsatz von Einmalpasswörtern

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator

In Netzen, in denen Passwörter unverschlüsselt übertragen werden, können diese relativ einfach abgehört werden. Außerdem können Implementierungs- oder Protokollfehler in Betriebssystemen und Applikationssoftware dazu führen, dass auch verschlüsselte Passwörter kompromittiert werden können.

Daher empfiehlt sich die Verwendung von Einmalpasswörtern, also Passwörtern, die nach einmaligem Gebrauch gewechselt werden müssen. Einmalpasswörter können software- oder hardwaregestützt erzeugt werden.

Bei der Verwendung von Einmalpasswörtern muss der Benutzer das Einmalpasswort auf dem lokalen IT-System oder über ein Token generieren oder aus einer Liste einlesen, die vom entfernten IT-System generiert worden ist und die sicher aufzubewahren ist. Das entfernte IT-System muss dann das Einmalpasswort verifizieren.

Für den Einsatz von Einmalpasswörtern können z. B. Public-Domain-Programme wie OPIE bzw. S/Key benutzt werden. OPIE (One-time Passwords in Everything) ist die Public-Domain-Weiterentwicklung von S/Key, das mittlerweile als kommerzielles Produkt vertrieben wird.

S/Key benutzt im Gegensatz zu OPIE noch standardmäßig den MD4-Algorithmus zum Erzeugen und Verifizieren der Einmalpasswörter. Wegen der bekannten Schwachstellen des MD4-Algorithmus sollte der im Lieferumfang enthaltene MD5-Algorithmus benutzt werden.

OPIE bzw. S/Key bestehen aus einem Programmteil auf dem Server zum Verifizieren der eingegebenen Passwörter und einem Programmteil auf dem IT-System des Benutzers. Ein Benutzer bekommt beim Login auf dem entfernten IT-System nach Eingabe seines Benutzernamens die Sequenznummer des einzugebenden Einmalpasswortes und eine Kennung angezeigt. Mit diesen beiden Angaben und einem geheim zu haltenden Passwort berechnen OPIE bzw. S/Key auf dem lokalen IT-System das Einmalpasswort für diese Sitzung. Steht dem Benutzer zur Berechnung der Einmalpasswörter lokal kein Programm zur Verfügung, kann vom entfernten System eine Liste mit Einmalpasswörtern erzeugt werden, die dann entsprechend sicher zu verwahren ist.

Einmalpasswörter können auch über Token erzeugt werden, die die Generierung übernehmen. Dies können entweder Chipkarten oder taschenrechnerähnliche Geräte sein. Der Benutzer muss sich zunächst gegenüber dem Token authentisieren. Nach erfolgter Benutzer-Authentisierung authentisiert sich dann entweder der Token selbständig gegenüber dem Server oder er zeigt dem Benutzer an einem Display das am Client einzugebende Einmalpasswort an.

Nachdem immer mehr sensible Informationen nur durch Passwörter vor Fremdzugriff geschützt sind, kommt Einmalpasswortsystemen und hardwarebasierten Authentikationsmethoden ein wachsender Stellenwert zu. Wo der Einsatz von softwarebasierten Einmalpasswortsystemen wie OPIE auf

Akzeptanzprobleme stößt, sollten hardwarebasierte Systeme eingesetzt werden. Viele hardwarebasierte Systeme bieten darüber hinaus auch die Möglichkeit, "Single-Sign-On"-Lösungen aufzubauen. Über "Single-Sign-On"-Verfahren wird erreicht, dass sich Benutzer nicht an jedem IT-System mit einem anderen Passwort ausweisen müssen, sondern dass sie sich auch bei großen heterogen Netzen ausschließlich am ersten benutzten IT-System authentisieren müssen, das diese Informationen dann an alle weiteren IT-Systeme weiterreicht.

Durch hardwarebasierte Einmalpasswortsysteme werden außerdem viele der unter M 2.11 *Regelung des Passwortgebrauchs* aufgeführten Regelungen, die die einzelnen Benutzer beachten müssen, überflüssig, da dies von den Einmalpasswortsystemen übernommen wird.

Ergänzende Kontrollfragen:

- Werden in den eingesetzten Netzen Passwörter unverschlüsselt übertragen?
- Werden Einmalpasswörter eingesetzt?

M 5.35 Einsatz der Sicherheitsmechanismen von UUCP

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator

Das im Standardumfang von Unix-Systemen enthaltene und ebenfalls für andere Betriebssysteme verfügbare Programmpaket UUCP (Unix-to-Unix Copy) erlaubt den Datenaustausch zwischen IT-Systemen und die Ausführung von Kommandos auf entfernten IT-Systemen. Voraussetzung ist lediglich die Kompatibilität der *uucico*-Programme auf den beiden beteiligten Systemen. UUCP ist stark verbreitet, auch wenn seine Bedeutung zurückgegangen ist z.B. durch die Möglichkeit, Rechner über ISDN mittels TCP/IP zu verbinden.

UUCP wird in der Regel zum Austausch von E-Mail und News zwischen Rechnern benutzt (*uucp*). Es ermöglicht auch das Einloggen (*cu*) und das Ausführen von Programmen (*uux*) auf fremden Rechnern.

Es gibt verschiedene UUCP-Varianten: Neben der Implementation von Peter Honeyman, David Nowitz und Brian E. Redman von 1983 (HoneyDanBer UUCP) werden auch häufig das ursprüngliche UUCP-System der AT&T UNIX Version 7, dessen zweite Version aktuell ist (diese UUCP-Implementation wird daher auch Version 2 UUCP genannt) oder das Tahoe-UUCP (das mit BSD 4.3 ausgeliefert wurde) eingesetzt.

Die eingesetzte UUCP-Variante kann an den Dateien im Verzeichnis */usr/lib/uucp* (auf einigen Systemen */etc/uucp*) erkannt werden: Bei Version 2 UUCP findet sich hier die Datei *L.sys*, beim HoneyDanBer UUCP die Datei *Systems*.

Version 2 UUCP hat gravierende Sicherheitsprobleme (Fehler in *uucico*, Gefahr fehlerhafter Konfiguration durch die komplizierte Form der sicherheitsrelevanten Administrationsdateien). Sie sollte daher nicht benutzt werden, stattdessen sollte das HoneyDanBer UUCP eingesetzt werden.

Allgemein sollten folgende Sicherheitsfragen beim Einsatz von UUCP bedacht werden:

- Die Administration von UUCP setzt eine intensive Beschäftigung mit den Konfigurationsmöglichkeiten und den zugehörigen Dateien voraus. Es muss berücksichtigt werden, dass es zwischen den UUCP-Paketen der verschiedenen Unix-Derivate Abweichungen geben kann, auch wenn diese auf dem HoneyDanBer UUCP basieren.
- Für die Administration der UUCP-Dateien, -Programme und -Verzeichnisse gelten dieselben Anforderungen wie für die Administration von Systemdateien und -verzeichnissen (siehe M 2.25 *Dokumentation der Systemkonfiguration*, M 2.31 *Dokumentation der zugelassenen Benutzer und Rechteprofile*, M 4.19 *Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen*).
- Auf den meisten Systemen gibt es einen Benutzer namens *uucp*. Diesem Benutzer gehören die UUCP-Dateien, -Programme und -Verzeichnisse. Es ist sicherzustellen, dass dieser Account ein Passwort gemäß den Vorgaben der Maßnahme M 2.11 *Regelung des Passwortgebrauchs* hat.

Das Heimatverzeichnis für den Benutzer *uucp* darf nicht das öffentliche Verzeichnis */usr/spool/uucppublic* sein, sondern ein eigenes, auf das nur der Benutzer *uucp* Zugriff hat.

- Für jedes IT-System, das sich per UUCP am lokalen IT-System anmelden können soll, muss in der */etc/passwd* eine eigene Benutzer-Kennung und ein Passwort eingetragen werden. Als UID darf nicht die des Benutzers *uucp* gewählt werden, sondern für jedes entfernte IT-System eine beliebige individuelle UID.
- UUCP-Passwörter werden bei Kommunikationsanforderungen unverschlüsselt übertragen und sind in der entsprechenden UUCP-Konfigurationsdatei für Anforderungen an entfernte Rechner unverschlüsselt gespeichert. Je nach Anwendung und Umgebung (insbesondere bei Benutzung von Weitverkehrsnetzen) sind entsprechende Sicherheitsmaßnahmen wie z. B. der Einsatz von Einmalpasswörtern zu ergreifen.

Für die Benutzung von UUCP müssen verschiedene Konfigurationsdateien eingerichtet werden. Alle Einstellungen sollten dokumentiert und Abweichungen der im Folgenden vorgeschlagenen Einstellungen kurz begründet werden, damit später nachvollziehbar ist, wozu diese Änderung notwendig war.

Die Verwaltung der folgenden Dateien muss besonders sorgfältig gehandhabt werden, da sie sicherheitskritische Informationen enthalten. Sie befinden sich im Verzeichnis */usr/lib/uucp* bzw. */etc/uucp*). Auf diese Verzeichnisse darf nur der Benutzer *uucp* schreibenden Zugriff haben.

- *Systems*: Diese Datei enthält die für einen Verbindungsaufbau mit entfernten IT-Systemen benötigten Informationen. Hier können für jedes einzelne IT-System die Zeiträume festgelegt werden, in denen die Übertragung per UUCP zugelassen ist. Diese Zeiträume sind möglichst eng zu fassen. Die Datei enthält außerdem die Telefonnummern und Login-Sequenzen der IT-Systeme, zu denen per UUCP eine Verbindung aufgebaut werden kann. Auf *Systems* darf nur der Eigentümer *uucp* lesenden Zugriff haben, da hier auch die Passwörter für die entfernten IT-Systeme eingetragen sind.
- *Permissions*: Hier werden Zugriffsrechte für entfernte Systeme festgelegt. Bei Auslieferung sind in *Permissions* keine IT-Systeme eingetragen, d. h. über UUCP sind keine Zugriffe möglich. Für jeden Rechner, der anrufen und sich einloggen darf, und für jeden Rechner, der angerufen werden darf, müssen hier Einstellungen zur Festlegung der jeweilig notwendigen Zugriffsrechte und anderer Bedingungen vorgenommen werden. Die Zugriffsrechte für die IT-Systeme, die vom lokalen IT-System angerufen werden, werden unter den auf MACHINE folgenden Einträgen spezifiziert, die für die anrufenden IT-System unter den auf LOGNAME folgenden. Durch Ausnutzung dieser Konfigurationsmöglichkeiten kann die Sicherheit beachtlich erhöht werden.

  Mit dem Kommando *uucheck -v* sollten die in der Datei *Permissions* gesetzten Optionen regelmäßig überprüft werden. Die Optionen sollten wie folgt gesetzt sein:

REQUEST

Diese Option sollte auf NO (Default-Wert) gesetzt sein, um entfernten Systemen das Lesen lokaler Dateien zu verbieten.

COMMANDS

Hier darf auf keinen Fall ALL eingetragen sein, es dürfen nur die Kommandos zugelassen werden, die nötig sind wie *rnews* oder *rmail*. Die Kommandos sollen mit vollem Pfadnamen angegeben werden.

WRITE/READ

Wenn diese Optionen nicht angegeben sind, ist der schreibende bzw. lesende Zugriff ausschließlich auf das Verzeichnis */usr/spool/uucppublic* möglich.

Falls hiermit Verzeichnisse angegeben werden, auf die zugegriffen werden darf, ist zu dokumentieren, auf welche und warum. Auf keinen Fall darf hier das Root-Verzeichnis oder das Verzeichnis, in dem sich die UUCP-Konfigurationsdateien befinden, eingetragen sein.

NOWRITE/NOREAD

Hiermit werden Ausnahmen zu den mit WRITE/READ festgelegten Optionen festgelegt. Verzeichnisse mit sensitiven Inhalten sollten hier generell aufgeführt werden. Dann kann nicht dadurch, dass das Setzen von Restriktionen vergessen wird, von entfernten IT-Systemen auf solche Verzeichnisse zugegriffen werden, wenn darüberliegende Verzeichnisse über READ/WRITE freigegeben werden.

PUBDIR

Hiermit kann statt */usr/spool/uucppublic* ein anderes öffentliches UUCP-Verzeichnis angegeben werden. Bei UUCP-Kommunikation mit mehreren IT-Systemen sollte für jedes IT-System ein eigenes UUCP-Verzeichnis angegeben werden.

CALLBACK

Wenn CALLBACK auf YES gesetzt ist, muss das lokale IT-System das anrufende IT-System zurückrufen, bevor ein Datenaustausch stattfinden kann. Dies macht natürlich nur für LOGNAME Einträge Sinn. Es sollte zwischen den Kommunikationspartnern abgesprochen sein, welche einen CALLBACK aktiviert.

MYNAME

Wenn MYNAME=*name* gesetzt ist, identifiziert sich das lokale System beim Aufbau einer UUCP-Verbindung beim entfernten System nicht mit dem Rechnernamen, sondern mit *name*. Diese Möglichkeit sollte benutzt werden, um sich mit

einem Namen identifizieren zu können, der nur speziell für diese Verbindung benutzt wird und daher nicht so leicht herausgefunden werden kann.

VALIDATE

Wenn VALIDATE=*namen* gesetzt ist, können nur die unter *namen* aufgeführten IT-Systeme über die unter LOGNAME angegebenen Systemnamen eine Verbindung aufbauen. Bei dieser Option muss unbedingt ein Eintrag vorhanden sein, da sonst ein entferntes IT-System eine Maskerade durchführen könnte, indem über MYNAME ein anderer Rechnername vorgespiegelt wird.

SENDFILES

Hier sollte die Voreinstellung (SENDFILE=CALL) beibehalten werden, da dann lokal in der Queue befindliche Aufträge nur nach extern übertragen werden, wenn das lokale IT-System die Verbindung aufgebaut hat.

- Die Datei */usr/lib/uucp/remote.unknown* des HoneyDanBer UUCP wird ausgeführt, wenn ein unbekanntes, also ein nicht in der Datei *Systems* eingetragenes IT-System einen Verbindungsaufbau versucht. Es protokolliert den Versuch und weist ihn ab. Wenn *remote.unknown* nicht ausführbar ist, geht das lokale IT-System auf alle Verbindungsanforderungen entfernter IT-Systeme ein. Es muss daher darauf geachtet werden, dass *remote.unknown* stets ausführbar ist. *remote.unknown* ist je nach Unix-System als ausführbares Shellskript oder als C-Programm realisiert. Falls *remote.unknown* auf dem lokalen IT-System als Shellskript realisiert ist, sollte es aus Sicherheitsgründen durch ein Programm ersetzt werden. Sonst besteht die Gefahr, dass ein anrufendes IT-System ein Kommando wie "cat < /etc/passwd" als Systemnamen einträgt, das dann zur Ausführung gelangen kann.
- Für UUCP gibt es einige Cleanup-Shellskripte, die automatisch über den *crontab*-Dämon ausgeführt werden. Dies darf nicht von *root* inititiert werden, wie es auf vielen Systemen üblich ist, sondern muss durch den Benutzer *uucp* erfolgen.

Bei der Benutzung von UUCP werden automatisch verschiedene Protokollierungsdateien angelegt. Beim HoneyDanBer UUCP finden sich diese in Unterverzeichnissen von */usr/spool*. Hier werden erfolgreiche und abgelehnte Verbindungsversuche festgehalten, die gesendeten und empfangenen Datenmengen, Fehlermeldungen und Datentransferstatistiken. Diese Protokollierungsdateien müssen regelmäßig ausgewertet werden (siehe auch M 4.25 *Einsatz der Protokollierung im Unix-System*).

Ergänzende Kontrollfragen:

- Wurde der Administrator im Umgang mit UUCP geschult?
- Sind Handbücher über UUCP vorhanden?
- Welche UUCP-Variante wird eingesetzt?
- Sind die Einstellungen der Konfigurationsdateien dokumentiert?
- Werden die UUCP-Protokollierungsdateien regelmäßig ausgewertet?

M 5.36 Verschlüsselung unter Unix und Windows NT

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Benutzer, Administrator

Verschlüsselung und/oder digitale Signaturen

Bei der Übertragung von Nachrichten über ein Netz sollten sich alle Kommunikationspartner darüber im Klaren sein, dass unverschlüsselte Nachrichten während ihres gesamten Weges unbemerkt gelesen, geändert bzw. abgefangen werden können. Daher ist zu überlegen, ob die Nachrichten verschlüsselt und / oder digital signiert werden sollten.

In vielen Unix-Systemen stehen Verschlüsselungsprogramme wie crypt zur Verfügung, bei anderen sind die Verschlüsselungsprogramme beim Export aus den USA entfernt worden.

Public-Domain-Programme nutzen

Unter Windows NT und Unix stehen verschiedene Verschlüsselungsprogramme von kommerziellen Software-Anbietern zur Verfügung. Darüber hinaus können auch viele Public-Domain-Programme für Unix, DOS und Windows, wie z. B. das weiter unten genannte Programm PGP auch unter Windows NT eingesetzt werden.

Zur Verschlüsselung von Nachrichten stehen u. a. mehrere Public-Domain-Verschlüsselungsprogramme betriebssystemübergreifend zur Verfügung:

DES ist ein einfaches Verschlüsselungsprogramm, das auf dem gleichnamigen Algorithmus basiert. Zum Entschlüsseln der Nachricht muss der Empfänger denselben Schlüssel verwenden, den der Sender zum Verschlüsseln benutzt hat.

PGP (Pretty Good Privacy) ist ein verbreitetes Verschlüsselungsprogramm, das auf den Algorithmen RSA (für das Schlüsselmanagement) und IDEA (zur Datenverschlüsselung) basiert. Mit PGP können Nachrichten zum einen verschlüsselt und zum anderen zum Schutz vor Veränderungen mit einer digitalen Signatur versehen werden (siehe auch M 5.63 *Einsatz von GnuPG oder PGP*).

Die Unix-Sourcen von PGP sind beispielsweise von dem FTP-Server *ftp.de.uu.net (192.76.144.75)* oder dem Mailserver *archive-server@de.uu.net* beziehbar.

Schlüssel nicht als Argument von Programmen übergeben

Die Unix-Standard-Editoren ed, ex und vi können in einem Verschlüsselungsmodus benutzt werden, so dass Texte direkt bei der Erstellung verschlüsselt werden. Dabei wird im Allgemeinen das Verschlüsselungsprogramm crypt benutzt. Es ist darauf zu achten, dass der Schlüssel nie als Argument für den Kommandoaufruf benutzt wird, da er sonst, z. B. mit dem Kommando ps, ausgespäht werden kann.

leicht zu brechende Verfahren vermeiden

Viele Mailprogramme enthalten ebenfalls Optionen zur Verschlüsselung der Nachrichten. Hier ist zu überprüfen, welche Verfahren zur Verschlüsselung eingesetzt werden. In vielen Fällen werden hier nur leicht zu brechende Verfahren eingesetzt. Die Benutzung solcher Verschlüsselungsverfahren erhöht auf jeden Fall den Schutz der Nachricht, es sollte aber überlegt werden, höherwertige Verfahren wie DES oder RSA einzusetzen.

Die Sicherheit der Verschlüsselung hängt von drei verschiedenen Punkten zentral ab:

- Der verwendete Verschlüsselungsalgorithmus muss so konstruiert sein, dass es ohne Kenntnis des verwendeten Schlüssels nicht möglich ist, den Klartext aus dem verschlüsselten Text zu rekonstruieren. Nicht möglich bedeutet dabei, dass der erforderliche Aufwand zum Brechen des Algorithmus bzw. zum Entschlüsseln in keinem Verhältnis steht zum dadurch erzielbaren Informationsgewinn.

Klartext nicht rekonstruierbar

- Der Schlüssel ist geeignet zu wählen. Nach Möglichkeit sollte ein Schlüssel zufällig erzeugt werden. Wenn es möglich ist, einen Schlüssel wie ein Passwort zu wählen, sollten die diesbezüglichen Regeln aus M 2.11 *Regelung des Passwortgebrauchs* beachtet werden.

Schlüssel geeignet wählen

- Der verschlüsselte Text und die Schlüssel dürfen nicht zusammen auf einem Datenträger gespeichert werden. Dies kann einfach dadurch erreicht werden, dass der Schlüssel schriftlich fixiert und anschließend wie eine Scheckkarte im Portemonnaie aufbewahrt wird. Werden die Schlüssel auf Disketten gespeichert, so sollten die Disketten getrennt vom IT-System aufbewahrt werden.

Chiffrat und Schlüssel trennen

Ergänzende Kontrollfragen:

- Werden die Benutzer im Umgang mit den Verschlüsselungsprodukten geschult?
- Welche Verschlüsselungsverfahren werden eingesetzt?
- Werden Daten und Schlüssel getrennt aufbewahrt?

M 5.37 Einschränken der Peer-to-Peer-Funktionalitäten in einem servergestützten Netz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Werden in einem servergestützten Netz auf Clients Peer-to-Peer-Dienste aktiviert, so werden dadurch neue Kommunikationsmöglichkeiten geschaffen, die auf dem Server nicht protokolliert werden.

Peer-to-Peer-Dienste sind in servergestützten Netzen nicht sinnvoll!

In einer solchen Konstellation ist der Parallelbetrieb der beiden Netzstrukturen nicht sinnvoll, da die gewünschte Funktionalität im Allgemeinen vom Server übernommen werden kann. Daher sollte in einem servergestützten LAN auf eine Installation der Peer-to-Peer-Funktionalität ganz verzichtet werden. Der Administrator sollte im Einzelfall entscheiden, ob auf speziellen Clients Peer-to-Peer-Dienste freigeschaltet werden, beispielsweise die Funktionalitäten "Dateifreigabe" und "Netz-DDE-Freigabe" unter Windows. Druckdienste auf Clients können in bestimmten Fällen eine sinnvolle Ergänzung sein.

Unter Windows NT/2000/XP können nur Administratoren Ressourcen zum Netzzugriff (unter Verwendung des Dateimanagers bzw. Explorers) freigeben. Vor einer derartigen Freigabe ist zu prüfen, ob sie mit den festgelegten Sicherheitsstrategien zu vereinbaren ist (siehe auch M 2.67 *Festlegung einer Sicherheitsstrategie für Peer-to-Peer-Dienste*, M 2.91 *Festlegung einer Sicherheitsstrategie für das Windows NT Client-Server-Netz*, M 2.228 *Festlegen einer Windows 2000 Sicherheitsrichtlinie* und M 2.325 *Planung der Windows XP Sicherheitsrichtlinie*).

Ähnliches gilt für Clients unter Unix bzw. Linux. Auch hier sind für die Bereitstellung von Ressourcen im Netz in der Regel Administrator-Rechte erforderlich.

Ergänzende Kontrollfragen:

- Wer hat entschieden, ob Peer-to-Peer-Funktionen in einem servergestützten Netz zum Einsatz kommen sollen?

M 5.38 Sichere Einbindung von DOS-PCs in ein Unix-Netz

Diese Maßnahme ist mit Version 2006 entfallen.

M 5.39 Sicherer Einsatz der Protokolle und Dienste

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Die folgenden kurzen Beschreibungen häufig im Internet verwendeter Protokolle und Dienste sollen als Hinweis dienen, welche Informationen von diesen Protokollen übertragen werden und somit für eine Filterung durch ein Sicherheitsgateway zur Verfügung stehen. Des weiteren ist kurz beschrieben, welche Randbedingungen beim Einsatz der verschiedenen Protokolle und Dienste zu beachten sind.

Grundlegende Protokolle der tieferen Schichten des ISO/OSI Schichtenmodells

IP

Das Internet Protocol (IP) ist das Protokoll, auf dem praktisch alle gebräuchlichen Protokolle in lokalen Netzen aufbauen. IP ist ein verbindungsloses Protokoll. Ein IP-Header enthält u. a. zwei 32-Bit Adressen (IP-Adressen) für Ziel und Quelle der kommunizierenden Rechner.

Da die IP-Adressen leicht gefälscht werden können (siehe auch G 5.48 *IP-Spoofing*), können sie nur in ganz bestimmten Topographien zur Authentisierung benutzt werden, also nur wenn sichergestellt ist, dass die Adressen nicht geändert werden können. Beispielsweise dürfen Pakete, die von außen kommen, aber als Quelladresse eine Adresse aus dem zu schützenden Netz haben, von dem Sicherheitsgateway nicht durchgelassen werden.

ARP

Das Address Resolution Protocol (ARP) dient dazu, zu einer 32-Bit großen IP-Adresse die zugehörige 48-Bit lange MAC-Adresse ("Media Access Control", auch Hardware- oder Ethernet-Adresse genannt) zu finden. Jeder Rechner führt für andere Stationen in seiner Broadcast-Domain eine Tabelle, in der die Zuordnung zwischen IP- und Hardware-Adressen gespeichert ist. Falls in dieser Tabelle kein entsprechender Eintrag gefunden wird, wird ein ARP-Broadcast-Paket mit der IP-Adresse ausgesandt, zu der die MAC-Adresse gesucht wird. Der Rechner mit dieser IP-Adresse sendet dann ein ARP-Antwort-Paket mit seiner MAC-Adresse zurück. ARP-Antwort-Pakete sind nicht manipulationssicher ("ARP-Spoofing", siehe auch G 5.112 *Manipulation von ARP-Tabellen*).

ICMP

Das Internet Control Message Protocol (ICMP, spezifiziert in RFC 792) hat die Aufgabe, Fehler- und Diagnoseinformationen für IP zu transportieren. Es wird intern von IP, TCP oder UDP angestoßen und verarbeitet. ICMP kennt eine Anzahl verschiedener sogenannter Nachrichtentypen für verschiedene Zwecke.

Je nach Einsatzszenario sollten bestimmte ICMP Nachrichtentypen selektiv zugelassen beziehungsweise blockiert werden. Zur Behandlung von ICMP am Sicherheitsgateway siehe M 5.120 *Behandlung von ICMP am Sicherheitsgateway*.

Routing Protokolle

Routing Protokolle wie RIP (Routing Information Protocol) oder OSPF (Open Shortest Path First) dienen dazu, Veränderungen der Routen zwischen zwei vernetzten Systemen an die beteiligten Systeme weiterzuleiten und so eine dynamische Änderung der Routing-Tabellen zu ermöglichen. Es ist leicht möglich, falsche RIP-Pakete zu erzeugen und somit unerwünschte Routen zu konfigurieren. Dynamisches Routing sollte daher nur in ganz bestimmten Topographien angewendet werden.

Keine Routing-Protokolle über das Sicherheitsgateway

Am Sicherheitsgateway sollten Routing-Protokolle nur im unbedingt notwendigen Umfang eingesetzt werden. Wo dies möglich ist sollten nur sichere Routing-Protokolle eingesetzt werden. Mehr Informationen finden sich in M 5.112 *Sicherheitsaspekte von Routing-Protokollen*.

UDP

Das User Datagram Protocol (UDP) ist ein verbindungsloses Protokoll der Transportschicht. Es gibt keine Transportquittungen oder andere Sicherheitsmaßnahmen für die Korrektheit der Übertragung. Der Header enthält (analog zu TCP) unter anderem zwei 16-Bit Portnummern, die aber unabhängig von den bei TCP benutzten Portnummern sind. Da sie leicht gefälscht werden können, können sie nur in ganz bestimmten Topographien zur Authentisierung benutzt werden.

Da in der Protokolldefinition keine Unterscheidung zwischen einem Verbindungsaufbau und einer Datenübertragung vorgesehen ist, muss diese Unterscheidung von einer Komponente des Sicherheitsgateways übernommen werden. Es muss eine Kontrolle über den Zustand der Verbindung möglich sein, und es muss möglich sein, die Zugehörigkeit eines Paketes zu einer Verbindung eindeutig festzustellen.

Dies kann z. B. erreicht werden, indem bei einem UDP-Verbindungsaufbau der Zielport gespeichert und temporär freigegeben wird, Antwortpakete nur zu diesem Port durchgelassen werden und nach der Beendigung der Verbindung oder nach einem Timeout der Port wieder gesperrt wird.

Protokolle der Anwendungsschicht

DNS

Der Domain Name Service (DNS) dient zur Umsetzung von Rechnernamen in IP-Adressen und umgekehrt und stellt ferner Informationen über im Netz vorhandene Rechnersysteme zur Verfügung. DNS kann sowohl über TCP als auch über UDP abgewickelt werden, der Server benutzt bei beiden Träger-Protokollen standardmäßig den Port 53. Meist wird UDP als Trägerprotokoll verwendet.

Die übertragenen Informationen sind nicht durch kryptographische Verfahren geschützt, so dass durch gefälschte Daten Spoofing-Angriffe möglich sind (siehe auch G 5.78 *DNS-Spoofing*). Dies sollte insbesondere bei DNS-Antworten aus dem Internet berücksichtigt werden.

Prinzipiell muss beachtet werden, dass alle von DNS zur Verfügung gestellten Informationen missbraucht werden können.

Zur Integration von DNS in ein Sicherheitsgateway erforderlich (siehe auch M 2.77 *Integration von Servern in das Sicherheitsgateway* und M 5.118 *Integration eines DNS-Servers in ein Sicherheitsgateway* .

SMTP

Das Simple Mail Transfer Protocol (SMTP) wird für die Übertragung von E-Mail benutzt. SMTP-Server (Mail-Server, auch Mail Transport Agents (MTAs) genannt) benutzen standardmäßig den TCP-Port 25. SMTP, das im RFC 821 definiert wird, besteht aus einer geringen Zahl von Kommandos, die teilweise aus Sicherheitssicht bedenklich sind.

Mit den Befehlen *VRFY* und *EXPN* können beispielsweise interne Informationen über Benutzer abgerufen werden, daher sollte die Verwendung dieser Befehle nur innerhalb des geschützten Netzes erlaubt werden. Für nicht vertrauenswürdige Benutzer, insbesondere für Anfragen aus dem Internet, sind *VRFY* und *EXPN* entweder am ALG (Application-Level-Gateway) oder direkt auf dem MTA (Mail Transport Agent, Mail-Server) zu sperren.

Idealerweise sollte ein Sicherheitsgateway in der Lage sein, SMTP-Verbindungen zwischen vertrauenswürdigen Benutzern zu verschlüsseln. Sinnvoll ist dies aber nur dann, wenn ein starker Authentisierungsmechanismus benutzt wird.

HTTP

Das Hypertext Transfer Protokoll (HTTP) wird für die Übertragung von Daten zwischen WWW-Clients (meist Webbrowsern) und Webservern benutzt. HTTP und diverse Erweiterungen werden in einer Reihe von RFCs definiert, der RFC 2616, in dem die aktuelle Variante HTTP 1.1 spezifiziert wird, enthält eine Reihe von Referenzen auf ältere Dokumente. Standardmäßig benutzt ein Webserver den TCP-Port 80.

HTTP ist ein Klartextprotokoll, das keine Unterstützung für eine sichere Authentisierung und keine Gewährleistung für die Vertraulichkeit und Integrität der übertragenen Daten bietet. Dies sollte bei der Entscheidung, welche Transaktionen über HTTP abgewickelt werden können, berücksichtigt werden.

Weitere Informationen über Maßnahmen im Zusammenhang mit HTTP finden sich in M 4.222 *Festlegung geeigneter Einstellungen von Sicherheitsproxies* und M 4.100 *Sicherheitsgateways und aktive Inhalte*.

HTTPS

HTTPS (HTTP über SSL bzw. HTTP über TLS) ist eine Variante von HTTP, bei der Authentisierung und Datenübertragung durch Verschlüsselung und Zertifikate geschützt werden können. HTTPS wird im RFC 2818 spezifiziert. Meist benutzt ein Webserver, der HTTPS unterstützt, den TCP-Port 443.

Beim Einsatz von HTTPS muss beachtet werden, dass TLS auch einen Betriebsmodus kennt, in dem keine Verschlüsselung stattfindet. Bei entsprechenden Sicherheitsanforderungen sollte am HTTPS-Proxy verhindert werden, dass entsprechende Verbindungen aufgebaut werden können.

Weitere Informationen finden sich in M 4.222 *Festlegung geeigneter Einstellungen von Sicherheitsproxies* und M 4.100 *Sicherheitsgateways und aktive Inhalte*, sowie in M 5.66 *Verwendung von SSL*.

Secure Shell / Secure Copy

Das Secure Shell (SSH) Protokoll erlaubt den Aufbau einer gesicherten Kommandozeilen-Verbindung zu einem entfernten Rechner. Das SSH-Protokoll erlaubt eine gesicherte Authentisierung mit einer Reihe verschiedener Authentisierungsmechanismen (unter anderem über Benutzername und Passwort, mit speziellen Zertifikaten, über eine zentral verwaltete PKI-Infrastruktur oder über Kerberos). SSH eignet sich daher als Ersatz für Telnet. Wo immer möglich sollte Telnet durch SSH ersetzt werden. Standardmäßig benutzt ein SSH-Server den TCP-Port 22.

Zur SSH-Protokollfamilie gehört auch das Protokoll SCP (Secure Copy Protocol), das zur Übertragung von Dateien die Authentisierungs- und Verschlüsselungsmechanismen von SSH benutzt. SCP stellt eine sichere Alternative zu FTP dar.

Für SSH existiert eine Reihe verschiedener Implementierungen für praktisch alle gebräuchlichen Betriebssysteme, sowie zusätzlich betriebssystemunabhängige Implementierungen beispielsweise in Java. Die verschiedenen Implementierungen unterscheiden sich jedoch teilweise bei der Anzahl der unterstützten Authentisierungsmechanismen und in anderen Details.

Tunneling

Die meisten SSH-Clients bieten zusätzlich die Möglichkeit, andere Protokolle über eine bestehende SSH-Verbindung zu "tunneln" und so die Nachteile beispielsweise von Klartextprotokollen zu vermeiden. Andererseits stellt diese Option auch ein gewisses Risiko dar, da auf diese Weise Datenübertragungen "versteckt" werden können. Beim Einsatz von SSH sollte daher sorgfältig geprüft werden, mit welchen Kommunikationspartnern Verbindungen zugelassen werden. Gegebenenfalls sollte ein entsprechender Sicherheitsproxy eingesetzt werden, der die verschlüsselte Verbindung am Sicherheitsgateway unterbricht.

Die ursprüngliche Version des SSH-Protokolls (ssh1) besitzt einen Designfehler, der einen Man-in-the-Middle Angriff zulässt. Aus diesem Grund wurde eine neue Version des Protokolls (ssh2) entwickelt, die diese Schwachstelle beseitigt. Die Protokollversion ssh1 sollte zumindest über öffentliche Netze hinweg nicht mehr verwendet werden. Wird für SSH ein Sicherheitsproxy auf dem Sicherheitsgateway eingesetzt, so sollte der Proxy die Möglichkeit bieten, ssh2-Verbindungen zu erzwingen und keine ssh1-Verbindungen zuzulassen.

Telnet

Das Telnet-Protokoll wird in RFC 854 spezifiziert. Es erlaubt (analog zu SSH) den Aufbau einer Terminalsitzung auf einem entfernten Rechner. Telnet ist ein Klartextprotokoll, das keine Mechanismen zur Sicherung der Authentisierungsinformationen und der übertragenen Daten und Kommandos bietet. Ein Telnet-Server benutzt standardmäßig den TCP-Port 23.

Telnet durch SSH ersetzen

Da Telnet einen vollständigen Kommandozeilenzugriff auf einen Rechner erlaubt, jedoch keine Sicherungsmechanismen bietet, sollte Telnet wo immer

möglich durch SSH ersetzt werden. Alternativ können Telnet-Verbindungen über SSH getunnelt werden. Falls aus zwingenden Gründen ein Ersatz von Telnet durch SSH oder ein Tunneln nicht möglich ist, kann im internen Netz weiterhin Telnet eingesetzt werden. Dabei sollten jedoch die erlaubten Kommunikationsverbindungen über entsprechende Paketfilterregeln auf das unbedingt notwendige Maß beschränkt werden. Für Administrationstätigkeiten sollte Telnet allenfalls noch in einem besonders abgeschotteten Administrationsnetz eingesetzt werden.

Kein Telnet über unsichere Netze

Telnet-Verbindungen können von einem Angreifer übernommen werden, der Zugriff auf eine Netzkomponente besitzt, über die die betreffende Verbindung läuft (siehe G 5.89 *Hijacking von Netz-Verbindungen*). Auf ungesicherten Verbindungen (öffentliche Netze) sollte Telnet daher auch dann nicht mehr eingesetzt werden, wenn der eingesetzte Telnet-Server erweiterte Authentisierungsmechanismen wie Einmalpasswörter unterstützt.

FTP

Das File Transfer Protocol (FTP) wird im RFC 959 spezifiziert. Es ermöglicht den Austausch von Dateien zwischen entfernten Rechnern. Wie Telnet ist FTP ein Klartextprotokoll, das keine Sicherung der übertragenen Authentisierungsinformationen und Daten bietet.

Bei Benutzung von FTP werden zwei Verbindungen aufgebaut, wobei die Kommandos über den TCP-Port 21 übertragen werden und die Daten über TCP-Port 20. Telnet definiert eine Anzahl an Standard-Befehlen, mit denen Art und Format der Datenübertragung gesteuert werden und die einem FTP Client eine Navigation im Dateibaum eines FTP-Servers erlauben. Für das Sicherheitsgateway sind diese Standardbefehle relevant, da nur diese tatsächlich übertragen werden.

Eine FTP-Kommandoverbindung wird vom Client zum Port 21 des Servers aufgebaut. Für die Datenverbindungen gibt es bei FTP zwei Betriebsmodi, den *Active* und den *Passive Mode*. Beim *Active Mode* baut der FTP-Server die Datenverbindung zum Client auf, beim *Passive Mode* wird auch die Datenverbindung vom Client aus aufgebaut.

Bei FTP stets den Passive Mode verwenden

Der *Active Mode* stellt eine Sicherheitslücke dar, da sich ein Angreifer als Server ausgeben kann und auf diese Weise die Möglichkeit bekommen würde, eine Verbindung ins interne Netz aufzubauen. Falls FTP eingesetzt wird, so sollte stets der *Passive Mode* verwendet werden, bei dem sowohl die Kommando- als auch die Datenverbindung vom zu schützenden ins externe Netz stattfinden.

Alle Befehle, die Dateien oder Verzeichnisse manipulieren oder lesen (*CWD, CDUP*, *RETR, STOR, DELE, LIST, NLIST*), müssen an eine entsprechende Rechteverwaltung gekoppelt sein. Zugriffe nicht vertrauenswürdiger Benutzer werden damit auf bestimmte Dateien eingeschränkt oder ganz unterbunden. Dies setzt einen starken Authentisierungsmechanismus voraus.

Auch der Befehl *SYST*, mit dem ein Client nach der Betriebssystem-Version des Servers fragt, sollte an eine Rechteverwaltung gekoppelt sein bzw. für nicht vertrauenswürdige Benutzer gesperrt werden.

Ferner muss es möglich sein, die Übertragung der Dateien, der Verzeichnisinformationen und der Passwörter zu verschlüsseln.

FTP möglichst durch SCP ersetzen

FTP sollte nicht zur Übertragung schutzbedürftiger Daten über öffentliche Netze verwendet werden. Sollen schutzbedürftige Daten über eine externe FTP-Verbindung übertragen werden, müssen sie auf andere Weise geschützt (beispielsweise verschlüsselt) werden. Nach Möglichkeit sollte FTP durch ein sicheres Protokoll wie SCP ersetzt werden.

Häufig wird FTP eingesetzt, um Dateien von öffentlich zugänglichen Servern abzurufen. Sofern dafür keine Authentisierungsinformationen benutzt werden, die auch auf anderen Systemen verwendet werden (beispielsweise beim *anonymous FTP*), ist dies so lange unkritisch, wie keine Anforderungen an die Integrität und Authentizität der abgerufenen Daten gestellt werden (beispielsweise Abruf von Informationsmaterial). Sind die Integrität und Authentizität der Daten wichtig (beispielsweise beim Herunterladen von Programmpaketen, Patches oder wichtiger Dokumente), so sollten vom Anbieter digitale Signaturen zur Verfügung gestellt werden, mit denen die Unverfälschtheit der Daten geprüft werden kann.

POP3 und IMAP

Die Protokolle POP3 (Post Office Protocol Version 3, spezifiziert in RFC 1939) und IMAP (Internet Message Access Protocol, spezifiziert in RFC 3501) werden von E-Mail-Clients eingesetzt, um E-Mails von einem Mailserver abzurufen (POP3) oder auf dem Mailserver zu verwalten (IMAP).

Die Standard-Ports für diese Protokolle sind die Ports 110/TCP (POP3) und 143/TCP (IMAP). Beide Protokolle sind Klartextprotokolle und sollten daher nicht über öffentliche Netze verwendet werden. Für beide Protokolle existieren Varianten, bei denen die Verbindungen durch Verschlüsselung (SSL bzw. TLS) gesichert werden: POP3s (Standard-Port 995/TCP) und IMAPs (Standard-Port 993/TCP).

Auch wenn nur im internen Netz E-Mails abgerufen werden sollen wird empfohlen, möglichst nur die abgesicherten Varianten POP3s oder IMAPs einzusetzen. Sollen E-Mails von einem externen POP3 oder IMAP-Server (etwa bei einem E-Mail-Provider) abgerufen werden, so sollten unbedingt die abgesicherten Versionen der Protokolle verwendet werden, gegebenenfalls mit einer Unterbrechung der verschlüsselten Verbindung an einem entsprechenden Sicherheitsproxy.

Weitere Dienste

Verteilte Dateisysteme

Verteilte Dateisysteme, bei denen Daten nicht lokal auf einem Rechner, sondern auf einem Dateiserver gespeichert sind, auf den über das Netz zugegriffen wird, existieren seit langem und sind aus der IT-Welt nicht mehr wegzudenken.

Das verbreitetste Beispiel ist die Laufwerksfreigabe unter Microsoft Windows, das zu Grunde liegende Protokoll ist SMB / CIFS (Server Message Block / Common Internet File System). Für dieses Protokoll existiert mit SAMBA auch eine Implementierung für diverse Unix-Derivate. In der Unix-

Welt werden verteilte Dateisysteme seit langem über NFS (Network File System) realisiert. Für NFS existieren auch Implementierungen für Windows. Außerdem gibt es eine Reihe anderer verteilter Dateisysteme wie AFS.

Verteilte Dateisysteme sollten nach Möglichkeit nicht über Sicherheitsgateways hinweg eingesetzt werden, da sie eine Reihe von Problemen mit sich bringen (Sicherheit der Authentisierung, Sicherheit der übertragenen Daten), die einen sicheren Einsatz über ein Sicherheitsgateway hinweg schwierig machen.

Ist in Einzelfällen doch ein Zugriff auf ein verteiltes Dateisystem notwendig, so sollte dieser prinzipiell durch eine VPN-Lösung abgesichert werden.

Remote-Desktop Protokolle (Windows Terminal Server, X-Windows etc.)

Sowohl Microsoft Windows als auch das X-Window-System, mit dem unter Unix graphische Oberflächen realisiert werden, bieten die Möglichkeit, einzelne Fenster oder die gesamte Arbeitsoberfläche auch auf einem entfernten Rechner darzustellen.

Ein Remote-Desktop Protokoll, das keine oder nur schwache Sicherheitsfunktionen bietet, sollte auch im internen Netz nur in Ausnahmefällen eingesetzt werden, über das Sicherheitsgateway hinweg sollten Remote-Desktop Protokolle prinzipiell nicht verwendet werden. Muss dies in Ausnahmefällen trotzdem geschehen, so sollten unbedingt zusätzliche Maßnahmen ergriffen werden, etwa der Einsatz eines geeigneten VPN, das eine entsprechend gesicherte Verbindung zur Verfügung stellt.

Streaming-Protokolle

Für die Übertragung von Multimedia-Daten (Audio- und Video-Streaming) existiert eine Reihe von Protokollen mit unterschiedlichen Charakteristiken im Bezug auf Bandbreiten und verwendete Ports. Diese Protokolle sind meist für Sicherheitsgateways nicht unproblematisch, da sie teilweise schlecht über Paketfilterregeln abzusichern sind. Im Zweifelsfall sollte daher auf Streaming-Anwendungen verzichtet werden oder entsprechende Angebote können über gesonderte Internet-PCs (siehe Baustein B 3.210 *Internet-PC*) abgerufen werden.

Voice over IP

Es existieren verschiedene Lösungen, die es ermöglichen, Sprachkommunikation über IP-Netze zu übertragen (*Voice over IP, VoIP*). Bei VoIP-Lösungen sind normalerweise mehrere verschiedene Protokolle notwendig, beispielsweise unterschiedliche Protokolle für die Signalisierung und für die Übertragung der Gesprächsdaten selbst.

VoIP-Lösungen, (beispielsweise solche, die dem H.323 Standard entsprechen) sind für Sicherheitsgateways oft problematisch, da verwendete Ports teilweise dynamisch zwischen Endgeräten ausgehandelt werden und daher keine einfache Absicherung über Paketfilter möglich ist.

Bei VoIP zusätzliche Sicherheitsanalyse

Soll eine VoIP-Lösung eingesetzt werden, bei der auch eine Kommunikation über VoIP mit Gesprächspartnern außerhalb des eigenen Netzes stattfinden soll, so ist in jedem Fall eine zusätzliche Sicherheitsbetrachtung notwendig um zu vermeiden, dass durch die Anforderungen der VoIP-Lösung die

Sicherheit des Netzes dadurch gefährdet wird, dass die Einstellungen des Sicherheitsgateway zu sehr "geöffnet" werden müssen.

NTP

Das in RFC 1305 spezifizierte Network Time Protocol (NTP) dient dazu, von einem Zeitserver ein genaues Zeitsignal zu beziehen.

Wird im internen Netz, von Servern oder von Komponenten des Sicherheitsgateways NTP zur Zeitsynchronisation genutzt, so sollte nach Möglichkeit entweder ein eigener Zeitserver im internen Netz oder im Sicherheitsgateway eingesetzt werden. Gegebenenfalls kann ein NTP-Proxy genutzt werden, der seine Zeitinformationen von einem der zentralen Zeitserver bezieht und der dann für die internen Rechner als Zeitserver agiert. Siehe auch M 4.227 *Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation*.

NNTP

Das in RFC 977 spezifizierte Network News Transfer Protocol (NNTP) wird für die Übertragung von Newsartikeln benutzt. Ein Newsserver benutzt standardmäßig den TCP-Port 119. Wie die meisten anderen "frühen" Internetprotokolle ist auch NNTP ein Klartextprotokoll.

Wird ein interner Newsserver betrieben oder soll vom internen Netz auf einen externen Newsserver zugegriffen werden, so muss das Sicherheitsgateway in der Lage sein, den Transport bestimmter Newsgruppen ganz zu verhindern oder nur für einige Rechner zuzulassen. Es muss sichergestellt werden, dass beim Versenden eigener News keine Informationen über das zu schützende Netz (z. B. die Rechnernamen) ins externe Netz gelangen.

"r-Dienste"

Die so genannten "r-Dienste" wie rlogin, rsh, rcp und andere basieren auf UDP und bieten keine Möglichkeiten für eine sichere Authentisierung und für die Absicherung der Verbindung.

Diese Dienste sollten auch im internen Netz nur noch in Ausnahmefällen benutzt werden. Über ein Sicherheitsgateway hinweg sollten sie keinesfalls eingesetzt werden. Das Sicherheitsgateway sollte entsprechende Pakete blockieren.

Für die meisten Anwendungsfälle bietet SSH einen vollwertigen Ersatz für die "r-Dienste".

Hinweis zu den so genannten "Privilegierten Ports"

Bei einer TCP/IP-Kommunikation baut in der Regel ein Client-Prozess von einem zufälligen Port mit einer Portnummer > 1023 eine Verbindung zu einem Server-Prozess mit einer Portnummer < 1024 (well-known-port) auf. Die Ports mit einer Nummer < 1024 werden auch als privilegierte Ports bezeichnet, da sie beispielsweise unter Unix nur von Prozessen mit Root-Berechtigung benutzt werden dürfen. Diese Einschränkung, dass Ports < 1024 nur von Prozessen mit Root-Berechtigung benutzt werden dürfen, ist aber nur eine Konvention, die auch umgangen werden kann und die ohnehin in dem Fall keine Rolle spielt, wenn ein Angreifer die Kontrolle über einen Rechner

übernommen hat. Daher darf in einem Sicherheitskonzept nicht vorausgesetzt werden, dass tatsächlich alle IT-Systeme ihre privilegierten Ports auf diese Weise schützen. Auch wenn z. B. mit FTP auf die Ports 20 oder 21 zugegriffen wird, darf dies also nicht als sichere Verbindung angesehen werden.

Ergänzende Kontrollfrage:

- Welche Protokolle werden über das Sicherheitsgateway eingesetzt?

M 5.40 Sichere Einbindung von DOS-PCs in ein Windows NT Netz

Diese Maßnahme ist mit Version 2006 entfallen.

M 5.41 Sichere Konfiguration des Fernzugriffs unter Windows NT

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Über RAS (Remote Access Service) können sich Benutzer von entfernten IT-Systemen mit lokalen Windows NT Systemen verbinden. Dafür muss auf dem entfernten IT-System der RAS-Client und auf dem lokalen IT-System, das die Fernverbindung annimmt, der RAS-Server installiert sein. Diese Benutzer können über RAS so arbeiten, als wären sie direkt mit dem Netz verbunden. Die entfernten Clients verwenden dabei Standardprogramme, um auf Ressourcen zuzugreifen. Mit Hilfe des Dateimanagers bzw. Explorers werden beispielsweise Netzlaufwerke und Drucker verbunden. Diese Verbindungen sind permanent, d. h. Benutzer müssen Verbindungen zu Netzressourcen während ihrer Sitzung nicht erneut aufbauen. Als Clients werden die Systeme Windows NT, Windows 95, WfW, MS-DOS und OS/2 unterstützt.

Der Benutzer baut eine Verbindung zum RAS-Server mit Hilfe eines lokalen Modems, X.25 oder einer ISDN-Karte auf. Der RAS-Server, der auf einem Windows NT Server ausgeführt wird, authentisiert den Benutzer und bedient die Sitzungen, bis diese durch den Benutzer oder den Netzadministrator beendet werden. Alle Dienste, die normalerweise einem mit einem LAN verbundenen Benutzer zur Verfügung stehen (Datei- und Druckfreigabe, Datenbankzugriff und Benachrichtigung), sind über die RAS-Verbindung möglich.

Der Zugriff auf RAS wird aus dem Pool sämtlicher Windows NT Benutzerkonten gewährt. Mit Hilfe des Benutzer-Managers können einem einzigen Benutzer, einer Benutzergruppe oder sämtlichen Benutzern die Einwählberechtigung ins lokale Netz erteilt werden. Weiterhin bietet die RAS-Verwaltung eine Option, die den Zugriff auf alle Ressourcen ermöglicht, auf die der RAS-Host im Netz zugreifen kann, bzw. nur auf die lokal auf dem Computer vorhandenen Ressourcen. Dann nutzen die Anwender ihre Domänenanmeldung zum Herstellen der Verbindung über RAS. Wurde die Zugriffsberechtigung des Benutzers vom RAS geprüft, kann er die lokalen Ressourcen oder, falls ihm die Berechtigung dazu erteilt wurde, die Ressourcen in der ganzen Domäne sowie in den vertrauten Domänen nutzen.

Über das *Challenge Handshake Authentication Protocol* (kurz CHAP) vermittelt der Remote Access Server die sicherste der angebotenen Formen verschlüsselter Zugriffsberechtigung, die sowohl vom Server als auch vom Client unterstützt wird. CHAP ermöglicht dem RAS-Server die abwärts gerichtete Aushandlung vom sichersten Verschlüsselungsmechanismus bis zum unsichersten Verfahren mit Klartextübertragung und schützt die in diesem Prozess übertragenen Kennwörter.

CHAP lässt den Einsatz diverser Verschlüsselungsalgorithmen zu. RAS arbeitet insbesondere mit dem kryptographischen Protokoll MD5. RAS greift für die Authentisierung auf DES-Verschlüsselung zurück, wenn sowohl der Client als auch der Server mit RAS arbeiten. Windows NT, Windows für Workgroups sowie Windows 95 handeln bei der Datenkommunikation untereinander immer die DES-verschlüsselte Echtheitsbestätigung aus. Bei Ver-

bindung mit externer RAS-Server- oder Client-Software ist eine Echtheitsbestätigung mit SPAP oder unverschlüsseltem Text möglich, falls das externe Produkt keine verschlüsselte Echtheitsbestätigung unterstützt.

MD5, ein Verschlüsselungsschema, das von diversen PPP-Implementationen für verschlüsselte Echtheitsbestätigungen eingesetzt wird, kann vom Microsoft RAS-Client ausgehandelt werden, wenn eine Verbindung zu anderen RAS-Servern besteht.

PAP arbeitet mit einfachen, unverschlüsselten Kennwörtern und hat damit als für Echtheitsbestätigungen verantwortliches Protokoll am wenigsten zu bieten. Dieses Protokoll wird normalerweise ausgehandelt, wenn die externe Arbeitsstation und der Server sich nicht auf eine Verschlüsselungsform einigen können, die mehr Sicherheit bietet.

Das RAS-Verschlüsselungsprotokoll sollte gemäß der folgenden Tabelle in Abhängigkeit vom zu erreichenden Schutzbedarf so gewählt werden, dass mindestens das dort angegebene Protokoll verwendet wird. Dies kann bedeuten, dass bei hohen Sicherheitsanforderungen die Verwendung von Clients, die das geforderte Protokoll nicht unterstützen, ausgeschlossen werden muss.

Schutzbedarf	*Verschlüsselungsart*	RAS-*Verschlüsselungsprotokoll*
Hoch	Einseitig	CHAP, MD5
Mittel	Beidseitig	SPAP
Niedrig	Unverschlüsselter Text	PAP

Tabelle: RAS-Verschlüsselungsprotokoll in Abhängigkeit vom Schutzbedarf

Datenverschlüsselung schützt Daten und gewährleistet eine sichere Anwählverbindung. Der RAS-Administrator kann den RAS-Server so einstellen, dass die Datenübertragung immer in verschlüsselter Form zu erfolgen hat. Die Benutzer, die an diesem Server angeschlossen sind, verschlüsseln automatisch alle gesendeten Daten.

Hinweis: Diese Option setzt voraus, dass alle angeschlossenen Clients verschlüsseln können. Falls dies gegeben ist, wie z. B. in einem homogenen Windows NT Netz, so ist diese Option auf jeden Fall zu aktivieren.

Die Startoptionen von RAS werden über die Systemsteuerungsoption "*Dienste*" eingestellt, und die Konfigurierung erfolgt über die Systemsteuerungsoption "*Netzwerk*", wobei hier auch die Wahl des Authentisierungsverfahrens geschieht. Durch Wahl der Option "*Nur Microsoft-verschlüsselte Echtheitsbestätigung*" kann die Wahl von CHAP mit MD5 erzwungen werden; zusätzlich lässt sich dann auch die Verschlüsselung des Datenstroms einschalten. Dabei werden die übertragenen Daten in den deutschen Versionen von Windows NT nicht mit DES, sondern mit RC4 verschlüsselt.

RAS unterstützt Sicherheits-Hosts anderer Hersteller, wobei der Sicherheits-Host zwischen den Fernbenutzer und den RAS-Server geschaltet ist. Ein Sicherheits-Host ist ein zusätzlicher Rechner im Netz, der Sicherheitsdienste wie die Unterstützung von Chipkarten anbietet. Ein derartiger Sicherheits-

Host bietet im Allgemeinen eine zusätzliche Sicherheitsstufe, indem er eine Ausweiskarte zur Echtheitsbestätigung anfordert oder ähnliche starke Authentisierungsverfahren unterstützt, bevor der Zugriff auf den RAS-Server erteilt wird.

Als zusätzliche Sicherheitsmaßnahme bietet RAS die Zugriffsüberwachung per Rückruf (*Callback*). Mit dieser Funktion kann der Systemadministrator verlangen, dass ein bestimmter Fernbenutzer von einer vorher festgelegten Stelle aus (z. B. privater Telefonanschluss) anruft oder dieser von einer beliebigen Stelle aus zurückgerufen werden kann. Bei der Zugriffsüberwachung per Rückruf leitet der Anwender einen Anruf ein und stellt die Verbindung mit dem RAS-Server her. Der RAS-Server legt dann auf und ruft einen Augenblick später die vorher zugeteilte Rückrufnummer an. Bei Verwendung des analogen Telefonnetzes sind hierzu Rückrufmodems einzusetzen, während bei Übertragung über ISDN bzw. X.25 (z. B. Datex-P) die Leistungen dieser Netze in Anspruch genommen werden können. Dabei ist allerdings zu beachten, dass die Sicherheit der Partneridentifikation bei Wechsel des X.25-Carriers, also bei grenzüberschreitender Datenübertragung, nicht mehr gewährleistet ist.

Unter RAS wird der Fernzugriff auf das Netz vom Systemadministrator gesteuert. Zusätzlich zu den Dienstprogrammen, die zusammen mit Windows NT Server geliefert werden, bietet das Dienstprogramm RAS-Verwaltung dem Administrator die Möglichkeit, Zugriffsberechtigungen für einzelne Benutzer und/oder Gruppen zu erteilen bzw. wieder zu entziehen. Das bedeutet, dass der Zugriff auf das Netz - obwohl RAS auf einem Computer mit Windows NT Server läuft - jedem Benutzer, der auf das Netz über RAS zugreifen darf, ausdrücklich erteilt werden muss. Dabei gewährleistet dieses Verfahren nicht nur, dass Fernzugriff ausdrücklich erlaubt werden muss, sondern erlaubt zudem das Festlegen von Rückrufbeschränkungen.

RAS bietet ein zusätzliches Maß an Sicherheit. Die RAS-Verwaltung bietet eine Option, die den Zugriff auf alle Ressourcen ermöglicht, die der RAS-Host wahrnimmt, bzw. nur auf die lokal auf dem Computer vorhandenen Ressourcen. Somit kann der Administrator genau steuern, welche Daten einem Fernbenutzer zur Verfügung stehen. Nach Möglichkeit sollte die Erlaubnis zum Durchgriff auf weitere Rechner im Netz nur sehr restriktiv oder überhaupt nicht erteilt werden, um bei einem Durchbrechen der Sicherheitsbarrieren den möglichen Schaden zu begrenzen.

Hinweis: Wird RAS in einer Domäne verwendet, wirken sich Änderungen der RAS-Berechtigung nicht sofort auf alle Server aus. Es kann bis zu 15 Minuten dauern, bis eine Änderung auf alle Server der Domäne repliziert worden ist. Bei Bedarf können die Domänen explizit neu synchronisiert werden, um sicherzustellen, dass ein Benutzer mit entzogenen Berechtigungen bis zur automatischen Replikation der Änderung bereits keinen Zugriff auf das Netz mehr hat.

Ergänzende Kontrollfragen:

- Werden die Funktionen der verschlüsselten Authentisierung und der Rückruf-Sicherheit für alle externen Zugriffe genutzt?
- Ist nur der Zugriff auf den RAS-Server, nicht jedoch auf den Rest des Netzes aktiviert?
- Wird die Liste der für RAS-Zugriff autorisierten Benutzer regelmäßig überprüft und aktualisiert?

M 5.42 Sichere Konfiguration der TCP/IP-Netzverwaltung unter Windows NT

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Bei der Einbindung von Windows NT Systemen in ein Rechnernetz kommt der korrekten Konfiguration der installierten Netzdienste eine besondere Bedeutung zu. In den folgenden Abschnitten werden einige Hinweise zu den meistgenutzten Diensten gegeben; diese ersetzen jedoch nicht eine detaillierte Prüfung der Sicherheitsanforderungen und die Notwendigkeit zur genauen Kenntnis der Systemdokumentation.

DHCP (Dynamic Host Configuration Protocol)

Um den Aufwand für die Verwaltung von IP-Adressinformationen zu reduzieren, können über DHCP IP-Adressen und die zugehörigen Daten dynamisch konfiguriert werden.

Ein Windows NT Rechner wird ein DHCP-Client, wenn er bei der Installation von TCP/IP für automatische DHCP-Konfiguration konfiguriert wird. Nach dem Start eines DHCP-Clients stellt dieser eine Verbindung zu einem DHCP-Server her, um die erforderlichen TCP/IP-Konfigurationsdaten zu erhalten. Diese Konfigurationsdaten enthalten zumindest eine IP-Adresse, eine Subnetz-Maske sowie die für die Konfiguration geltende Gültigkeitsdauer der Adresse.

Die Installation eines DHCP-Servers, die nur von einem Mitglied der Gruppe "*Administratoren*" durchgeführt werden kann, gehört zur Installation von Microsoft TCP/IP.

Hinweis: Vor der Installation eines neuen DHCP-Servers muss geprüft werden, ob im Netz bereits andere DHCP-Server vorhanden sind, um einen eventuellen Konflikt zu vermeiden.

Eine automatische Konfiguration eines neuen DHCP-Servers kann nicht über DHCP vorgenommen werden, da ein Computer nicht gleichzeitig DHCP-Client und DHCP-Server sein kann.

Hinweis: Alle Einträge der Registrierung, die sich auf den DHCP Server beziehen, befinden sich unter dem Pfad:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPserver\Parameters.

Mittels des Dienstprogramms DHCP-Manager können folgende grundlegenden Aufgaben ausgeführt werden:

- Einen oder mehrere DHCP-Bereiche anlegen, damit die DHCP-Dienste zur Verfügung stehen.
- Definieren der Eigenschaften des Bereichs, einschließlich der Nutzungsdauer und der IP-Adressen-Pools, die möglichen DHCP-Clients von Servern in diesem Bereich zugewiesen werden sollen.

- Festlegen von Standardwerten für Optionen wie Standard-Gateway, DNS-Server oder WINS-Server, die zusammen mit einer IP-Adresse zugewiesen werden sollen, und Hinzufügen von eigenen Optionen.

Ein DHCP-Bereich stellt eine Gruppe von Rechnern dar, die den DHCP-Client Dienst in einem Teilnetz ausführen. Der Bereich wird zum Definieren von Parametern für jedes Teilnetz verwendet. Jeder Bereich hat die folgenden Eigenschaften:

- Eine eindeutige Subnetz-Maske, die zum Ermitteln des Teilnetzes verwendet wird, das einer bestimmten IP-Adresse zugeordnet ist.
- Ein Bereichsname, der vom Administrator beim Erstellen des Bereichs zugewiesen wird.
- Werte für die Nutzungsdauer dynamischer Adressen, die den DHCP-Clients zugewiesen werden.

Jedes Teilnetz kann nur einen einzigen Bereich mit einem durchgehenden IP-Adressen-Pool haben; diese Adressen müssen für das Teilnetz gelten. Sollen in einem Teilnetz mehrere Adressenpools realisiert werden, wird ein durchgehender Bereich angelegt, der all diese Adressenpools umfasst, und dann werden die Adressen zwischen den gewünschten Pools ausgeschlossen. Falls mehr Adressen benötigt werden, kann der Bereich später immer noch ausgeweitet werden.

Die Konfigurationsparameter, die ein DHCP-Server einem Client zuweist, werden unter Verwendung des DHCP-Managers als DHCP-Optionen definiert. Die meisten Optionen sind auf der Grundlage der Standardparameter, die in den Internet-Standards RFC 1541 bzw. RFC 1542 festgelegt wurden, vordefiniert. Wird ein DHCP-Bereich konfiguriert, so können ihm Optionstypen zugewiesen werden, die alle Konfigurationsparameter regulieren.

Zusätzlich zu den IP-Adressinformationen müssen für jeden Bereich weitere DHCP-Optionen konfiguriert werden, die an DHCP-Clients zu übergeben sind. Diese Optionen können global für alle Bereiche, speziell für einzelne Bereiche oder für einzelne DHCP-Clients mit reservierten Adressen definiert werden. Aktive globale Optionen gelten, sofern sie nicht durch Bereichsoptionen oder DHCP-Client-Einstellungen außer Kraft gesetzt werden. Aktive Optionstypen für einen Bereich gelten für alle Computer in diesem Bereich, sofern sie nicht für einen einzelnen DHCP-Client außer Kraft gesetzt werden.

Hinweis: Eine Veränderung der voreingestellten Werte darf nur bei genauer Kenntnis der Auswirkungen dieser Änderungen erfolgen. Die zu verwendenden Werte sind im Rahmen einer spezifischen Sicherheitsanalyse festzulegen.

Für einen Client kann eine bestimmte IP-Adresse reserviert werden. Das ist in der Regel in den folgenden Fällen notwendig:

- für Domänencontroller, wenn das Netz auch mit *LMHOSTS*-Dateien arbeitet, die IP-Adressen für Domänencontroller definieren,
- für Clients, die mit IP-Adressen arbeiten, die zur TCP/IP-Konfiguration über ein anderes Verfahren zugewiesen wurden,
- zur Zuweisung durch RAS-Server an Clients, die nicht mit DHCP arbeiten,

- für DNS-Server.

Falls mehrere DHCP-Server Adressen im selben Bereich verteilen, müssen die Client-Reservierungen auf jedem DHCP-Server identisch sein, ansonsten erhält der reservierte Client - in Abhängigkeit vom antwortenden Server - unterschiedliche IP-Adressen.

Hinweis: Die IP-Adresse und der statische Name, die in WINS angegeben werden, haben Vorrang vor der IP-Adresse, die vom DHCP-Server zugewiesen wird. In diesen Fällen wird für den Client eine Client-Reservierung mit der IP-Adresse generiert, die in der WINS-Datenbank festgelegt ist.

Folgenden Dateien sind im Verzeichnis *%SystemRoot%\SYSTEM32\DHCP* gespeichert, das beim Einrichten eines DHCP-Servers angelegt wird:

- *DHCP.MDB* ist die DHCP-Datenbankdatei.
- *DHCP.TMP* ist eine temporäre Datei, die DHCP für temporäre Datenbankdaten anlegt.
- Die Dateien *JET.LOG* und *JET*.LOG* enthalten Protokolle mit sämtlichen Transaktionen, die mit der Datenbank ausgeführt wurden. Mit Hilfe dieser Dateien stellt DHCP eventuell verloren gegangene Daten bei Bedarf wieder her.
- *SYSTEM.MDB* wird von DHCP zum Ablegen der Daten über die Struktur seiner Datenbank genutzt.

Hinweis: Die Dateien *DHCP.TMP*, *DHCP.MDB*, *JET.LOG* und *SYSTEM.MDB* sollten weder gelöscht noch in irgendeiner Weise verändert werden, da dies zu Fehlfunktionen von DHCP führen kann. Zugriff auf diese Dateien darf nur den Administratoren gegeben werden, da sonst unkontrollierte Veränderungen der DHCP-Konfiguration möglich sind.

WINS (Windows Internet Name Service)

Über WINS können NetBIOS-Computer-Namen zu IP-Adressen zugeordnet werden. Die Installation eines WINS-Servers läuft als Teil der Installation von TCP/IP unter Windows NT Server ab. Damit die einzelnen Server besser verfügbar sind und die Arbeitslast gleichmäßig auf diese Server verteilt ist, sollten mehrere WINS-Server eingerichtet sein. Jeder WINS-Server muss dann so konfiguriert sein, dass er gleichzeitig als Reproduktionspartner für mindestens einen anderen WINS-Server fungiert.

Zur Konfiguration eines WINS-Servers gehört die Angabe von Informationen darüber, wann die Datenbankeinträge für die Partner reproduziert werden. Unter einem Pull-Partner ist ein WINS-Server zu verstehen, der sich Kopien der Datenbankeinträge von seinem Partner beschafft, indem er zuerst eine Anforderung ausgibt und die gewünschten Kopien dann annimmt. Ein Push-Partner ist ein WINS-Server, der seine Partner mit einer Aktualisierungsmeldung benachrichtigt, wenn sich in der WINS-Datenbank etwas geändert hat. Wenn sein Partner auf diese Mitteilung mit einer Reproduktionsanforderung reagiert, sendet der Push-Partner eine Kopie der aktuellen WINS-Datenbank an diesen Reproduktionspartner. Damit die Datenbanken auf dem primären WINS-Server und auf dem Backup-Server immer übereinstimmen,

müssen beide jeweils die Rolle des Push- bzw. des Pull-Partners übernehmen. Es ist ohnehin stets zweckmäßig für Reproduktionspartner, beide Rollen zu übernehmen, d. h. sowohl Push- als auch Pull-Partner zu sein.

Für jeden WINS-Server muss ein bestimmter Zeitpunkt, eine Zeitdauer oder eine bestimmte Anzahl von Datensätzen als Schwellwert festgelegt werden. Wird dieser Wert erreicht, so erfolgt die Datenbankreproduktion. Wird für die Reproduktion ein bestimmter Zeitpunkt festgelegt, so wird diese einmal durchgeführt. Ist dagegen eine Zeitdauer festgelegt, so wiederholt sich die Reproduktion in den jeweiligen Abständen. Diese können z. B. in einer geographischen Region im Bereich von 1/4 bis 1/2 Stunde liegen, während über größere Entfernungen auch Abstände von einigen Stunden gewählt werden können.

Hinweis: Alle Einträge der Registratur, die sich auf die Konfiguration des WINS-Servers beziehen, befinden sich unter dem Pfad:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WINS\Parameters.

WINS-Server verständigen sich untereinander, um eine vollständige Reproduktion ihrer Datenbanken zu erreichen und zu gewährleisten, dass ein in einem WINS-Server registrierter Name letztlich in allen anderen WINS-Servern des Netzverbundes reproduziert wird. Alle Zuordnungsänderungen werden innerhalb der so genannten Reproduktionsperiode (maximaler Zeitraum für die Weitergabe der Änderungen an alle WINS-Server) für das gesamte WINS-System gesammelt. Alle freigegebenen Namen werden, sobald sie entsprechend dem im WINS-Manager festgelegten Intervall veraltet sind, an alle WINS-Server weitergeleitet.

Die Reproduktion erfolgt unter den Reproduktionspartnern, und nicht zwischen einem Server und den jeweils anderen Servern. Letztendlich werden sämtliche Kopien von den anderen WINS-Servern in einem Netzverbund angefordert, aber die WINS-Server senden Startsignale aus, um darauf hinzuweisen, wann eine Reproduktion eingeleitet werden soll. Damit eine Reproduktion stattfinden kann, muss jeder WINS-Server der Push- oder Pull-Partner von mindestens einem weiteren WINS-Server sein.

Hinweis: Alle Einträge der Registratur, die sich auf die WINS-Reproduktion beziehen, befinden sich unter dem Pfad:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WINS\Partners.

Statische Zuordnungen sind feststehende Listen, in denen Rechnernamen IP-Adressen zugeordnet sind. Diese Zuordnungen lassen sich nicht anzweifeln oder löschen, es sei denn, der Administrator entfernt eine bestimmte Zuordnung. Über den Befehl "*Statische Zuordnungen*" im WINS-Manager können statische Zuordnungen für diejenigen Clients im Netz hinzugefügt, editiert, importiert oder gelöscht werden, auf denen der WINS-Dienst nicht aktiviert ist.

Hinweis: Ist auf dem Netz auch DHCP im Einsatz, setzt eine reservierte (oder statische) IP-Adresse alle Einstellungen des WINS-Servers außer Kraft.

Statische Zuordnungen sollten einem Computer nicht zugewiesen werden, wenn auf diesem Computer WINS aktiv ist.

Folgenden Dateien werden im Verzeichnis *%SystemRoot%\SYSTEM32\WINS* gespeichert. Dieses Verzeichnis wird automatisch bei der Konfiguration eines WINS-Servers erstellt.

- *JET.LOG* ist die Protokolldatei für alle Transaktionen, die in der Datenbank durchgeführt werden. WINS verwendet die Datei bei Bedarf zur Wiederherstellung der Daten.
- Mit Hilfe von *SYSTEM.MDB* hält WINS Informationen über die Struktur der Datenbank fest.
- *WINS.MDB* ist die WINS-Datenbankdatei.
- *WINSTMP.MDB* ist eine durch WINS erstellte temporäre Datei. Sie kann nach einem Systemausfall im Verzeichnis \WINS übrig bleiben.

Hinweis: Die Dateien *JET.LOG*, *SYSTEM.MDB*, *WINS.MDB* und *WINSTMP.MDB* sollten weder gelöscht noch in irgendeiner Form verändert werden, da dies zu Fehlfunktionen von DHCP führen kann. Zugriff auf diese Dateien darf nur den Administratoren gegeben werden, da sonst unkontrollierte Veränderungen der WINS-Konfiguration möglich sind.

SNMP (Simple Network Management Protocol)

SNMP dient zur Überwachung und Administration von TCP/IP-basierten Netzen. Der SNMP-Dienst wird installiert, wenn die entsprechende Option bei der Installation von Windows NT TCP/IP gewählt wird. Nach der Installation muss der SNMP-Dienst mit den gültigen Informationen konfiguriert werden, damit SNMP betriebsbereit ist.

Nur Mitglieder der Gruppe der Administratoren des lokalen Computers können SNMP konfigurieren. Bei der Konfiguration von SNMP werden Communities und Trap-Ziele bestimmt:

- Unter einer *Community* ist eine Gruppe von Hosts zu verstehen, zu der ein Server gehört, der den SNMP-Dienst ausführt. Es können eine oder mehrere Communities angegeben werden, an die das Windows NT System, auf dem SNMP installiert wird, Traps sendet. Der Name der Community wird beim Senden des Traps in das SNMP-Paket aufgenommen. Empfängt der SNMP-Dienst eine Anforderung, die nicht den richtigen Community-Namen enthält und nicht zu einem der akzeptierten Hosts für den Dienst passt, kann der SNMP-Dienst ein Trap an das (die) Trap-Ziel(e) senden, das darauf hinweist, dass die Echtheitsbestätigung der Anforderung fehlschlug.
- *Trap-Ziele* sind die Namen oder IP-Adressen von Hosts, an die der SNMP-Dienst Traps, d. h. Meldungen vordefinierter Ereignisse, mit dem ausgewählten Community-Namen senden soll.

Hinweis: SNMP sollte grundsätzlich so konfiguriert werden, dass es nur Anforderungen definierter Communities (und möglichst nicht der vordefinierten Community *public*) annimmt.

Die SNMP Sicherheit gestattet es, die Communities und Hosts festzulegen, von denen ein Computer Anforderungen entgegen nimmt. Ferner kann festgelegt werden, ob ein Echtheitsbestätigungs-Trap gesendet wird, wenn eine Community oder ein Host unberechtigterweise Informationen anfordern. Diese Festlegungen sind sorgfältig zu planen, und die Möglichkeit des Versendens von Traps ist zu nutzen. Die dabei entstehenden Protokolle sind regelmäßig auszuwerten.

Ergänzende Kontrollfragen:

- Sind nur die minimal erforderlichen Netzdienste installiert / aktiviert?

M 5.43 Sichere Konfiguration der TCP/IP-Netzdienste unter Windows NT

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

TCP/IP

Bei der Installation des Protokolls TCP/IP werden dessen Eigenschaften mit der Systemsteuerungsoption "*Netzwerk*" festgelegt. Dabei ist zu beachten, dass, sofern der betreffende Rechner über mehr als eine Netzkarte verfügt und/oder Fernzugriff über RAS (Remote Access Server, siehe M 5.41 *Sichere Konfiguration des Fernzugriffs unter Windows NT*) installiert ist, das Routing zwischen diesen Karten bzw. zwischen dem Fernzugriffsinterface und der Netzkarte über die Registerkarte "*Routing*", Option "*IP-Forwarding aktivieren*" eingeschaltet werden kann. Diese Option sollte bei Rechnern, die eine Verbindung zu einem externen Netz, etwa dem Internet, haben, in der Regel nicht aktiviert werden, da sie dann externen Rechnern transparent Zugriff auf das lokale Netz gewähren.

In der Version 4.0 lässt sich in begrenztem Maße auch eine Filterung des Datenverkehrs über TCP/IP erreichen. Dazu ist auf der Registerkarte "*IP-Adressen*" die Option "*Erweitert*" zu wählen und in dem dann dargestellten Fenster die Option "*Sicherheit aktivieren*" zu wählen. Mit der Option "*Konfigurieren*" lassen sich dann die für die einzelnen Netzkarten zuzulassenden bzw. zu sperrenden TCP- und UDP-Anschlüsse (Ports) und IP-Protokolle wählen. Die hier einzutragenden Werte sollten unter Berücksichtigung der notwendigen Funktionalität und der gegebenen Sicherheitsanforderungen gewählt werden. Für einen Rechner mit externen Verbindungen sollte dabei ein Sicherheitskonzept für die Nutzung der Internet-Dienste vorhanden sein. Hierzu sollten ähnliche Überlegungen wie bei der Installation einer Firewall angestellt werden (siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)*, insbesondere M 2.76 *Auswahl und Einrichtung geeigneter Filterregeln*).

FTP (File Transfer Protocol)

Ein FTP-Server wird unter Version 3.51 während der Installation von TCP/IP eingerichtet; in der Version 4.0 kann der FTP-Server als Teil der Installation der Peer-Web-Dienste installiert werden. Wird der FTP-Serverdienst auf einem Windows NT System ausgeführt, können andere IT-Systeme über das Dienstprogramm FTP als Clients den Anschluss zu diesem Windows NT System herstellen und Dateien übertragen. Benutzer, die eine Verbindung zum FTP-Serverdienst herstellen, werden über ihr Benutzerkonto unter Windows NT authentisiert und erhalten je nach ihrem Benutzerprofil Zugriff. Aus diesem Grund ist es erforderlich, den FTP-Serverdienst auf einer NTFS-Partition zu installieren, damit die Dateien und Verzeichnisse, die über FTP zugänglich gemacht werden, geschützt werden können.

Nach Installation des FTP-Serverdienstes muss dieser Dienst konfiguriert werden, bevor damit gearbeitet werden kann. Bei der Konfiguration führen die Einstellungen zu einer der folgenden Situationen:

- Es ist keine anonyme FTP-Verbindung zulässig. In diesem Fall muss jeder Benutzer einen unter Windows NT gültigen Benutzernamen und ein Kennwort eingeben.
- Sowohl anonyme Benutzer als auch Benutzer unter Windows NT können eine Verbindung herstellen. In diesem Fall kann ein Benutzer zwischen einem anonymen Anschluss oder einer Verbindung über einen Benutzernamen und ein Kennwort unter Windows NT wählen.
- Es sind nur anonyme FTP-Verbindungen zulässig. In diesem Fall kann ein Anwender durch Eingabe eines Benutzernamens und eines Kennwortes unter Windows NT keine Verbindung herstellen.

Hinweis: FTP überträgt standardmäßig die Benutzerkennwörter unverschlüsselt über das Netz. Ein Benutzer mit einem Netzanalyseprogramm kann daher die Benutzerkennwörter für Fernkonten während der FTP-Authentisierung herausfinden.

Ob anonyme FTP-Verbindungen zugelassen werden sollten, hängt von verschiedenen Faktoren ab:

- In einem reinen NT-Netz gibt es sicherere Arten der Datenübertragung, FTP sollte daher überhaupt nicht zugelassen werden.
- In einem heterogen LAN mit NT-Rechnern kann FTP zur Datenübertragung zwischen verschiedenen Systemen erforderlich sein. Um zu verhindern, dass die NT-Benutzer-Kennungen inklusive Passwörtern abgehört werden, beispielsweise mit Sniffern, sollte auf den NT-Rechnern nur anonymes FTP zugelassen werden.
- Beim Einsatz von FTP in WANs muss das lokale Netz zusätzlich durch eine Firewall geschützt werden. Anonyme Verbindungen sollten nur auf speziell hierfür eingerichteten Systemen erlaubt werden; auf diesen Systemen darf keine andere Information als nur die über FTP anzubietende gespeichert werden.

Für anonyme Verbindungen muss der Benutzername "Anonymous" eingegeben werden, ein Passwort wird nicht benötigt, aber der Benutzer wird aufgefordert, seine E-Mail-Adresse einzugeben. Unter Windows NT muss für anonyme Verbindungen ein lokales Benutzerkonto eingerichtet werden, standardmäßig ist dies "Gast". Sobald über eine anonyme FTP-Verbindung eine Datenübertragung erfolgt, überprüft Windows NT den in diesem Dialogfenster zugewiesenen Benutzernamen und stellt anhand dieses Namens fest, welche Dateizugriffe zulässig sind.

Die für anonyme Verbindungen verwendete Benutzer-Kennung sollte Mitglied der Gruppe "*Gäste*" und auf keinen Fall Mitglied der Gruppe "*Benutzer*" sein, da im zweiten Fall leicht zu umfangreiche Zugriffsmöglichkeiten bestehen können.

Bei der Erstinstallation des FTP-Serverdienstes müssen zusätzlich die Zugriffsrechte dieses Dienstes konfiguriert werden. Dabei sind die Laufwerke bzw. Partitionen auszuwählen, deren Zugriffsrechte konfiguriert werden sollen. Je nach gewünschter Sicherheit für die ausgewählte Partition wird der Lesezugriff oder Schreibzugriff oder beide aktiviert. Die so vergebenen Berechtigungen gelten auf FAT-Partitionen und HPFS-

Partitionen für alle Dateien der gesamten Partition. Auf NTFS-Partitionen kann mit Hilfe dieser Einstellung der Lese- oder Schreibzugriff (oder beides) für die gesamte Partition gesperrt werden.

Alle so festgelegten Einschränkungen gelten zusätzlich zu den Sicherheitsmaßnahmen, die unter Umständen einen Teil des Dateisystems bilden. Das heißt, dass ein Administrator über dieses Dialogfeld die Berechtigungen für bestimmte Datenträger entfernen, aber über die im Dateisystem festgehaltenen Berechtigungen hinaus keine weiteren erteilen kann. Wenn z. B. für eine Partition nur Lesezugriff erteilt wurde, kann über FTP niemand auf diese Partition schreiben, unabhängig davon, welche Berechtigungen für FTP festgelegt wurden.

Es besteht die Möglichkeit, eingehende FTP-Verbindungen im System-Ereignisprotokoll festzuhalten, indem für Version 3.51 von Windows NT die Werte für *LogAnonymous* und *LogNonAnonymous* im Registrierungsschlüssel *HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\ftpsvc\ Parameters* auf 1 gesetzt werden. Diese Werte sind standardmäßig nicht in der Registrierung vorgesehen. Damit eingehende Verbindungen protokolliert werden, müssen die Werte neu eingetragen werden. Es kann angegeben werden, ob sowohl für anonyme als auch für nicht-anonyme Benutzer, die eine Verbindung zum FTP-Server herstellen, Einträge in das Ereignisprotokoll vorgenommen werden sollen.

In Version 4.0 von Windows NT können die entsprechenden Einstellungen für die Sicherheit des FTP-Serverdienstes mit Hilfe des Internet Service Managers vorgenommen werden; direkte Änderungen der Registrierung sind hier nicht mehr erforderlich.

Telnet

Windows NT stellt selbst keinen Telnet-Server zur Verfügung; dieses System kann nur als Telnet-Client arbeiten. Der Telnet-Client wird zusammen mit TCP/IP installiert. Falls ein Telnet-Server benötigt wird, kann der als Bestandteil des Windows NT Resource Kits Version 4.0 verfügbare Telnet-Dämon bzw. ein Produkt eines Fremdherstellers oder Shareware eingesetzt werden.

Hinweis: Da Telnet beim Logon die Benutzer-Passwörter im Klartext überträgt, sollte die Installation und Nutzung von Telnet nur dann erlaubt werden, wenn das Rechnernetz zuverlässig gegen Abhören geschützt ist. Nach Möglichkeit sollte deshalb auf die Verwendung von Telnet grundsätzlich verzichtet werden.

NFS (Network File System)

Windows NT stellt selbst weder einen NFS-Client noch einen NFS-Server zur Verfügung. Sofern NFS genutzt werden soll, müssen Produkte von Drittherstellern eingesetzt werden. Zur Konfiguration dieser Produkte können keine allgemeinen Angaben gemacht werden, doch sollten, soweit dies unterstützt wird, die entsprechenden Vorgaben für die Konfiguration von NFS unter dem Betriebssystem Unix umgesetzt werden.

Ergänzende Kontrollfragen:

- Sind nur die minimal erforderlichen Netzdienste installiert / aktiviert?

M 5.44 Einseitiger Verbindungsaufbau

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

In den meisten Fällen gibt es für ein Modem genau einen Telefonanschluss. Über diesen Telefonanschluss initiiert das Modem einerseits ausgehende Anrufe und nimmt andererseits auch die eingehenden Anrufe entgegen. Damit kein Angreifer unbemerkt Zugriff auf das angeschlossene IT-System nehmen kann, sollte hier zumindest ein Callback-Mechanismus eingesetzt werden (siehe auch M 5.30 *Aktivierung einer vorhandenen Callback-Option*).

Trotz eines aktivierten Callback kann das Problem bestehen, dass eine kommende Verbindung nicht ausgelöst wird, solange der Anrufer nicht auflegt. Die öffentliche Vermittlungsstelle löst eine solche Verbindung erst nach einem gewissen Zeitraum aus. Dies Problem tritt in erster Linie dann auf, wenn keine TK-Anlage die Verbindung zusätzlich auslöst.

Damit kann ein Angreifer einen Callback initiieren, aber gleichzeitig die Leitung belegt halten, so dass das Modem zwar korrekt die gespeicherte Rufnummer für den Callback anwählt, aber nach wie vor mit dem Angreifer verbunden bleibt.

Um dies zu verhindern, sollte zunächst überprüft werden, ob eine kommende Verbindung auch dann getrennt wird, wenn der Anrufer nicht auflegt. Ist dies nicht der Fall und kann es außerdem nicht gewährleistet werden, dass alle Modem-Verbindung durch einen Betreuer überwacht werden, sollte überlegt werden, mit getrennten Telefonanschlüssen mit einseitigem Verbindungsaufbau zu arbeiten, d. h. mit einem Anschluss für gehende und einem für kommende Verbindungen. Dies erfordert für jeden Anschluss ein eigenes Modem und die Durchführung des Callback über die Applikation. Dabei ist darauf zu achten, dass das Modem für gehende Verbindungen keine Anrufe automatisch entgegennimmt (*S0=0*, d. h. kein Auto-Answer). Damit vom Modem für kommende Verbindungen keine Verbindungen nach außen aufgebaut werden können, sollte der Modem-Anschluss entweder an der internen TK-Anlage für gehende Verbindungen gesperrt werden oder eine entsprechende Sperre bei der Telekom beantragt werden.

M 5.45 Sicherheit von WWW-Browsern

Verantwortlich für Initiierung: Leiter IT, Planer

Verantwortlich für Umsetzung: Administrator, Benutzer

Beim Zugriff auf das World Wide Web (WWW) können verschiedene Sicherheitsprobleme auf den angeschlossenen Arbeitsplatzrechnern auftreten. Diese können durch falsche Handhabung der benutzten Web-Browser (Programme für den Zugriff auf das WWW, meist kurz Browser genannt) durch die Benutzer bzw. durch eine unzureichende Konfiguration der Browser, aber auch durch Sicherheitslücken in den Browsern verursacht werden.

Eine Gefährdung der lokalen Daten geht beispielsweise von Programmen aus, die aus dem Internet geladen werden und ohne Nachfrage auf dem lokalen Rechner ausgeführt werden (z. B. ActiveX-Programme, Java-Applets oder Ähnliches). Auch innerhalb von Dokumenten oder Animationen können Befehle enthalten sein, die automatisch beim Betrachten ausgeführt werden und zu Schäden führen können (z. B. JavaScript Code, Flash-Objekte, ActiveX Controls und andere aktive Inhalte in Webseiten, Makro-Viren in Winword- oder Excel-Dokumenten). Um solche Probleme zu vermeiden, sollten die im Folgenden beschriebenen Maßnahmen umgesetzt werden.

Laden von Dateien und/oder Programmen

Viren und trojanische Pferde

Beim Laden von Dateien und/oder Programmen können eine Vielzahl von Sicherheitsproblemen auftreten. Die bekanntesten sind sicherlich Viren, Makro-Viren und trojanische Pferde. Die Benutzer dürfen sich bei der Nutzung des WWW nie darauf verlassen, dass die geladenen Dateien oder Programme aus vertrauenswürdigen Quellen stammen.

Bei der Konfiguration des Browsers ist darauf zu achten, dass bei Dateitypen, die Computer-Viren, z. B. Makro-Viren, enthalten können, die zugehörigen Anwendungen nicht automatisch gestartet werden (siehe dazu auch M 4.3 *Regelmäßiger Einsatz eines Anti-Viren-Programms*).

Alle Benutzer müssen darauf hingewiesen werden, dass sie selber dafür verantwortlich sind, beim Herunterladen von Dateien alle entsprechenden Vorsichtsmaßnahmen zu ergreifen. Selbst wenn über die Firewall automatisch die geladenen Informationen auf Viren überprüft werden, bleiben die Benutzer verantwortlich für die Schadensfreiheit von aus dem Internet geladenen Dateien oder Programmen. Bei der Installation von Programmen müssen die organisationsinternen Sicherheitsregeln beachtet werden. Insbesondere dürfen nur getestete und zugelassene Programme installiert werden. Vor der Installation sollten auf Stand-alone-Rechnern Tests auf die Schadensfreiheit der Programme durchgeführt werden. Die Berechtigung zum Installieren von Software sollte auf die Systemadministratoren beschränkt werden (siehe dazu auch M 4.177 *Sicherstellung der Integrität und Authentizität von Softwarepaketen*).

Plug-Ins und Zusatzprogramme

Viele Dateiformate werden von Browsern nicht direkt verarbeitet, sondern von zusätzlichen Programme, die häufig von Drittanbietern kommen. Oft können diese Programme als so genannte *Plug-Ins* direkt in den Browser integriert

werden, und die Anzeige der betreffenden Datei erfolgt dann im Browser anstatt in einem anderen Anwendungsfenster.

Bei Plug-Ins handelt es sich um Bibliotheksdateien (z. B. DLL-Dateien), die von Installationsprogrammen ins Plug-In-Verzeichnis geladen werden und bei Aufruf des entsprechenden Dateiformates vom Browser ausgeführt werden.

Zusatzprogramme, z. B. Viewer, sind eigenständige Programme, die in der Lage sind, bestimmte Dateiformate zu verarbeiten. Der Aufruf eines solchen Zusatzprogramms wird über eine Konfigurationsdatei des Browsers gesteuert, in der Dateiendung und Programm verknüpft sind.

Nachdenken vor dem Installieren

Beim Hinzufügen von Plug-Ins bzw. Zusatzprogrammen für einen Browser sind dieselben Vorsichtsmaßnahmen wie beim Herunterladen von Dateien und der Installation von Programmen zu beachten: Es dürfen keine Programme installiert werden, denen man nicht unbedingt vertrauen kann.

Alle nicht benötigten Plug-Ins sollten so weit wie möglich entfernt werden.

Cookies

Cookies stellen eine Möglichkeit dar, Informationen für bestimmte Websites lokal auf dem Clientrechner zu speichern. Cookies können beispielsweise von Betreibern von Webseiten genutzt werden, um Benutzereinstellungen für personalisierte Webangebote oder "Einkaufskörbe" in Webshops zu realisieren. Dabei sind die Informationen in der Regel nicht im Cookie selbst gespeichert. Vielmehr ist ein Cookie eine Art Seriennummer, die beim Webseiten-Betreiber gespeicherten benutzerspezifischen Informationen zugeordnet werden kann. Ein Cookie enthält typischerweise

- Informationen über die Webseiten, an die es zurückgeschickt werden soll (beispielsweise nur an den Server, von dem es erzeugt wurde oder an alle Server in der Domain des Servers, von dem es erzeugt wurde),
- eine Gültigkeitsdauer (beispielsweise nur für die laufende Browsersitzung oder bis zu einem vorgegebenen Ablaufdatum) und
- andere, vom Betreiber des Webservers frei vorgebbare Daten, etwa eine Benutzer-Kennung oder eine *SessionId.*

Neben den potentiell nützlichen Anwendungen in Webshops oder für personalisierte Webangebote können WWW-Anbieter hiermit allerdings auch Benutzerprofile erstellen, z. B. für zielgruppenorientierte Werbung. Cookies sind insofern kein Problem der Sicherheit im engeren Sinne, sondern eher ein Problem des Datenschutzes.

In den Browsereinstellungen sollte die generelle Annahme von Cookies deaktiviert werden. Die meisten Browser bieten stattdessen zumindest die Möglichkeit, den Benutzer vor der Speicherung eines Cookies zu fragen, ob dieses akzeptiert werden soll. Einige Browser erlauben eine relativ detaillierte Einstellung der Kriterien, nach denen Cookies akzeptiert oder zurückgewiesen werden. Die folgenden Punkte können als Grundlage für die Entscheidung dienen, ob ein Cookie abgelehnt werden sollte oder ob es unbedenklich ist:

- Cookies, die an Server aus einer *anderen* Domain zurückgeschickt werden sollen, als der Domain des Servers, von dem die aktuell besuchte Seite stammt, sollten generell abgelehnt werden. Ebenso sollten alle Cookies mit außergewöhnlich langen Lebensdauern abgelehnt werden.
- Cookies, die an alle Server in einer bestimmten Domain zurückgeschickt werden sollen, und nicht nur an den Server, von dem die aktuell besuchte Seite stammt, sollten normalerweise abgelehnt werden.
- Cookies, die zur Speicherung von Benutzereinstellungen für personalisierte Sites dienen, können akzeptiert werden. Um solche Cookies zu identifizieren ist allerdings stets die Entscheidung des Benutzers notwendig. Seriöse Anbieter zeigen oft auf den Seiten, auf denen ein Benutzer seine Einstellungen treffen kann, einen Hinweis an, dass die Einstellungen in einem Cookie gespeichert werden sollen.
- Cookies, die nur für die aktuelle Browsersitzung Gültigkeit besitzen sollen (oft auch *Session-Cookies* genannt) und nur an den jeweiligen Server zurück geschickt werden, können in der Regel akzeptiert werden.

Manche Browser bieten die Möglichkeit, die aktuell gespeicherten Cookies anzuzeigen und gegebenenfalls selektiv zu löschen. Zusätzlich ist es unter Umständen möglich festzulegen, dass der Cookie-Speicher beim Beenden des Browsers geleert werden soll.

Bei der Entscheidung, ob und in welchem Umfang Cookies akzeptiert werden sollen, sollte stets in Betracht gezogen werden, dass die in Cookies gespeicherte Information eventuell auch von arglistigen Webseiten-Betreibern ausgelesen werden kann. So sind in der Vergangenheit des öfteren Schwachstellen insbesondere im Microsoft Internet Explorer bekannt geworden, die es erlaubten, Cookies des Benutzers auszulesen. Dies stellt insbesondere bei Cookies, die zur Speicherung von Benutzer-Kennungen und -Einstellungen benutzt werden, ein nicht unbeträchtliches Risiko dar. Daher sollte bei der Entscheidung, ob und welche Cookies akzeptiert werden sollen, eher restriktiv vorgegangen werden.

Eventuell kann es hilfreich sein, bei Browsern, die Cookies in einer Datei speichern, das regelmäßige Löschen der Cookies über eine Batch-Datei zu steuern, die beispielsweise bei jedem Systemstart oder jeder Benutzeranmeldung die alten Cookie-Dateien löscht. Manchmal reicht es auch, die entsprechende Datei oder das Verzeichnis, in dem Cookies gespeichert werden, mit einem Schreibschutz zu versehen, so dass keine neuen Cookies angelegt werden können.

Datensammlungen

History, Hotlists und Cache

Nicht nur extern werden Daten über die Internet-Nutzung der verschiedenen Benutzer gesammelt, sondern auch lokal. Hier muss sichergestellt werden, dass nur Befugte darauf Zugriff haben können. Dies gilt insbesondere für die von Browsern angelegten Dateien über History, Hotlists und Cache. Die Benutzer müssen informiert werden, wo auf ihren lokalen Rechner solche Daten gespeichert werden und wie sie diese löschen können. Bei einigen Browsern ist es möglich, alle Daten und Dateien, die auf das persönliche Surfverhalten zurückschließen lassen, per Mausklick zu löschen.

Die Dateien auf Proxy-Servern sind besonders sensibel, da auf einem Proxy-Server alle externen WWW-Zugriffe aller Mitarbeiter protokolliert werden, inklusive der IP-Nummer des Clients, der die Anfrage gestartet hat, und der nachgefragten URL. Mit Hilfe der IP-Nummer des Clients ist es in der Regel möglich, auf einen konkreten Mitarbeiter zurückzuschließen. Ein schlecht administrierter Proxy-Server kann daher massive Datenschutzverletzungen nach sich ziehen.

Von den meisten Browsern werden viele Informationen über den Benutzer und sein Nutzerverhalten gesammelt, von denen dieser vielleicht nicht will, dass sie weitergegeben werden. Zu diesen Informationen gehören:

- Favoriten,
- abgerufene WWW-Seiten bzw. Informationen im Cache,
- News-Server Visiten,
- History-Datenbank bzw. URL-Liste,
- Cookie-Liste,
- Informationen über Benutzer, die im Browser gespeichert und eventuell auch weitergegeben werden.

Informationen über News-Server Visiten

Aus den meisten Browsern heraus kann direkt auf News-Server zugegriffen werden.

Unabhängig vom verwendeten Browser bzw. Newsreader wird immer gespeichert, welche Newsgroups abonniert werden und welche Artikel gelesen wurden. Damit kann für ein Benutzerprofil festgestellt werden, welche Newsgruppen und welche News ein Benutzer gelesen hat.

Das im Microsoft Internet Explorer als Newsreader verwendete Outlook Express geht noch einen Schritt weiter und speichert den vollständigen Inhalt aller gelesenen News für einen bestimmten Zeitraum.

History-Datenbank / Verlaufsanzeige

Praktisch alle Browser führen ein Protokoll über die URLs, die der Benutzer innerhalb eines bestimmten Zeitraums abgerufen hat (*History* bei Mozilla bzw. Netscape, *Verlauf* beim Microsoft Internet Explorer). Ein solches Protokoll kann sich entweder nur über die aktuelle Sitzung erstrecken oder auch Informationen über vergangene Sitzungen enthalten.

Diese Datenbank enthält Informationen über besuchte Webseiten und abgerufene Seiten (URL und Titel). Auch interne Dokumente, die im Browser geöffnet werden, werden mit diesen Informationen in der Datenbank verzeichnet. Dadurch können eventuell sensitive vertrauliche Informationen preisgegeben werden.

Die History-Datenbank sollte regelmäßig aufgeräumt werden. Die meisten Browser bieten in ihren Konfigurationsdialogen die Möglichkeit, die History-Datenbank komplett zu leeren. Außerdem kann meist festgelegt werden, welcher Zeitraum von der History-Datenbank abgedeckt werden soll, ältere Informationen werden automatisch gelöscht.

Informationen über Benutzer

In einem Browser können diverse Informationen über Benutzer gespeichert und eventuell auch weitergegeben werden, z. B. Realname, E-Mail-Adresse, Organisation. Beispielsweise kann bei Mozilla bzw. Netscape eine E-Mail-Adresse angegeben werden, die bei der Verwendung von *Anonymous-Ftp* an den ftp-Server übermittelt werden soll. Um nicht mit Werbe-E-Mail überflutet zu werden, empfiehlt es sich, hierfür einen Alias zu verwenden.

Passwörter nicht im Browser speichern!

Viele Browser bieten die Möglichkeit, die Eingaben des Benutzers für bestimmte Web-Formulare zu speichern und beim nächsten Aufruf der entsprechenden Seite automatisch einzufügen. Von dieser Option sollte allenfalls in Ausnahmefällen Gebrauch gemacht werden. In keinem Fall sollten Zugangspasswörter auf diese Weise gespeichert werden. Sofern die Möglichkeit besteht, die Daten verschlüsselt abzuspeichern, sollte diese unbedingt genutzt werden.

Informationen im Browser-Cache

Praktisch alle Browser legen in einem eigenen Cache-Verzeichnis große Mengen an Dateien ab, die den Text und die Bilder aller besichtigten Web-Seiten enthalten, seit der Cache das letzte Mal gelöscht wurde.

Der Cache dient dazu, das mehrfache Laden von Dateien zu verhindern, und dadurch unnötige Übertragungen zu vermeiden. Die Dateien im Browser-Cache können, ähnlich wie die History Datenbank, dazu verwendet werden, die vom Benutzer abgerufenen Informationen zu rekonstruieren. Dies kann zum Erstellen von Benutzerprofilen missbraucht werden, aber im Extremfall sogar dazu führen, dass vertrauliche Informationen an die Öffentlichkeit gelangen, wenn beispielsweise ein Notebook gestohlen wird, das auch im Intranet benutzt wurde.

Cache regelmäßig löschen

Daher sollte der Cache ebenso wie der Verlaufsordner regelmäßig gelöscht werden, vor allem, wenn ein am Arbeitsplatz im Intranet genutztes Notebook außerhalb der Behörde oder des Betriebes benutzt wird. In einem solchen Fall ist es daher empfehlenswert, die Größe des Caches auf 0 MByte zu setzen, um ein Zwischenspeichern von Dateien zu verhindern. Wenn auf mit SSL gesicherte WWW-Seiten zugegriffen wird, dient dies oft dazu, sensible Informationen wie Kreditkartennummern verschlüsselt über das Internet zu übertragen. Solche Seiten sollten daher von vorneherein nicht im Cache abgelegt werden, sofern diese Einstellungsoption verfügbar ist.

Sicherheitslücken

In der Vergangenheit sind in praktisch allen Browsern immer wieder gravierende Sicherheitslücken aufgetaucht. Die Auswirkungen dieser Sicherheitslücken reichten vom Absturz des Browsers bis hin zu einer potentiellen Kompromittierung des gesamten Rechners, indem ein arglistiger Webseiten-Betreiber Programme auf dem Client-Rechner mit den Rechten des jeweils angemeldeten Benutzers ausführen konnte.

Aktive Inhalte und Zugriff auf lokale Ressourcen

Die meisten dieser Sicherheitslücken tauchten im Zusammenhang mit *aktiven Inhalten* wie JavaScript, ActiveX, Flash oder Java, aber auch im Zusammen-

hang mit anderen Plug-Ins auf. Aktive Inhalte werden über den Browser auf dem Client ausgeführt anstatt auf dem Server. Dies kann zu Sicherheitsproblemen auf dem Client führen. Zwar sind in Java, JavaScript und ActiveX verschiedene Sicherheitsmechanismen eingebaut, um einen möglichen Missbrauch zu verhindern oder zumindest zu erschweren, allerdings werden regelmäßig Sicherheitslücken entdeckt, die Angreifern eine Umgehung der Sicherheitsmechanismen ermöglichen.

Bei einigen Browsern (wie z. B. Netscape oder Microsoft Internet Explorer) wird WWW-Servern die Möglichkeit gegeben, über aktive Inhalte auf die Festplatte des Clients zuzugreifen. ActiveX erlaubt unter bestimmten Bedingungen die Nutzung lokaler Ressourcen. Bei Java ist ein solcher Zugriff ebenfalls möglich, jedoch nur wenn der Anwender dies explizit gestattet. Das Sicherheitskonzept von ActiveX basiert darauf, dass der Anwender dem Anbieter und einer authentisierten dritten Stelle vertraut. Dieses Vertrauen ist problematisch, wenn Web-Seiten eines unbekannten oder eines neuen Anbieters aufgerufen werden.

ActiveX, JavaScript und Java deaktivieren

Aus diesen Gründen sollten ActiveX, JavaScript und Java deaktiviert werden, und die Menge der installierten Plug-Ins sollte auf das unbedingt notwendige beschränkt werden.

Falls die Benutzung von ActiveX, Java und JavaScript unbedingt notwendig ist, sollten diese nur auf Rechnern zugelassen sein, die gegenüber anderen internen Rechnern so abgeschottet sind, dass die Verfügbarkeit, Vertraulichkeit und Integrität sicherheitsrelevanter Daten nicht beeinträchtigt werden können.

Verschlüsselung

Das normalerweise im WWW benutzte Übertragungsprotokoll HTTP (*Hypertext Transfer Protocol*) überträgt alle Informationen im Klartext. Bei normalen Webseiten gibt es keine Gewähr dafür, dass die Vertraulichkeit der übertragenen Informationen gewahrt bleibt. Ebenso werden die Authentisierungsdaten beim Zugriff auf passwortgeschützte Webangebote unverschlüsselt übertragen, es besteht daher die Gefahr, dass diese ausgelesen werden können.

sensitive Informationen verschlüsseln

Falls bei einem Webangebot die Angabe sensitiver Informationen (etwa der Kreditkartennummer oder Bankverbindung, aber auch nur personenbezogener Daten) erforderlich ist, so sollten diese Daten nur dann übermittelt werden, wenn das Angebot nicht über eine normale HTTP-Verbindung, sondern über eine mit Hilfe des HTTPS-Protokolls verschlüsselte Verbindung zugänglich ist.

Entsprechende URLs sind meist daran erkennbar, dass sie mit dem Präfix *https://* beginnen. Leider gibt es auch hier Ausnahmen, zum Beispiel:

- Das meist für die Verschlüsselung verwendete Protokoll *SSL v3* sieht auch einen Betriebsmodus vor, in dem gar nicht verschlüsselt wird (authentication only). In diesem Fall besteht die Gefahr, dass der Benutzer fälschlicherweise davon ausgeht, dass die Informationen ausreichend geschützt werden.

- Falls die zu verschlüsselnden Informationen in einem so genannten *Frame* untergebracht sind, wird unter Umständen im Browser nur *http://* angezeigt, obwohl alle relevanten Daten verschlüsselt werden.

Wenn eine verschlüsselte Verbindung zu einem Server besteht, zeigen dies die meisten Browser durch ein entsprechendes Symbol an, Netscape und Mozilla beispielsweise durch ein geschlossenes Schlosssymbol in der rechten unteren Ecke des Browserfensters, der Microsoft Internet Explorer durch ein ähnliches Symbol in der Statuszeile.

Um sensitive Informationen und sicherheitskritische Transaktionen zu schützen, sollten folgende Empfehlungen beachtet werden:

- Es sollte regelmäßig geprüft werden, ob die jeweilige Webseite mit einer ausreichenden Schlüssellänge verschlüsselt ist. Informationen über die HTTPS-Verschlüsselung der aktuellen Webseite und die Schlüssellängen lassen sich in den meisten Browsern durch einen (Doppel-)Klick auf das oben erwähnte Schlosssymbol abfragen. Stand der Technik ist eine Schlüssellänge von 128 Bit.
- Soweit dies im benutzten Browser möglich ist, sollten alle unsicheren Betriebsmodi des HTTPS-Protokolls im Browser deaktiviert werden. Dies betrifft insbesondere die veraltete SSL-Version 2 und Betriebsmodi mit Schlüssellängen von weniger als 80 Bit.

Nutzung vorhandener Sicherheitsfunktionalitäten

Die vorhandenen Sicherheitsfunktionalitäten der Browser (insbesondere die Rückfrage vor dem Ausführen von Programmen) sollten auf jeden Fall genutzt werden.

automatische Ausführung von Programmen verhindern

Beim Surfen im Internet sollte die automatische Ausführung von Programmen verhindert und nur bei vertrauenswürdigen Servern wieder eingeschaltet werden. Beim Microsoft Internet Explorer sollte unter *Extras* | *Internetoptionen* | *Sicherheit* in den Abschnitten *ActiveX Steuerelemente und Plugins* und *Scripting* die Optionen *Deaktivieren* oder *Eingabeaufforderung* gewählt werden. Bei Netscape bzw. Mozilla sollten die Optionen *Enable Java* und *Enable JavaScript* deaktiviert werden.

Die Deaktivierung von ActiveX-Steuerelementen im Internet Explorer bewirkt in der Regel, dass PDF-Dateien nicht mehr direkt im Browser angezeigt werden können. Diese Funktionseinschränkung ist jedoch in der Praxis meist nicht gravierend, da die üblichen separaten PDF-Viewer ohnehin mehr Bedienungskomfort als das Browser-Plug-In bieten.

E-Mail-Anhänge nicht automatisch ausführen

News-Reader und Mail-Clients bieten häufig die Möglichkeit, beliebige Daten im MIME-Format zu lesen. Auch in diesen Daten können Befehle enthalten sein, die zu einem automatischen Starten von Programmen auf dem lokalen Rechner führen. Die entsprechenden Möglichkeiten sollten daher in den Konfigurationsdateien entfernt werden bzw. nur nach Rückfrage gestartet werden können.

Einsatz von Application-Level-Gateways bzw. Filter-Proxies

Um einen zuverlässigen Schutz vor der Gefährdung durch bösartige aktive Inhalte zu erzielen sind die beschriebenen client-seitigen Schutzmaßnahmen

eventuell nicht ausreichend. Es sollte daher in Betracht gezogen werden, den Zugriff auf das Internet nur über einen Application-Level-Gateway zuzulassen. Auf diesem Filter-Proxy-Server sollten aktive Inhalte grundsätzlich erst einmal ausgefiltert werden, so dass sie die Arbeitsplatzrechner gar nicht erst erreichen. Nur in Einzelfällen kann dann die Filterung für bestimmte URLs deaktiviert werden. Die technische Realisierung solcher Filterfunktionen ist in der Praxis allerdings mit einem gewissen Aufwand verbunden. Daher sollte anhand des vorliegenden Schutzbedarfs entschieden werden, ob der Einsatz eines Filter-Proxy-Servers zweckmäßig ist.

Dies kann jedoch eine sichere Konfiguration der Arbeitsplatzrechner nicht ersetzen, sondern nur ergänzen, so dass in jedem Fall auch die entsprechenden Maßnahmen ergriffen werden sollten.

Informationsbeschaffung über Sicherheitslücken

Da immer wieder neue Sicherheitslücken in Browsern bekannt werden, ist eine regelmäßige Informationsbeschaffung über solche Sicherheitslücken und deren Beseitigung erforderlich. Hierbei braucht nicht unbedingt die Beschaffung der aktuellsten Version des Produkts im Vordergrund zu stehen, da durch neue Programmteile auch neue Sicherheitsprobleme auftreten können. In jedem Fall sollte jedoch durch das Einspielen von Patches sichergestellt werden, dass bekannte Sicherheitslücken beseitigt werden (siehe auch M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*).

Auch Sicherheitspatches müssen getestet werden!

Wenn mit Hilfe des Browsers wichtige Anwendungen des Unternehmens bzw. der Behörde bedient werden oder wenn ein erhöhter Schutzbedarf in Bezug auf Verfügbarkeit vorliegt, sollten die Patches auf jeden Fall vorher auf einem Testsystem getestet werden. Dabei sollte geprüft werden, ob keine unerwünschten Seiteneffekte auftreten, die den sicheren und reibungslosen Betrieb stören.

Regelungen

Ein Teil der oben beschriebenen Maßnahmen liegt im Verantwortungsbereich der Benutzer, da deren Umsetzung, wie beispielsweise die Aktivierung bestimmter Optionen, nicht ständig durch die Systemadministration überprüft werden kann. Wenn möglich, sollten jedoch administrationsseitig Maßnahmen ergriffen werden, die die Veränderung bestimmter Einstellungen durch Benutzer erschweren oder ganz unterbinden. Beispielsweise können bei einigen Produkten bestimmte Konfigurationsdateien schreibgeschützt werden.

In jedem Fall muss aber die Systemadministration durch die Vorgabe sicherer Grundeinstellungen dafür sorgen, dass ohne Benutzereingriff ein größtmögliches Maß an Sicherheit erzielt wird.

Schulung

Außerdem sollte jeder Benutzer über die möglichen Risiken informiert sein und vor der Nutzung von Internet-Diensten durch entsprechende Anweisungen verpflichtet werden, die aufgeführten Sicherheitsrichtlinien zu beachten. Es empfiehlt sich vor der Zulassung von Benutzern zu Internet-Diensten diese auf eine Benutzerordnung zu verpflichten. Die Inhalte der Internet-Sicherheitsrichtlinie und der Benutzerordnung sind in einer Schulung den Benutzern darzulegen.

Weiterhin müssen die Benutzer darauf hingewiesen werden,

- welche Daten protokolliert werden,
- wer die Ansprechpartner bei Sicherheitsproblemen sind und
- dass die Konfiguration der WWW-Programme nicht eigenmächtig geändert werden darf.

Kenntnisnahme bestätigen lassen

In der Benutzerordnung sollten die zur Verfügung stehenden Kommunikationsdienste kurz erläutert und alle relevanten Regelungen aufgeführt werden. Jeder Benutzer sollte durch Unterschrift bestätigen, dass die dargestellten Regelungen zur Kenntnis genommen wurden und bei Benutzung der Kommunikationsdienste beachtet werden.

Regelung für private Internet-Nutzung

Bei der Festlegung der Benutzerordnung sollte auch eine Regelung über die private Internet-Nutzung am Arbeitsplatz getroffen werden. Gesetzliche Vorgaben, insbesondere zum Datenschutz, müssen dabei selbstverständlich beachtet werden. Der Datenschutzbeauftragte und die Personalvertretung sollten frühzeitig beteiligt werden.

M 5.46 Einsatz von Stand-alone-Systemen zur Nutzung des Internets

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um die Gefährdungen, die durch Angriffe aus dem Internet auf lokale Daten oder Rechner im LAN entstehen, zu verringern, ist es sinnvoll Rechner einzusetzen, die nur mit dem Internet vernetzt sind und keine weitere Netzverbindung zu einem LAN haben.

Hierfür bieten die verschiedenen Betriebssysteme unterschiedliche Möglichkeiten mit jeweils spezifischen Gefährdungen für die Vertraulichkeit und Integrität der Daten auf diesem Rechner.

Detailliertere Beschreibungen, wie Stand-alone-Systeme sicher zur Nutzung des Internets eingesetzt werden können, finden sich im Baustein B 3.208 *Internet-PC*.

M 5.47 Einrichten einer Closed User Group

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, TK-Anlagen-Verantwortlicher

Verantwortlich für Umsetzung: Administrator

Das Integrated Services Digital Network (ISDN) ermöglicht die Einrichtung einer geschlossenen Benutzergruppe (GBG), auch als Closed User Group (CUG) bezeichnet. Merkmal einer solchen Gruppe ist, dass alle Teilnehmer einer CUG untereinander über das öffentliche ISDN kommunizieren können, Verbindungswünsche von außerhalb der CUG an CUG-Teilnehmer jedoch genauso abgewiesen werden wie Verbindungswünsche von CUG-Teilnehmer an Teilnehmer des öffentlichen ISDN.

Funktionsweise:

Alle Kommunikationspartner sind Mitglied in einer Closed User Group des Netzbetreibers (z. B. Deutsche Telekom AG). Die Berechtigungsprüfung zur Kommunikation erfolgt über den einer CUG eindeutig zugeordneten Interlock Code durch die jeweilige digitale Vermittlungsstelle (DIV) der Kommunikationspartner. Zu Beginn übermittelt der rufende Kommunikationspartner eine Verbindungsanforderung an die ihm zugeordnete DIV. Die DIV fügt der Verbindungsanforderung nicht nur die ISDN-Rufnummer des rufenden Kommunikationspartners, sondern auch den eindeutigen Interlock Code der entsprechenden Closed User Group hinzu. Die DIV des gerufenen Kommunikationspartners erkennt anhand des Interlock Codes, ob der Verbindungsanforderung stattgegeben werden kann. Ist die Identifikation erfolgreich, wird der Verbindungswunsch an den gerufenen Kommunikationspartner weiter vermittelt.

Vorteilhaft an der beschriebenen Funktionalität ist, dass unerlaubte Zugriffsversuche bereits von der DIV des Netzbetreibers abgewiesen werden und nicht bis zu Netzkoppelelementen eines Kommunikationspartners gelangen.

Nachteilig ist, dass Änderungen der Mitgliedschaft in einer CUG immer dem Netzbetreiber mitgeteilt werden müssen, da nur dieser die notwendigen Berechtigungsänderungen durchführen kann. Weiterhin bedeutet dies auch, dass der Netzbetreiber die vollständige Kontrolle über die Mitgliedschaft in einer CUG besitzt und von ihm vorgenommene Änderungen durch den Nutzer einer CUG nicht kontrolliert werden können. Hingewiesen werden soll ebenfalls darauf, dass sowohl für das Einrichten als auch für den Betrieb einer CUG durch einen Netzbetreiber einmalige und fortlaufende Kosten entstehen.

Das Einrichten einer Closed User Group durch den Betreiber eines öffentlichen Netzes empfiehlt sich immer dann, wenn

- Hard- und Software für andere Verfahren (z. B. M 5.48 *Authentisierung mittels CLIP/COLP*) erst beschafft werden müsste,
- die Mitglieder einer CUG nur selten wechseln und
- der Netzbetreiber ausreichend vertrauenswürdig ist.

Ergänzende Kontrollfragen:

- Findet eine ausreichende und nachvollziehbare Dokumentation der eingerichteten CUG statt? Ist sie aktuell?
- Wird regelmäßig überprüft, ob die im allgemeinen kostenpflichtige Funktionalität der CUG noch notwendig ist?

M 5.48 Authentisierung mittels CLIP/COLP

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, TK-Anlagen-Verantwortlicher

Verantwortlich für Umsetzung: Administrator

Das Integrated Services Digital Network (ISDN) liefert die Möglichkeit, Rufnummern von Teilnehmern nicht nur für die öffentlichen Vermittlungskomponenten, sondern auch direkt für die beteiligten Kommunikationspartner zu signalisieren. Diese ISDN-Leistungsmerkmale bezeichnet man als

- CLIP = Calling Line Identification Presentation und
- COLP = Connected Line Identification Presentation oder allgemeiner als
- Rufnummernanzeige.

Die Auswertung der Rufnummernangabe kann von den jeweiligen Kommunikationspartnern zur Authentisierung genutzt werden.

Funktionsweise:

In einem ersten Schritt wird seitens des rufenden Kommunikationspartners eine Verbindungsanforderung an die ihm zugeordnete digitale Vermittlungsstelle (DIV) abgesetzt. Die DIV vermittelt die Verbindungsanforderung an den zu rufenden Kommunikationspartner innerhalb des ISDN incl. der Rufnummer des rufenden Kommunikationspartners. Die gegenüberliegende DIV vermittelt anschließend den Verbindungswunsch an die ISDN-Kommunikationseinrichtung des gewünschten Kommunikationspartners. Anhand der übermittelten Rufnummer kann diese Kommunikationseinrichtung (z. B. ein ISDN-Router oder eine TK-Anlage) den rufenden Kommunikationspartner identifizieren (CLIP). Bei erfolgreicher Identifikation wird der Verbindungswunsch angenommen und der Datenaustausch kann beginnen.

Vorteilhaft an der beschriebenen Funktionalität ist, dass die Identifikation durch Komponenten der jeweiligen Kommunikationspartner (ISDN-Router, TK-Anlage) durchgeführt wird und somit vollständig in deren Kontrollbereich liegt.

Nachteilig ist, dass die über den ISDN-D-Kanal übertragenen Rufnummern grundsätzlich manipulierbar sind (siehe G 5.63 *Manipulationen über den ISDN-D-Kanal*). Eine einfache Authentisierung durch die übermittelte Rufnummer ist somit entweder nur in Zusammenhang mit dem Einsatz einer Callback-Funktion (siehe M 5.49 *Callback basierend auf CLIP/COLP*) oder in Kombination mit dem Einsatz eines D-Kanal-Filters (siehe M 4.62 *Einsatz eines D-Kanal-Filters*), das Protokollmanipulationen aufdeckt, möglich.

Ergänzende Kontrollfrage:

- Können die eingesetzten ISDN-Komponenten die Leistungsmerkmale CLIP und COLP verarbeiten sowie ausreichend große Rufnummerntabellen pflegen?

M 5.49 Callback basierend auf CLIP/COLP

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator

Viele Kommunikationskarten bieten die Option automatischer Rückruf (Callback). Ist diese Option aktiviert, trennt die Kommunikationskarte, wenn sie einen Anruf erhält, sofort nach dem erfolgreichen Verbindungsaufbau die Verbindung und ruft eine voreingestellte Nummer zurück. Dadurch wird verhindert, dass ein nicht autorisierter Anrufer diesen Fernzugang missbrauchen kann, solange er nicht unter der voreingestellten Nummer erreichbar ist. Callback ist immer dann einzusetzen, wenn ein fester Kommunikationspartner sich automatisch einwählen können soll. Zu beachten ist, dass mit dem automatischen Rückruf auch die Kosten der Datenübertragung übernommen werden.

Mit Hilfe des ISDN ist eine Variante des Callback zu einer festen Rufnummer möglich: Die angesprochene ISDN-Karte prüft mit Hilfe des ISDN-Leistungsmerkmals Calling Line Identification Presentation (CLIP), von welcher Stelle aus die Verbindungsanforderung erfolgte, und vergleicht die übermittelte Rufnummer mit einer Rufnummerntabelle. Wurde über CLIP eine gültige Rufnummer übermittelt, wird die in der Rufnummerntabelle hinterlegte Rufnummer zurückgerufen.

Vorteilhaft ist gegenüber der ausschließlichen Authentisierung über CLIP/COLP (siehe M 5.48 *Authentisierung mittels CLIP/COLP*), dass selbst beim Vorspiegeln einer autorisierten Rufnummer von einem nicht autorisierten Teilnehmer aus keine Verbindung zustande kommt, da der nicht autorisierte Teilnehmer tatsächlich ja nicht unter der vorgegebenen Rückrufnummer erreichbar ist.

Ergänzende Kontrollfragen:

- Ist die Kostenübernahme im Callback-Modus geklärt?
- Wann wurden letztmalig die voreingestellten Rufnummern überprüft?

M 5.50 Authentisierung mittels PAP/CHAP

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator

Viele ISDN-Karten unterstützen die Kommunikation über das Point-to-Point Protocol (RFC 1661), nachdem eine ISDN-Wählverbindung aufgebaut wurde. Innerhalb dieses Internet-Standards werden auch Authentisierungsprotokolle, wie das Password Authentication Protocol (PAP) und das Challenge Handshake Authentication Protocol (CHAP) angeboten (RFC 1994). Bietet die verwendete ISDN-Karte diese Funktionalitäten, sollte zur Authentisierung anstelle des Password Authentication Protocols das Challenge-Handshake Authentication Protocol genutzt werden, da bei PAP das zur Authentisierung verwendete Passwort unverschlüsselt übertragen wird.

Die bei PAP bzw. CHAP verwendeten Passwörter werden im Allgemeinen nicht bei jeder Authentisierung vom Benutzer erneut eingegeben, sondern in den IT-Systemen gespeichert. Damit sich diese Verfahren auch nach einer erneuten Installation wieder aufsetzen lassen, sollten die benötigten Passwörter notiert und sicher verwahrt werden (siehe M 2.22 *Hinterlegen des Passwortes*).

Funktionsweise:

Bei CHAP werden grundsätzlich zwei Kommunikationspartner unterschieden: Authenticator und Peer. Dabei handelt es sich beim Authenticator um den Kommunikationspartner, der die Authentisierung abfordert, und beim Peer um den Kommunikationspartner, der die Authentisierung erbringen soll. Im Allgemeinen wird also der Authenticator der Server sein, an dem sich der Benutzer von seinem IT-System aus als Peer anmelden will.

Bei CHAP wird auf beiden Seiten die Kenntnis eines gemeinsamen Geheimnisses (Passwort) überprüft. Dabei wird das Geheimnis nicht im Klartext über die Leitung gesandt und durch die Einbindung von Zufallszahlen vor Wiedereinspielen geschützt.

Das eingesetzte Challenge-Response-Protokoll läuft wie folgt ab:

In einem ersten Schritt errechnet der Authenticator eine Zufallszahl. Mittels eines Hash-Algorithmus wird der Hashwert der eben berechneten Zufallszahl gebildet. Eine Hashfunktion ist eine Rechenvorschrift, durch die eine Eingabe beliebiger Länge in einen Ausgabewert fester (im Allgemeinen kürzerer) Länge umgewandelt wird. Eine Einweg-Hashfunktion funktioniert nur in eine Richtung, d. h. aus der Eingabe lässt sich problemlos der Hashwert berechnen, aber es sollte sehr schwer bis unmöglich sein, zu einem Hashwert passende Eingabedaten zu berechnen.

Im nächsten Schritt überträgt der Authenticator das so genannte Challenge, also die eben errechnete Zufallszahl, an den Peer. Da Authenticator und Peer über den gleichen Hash-Algorithmus verfügen, kann in einem vierten Schritt ebenfalls der Peer den Hashwert der eben übermittelten Zufallszahl bilden. Der Peer berechnet den Hashwert über die drei Werte Identifier (Benutzer-Kennung), Secret (Passwort) und der gesendeten Zufallszahl. Den Hashwert überträgt er dann als Antwort an den Authenticator. Der Authen-

ticator überprüft die Korrektheit des Passworts, indem er ebenfalls den entsprechenden Hashwert berechnet und mit dem übermittelten Hashwert vergleicht. Fällt der Vergleich positiv aus, hat sich der Peer gegenüber dem Authenticator authentisiert und die Kommunikationsverbindung kann aufgebaut werden.

Die Authentisierung nach dem eben beschriebenen Verfahren sollte auch während einer bestehenden Kommunikationsverbindung mehrfach wiederholt werden, um auch Attacken auf bereits bestehende Verbindungen zu verhindern. Dies wird, ohne das der Benutzer eingreifen muss, in zufälligen Zeitabständen durch den Authenticator angestoßen.

Ergänzende Kontrollfragen:

- Verfügt die eingesetzte ISDN-Karte bzw. die verwendete Kommunikationssoftware über die Möglichkeit, Authentisierungsprotokolle wie PAP und CHAP zu nutzen?
- Werden vorhandene Authentisierungsprotokolle genutzt?

M 5.51 Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator, Telearbeiter

Erfolgt im Rahmen der Telearbeit eine Datenübertragung zwischen einem Telearbeitsrechner und dem Kommunikationsrechner der Institution, werden dabei dienstliche Informationen üblicherweise über öffentliche Kommunikationsnetze übertragen. Da weder die Institution noch der Telearbeiter großen Einfluss darauf nehmen können, ob die Vertraulichkeit, Integrität und Verfügbarkeit im öffentlichen Kommunikationsnetz gewahrt werden, sind ggf. zusätzliche Maßnahmen erforderlich, falls das öffentliche Netz keine ausreichende Sicherheit bieten kann.

Generell muss die Datenübertragung zwischen Telearbeitsrechner und Institution folgende Sicherheitsanforderungen erfüllen:

- *Sicherstellung der Vertraulichkeit der übertragenen Daten*: es muss durch eine ausreichend sichere Verschlüsselung erreicht werden, dass auch durch Abhören der Kommunikation zwischen Telearbeitsrechner und Kommunikationsrechner der Institution kein Rückschluss auf den Inhalt der Daten möglich ist. Dazu gehört neben einem geeigneten Verschlüsselungsverfahren auch ein angepasstes Schlüsselmanagement mit periodischem Schlüsselwechsel.
- *Sicherstellung der Integrität der übertragenen Daten*: die eingesetzten Übertragungsprotokolle müssen eine zufällige Veränderung übertragener Daten erkennen und beheben. Bei Bedarf kann auch ein zusätzlicher Fehlererkennungsmechanismus benutzt werden, um absichtliche Manipulationen während der Datenübertragung detektieren zu können.
- *Sicherstellung der Verfügbarkeit der Datenübertragung*: falls zeitliche Verzögerungen bei der Telearbeit nur schwer zu tolerieren sind, sollte ein redundant ausgelegtes öffentliches Kommunikationsnetz als Übertragungsweg ausgewählt werden, in dem der Ausfall einzelner Verbindungsstrecken nicht den Totalausfall der Kommunikationsmöglichkeiten bedeutet. Auf eine redundante Einführung der Netzanbindung an den Telearbeitsrechner und die Schnittstelle der Institution kann ggf. verzichtet werden.
- *Sicherstellung der Authentizität der Daten*: bei der Übertragung der Daten zwischen Telearbeitsrechner und Institution muss vertrauenswürdig feststellbar sein, ob die Kommunikation zwischen den richtigen Teilnehmern stattfindet, so dass eine Maskerade ausgeschlossen werden kann. Dies bedeutet, dass Daten mit Absender "Telearbeitsrechner" auch tatsächlich von dort stammen. Ebenso muss der Ursprung von Institutionsdaten zweifelsfrei auf die Institution zurückgeführt werden können.
- *Sicherstellung der Nachvollziehbarkeit der Datenübertragung*: um eine Kommunikation nachvollziehbar zu machen, können Protokollierungs-

funktionen eingesetzt werden, die nachträglich feststellen lassen, welche Daten wann an wen übertragen wurden.

- *Sicherstellung des Datenempfangs*: ist es für die Telearbeit von Bedeutung, ob Daten korrekt empfangen wurden, so können Quittungsmechanismen eingesetzt werden, aus denen hervorgeht, ob der Empfänger die Daten korrekt empfangen hat.

Die Stärke der dazu erforderlichen Mechanismen richtet sich dabei nach dem Schutzbedarf der übertragenen Daten.

Ergänzende Kontrollfragen:

- Stellen die eingesetzten Kommunikationsprotokolle die oben genannten Anforderungen in ausreichender Güte zur Verfügung?

M 5.52 Sicherheitstechnische Anforderungen an den Kommunikationsrechner

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Je nach Art der Telearbeit und der dabei durchzuführenden Aufgaben gestaltet sich der Zugriff des Telearbeiters auf Institutionsdaten anders. Denkbar ist es, dass zwischen Telearbeiter und Institution nur E-Mails ausgetauscht werden. Andererseits kann auch ein Zugriff auf Server in der Institution für den Telearbeiter notwendig sein. Unabhängig von den Zugriffsweisen muss der Kommunikationsrechner der Institution dennoch folgende Sicherheitsanforderungen erfüllen:

- *Identifikation und Authentisierung*: Sämtliche Benutzer des Kommunikationsrechners, also Administratoren, Mitarbeiter in der Institution und Telearbeiter, müssen sich vor einem Zugriff auf den Rechner identifizieren und authentisieren. Nach mehrfachen Fehlversuchen ist der Zugang zu sperren. Voreingestellte Passwörter sind zu ändern.

  Ggf. muss es für den Kommunikationsrechner auch möglich sein, während der Datenübertragung eine erneute Authentisierung des Telearbeiters oder des Telearbeitsrechners anzustoßen, um aufgeschaltete Angreifer abzuwehren.

  Im Rahmen der Identifikation und Authentisierung der Benutzer sollte auch zusätzlich eine Identifizierung der Telearbeitsrechner stattfinden (zum Beispiel über Rufnummern und Callback-Verfahren).

- *Rollentrennung*: die Rollen des Administrators und der Benutzer des Kommunikationsrechners sind zu trennen. Eine Rechtevergabe darf ausschließlich dem Administrator möglich sein.

- *Rechteverwaltung und -kontrolle*: der Zugriff auf Dateien des Kommunikationsrechners darf nur im Rahmen der gebilligten Rechte erfolgen können. Darüber hinaus muss insbesondere der Zugang zu angeschlossenen Rechnern in der Institution und darauf gespeicherten Dateien reglementiert sein. Zugangs- und Zugriffsmöglichkeiten sind auf das notwendige Mindestmaß zu beschränken.

  Bei Systemabsturz oder bei Unregelmäßigkeiten muss der Kommunikationsrechner in einen sicheren Zustand übergehen, indem ggf. kein Zugang mehr möglich ist.

- *Minimalität der Dienste*: Dienste, die durch den Kommunikationsrechner zur Verfügung gestellt werden, müssen dem Minimalitätsprinzip unterliegen: alles ist verboten, was nicht ausdrücklich erlaubt wird. Die Dienste selbst sind auf den Umfang zu beschränken, der für die Aufgaben der Telearbeiter notwendig ist.

- *Protokollierung*: Datenübertragungen vom, zum und über den Kommunikationsrechner sind mit Uhrzeit, Benutzer, Adressen und Dienst zu protokollieren.

  Dem Administrator bzw. dem Revisor sollten Werkzeuge zur Verfügung stehen, um die Protokolldaten auszuwerten. Dabei sollten Auffälligkeiten automatisch gemeldet werden.

- *Automatische Computer-Viren-Prüfung*: übertragene Daten sind einer automatischen Prüfung auf Computer-Viren zu unterziehen.

- *Verschlüsselung*: Daten, die auf dem Kommunikationsrechner für die Telearbeiter vorgehalten werden, sind bei entsprechender Vertraulichkeit zu verschlüsseln.

- *Vermeidung oder Absicherung von Fernadministration*: benötigt der Kommunikationsrechner keine Fernadministration, so sind sämtliche Funktionalitäten zur Fernadministration zu sperren. Ist eine Fernadministration unvermeidbar, so muss sie ausreichend abgesichert werden. Jegliche Fernadministration darf nur nach vorhergehender erfolgreicher Identifikation und Authentisierung stattfinden. Administrationstätigkeiten sind zu protokollieren. Administrationsdaten sollten verschlüsselt übertragen werden. Voreingestellte Passwörter und kryptographische Schlüssel sind zu ändern.

Ergänzende Kontrollfragen:

- Welche Funktionalitäten bietet der Kommunikationsrechner?
- In welchen Zeitabständen wird überprüft, ob die gewählten Einstellungen und Rechte noch den Notwendigkeiten entsprechen?

M 5.53 Schutz vor Mailbomben

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Mailbomben sind E-Mails, die absichtlich eingebaute Schadfunktionen enthalten. Als Mailbombe kann sich beispielsweise eine als Anlage mitversandte komprimierte Datei erweisen, die nach dem Auspacken Unmengen von Unterverzeichnissen anlegt oder sehr viel Festplattenplatz beansprucht.

Archive, also mit Packprogrammen komprimierte Dateien, sollten niemals ohne vorhergehende Prüfung ausgepackt werden. Um sich vor trojanischen Pferden oder anderen Schadfunktionen in komprimierten Dateien zu schützen, sollte man sich vor dem Auspacken solcher Dateien das Inhaltsverzeichnis über die archivierten Dateien und deren Größe anzeigen lassen. Weiterhin sollten Archivdateien bereits vor dem Auspacken auf Computer-Viren überprüft werden.

Auf Arbeitsplatzrechnern sollten selbstextrahierende Archive, also solche mit Endungen wie *.EXE, niemals aufgerufen werden, da vor dem Auspacken der Inhalt nicht geprüft kann.

Neue Programme sollten immer zunächst auf von den Produktionssystemen getrennten IT-Systemen getestet werden (siehe M 4.65 *Test neuer Hard- und Software*).

Bei Unix-Systemen und anderen Server-Betriebssystemen sind außerdem folgende Punkte zu beachten:

- Unbekannte Archive dürfen nie unter Superuser-Berechtigung ausgepackt werden, sondern nur unter einer Benutzer-Kennung mit möglichst wenig Schreibrechten.
- Es sollte ein Filesystem mit Disk-Quota verwendet werden, um den Festplattenplatz zu begrenzen, den ein solches Programm im schlimmsten Fall belegen kann.

Ergänzende Kontrollfragen:

- Sind die Benutzer über die Mailbomben-Problematik informiert?

M 5.54 Schutz vor Mailüberlastung und Spam

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Mit "Spam" werden E-Mails bezeichnet, die in Massen verschickt werden und die die Empfänger belästigen. Dazu gehören Kettenbriefe, unerwünschte Werbung, Bettelbriefe und Junkmails. Durch die Überhäufung mit Werbemails oder durch absichtliche Überlastung durch eingehende E-Mails kann nicht nur das E-Mail-System blockiert werden, sondern es kann auch für den Empfänger solcher E-Mail teuer werden. Kosten entstehen unter anderem durch Übertragungsgebühren, insbesondere dann, wenn Bilder oder Multimediadateien in den unerwünschten E-Mails enthalten sind. Dazu kommt auch noch die Arbeitszeit, die benötigt wird, um die eingegangene Spam-Mail zu sichten und zu löschen.

Um sich vor Spam zu schützen, sollte jeder Benutzer überlegen, wann und an wen er seine E-Mail-Adresse weitergibt. Besonders vorsichtig sollten Benutzer mit der Herausgabe der Adresse beispielsweise in Newsgroups oder Mailinglisten, bei Gewinnspielen, bei Umfragen oder in ähnlichen Formularen sein.

Umgekehrt sollte auch darauf geachtet werden, die E-Mail-Adressen von Kommunikationspartnern nicht ungeprüft weiterzugeben. Besonders wenn mehrere Personen gleichzeitig mit einer E-Mail angeschrieben werden, sollte nicht jeder wissen, wer noch unter welcher E-Mail-Adresse angeschrieben worden ist. Um dies zu vermeiden, kann z. B. die Funktion "BCC" (*Blind Carbon Copy*) genutzt werden, die praktisch jeder E-Mail-Client bietet.

Spam löschen!

Grundsätzlich sollten alle Benutzer Spam ignorieren und löschen. Keinesfalls darf geantwortet werden, da dies eine Bestätigung für eine erfolgreich zugesendete E-Mail wäre. Darüber sollten auch alle Mitarbeiter informiert werden.

Mögliche Maßnahmen gegen Werbemails bzw. "Spam" sind die folgenden:

- Es können Anonymisierungsdienste (Anonyme Remailer Dienste) benutzt werden, die E-Mails "entpersonalisieren". Ein Remailer ermöglicht es, in eine Newsgruppe zu posten oder eine E-Mail zu versenden, ohne dass der Empfänger die E-Mail-Adresse des Absenders erkennen kann. Dies hat allerdings den Nachteil, dass häufig andere Personen den E-Mail-Kontakt verweigern, weil sie den Absender nicht identifizieren können.
- Auf dem E-Mail-Server bzw. der Firewall können E-Mail-Filterprogramme eingesetzt werden, die nur E-Mails von und/oder zu definierten Kommunikationspartnern zulassen oder über andere Header-Einträge versuchen, Spam auszugrenzen. Hierbei muss mit Bedacht vorgegangen werden, damit der Filterung keine erwünschten E-Mails zum Opfer fallen.

  Übersteigt die Anzahl der Werbe-E-Mails ein bestimmtes Maß, sollte überprüft werden, ob die Löschung dieser E-Mails an zentraler Stelle automatisiert durchgeführt werden sollte. So gibt es Programme, die Werbe-E-Mails automatisch erkennen und löschen. Die Erkennungsquote ist zwar nicht hundertprozentig, aber der Endanwender wird merklich entlastet. Der

Datendurchsatz kann je nach Prüfungsumfang geringer werden. Problematisch wäre jedoch, wenn normale E-Mails fälschlich als Werbung identifiziert und gelöscht werden. Ob und wie häufig dies eventuell eintritt, ist zu prüfen. Es gibt auch die Möglichkeit, Absenderadressen, von denen häufiger Werbe-E-Mails empfangen wurden, auf eine eigene Liste zu setzen und nachfolgende E-Mails von dieser Absenderadresse automatisch zu löschen oder zu ignorieren. Dieses Verfahren ist oft zuverlässiger als eine automatische Erkennung von Inhalten.

Filterung

Vor dem Einsatz zentraler Filterprogramme muss unbedingt festgelegt werden, wer was wann bewertet, in welche Listen was eingetragen und überwacht wird. Der Datenschutzbeauftragte und die Personalvertretung sind dabei zu beteiligen, außerdem müssen die Benutzer über die ergriffenen Maßnahmen informiert werden.

- Die meisten E-Mail-Clients können ebenfalls so konfiguriert werden, dass entweder nur E-Mails bestimmter Absender durchgelassen werden oder dass Post von bestimmten Absendern - also Spammern - ausgefiltert wird. Bei Outlook Express etwa können eingehende Nachrichten mit Hilfe des Posteingangs-Assistenten direkt in den gewünschten Ordner verteilt werden - im Fall von Spam z. B. in den Ordner G*elöschte Objekte*.
- Jede Organisation sollte festlegen, ob ihre Mitarbeiter Artikel in Newsgruppen posten dürfen und wenn ja, in welcher Form und zu welchen Themen. Dabei sind die Benutzer darauf hinzuweisen, dass die Netiquette zu beachten ist, insbesondere ist die Verbreitung von für die Allgemeinheit irrelevanten Informationen zu unterlassen.
- Es kann u. U. sinnvoll sein, keine leicht erratbaren E-Mailadressen zu verwenden (siehe auch M 2.122 *Einheitliche E-Mail-Adressen*).

  Wenn die Angabe einer Adresse für Mailinglisten, Abfragen oder ähnliches erforderlich ist, besteht eine andere Möglichkeit darin, eine spezielle E-Mail-Adresse dafür einzurichten. E-Mail an diese Adresse kann dann gefiltert, ignoriert oder gelöscht werden. Falls hierzu keine Absenderadressen aus der eigenen Domain gewählt werden sollen, kommen hierfür auch die Anbieter von kostenlosen E-Mail-Accounts in Betracht.
- Auf keinen Fall sollte versucht werden, Spam-Verursacher durch Mailbomben oder ähnliches zu bestrafen. Spam sollte nicht einmal durch ein Reply beantwortet werden. Häufig sind die Absenderangaben in Spam-Mail gefälscht. Antworten erreichen dann nur Unschuldige oder kommen als unzustellbar zurück. Auf jeden Fall verursachen auch Antworten wiederum ein erhöhtes Netzaufkommen und im schlimmsten Fall bestätigen sie Werbemailern sogar noch die Korrektheit angeschriebener E-Mail-adressen.
- Auch wenn bei Spam-Mail die Möglichkeit angeboten wird, sich für weitere E-Mails streichen zu lassen, sollte auf keinen Fall auf solche E-Mails reagiert werden. Anderenfalls kann der Spammer die Antwort als Bestätigung nutzen, dass die angeschriebene E-Mail-Adresse korrekt ist.

- Eine weitere Maßnahme gegen akute Belästigung durch Spam ist die Benachrichtigung des eigenen Mailproviders sowie des Mailproviders des Verursachers, damit diese gegen den Verursacher vorgehen können. Allerdings sollte dabei berücksichtigt werden, dass nicht alle Mailprovider zeitnah auf solche Beschwerden reagieren.

Dabei ist zu beachten, dass nicht alle dieser Maßnahmen in allen Umgebungen sinnvoll sind, weil sie diverse Einschränkungen mit sich bringen. So kann es einerseits sinnvoll sein, nicht aus den Benutzernamen abgeleitete E-Mailadressen zu verwenden, um sich vor unerwünschten Werbemails zu schützen. Andererseits können abstrakte E-Mailadressen die Kommunikation mit Externen erschweren, da sie schwerer zu merken sind. Die Form der E-Mailadressen muss auf jeden Fall den organisationsinternen Regelungen genügen.

Mailinglisten

Durch die Eintragung auf Mailinglisten kann ebenfalls eine hohe Mailbelastung entstehen. Generell sollte regelmäßig überprüft werden, ob die in einer Mailingliste diskutierten Inhalte das Lesen lohnen, sonst ist sie abzubestellen. Die Benutzer müssen darüber informiert sein, dass nach der Eintragung auf Mailinglisten die dadurch entstehende Mailbelastung regelmäßig, d. h. möglichst täglich, zu kontrollieren ist. In größeren Organisationen sollten für die Arbeit interessante Mailinglisten nur über einen Mitarbeiter (z. B. den Mail-Administrator) abonniert werden und dann zentral allen zur Verfügung gestellt werden.

E-Mail-Adressen auf Webseiten

Auch bei der Gestaltung von Webseiten sollte an Spam gedacht werden. Spammer versuchen u. a. ihren Adresspool dadurch zu erweitern, dass sie mit Tools Webseiten automatisch darauf absuchen, ob dort E-Mail-Adressen genannt sind, z. B. für Nachfragen. Es gibt leider kaum wirksame Möglichkeiten, solche automatischen Auswerte-Tools scheitern zu lassen. Daher sollte genau überlegt werden, ob und welche E-Mail-Adressen auf Webseiten bekannt gegeben werden. Hierfür können beispielsweise aufgabenbezogene E-Mail-Adressen eingerichtet werden. Auch diese werden natürlich mit Spam belästigt werden, aber das Problem kann auf diese Weise begrenzt werden. Für die Sichtung der eingehenden Mails und die Trennung der "echten" Mail-Eingänge vom Spam sollte ausreichend Zeit vorgesehen werden.

Ergänzende Kontrollfragen:

- Sind die Benutzer über die Spam-Problematik informiert?
- Wer hat welche Mailinglisten abonniert?
- Welche E-Mail-Adressen werden auf den Webseiten der Organisation verwendet?

M 5.55 Kontrolle von Alias-Dateien und Verteilerlisten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Um die Adressierung von E-Mails zu vereinfachen, werden häufig Alias-Dateien oder Verteilerlisten geführt. Werden sowohl auf den Mailservern als auch auf den Mail-Clients Alias-Dateien geführt, ist zunächst zu klären, welche Einträge Priorität haben, d. h. ob bei gleicher Wahl eines Alias der vom Mailserver oder der vom Mail-Client akzeptiert wird. Beim Empfang von E-Mails sollte die Alias-Umsetzung des Mailservers ausschlaggebend sein, beim Versand die des Mail-Clients. Die Benutzer müssen darüber informiert sein, welche Aliase auf dem Mailserver aufgelöst werden, damit sie dies bei der Weitergabe von E-Mailadressen berücksichtigen können.

Damit die Benutzer die Alias-Dateien auf dem Mailserver verwenden können, müssen sie lesend darauf zugreifen können. Schreibrecht darauf sollte aber nur der Mail-Administrator haben.

Um zu verhindern, dass E-Mails aufgrund fehlerhafter, nicht aktueller oder manipulierter Verteilerlisten an falsche Empfänger übertragen werden, müssen die Verteilerlisten regelmäßig auf Korrektheit und Aktualität überprüft werden.

Ergänzende Kontrollfragen:

- Wo sind Alias-Dateien bzw. Verteilerlisten angelegt?
- Wer hat Zugriff auf Alias-Dateien bzw. Verteilerlisten?
- Wann wurden die Alias-Dateien, Verteilerlisten und gespeicherte E-Mailadressen zuletzt auf Aktualität geprüft?

M 5.56 Sicherer Betrieb eines Mailservers

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der sichere Betrieb eines Mailservers setzt voraus, dass sowohl die lokale Kommunikation als auch die Kommunikation auf Seiten des öffentlichen Netzes abgesichert wird. Der Mailserver nimmt von anderen Mailservern E-Mails entgegen und leitet sie an die angeschlossenen Benutzer oder Mailserver weiter. Weiterhin reicht der Mailserver die gesendeten E-Mails lokaler Benutzer an externe Mailserver weiter. Der Mailserver muss hierbei sicherstellen, dass lokale E-Mails der angeschlossenen Benutzer nur intern weitergeleitet werden und nicht in das öffentliche Netz gelangen können.

Ein Mailserver speichert die E-Mail bis zur Weitergabe zwischen. Viele Internet-Provider und Administratoren archivieren zusätzlich die ein- und ausgehenden E-Mails. Damit Unbefugte nicht über den Mailserver auf Nachrichteninhalte zugreifen können, muss der Mailserver gegen unbefugten Zugriff gesichert sein. Dafür sollte er gesichert (in einem Serverraum oder Serverschrank) aufgestellt sein. Für den ordnungsgemäßen Betrieb sind ein Administrator und Stellvertreter zu benennen und zum Betrieb des Mailservers und dem zugrunde liegenden Betriebssystems zu schulen. Es muss ein Postmaster-Account eingerichtet werden, an den alle unzustellbaren E-Mails und alle Fehlermeldungen weitergeleitet werden (siehe auch M 2.120 *Einrichtung einer Poststelle*).

Auf die Mailboxen der lokal angeschlossenen Benutzer dürfen nur diese Zugriff haben. Auf die Bereiche, in denen E-Mails nur temporär für die Weiterleitung zwischengespeichert werden (z. B. Spooldateien), ist der Zugriff auch für die lokalen Benutzer zu unterbinden.

Es muss regelmäßig kontrolliert werden, ob die Verbindung mit den benachbarten Mailservern, insbesondere dem Mailserver des Mailproviders, noch stabil ist. Es muss regelmäßig überprüft werden, ob der für die Zwischenspeicherung der Mail zur Verfügung stehende Plattenplatz noch ausreicht, da ansonsten kein weiterer Nachrichtenaustausch möglich ist.

Umfang und Inhalt der Protokollierung der Aktivitäten des Mailservers sind festzulegen. Die Protokolldaten müssen regelmäßig ausgewertet werden, vor allem um festzustellen, ob Angriffe auf den Mailserver erfolgt sind und welche Auswirkungen diese nach sich gezogen haben.

Von der Verfügbarkeit des Mailservers sollten keine weiteren Dienste abhängig sein, beispielweise sollte der Mailserver nicht gleichzeitig auch als Fileserver dienen. Es sollte jederzeit kurzfristig möglich sein, ihn abzuschalten, z. B. bei Denial-of-Service-Angriffen oder bei Verdacht auf Manipulationen (siehe auch M 4.97 *Ein Dienst pro Server*).

Die Benutzernamen auf dem Mailserver sollten nicht aus den E-Mailadressen unmittelbar ableitbar sein, um mögliche Angriffe auf Benutzer-Accounts zu erschweren.

Der Status einer E-Mail kann dem Sender mit einer Delivery Status Notification übermittelt werden. Grundsätzlich sind Non Delivery Notifications RFC-konform und sinnvoll. So können beispielsweise

Schreibfehler bei der Empfängeradresse bemerkt werden. Andererseits können Delivery Status Notifications zur Überlastung von E-Mail-Servern beitragen, wenn E-Mails in Massen an nicht existierende Empfänger versendet werden, was beispielsweise durch Spam oder Schadsoftware ausgelöst werden kann.

Um beiden Punkten gerecht zu werden, kann folgendes Vorgehen ratsam sein: Non Delivery Notifications werden grundsätzlich erlaubt. Gleichzeitig wird die Auslastung des eigenen E-Mail-Servers beobachtet. Steigt die Anzahl der Non Delivery Notifications über einen zu definierenden Schwellwert an, wird der Versand von Delivery Status Notifications deaktiviert, da der Verdacht besteht, dass ein neuer Spam- oder Schadsoftware-Vorfall aufgetreten ist.

Firewall / DMZ

Naturgemäß muss der Mailserver aus dem Internet erreichbar sein. Daher sollte der Server durch entsprechende Maßnahmen auch auf Netzebene abgesichert werden. Dies kann beispielsweise dadurch geschehen, dass von einer vorgeschalteten Firewall Verbindungen von außen nur zu den entsprechenden Ports zugelassen werden. Noch besser ist es, den Mailserver in einer Demilitarisierten Zone (DMZ) anzusiedeln und auch die Verbindungen zum internen Netz auf die notwendigen Protokolle und Dienste zu beschränken.

Protokolle und Dienste festlegen

Es ist festzulegen, welche Protokolle und Dienste am Mailserver erlaubt sind. Beispielsweise ist es meist nötig, SMTP (TCP-Port 25) nach außen und innen zuzulassen. Hingegen sollten die Protokolle POP3 oder IMAP (TCP Ports 110 bzw. 143, je nachdem, auf welche Art und Weise Mails vom Server abgerufen werden) nur für Zugriffe aus dem internen Netz zugelassen werden. Sowohl für POP3 als auch für IMAP existieren Varianten, bei denen Anmeldung und Datenübertragung durch SSL gesichert werden. Falls die eingesetzte Software diese Varianten unterstützt, sollten sie nach Möglichkeit auch eingesetzt werden.

Schutz vor Computer-Viren

E-Mails sind eines der verbreitesten Medien, um Computer-Viren zu verbreiten. Um sich hiergegen abzusichern, gibt es verschiedene Strategien (siehe auch M 2.156 *Auswahl einer geeigneten Computer-Virenschutz-Strategie*). Die Erfahrung hat gezeigt, dass E-Mails sowohl an der Firewall oder auf dem Mailserver als auch auf jedem Client-Rechner auf Computer-Viren oder -Würmer und andere schädliche Inhalte wie aktive Inhalte (z. B. eingebetteten JavaScript-Code) überprüft werden sollten (siehe M 5.109 *Einsatz eines E-Mail-Scanners auf dem Mailserver*). Alle eingesetzten Viren-Schutzprogramme müssen regelmäßig aktualisiert werden.

Filterregeln für Empfang oder Weiterleitung von E-Mails

Über Filterregeln kann der Empfang oder die Weiterleitung von E-Mails für bestimmte E-Mailadressen gesperrt werden. Dies kann beispielsweise sinnvoll sein, um sich vor Spam-Mail zu schützen. Auch über die Filterung anderer Header-Einträge kann versucht werden, Spam auszugrenzen. Hierbei muss allerdings mit Bedacht vorgegangen werden, damit der Filterung keine erwünschten E-Mails zum Opfer fallen. Daher sollten entsprechende Filterregeln sehr genau definiert werden, indem beispielsweise aus jeder Spam-Mail eine neue dedizierte Filterregel abgeleitet wird. Entsprechende Filterlisten sind im Internet verfügbar bzw. können von verschiedenen Herstellern der Kommunikationssoftware bezogen werden.

Durch entsprechende Filterregeln können Datei-Typen (z. B. *.VBS, *.WSH, *.BAT, *.EXE), die im täglichen Arbeitsablauf nicht als Anhänge von E-Mails vorkommen dürfen (siehe auch M 4.199 *Vermeidung gefährlicher Dateiformate*), zentral blockiert werden.

MX-Einträge und Relaying

Das Internet-Namensschema DNS sieht es vor, mittels eines so genannten MX-Eintrags einen bestimmten Server als *Mailexchanger* zu kennzeichnen. Normalerweise sollten dann E-Mails zwischen Rechnern verschiedener Domains nur über den den jeweils "zuständigen" Mailexchanger weiter geleitet werden. Das Weiterleiten von E-Mails zwischen verschiedenen Domains bezeichnet man als *Relaying*. Ein Mailserver sollte davor geschützt werden, als Spam-Relay verwendet zu werden. Dafür sollte der Mailserver so konfiguriert sein, dass er E-Mails nur für die eigene Organisation entgegennimmt und nur E-Mails verschickt, die von Mitarbeitern der Organisation stammen. Der Mailserver sollte eingehende E-Mails nur dann annehmen, wenn entweder die IP-Adresse des absendenden Mailservers in einem vom Administrator explizit zugelassenen IP-Netz liegt oder wenn er selbst für die Empfängeradresse als Mail-Exchanger fungiert. Alle anderen E-Mails sollten mit einer Fehlermeldung abgewiesen werden.

Berechtigte Benutzer können trotz dieser Maßnahmen weiterhin E-Mails an beliebige Empfänger versenden, ebenso können sie E-Mails von beliebigen Absendern empfangen. Durch die oben beschriebene Filterung eingehender E-Mails wird jedoch verhindert, dass der Mailserver von externen Nutzern als Spam-Relay missbraucht werden kann.

Sollten versehentlich IP-Netze, aus denen E-Mails angenommen werden sollen, nicht in obiger Liste stehen, muss der Administrator des Mailservers davon in Kenntnis gesetzt werden, damit er diese nachtragen kann.

Wenn eine Organisation keinen eigenen Mailserver betreibt, sondern über einen oder mehrere Mail-Clients direkt auf den Mailserver eines Providers zugreift, sollte mit dem Provider abgeklärt werden, welche Regelungen dort gelten und welche Sicherheitsmaßnahmen ergriffen worden sind (siehe M 2.123 *Auswahl eines Mailproviders*).

M 5.57 Sichere Konfiguration der Mail-Clients

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Die E-Mail-Progamme der Benutzer müssen durch den Administrator so vorkonfiguriert sein, dass ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht werden kann. Die Benutzer müssen darauf hingewiesen werden, dass sie die Konfiguration nicht selbsttätig ändern dürfen.

Insbesondere die folgenden Punkte sollten bei der Konfiguration der E-Mail-Clients berücksichtigt werden:

- Das E-Mail-Passwort darf keinesfalls dauerhaft vom E-Mail-Programm gespeichert werden. Dabei wird das Passwort auf der Client-Festplatte abgelegt, unter Umständen sogar im Klartext oder nur schwach verschlüsselt. Jeder, der Zugriff auf den Mail-Client hat, hat dann die Möglichkeit, das E-Mail-Passwort auszulesen oder unter fremden Namen E-Mails zu verschicken.
- Als Reply-Adresse muss die "offizielle" E-Mail-Adresse des Benutzers eingestellt werden. Dadurch wird vermieden, dass interne E-Mail-Adressen auf diesem Weg nach außen weitergegeben werden.
- Um die Netzbelastung niedrig zu halten, sollte der Mail-Client nicht zu häufig den Mailserver auf neue Nachrichten überprüfen. Ein automatischer Abholversuch alle 30 Minuten wird als Standardwert empfohlen und ist meist ausreichend. Falls Benutzer eine dringende Nachricht erwarten, sollten sie das E-Mail-Programm manuell dazu veranlassen, in ihrer Mailbox nachzusehen.
- Werden die Nachrichten per POP3 (*Post Office Protocol Version 3*) vom Mailserver abgeholt, so sollten sie dort auch gelöscht werden. Auf diese Weise kann ein mehrmaliges Abholen derselben Nachrichten verhindert und Speicherprobleme am Mailserver vermieden werden. Werden die Nachrichten auf dem Mailserver gespeichert und wird über IMAP (*Internet Message Access Protocol*) darauf zugegriffen, so sollte eine Größenbeschränkung für das serverseitige Postfach eingerichtet werden. Die Benutzer müssen in diesem Fall regelmäßig Mails vom Server löschen beziehungsweise in lokale Postfächer verschieben. Beim Erreichen der Obergrenze für die Postfachgröße sollten die Benutzer auf geeignete Weise darauf hingewiesen werden, beispielsweise mit einer entsprechenden Mail. Die Nachricht kann etwa folgendermaßen lauten:

  > *Ihr Postfach hat eine oder mehrere vom Administrator festgelegte Größenbeschränkungen überschritten.*
  >
  > *Die aktuelle Postfachgröße beträgt xxx KB.*
  >
  > *Maximale Postfachgröße: Sie werden benachrichtigt, wenn die Postfachgröße yyy KB überschreitet.*
  >
  > *Sie können möglicherweise keine neuen Nachrichten senden und empfangen, bis Sie die Postfachgröße verringern. Um Platz freizumachen, löschen oder verschieben Sie Objekte in lokale Ordner.*

- HTML-formatierte E-Mails können aktive Inhalte (beispielsweise Javascript, Flash, ActiveX oder Java) enthalten. Deshalb kommt es gerade durch HTML-formatierte E-Mails, etwa im Zusammenspiel mit Sicherheitslücken in E-Mail-Clients, oft zu Problemen. Um dies zu vermeiden, sollten E-Mail-Programme so eingestellt sein, dass sie aktive Inhalte in HTML-formatierten E-Mails nicht ohne Rückfrage ausführen. Möglichst sollten auch nur E-Mail-Clients eingesetzt werden, die HTML-formatierte E-Mails als solche vor dem Öffnen kenntlich machen. Falls der E-Mail-Client die Option bietet, HTML-formatierte E-Mails nicht automatisch formatiert darzustellen, sondern beim ersten Öffnen die Nachricht nur als Text (HTML-Quelltext) anzuzeigen, so sollte diese Möglichkeit genutzt werden.
- Wegen der möglichen Gefahren durch HTML-formatierte E-Mails sollten möglichst keine HTML-formatierten E-Mails verschickt werden. In der Konfiguration des E-Mail-Clients sollte "Nur Text" als Standardformat für neue E-Mails festgelegt werden.
- E-Mail-Anhänge (Attachments) sind ein beliebtes Transportmedium für Computer-Viren, Trojanische Pferde, Würmer und andere Schadprogramme. E-Mail-Programme sollten deshalb so eingestellt werden, dass ausführbare Dateien in Dateianhängen nicht automatisch oder direkt aus dem Mailprogramm heraus gestartet werden können, sondern zunächst auf die Festplatte gespeichert werden müssen. Vor dem Starten sollten die Benutzer die Dateien mit einem Viren-Schutzprogramm überprüfen. Noch besser ist der Einsatz eines Virensuchprogramms, das Dateien automatisch (*on-access*) überprüft.

Ergänzende Kontrollfragen:

- Sind die E-Mail-Clients so konfiguriert, dass die E-Mail-Passwörter nicht dauerhaft gespeichert werden?
- In welchen Abständen werden E-Mails vom Server abgerufen?
- Sind Größenbeschränkungen für die serverseitigen Postfächer eingerichtet?
- Wie sind die Einstellungen der E-Mail-Clients im Bezug auf HTML-formatierte E-Mails?
- Wie sind die Einstellungen der E-Mail-Clients im Bezug auf Attachments?

M 5.58 Auswahl und Installation von Datenbankschnittstellen-Treibern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Datenbankschnittstellen-Treiber, wie z.B. ODBC- (Open Database Connectivity), IDAPI- (Integrated Database Application Programming Interface) oder JDBC-Treiber (Java Database Connectivity), installieren zwischen Datenbankanwendungen und dem jeweiligen Datenbankprotokoll eine zusätzliche Software-Schicht. Durch die Installation des zur Datenbank passenden Treibers wird zwischen Anwendung und Datenbank eine einheitliche Schnittstelle geschaffen, über die die Kommunikation (Absetzen von Datenbankanfragen, Lesen von Daten) zur Datenbank abgewickelt wird. Die zugehörige ANSI-SQL-konforme SQL-Schnittstelle ermöglicht das Erstellen von Anwendungen, ohne auf die jeweiligen Spezifika unterschiedlicher Datenbank-Produkte Rücksicht nehmen zu müssen. Bei einem Wechsel der Datenbank-Software muss deshalb die Anwendung im Idealfall nicht angepasst werden, sondern es reicht aus, den Treiber auszutauschen. Ursprünglich für Produkte der Firmen Microsoft, Sun, etc. entwickelt, haben sich Datenbankschnittstellen-Treiber inzwischen als Standard etabliert und sind für alle gängigen Datenbank-Produkte erhältlich.

Bei der Auswahl eines Treibers müssen verschiedene Kriterien berücksichtigt werden. Die wichtigsten sind nachfolgend aufgeführt:

- Welche Treiber existieren für die anzusprechende Datenbank-Version?
- Welche Treiber existieren für die Betriebssystem-Version des Rechners, auf dem das Anwendungsprogramm läuft?
- Sollen Treiber des Datenbankherstellers (meist kostenlos) oder Treiber von Drittfirmen ausgewählt werden?
- Welcher SQL-Sprachumfang wird durch die Schnittstelle abgebildet?
- Welche sonstigen Anforderungen bringt die eingesetzte Rechnerarchitektur und die verwendete Software mit sich?

Anhand dieser Kriterien, und gegebenenfalls zusätzlicher Anforderungen, die vom Einsatzszenario abhängen, sollte ein geeigneter Treiber ausgewählt werden. Im Nachhinein sollte regelmäßig die getroffene Treiberauswahl überprüft werden. Anlass dazu können neben turnusmäßig vorgesehenen Systemprüfungen unter anderem Software-Upgrades der Datenbank oder des Betriebssystems bzw. neue Treiber-Versionen sein.

Bei der Installation von Datenbankschnittstellen-Treibern ist darauf zu achten, dass durch Fehler oder Nachlässigkeiten keine Sicherheitslücken hinsichtlich der Zugangskontrolle zum Datenbanksystem entstehen.

Um eine Anwendung mit einer Datenbank zu verbinden, muss mittels des Datenbankschnittstellen-Treibers eine sogenannte Datenquelle eingerichtet werden, die dann die Kommunikation zwischen Anwendung und Datenbank unterstützt. Diese Installation sollte nur von einem Administrator durchgeführt werden.

Einige Anwendungen installieren Datenquellen für Beispieldatenbanken oder unbenutzte Datenbankschnittstellen-Treiber. Um einen unerwünschten, eventuell unkontrollierten Zugriff über diese Datenquellen bzw. Treiber zu verhindern, sollten alle nicht benötigten Datenquellen und Treiber entfernt werden. Spezielle Hinweise hierzu finden sich in der Maßnahme M 5.101 *Entfernen nicht benötigter ODBC-Treiber beim IIS-Einsatz*.

Beispiel:

Für Microsoft Access Datenbanken ist die Verwendung von Benutzer-Kennungen optional und muss vom Entwickler explizit aktiviert werden. Wird die Zugangskontrolle aktiviert, so werden die Benutzer-Kennungen und Gruppenzugehörigkeiten über eine separate Microsoft Access Datenbank verwaltet, die sogenannte Arbeitsgruppen-Informationsdatei, die als eigene Datei (Standardname ab Microsoft Access 97: *system.mdw*, davor *system.mda*) gespeichert wird.

Bei der Installation eines ODBC-Treibers für den Zugriff auf eine Microsoft Access Datenbank wird die Arbeitsgruppen-Informationsdatei nicht automatisch integriert. Die Default-Einstellungen während der Installation lassen eine eventuell existierende Arbeitsgruppen-Informationsdatei unberücksichtigt. Wurde also während der Installation des ODBC-Treibers die Arbeitsgruppen-Informationsdatei nicht explizit angegeben, so führt dies unter Umständen dazu, dass ohne Identifizierung anhand der Arbeitsgruppen-Informationsdatei mittels ODBC auf die Datenbank zugegriffen werden kann. Somit kann gegebenenfalls die Zugangskontrolle unterlaufen werden.

Um dies zu verhindern, sind die Rechte in der jeweiligen Access-Anwendung so zu setzen, dass der Zugriff auf die Microsoft Access Datenbank nur mit der spezifizierten Arbeitsgruppen-Informationsdatei erfolgen kann.

Zusätzlich kann regelmäßig geprüft werden, ob die Arbeitsgruppen-Informationsdatei integriert ist, da dieser Mechanismus jederzeit wieder rückgängig gemacht bzw. manipuliert werden kann.

Ergänzende Kontrollfragen:

- Wurde ein Datenbankschnittstellen-Treiber für die Datenbank installiert?
- Wurden bei der Auswahl der Treiber-Version die Anforderungen des Datenbank-Systems und der Anwendung berücksichtigt?

M 5.59 Schutz vor DNS-Spoofing

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Gefahr durch DNS-Spoofing besteht dann, wenn eine Authentisierung anhand eines Rechnernamens durchgeführt wird. Eine hostbasierte Authentisierung, d. h. Rechte werden anhand eines Rechnernamens oder IP-Adresse gewährt, sollte durch eine der folgenden Konfigurationen (auch in Kombination) erschwert werden:

1. Es sollten IP-Adressen, keine Hostnamen verwendet werden.
2. Wenn Hostnamen verwendet werden, sollten alle Namen lokal aufgelöst werden (Einträge in der Datei */etc/hosts*).
3. Wenn Hostnamen verwendet werden und diese nicht lokal aufgelöst werden können, sollten alle Namen direkt von einem Nameserver aufgelöst werden, der für diese Namen der so genannte Primary- oder Secondary-Nameserver ist, d. h. er hat sie nicht in einem temporären Cache, sondern dauerhaft abgespeichert.

Punkt 1 bietet die höchste, Punkt 3 die niedrigste Sicherheit. Das Ziel obiger Konfigurationen ist es, die Zuordnung zwischen IP-Adressen und Rechnernamen in einem sicheren Umfeld vorzunehmen. Auf keinen Fall sollte ein hostbasierter Zugang über einen Hostnamen gewährt werden, wenn die Namensauflösung nicht direkt ausgeführt werden kann, also ein Cache zwischengeschaltet ist.

Ergänzende Kontrollfragen:

- Wird eine Zugriffssteuerung anhand von Rechnernamen durchgeführt? Falls ja: Welche Methode zum Schutz vor DNS-Spoofing wird eingesetzt?

M 5.60 Auswahl einer geeigneten Backbone-Technologie

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Die Auswahl des Netzprotokolls im Backbone-Bereich ist ein entscheidender Faktor für den Schutz der Verfügbarkeit der Anwendungen in einem lokalen Netz, da das gewählte Protokoll die Performance des Netzes und die zur Verfügung stehenden Bandbreiten wesentlich beeinflusst. Falls die zugrunde liegende Verkabelung ohne die Festlegung auf bestimmte Dienste (z. B. proprietäre Lösungen) geplant wurde (siehe G 2.45 *Konzeptionelle Schwächen des Netzes*), ist prinzipiell ein Wechsel der Backbone-Technologie problemlos möglich. Dennoch verursacht dies im Allgemeinen nicht unerheblichen organisatorischen, personellen und finanziellen Aufwand.

Eine generelle Empfehlung, unter IT-Sicherheitsgesichtspunkten eine bestimmte Backbone-Technologie auszuwählen, kann nicht gegeben werden, da viele individuelle Aspekte betrachtet werden müssen. Nachfolgend werden daher die Vor- und Nachteile der wichtigsten Netzzugangsprotokolle aufgeführt.

Es gibt die vier Basis-Technologien Ethernet, Token-Ring, FDDI und ATM, die sich wie folgt darstellen:

Ethernet

Die Ethernet-Technologie wird im **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers (IEEE) 802.3 Standard beschrieben und basiert auf dem CSMA/CD-Zugriffsverfahren (Carrier Sense Multiple Access / Collision Detection). Bei diesem Verfahren greifen alle Endgeräte gleichberechtigt auf das Übertragungsmedium zu, obwohl es jeweils nur exklusiv durch ein Endgerät genutzt werden kann. Sobald ein Endgerät Daten übertragen möchte, prüft es zunächst, ob das Medium für die Benutzung zur Verfügung steht (Carrier Sense). Ist dies der Fall, beginnt es mit der Datenübertragung. Geschieht dies durch mehrere Endgeräte gleichzeitig (Multiple Access), kommt es zu einer Kollision, die von den betroffenen Endgeräten erkannt wird (Collision Detection) und zu einer erneuten Prüfung des Mediums mit anschließender Wiederholung der Übertragung führt.

CSMA/CD ist ein stochastisches Verfahren und kann deshalb keine dedizierten Bandbreiten zusichern. Aus diesem Grund ist es beispielsweise für Multimedia-Anwendungen weniger geeignet, die eine feste Bandbreite benötigen. Auf Ethernet-basierten Netzen kann somit im Allgemeinen keine bestimmte Betriebsgüte (*Quality of Service* - QoS) zugesichert werden. Für Gigabit-Ethernet ist ein Analogon zur QoS vorgesehen.

Es gibt drei verschiedene Varianten des Ethernet, die sich prinzipiell nur in der unterstützten Übertragungsrate unterscheiden:

- **Standard Ethernet**

  Standard Ethernet ist der schon lange im Einsatz befindliche Standard und der Vorläufer der beiden anderen Varianten. Es ist durch eine

Übertragungsrate von 10 Mbit/s gekennzeichnet. Damit ist es für die meisten lokalen Netze als Backbone-Technologie ungeeignet, da es bei steigender Netzlast sehr schnell zu einer Vielzahl an Kollisionen kommt und dadurch der erzielbare Durchsatz immer mehr abnimmt.

- **Fast Ethernet**

  Aufgrund der steigenden Anzahl vernetzter Rechner und der damit verbundenen Netzlast wurde eine Weiterentwicklung des Standard Ethernet zwingend notwendig, um den gestiegenen Bedürfnissen Rechnung zu tragen. Dies führte zur Entwicklung des Fast Ethernet mit einer Übertragungsrate von 100 Mbit/s. Dies reicht zurzeit für die meisten Netze im Backbone-Bereich aus und hat außerdem den Vorteil, dass die bereits etablierte Technologie (CSMA/CD) weiter verwendet werden kann. Es müssen allerdings im Allgemeinen die aktiven Netzkomponenten ausgetauscht bzw. angepasst werden, und auch die Verkabelung ist auf eine Eignung für Fast Ethernet zu prüfen.

- **Gigabit Ethernet**

  Da die Einführung von Fast Ethernet sehr erfolgreich verlief, wurde die Forderung nach einer noch schnelleren Backbone-Technologie basierend auf Ethernet laut. Dies führte zur Gründung der Gigabit-Ethernet-Allianz (GEA) mit mehreren namhaften Herstellern, die eine Übertragungsrate von 1 Gbit/s erreichen wollen. Die Standardisierungsphase in Zusammenarbeit mit der IEEE befindet sich zur Zeit kurz vor dem Abschluss. Der neue Standard soll dann auch über eine Protokollerweiterung (Resource Reservation Protocol, RSVP) für zeitkritische Übertragungen (z. B. im Multimediabereich) dedizierte Bandbreiten über Gigabit-Ethernet zur Verfügung stellen. Damit wird versucht, zu ATM analoge Eigenschaften wie *Quality of Service* (QoS) bereitzustellen. Da der endgültige Standard aber noch nicht verabschiedet ist, wird momentan von dieser Variante abgeraten, um den Einsatz einer eventuell unvollständigen Implementation zu vermeiden.

Token-Ring

Die Token-Ring-Technologie wird im IEEE 802.5 Standard beschrieben und basiert auf dem Token-Passing-Verfahren. Dabei wird ein spezielles, im Ring kreisendes Datenpaket (das "Token") verwendet, um festzulegen, welches Endgerät das Übertragungsmedium benutzen darf. Erhält ein Endgerät das Token, belegt es das Medium und gibt das Token an das nächste Endgerät weiter. Hiermit ist gewährleistet, dass das Medium immer nur durch ein einziges Endgerät belegt wird.

Bei diesem deterministischen Verfahren kann es im Gegensatz zu Ethernet nicht dazu kommen, dass einzelne Endgeräte bei hoher Netzbelastung unbestimmt lange warten müssen, bis sie senden können. Token-Ring bietet dagegen eine fest bestimmbare maximale Wartezeit.

Ein Token-Ring-Netz ist meistens als physikalischer Doppelring ausgeführt, wodurch sich die Verfügbarkeit des Netzes merklich erhöht, da bei einem Ausfall einer Station oder der Unterbrechung eines Ringes die fehlerhafte Stelle durch die Nutzung des zweiten Ringes überbrückt werden kann.

Die Übertragungsrate von Token-Ring kann 4 oder 16 Mbit/s betragen, so dass mittlerweile auch hier von einem Einsatz als Backbone-Technologie für die meisten lokalen Netze abgeraten wird. Die zur Verfügung stehende Bandbreite ist zu gering. Mitte September 1997 wurde eine "High Speed Token Ring Alliance" (HSTR) von mehreren namhaften Herstellern gegründet mit dem Ziel, Übertragungsraten von 100 Mbit/s und später 1 Gbit/s zu erreichen. Dazu soll bis Mitte 1998 der IEEE 802.5 Standard erweitert werden. Da sich diese Varianten noch in der Entwicklung befinden, kann ein Einsatz zum jetzigen Zeitpunkt nicht befürwortet werden.

FDDI

Der FDDI (Fiber Distributed Data Interface) Standard wurde 1989 vom ANSI definiert und basiert wie Token-Ring auf dem Token-Passing-Verfahren. Allerdings kommt hier zusätzlich die Technik des Early-Token-Release zum Einsatz, bei der das Token direkt nach dem letzten Datenpaket an das nächste Endgerät weitergegeben wird. Dadurch werden die Leerlaufzeiten im Ring reduziert und es kann eine höhere Bandbreite erreicht werden.

FDDI nutzt Lichtwellenleiter als Übertragungsmedium mit einer Übertragungsrate von 100 Mbit/s. Durch seinen hohen Durchsatz ist es ideal für den Einsatz im Backbone-Bereich. Weitere Vorteile sind die Fehlertoleranz aufgrund der Doppelring-Topologie und die elektromagnetische Unempfindlichkeit durch die Verwendung von Lichtwellenleitern. Im Gegensatz zu Ethernet ist FDDI auch für laufzeitabhängige Multimedia-Anwendungen geeignet, da es eine maximale Verzögerungszeit garantieren kann.

Werden beide Ringe zur Übertragung genutzt, ist sogar eine Übertragungsrate von 200 Mbit/s erreichbar, allerdings entfällt dann der Vorteil der höheren Fehlertoleranz, da beim Ausfall eines Ringes nicht mehr automatisch auf den anderen Ring ausgewichen werden kann.

FDDI-Komponenten sind jedoch teurer als Ethernet-Komponenten vergleichbarer Funktion, so dass der erzielbare Nutzen durch den Einsatz von FDDI immer den entstehenden Kosten gegenübergestellt werden muss.

FDDI kann auch auf Kupferkabeln betrieben werden und wird dann CDDI (Copper Distributed Data Interface) genannt.

ATM

ATM steht als Abkürzung für Asynchronous Transfer Mode. Hinter diesem Begriff verbirgt sich ein Übertragungsverfahren, das sich sehr gut für den Einsatz im Backbone-Bereich eines Netzes eignet und dort auch Echtzeit-Dienste bereitstellen kann.

Bei ATM werden alle Arten von Informationen in Paketen mit fester Länge befördert, die als Zellen bezeichnet werden. Dabei kann es sich um beliebige Daten, wie z. B. auch Audio- und Video-Daten handeln. Durch die einheitliche Länge der Pakete wird es ermöglicht, dass die ATM-Switches die Verarbeitung der Zellen fast vollständig durch Hardware-Komponenten durchführen und somit einen höheren Durchsatz erreichen können. Dadurch entsteht eine kalkulierbare Verzögerung bei der Übertragung beliebiger

Informationen, so dass für einzelne Anwendungen garantierte Bandbreiten vergeben werden können. Damit ist ATM eine gut geeignete Technologie für Multimedia-Anwendungen, da ein berechenbares Echtzeitverhalten und damit *Quality of Service* (QoS) garantiert werden kann. Dies bedeutet, dass jedem angeschlossenen Gerät statisch oder dynamisch die benötigte Bandbreite zugeordnet werden kann.

Die Übertragung selbst beruht auf dem Prinzip der virtuellen Verbindungen. Dabei werden keine festen Kanäle zwischen den beteiligten Endgeräten geschaltet, vielmehr werden die Zellen erst zum Zeitpunkt ihrer Erzeugung über einen vorher festgelegten Weg durch das Netz transportiert. Die so erreichbaren Übertragungsraten liegen typischerweise bei 25 MBit/s, 155 MBit/s oder 622 MBit/s.

ATM-Komponenten sind allerdings derzeit noch sehr teuer, so dass eine Integration mit den im lokalen Netz bereits vorhandenen Komponenten anderer Technologien aus Gründen des Investitionsschutzes angestrebt werden sollte. ATM unterstützt jedoch keine Broadcasts oder die Benutzung von MAC-Adressen, was jedoch Voraussetzung für die Nutzung der meisten Protokollstapel wie TCP/IP oder SPX/IPX ist. Dazu existieren drei verschiedene Lösungsansätze:

- **Classical IP-over-ATM (CIP)**

  Für die Verwendung von IP über ATM wurde RFC 1577 (Classical IP-over-ATM) entwickelt, welches Endgeräten mit TCP/IP-Protokollstapel erlaubt, ATM als Transportmedium zu nutzen.

- **LAN Emulation (LANE)**

  Hier werden auf Schicht 2 des OSI-Modells alle relevanten LAN-Technologien für die Clients emuliert, für die sich ATM dann z. B. als Ethernet oder Token-Ring-Netz darstellt. Damit wird eine Kommunikation zwischen konventionellem LAN und ATM möglich.

- **Multiprotocol-over-ATM (MPOA)**

  MPOA ist prinzipiell eine Weiterentwicklung des klassischen ATM und LANE. Im Gegensatz zu LANE arbeitet MPOA auf der Schicht 3 des OSI-Modells und benutzt LANE zur Übertragung auf der Schicht 2. MPOA implementiert also sowohl Bridging (Schicht 2) als auch Routing (Schicht 3) und kann somit ein voll geroutetes ATM-Netz konfigurieren. Gleichzeitig bleiben jedoch alle Vorteile der ATM-Technologie, wie z. B. die garantierten Bandbreiten für bestimmte Anwendungen, erhalten.

Weiterhin ist zu beachten, dass z. Z. zwischen ATM-Komponenten verschiedener Hersteller keine Kompatibilität bzw. Interoperabilität garantiert ist. Dies ist daher im Einzelfall nachzuprüfen.

Eine allgemeine Empfehlung zur Auswahl einer Backbone-Technolgie kann, wie bereits eingangs erwähnt, nicht gegeben werden. Hier spielen neben Sicherheitsanforderungen auch Kriterien zur Zukunftssicherheit, Wirtschaftlichkeit, Skalierbarkeit und Integration vorhandener Komponenten eine Rolle.

Je nach ausgewähltem Protokoll können nur bestimmte Kabeltypen eingesetzt werden (z. B. LWL für FDDI), die wiederum durch bestimmte Längenrestriktionen eingeschränkt sind (siehe auch M 5.2 *Auswahl einer geeigneten Netz-Topographie*).

Ergänzende Kontrollfragen:

- Wurden die Anforderungen an den Backbone-Bereich des lokalen Netzes in bezug auf Verfügbarkeit, Bandbreiten und Performance formuliert und dokumentiert?
- Wurde eine Betrachtung aller relevanten Backbone-Technologien durchgeführt?

M 5.61 Geeignete physikalische Segmentierung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Unter einer physikalischen Segmentierung wird der Vorgang der Segmentbildung mit Hilfe von aktiven und passiven Netzkomponenten auf Schicht 1, 2 oder 3 verstanden. Eine geeignete physikalische Segmentierung kann zur Erhöhung der Verfügbarkeit, der Integrität und der Vertraulichkeit verwendet werden. Dies lässt sich durch den Einsatz unterschiedlicher Netzkomponenten (siehe M 5.13 *Geeigneter Einsatz von Elementen zur Netzkopplung*) erreichen.

Verfügbarkeit

Unter dem Gesichtspunkt der Verfügbarkeit wird auch die Performance bzw. die verfügbare Bandbreite eines Netzes betrachtet. Diese kann erhöht werden, wenn das Netz auf den Schichten 1, 2 oder 3 des OSI-Modells getrennt wird. Bei einer Auftrennung auf der Schicht 1 kann die geringste Erhöhung der Verfügbarkeit in den Einzelsegmenten, aber der höchste Durchsatz zwischen den Segmenten und bei einer Trennung auf Schicht 3 die größte Erhöhung der Verfügbarkeit und der geringste Durchsatz zwischen den Segmenten erzielt werden.

Durch eine Segmentierung auf Schicht 1 mit Hilfe eines Repeaters wird die Verfügbarkeit des Netzes dadurch erhöht, dass elektrische Fehler des einen Segmentes das andere nicht beeinflussen können.

Beispiel: Bei einem Netz aus zwei Thin-Ethernet-Segmenten, die durch einen Repeater miteinander verbunden sind, beeinflusst die fehlende Terminierung in einem Segment nicht die Funktion des anderen.

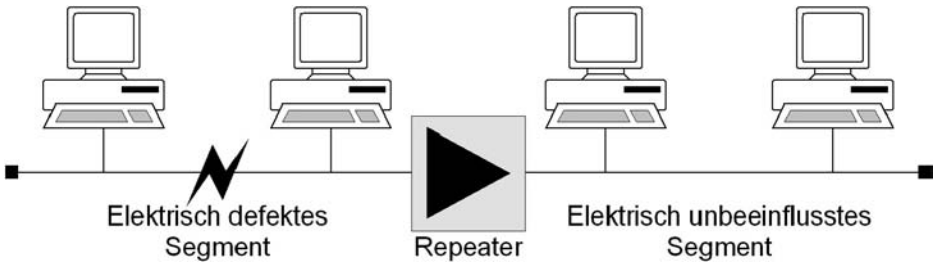


Abbildung: Elektrische Trennung von Segmenten durch einen Repeater zur Erhöhung der Verfügbarkeit

Für Bridges und Switches gilt zunächst einmal das gleiche wie für Repeater, da diese die Schicht 1 mit abdecken. Zusätzlich zu dieser Funktion werden fehlerhafte Datenpakete der Schicht 2 und Kollisionen in einem Segment isoliert. Weiterhin werden die Segmente entlastet, da Datenpakete zielgerichtet zwischen den Segmenten weitergeleitet werden können. Dabei ist darauf zu achten, dass die eingesetzte Bridge bzw. der Switch eine ausreichend hohe Kapazität (Filterrate und Transferrate) besitzt, um den Datenverkehr zwischen den Segmenten ohne große Verzögerungen zu verarbeiten.

Üblicherweise arbeiten Bridges/Switches auf der Schicht 2 des OSI-Modells. Diese werten für den Aufbau der Verbindungsmatrix die MAC-Adressen der beteiligten Systeme in den jeweiligen Segmenten aus. Von einigen Herstellern gibt es auch Switches, die auf Schicht 3 arbeiten, also beispielsweise die IP-Adresse zum Aufbau der Verbindungsmatrix verwenden. Dieser Aufbau geschieht in beiden Fällen automatisch, kann bei einigen Modellen jedoch auch manuell beeinflusst werden. Einige Hersteller bieten zusätzlich auch die Möglichkeit, die Verbindungsmatrix manuell (über ein zentrales Tool) auf Portebene, also auf der Ebene der tatsächlichen Kabelführung, vorzunehmen (Port- oder Configuration-Switching).

Router, die auf der Schicht 3 arbeiten, fassen die Eigenschaften von Repeatern und Bridges hinsichtlich der Verfügbarkeit zusammen und erweitern diese um die Fähigkeit, Protokolle der Schicht 3 auszuwerten. Hiermit erfolgt eine Lasttrennung auf einer höheren Ebene, wodurch der Netzverkehr fast vollständig kontrolliert werden kann. Insbesondere werden keine Broadcasts zwischen Segmenten (Teilnetzen) weitergeleitet, die durch einen Router getrennt sind. Ein Broadcaststurm auf dem einen Segment kann also das andere nicht beeinflussen.

Ausgehend von den Ergebnissen einer durchgeführten Verkehrsflussanalyse (siehe M 2.139 *Ist-Aufnahme der aktuellen Netzsituation*), sollte ggf. eine physikalische Segmentierung vorgenommen werden, um die Bandbreite bzw. Performance im erforderlichen Maße zu erhöhen.

Beispiel: Innerhalb eines Netzes sind zentrale Server für Datei- und Druckdienste sowie für die Anwendungen vorhanden bzw. geplant. Für eine hohe Performance und Verfügbarkeit kann es sinnvoll sein, diese dediziert an einen Switch anzuschließen und von diesem Switch die einzelnen Arbeitsplatzstationen anzubinden (shared oder switched). Wenn möglich, sollte die Verbindung zwischen den Servern und dem Switch zumindest eine Fast-Ethernet Verbindung sein.

Generell lässt sich festhalten, dass für eine höhere Performance ein geswitchtes Netz einem Shared-Netz vorzuziehen ist, da sich in einem Shared-Netz alle daran angeschlossenen Teilnehmer die verfügbare Bandbreite teilen müssen. In einem Switched-Netz dagegen steht jedem Teilnehmer zumindest bis zur nächsten aktiven Netzkomponente die volle Bandbreite zur Verfügung. Zu beachten sind hierbei allerdings die Notwendigkeit einer strukturierten Verkabelung (Sternform) und die relativ hohen Kosten für ein vollständig geswitchtes Netz.

Als Alternativen bieten sich Lösungen an, die im Backbone-Bereich oder im Bereich hoher Netzlast (z. B. Arbeitsgruppen) über einen Switch einzelne Netzsegmente koppeln, die wiederum als Shared-Media-LAN ausgelegt sind (siehe Abbildung 2). Zusätzlich besteht immer die Möglichkeit, einzelne Arbeitsplatzsysteme mit hohen Anforderungen an die Performance direkt an einen Switch anzuschließen. Während ein Shared-Netz bzw. Shared Segment sowohl in Bus- als auch in Sternform aufgebaut sein kann, ist es aus Gründen der Verfügbarkeit und des Investitionsschutzes sinnvoll, dieses ebenfalls in strukturierter Verkabelung (Sternform) auszuführen (siehe M 5.2 *Auswahl einer geeigneten Netz-Topographie*).

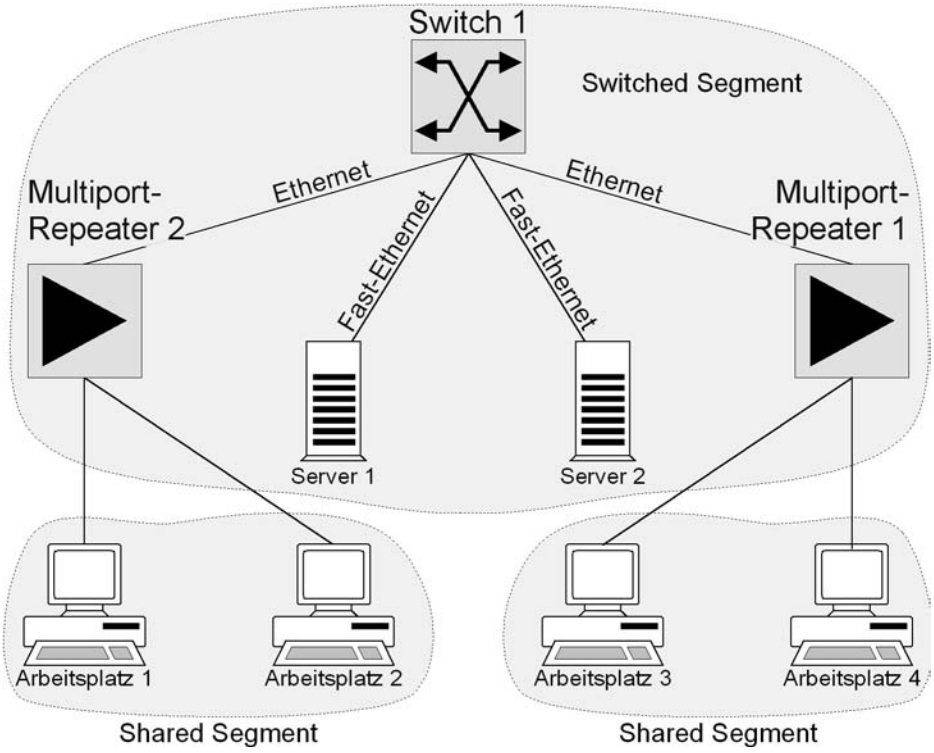


Abbildung: Beispiel für ein Netz, welches aus Switched und Shared Segmenten besteht. Die Anbindung der Server erfolgt über Fast-Ethernet.

Vertraulichkeit

Zur Erhöhung der Vertraulichkeit sind alle Maßnahmen geeignet, die einen Austausch von Daten zwischen zwei Segmenten verhindern. Aus diesem Grund ist ein reiner Repeater dafür ungeeignet. Einige Hersteller bieten Multiport-Repeater an, die so konfiguriert werden können, dass nur bestimmte Netzteilnehmer über solch einen Repeater im Netz arbeiten können. Hierdurch kann bis zu einem gewissen Grad ausgeschlossen werden, dass sich unberechtigte Nutzer auf das Netz aufschalten können. Bridges/Switches und Router erhöhen die Vertraulichkeit dadurch, dass sie den Datenverkehr auf Schicht 2 bzw. 3 verhindern und kontrollieren können bzw. dediziert auf Port-Ebene Segmente verbinden oder trennen können. Auch für Bridges/Switches einiger Hersteller gilt, dass hier der Zugang von Netzteilnehmern beschränkt werden kann. Router bieten die umfassendsten Kontrollmöglichkeiten der hier behandelten Komponenten. Mit Hilfe von Routern kann nicht nur der Zugang und die Wegewahl in andere Netze bestimmt werden, sondern zusätzlich auch, welcher Netzteilnehmer mit Systemen im anderen Segment auf welcher Basis kommunizieren darf. Durch den Ausschluss bestimmter Protokolle der Ebene 3 am Router kann verhindert werden, dass Daten dieses Protokolls in das andere Segment gelangen. Dies geschieht durch die Definition geeigneter Filterregeln in den Routern, die auf Protokollebene gebildet werden können. So können beispielsweise bei der Verwendung des TCP/IP-Protokollstapels einzelne TCP- und UDP-Ports für den Übergang in das andere Segment

selektiv gesperrt oder freigegeben werden. Komponenten, die auf höheren Schichten arbeiten, wie z. B. Application-Level-Firewalls, werden an dieser Stelle nicht behandelt (siehe M 2.75 *Geeignete Auswahl eines Application-Level-Gateways*).

Beispiel: Durch die Trennung eines Netzes mit Hilfe eines Routers und eine entsprechende Konfiguration der Filterregeln kann erreicht werden, dass kein FTP- und TFTP-Datentransfer (Port 20 und 21 bzw. 69) zwischen den Segmenten möglich ist und somit auch nicht vom jeweils anderen abgehört werden kann. Ebenso werden keine Broadcast-Daten zwischen den Teilnetzen übertragen. Außerdem müssen die Filter standardmäßig derart konfiguriert sein, dass zunächst die Kommunikation maximal eingeschränkt und erst nach Bedarf und dienstebezogen freigegeben wird. Hierbei sollte ggf. eine IP-bezogene Filterung berücksichtigt werden.

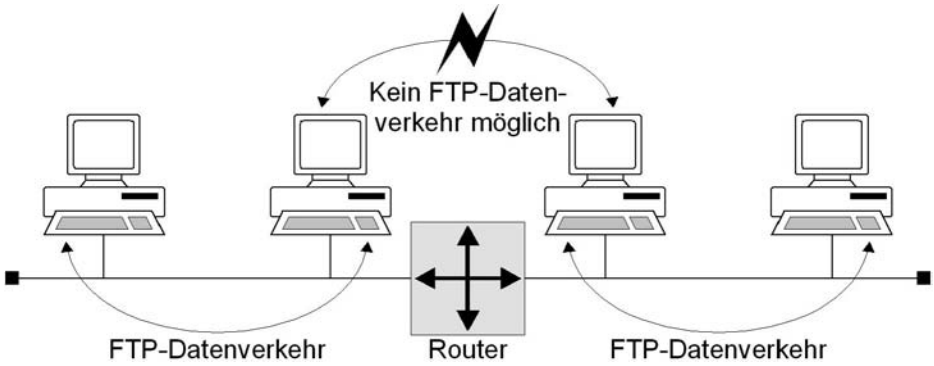


Abbildung: Beispiel für die Trennung von Teilnetzen auf Schicht 3 durch einen Router

Daten- und Netzintegrität

Die Integrität der Daten bis zur Schicht 3 wird in der Regel durch das eingesetzte Netzzugangsprotokoll sichergestellt, während die Sicherstellung der Netzintegrität, also dem Übereinstimmen der aktuellen Netzsituation mit der geplanten und vorgesehenen physikalischen und logischen Segmentierung, zusätzliche Maßnahmen erfordert. Diese Maßnahmen müssen sicherstellen, dass keine unautorisierten oder fehlgeleiteten Kommunikationsverbindungen aufgebaut oder unautorisierten Systemzugriffe durchgeführt werden, die im integren Netzzustand unterbunden sind.

Die Netzintegrität wird daher im wesentlichen dadurch sichergestellt, dass

- Veränderungen unmittelbar an Netzkomponenten (Umrangierungen, Installation neuer, nicht autorisierter Komponenten etc.) verhindert oder zumindest erkannt werden (Hardware-bezogene Sicherheit),
- Veränderungen an der Konfiguration der Netzkomponenten (z. B. an Routing-Protokollen, an der Port-Switching-Matrix oder an der VLAN-Zuweisung) verhindert oder zumindest erkannt werden (Software-bezogene Sicherheit).

Dazu ist es erforderlich, den Zugang zu den Netzkomponenten mit ausreichender Stärke zu verwehren (z. B. durch Infrastrukturmaßnahmen bezüblich Verteilerraum, Verkabelung etc.) und das Netzmanagement so zu konzipieren, dass unberechtigte Zugriffe über das Netz auf die Netzkomponenten verhindert werden.

Eine Erhöhung des Schutzes bezüglich der Integrität der Daten auf Schicht 3 (z. B. der Anwendungsdaten) kann nicht alleine durch den Einsatz von Netzkomponenten erreicht, aber ein gezielter Angriff auf die Datenintegrität kann erschwert werden. Hierzu können Netzkomponenten verwendet werden, die das Mithören und Verändern von Datenpaketen verhindern. Dies sind z. B. Bridges/Switches und Router, die ein Netz in Segmente bzw. Teilnetze aufspalten können, zwischen denen der Datenverkehr kontrolliert, beschränkt oder konfiguriert werden soll. Insbesondere bei den sich automatisch konfigurierenden Netzkomponenten wie Bridges und Switches, spielt die Abbildung der logischen Zusammengehörigkeit auf die physikalische Konfiguration eine große Rolle. Nur so kann erreicht werden, dass die Datenpakete einer logischen Gruppe auch tatsächlich im selben physikalischen Segment verbleiben. Bei Bridges/Switches, die eine Konfiguration der möglichen Verbindungen auf Portbasis erlauben (Port-Switching) können auch manuell die Verbindungsmöglichkeiten auf der Schicht 1 kontrolliert werden.

Beispiel: Systeme, die den Anschluss von Terminals an ein Netz erlauben (Terminalserver) und die Systeme, auf die vom Terminalserver aus zugegriffen werden soll, müssen in einem Segment durch eine Bridge vom Rest des Netzes abgetrennt werden. Nur so kann vermieden werden, dass der Austausch des Passwortes zwischen Terminalserver und dem angesprochenen System von einem anderen Segment aus abgehört und ggf. verändert werden kann.

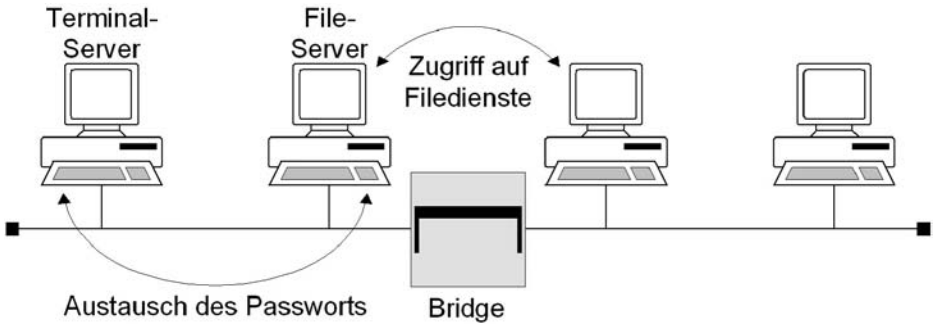


Abbildung: Trennung von Segmenten durch eine Bridge zur Erhöhung der Integrität und Vertraulichkeit

Zusätzlich ist durch die geeignete Dimensionierung und Auswahl von Netzkomponenten dafür Sorge zu tragen, dass weder durch deren Überlastung noch durch deren Fehlfunktion Datenpakete verloren gehen können bzw. verfälscht werden.

Ergänzende Kontrollfragen:

- Wurde beim Entwurf des lokalen Netzes an eine physikalische Segmentierung gedacht?
- Wurden die Anforderungen bezüglich Verfügbarkeit (insbesondere auch Performance), Vertraulichkeit und Integrität ermittelt und berücksichtigt?

M 5.62 Geeignete logische Segmentierung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Mit Hilfe geeigneter aktiver Netzkomponenten ist es möglich, trotz einer festen physikalischen Segmentierung des Netzes, dieses darüber hinaus logisch zu segmentieren. Die Möglichkeit hierzu bieten Switches, die auf der Schicht 2 und 3 des OSI-Modells arbeiten. Aufgrund der Eigenschaften solch eines Switches, die Protokolle der Schicht 2 bzw. 3 zu verstehen, können durch Kontrolle des Datenflusses zwischen den Anschlüssen am Switch so genannte virtuelle LANs (VLANs) gebildet werden. Hierdurch können Gruppen im Netz zusammengefasst werden, die in der physikalischen Segmentierung so nicht abgebildet sind. Vor allem ergibt sich hierdurch die Möglichkeit, Gruppen ohne Eingriff in die physikalische Vernetzung dynamisch und zeitnah neu zu bilden bzw. umzugruppieren.

Analog zur physikalischen Segmentierung auf der Schicht 2 bzw. 3 sind die Kriterien bezüglich Vertraulichkeit, Verfügbarkeit und Integrität auch hier anzuwenden. Kriterien für eine geeignete Segmentierung können ebenfalls analog wie für die physikalischen Segmente angewendet werden. Dabei muss beachtet werden, dass VLANs auf einem Switch nicht ohne weiteres für die sichere Trennung zweier Teilnetze mit unterschiedlichem Schutzbedarf geeignet sind. Sollen auf einem Switch zwei Teilnetze mit unterschiedlichen Anforderungen an die Vertraulichkeit der übertragenen Daten als VLANs realisiert werden, so sind in der Regel zusätzliche Maßnahmen erforderlich, um eine sichere Trennung zu gewährleisten.

In der folgenden Abbildung ist die Möglichkeit der VLAN-Bildung mit Hilfe mehrerer Schicht-3-Switches dargestellt. Die physikalische Anbindung der Endgeräte an die Switches erfolgt hierbei wie durch die Verbindungslinien angedeutet. Die logische Segmentierung erfolgt durch die Gruppierung mit Hilfe der Switches nach VLANs.

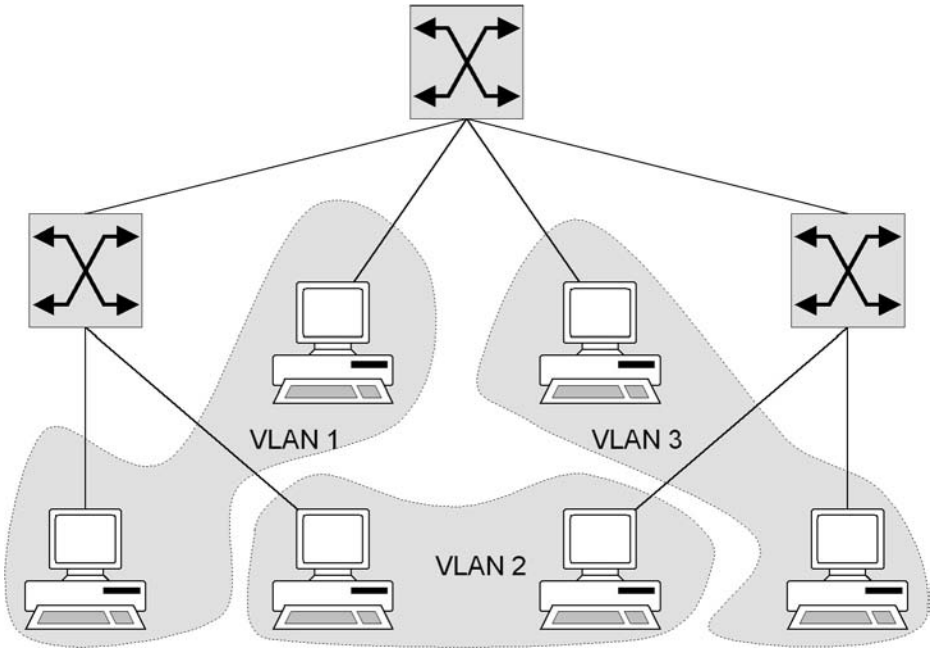
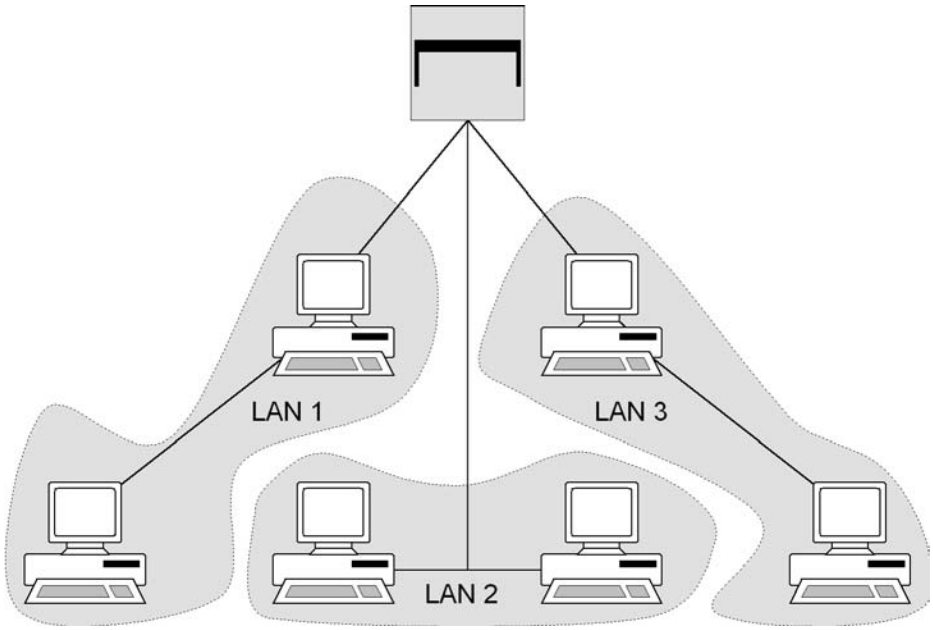


Abbildung: VLAN-Bildung mit Hilfe mehrerer Switches

Würde man die in der oben gezeigten Abbildung der VLAN-Struktur durch eine herkömmliche physikalische Segmentierung erreichen wollen, würde das wie in der nachfolgenden Abbildung dargestellt aussehen. Die einzelnen LANs können hier beispielsweise durch Shared Ethernet-Segmente abgebildet werden, die Verbindung der einzelnen LANs erfolgt durch eine Bridge.



Abbildulng: VLAN-Bildung mit Hilfe einer Bridge

Auf der Basis von VLAN-fähigen Netzkomponenten können ohne physikalische Umstrukturierung virtuelle LANs gebildet werden, die je nach eingesetzter Technologie analog zu LANs, mit Segmentierungen auf Schicht 2 oder 3 sind. Hiermit können in einem Netz analog zur Segmentierung von LANs Bereiche gebildet werden (siehe M 5.61 *Geeignete physikalische Segmentierung*). Je nach eingesetztem Produkt bieten diese bei der VLAN-Bildung unterschiedliche Funktionalitäten. Einige Produkte stellen die Möglichkeit zur Verfügung, VLANs auf Schicht 2 oder 3 zu bilden, die u. U. nur durch den Einsatz von Routern gekoppelt werden können, sog. sichere VLANs (*secure VLANs*). In diesem Fall muss mit Hilfe der Filterregeln des Routers ein kontrollierter Übergang zwischen den VLANs hergestellt werden. Andere Hersteller implementieren in Schicht-3-Switches bereits Routing-Funktionalität, die VLANs ohne zusätzliche Router verbinden. Der Einsatz entsprechender Technologien und Produkte muss insbesondere gegen die Anforderungen an die Vertraulichkeit und Integrität der Daten geprüft werden.

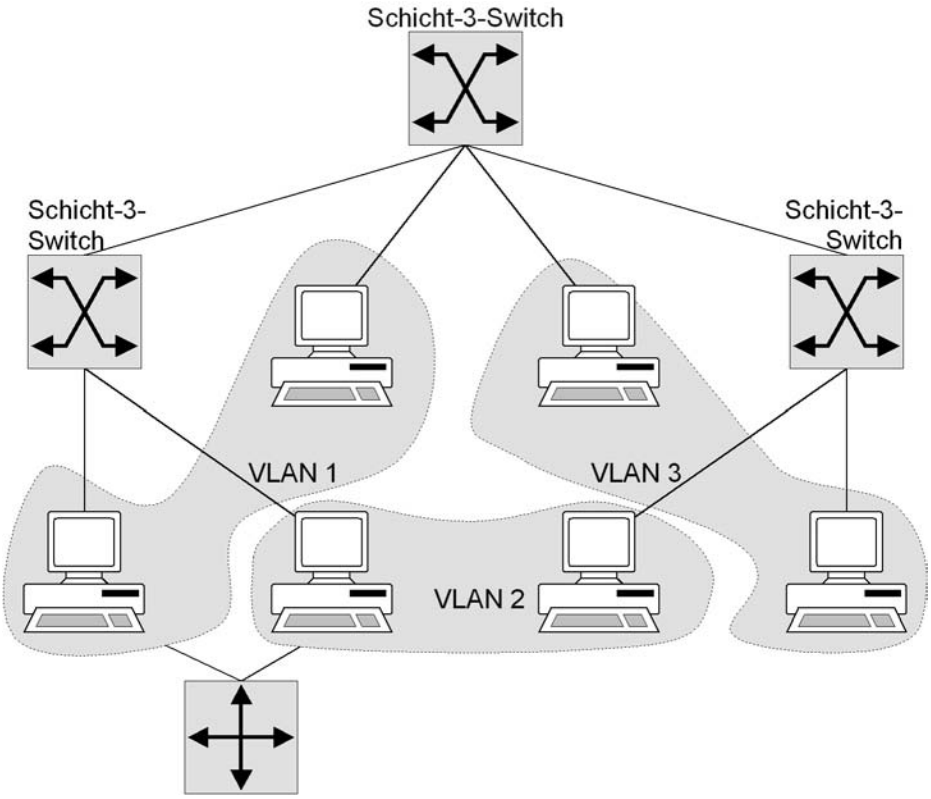


Abbildung: Bildung von sicheren VLANs mit Schicht-3-Switches

Der in der obigen Abbildung dargestellte Fall, wurden mit Hilfe von Schicht-3-Switches sichere VLANs, auf der Schicht 3 des OSI-Modells eingerichtet. Die dargestellten Switches sind in diesem Fall ohne Routing-Funktionalität. VLAN 1, VLAN 2 und VLAN 3 verhalten sich dabei so, als ob sie durch einen Router segmentiert wären, ohne dass ein Routing zwischen ihnen

stattfindet. VLAN 3 hat also keinerlei Verbindung mit den anderen VLANs, lediglich VLAN 1 und VLAN 2 können über einen Router miteinander kommunizieren. Die Kommunikation kann durch die Konfiguration des Routers entsprechend kontrolliert und gesteuert werden. Mit anderen Produkten, die Routing-Funktionalität in den Schicht-3-Switches implementieren, kann der dargestellte Router entfallen und das Routing mit Hilfe der Switches kontrolliert werden.

Eine allgemeine Empfehlung bezüglich einer logischen Segmentierung kann nicht gegeben werden. Für eine Neuinstallation eines Netzes ist aber zu prüfen, ob durch den Einsatz von VLANs die Anforderungen an die Verfügbarkeit, Vertraulichkeit und Integrität nicht einfacher erreicht werden können als durch eine aufwendigere physikalische Segmentierung. Allerdings muss dabei beachtet werden, dass Teilnetze mit unterschiedlichem Schutzbedarf bezüglich der Vertraulichkeit oder der Integrität der übertragenen Daten nicht ohne weiteres als VLANs auf demselben Switch realisiert werden sollten.

Als Vorteil einer logischen Segmentierung ist die einfache, zentrale Neu- und Umkonfigurierbarkeit der Segmente zu sehen. Auf der anderen Seite muss in diesem Fall auch ein besonderes Augenmerk auf den sicheren Remote-Zugang zu den aktiven Netzkomponenten gelegt werden, da die Segmentierung hier nur auf der Konfiguration von Software beruht. Es muss also bei einer Segmentierung über VLANs zwischen den Anforderungen an die Sicherheit des Netzes (sowohl vor unberechtigter Umkonfiguration als auch vor der Möglichkeit, dass die Grenzen zwischen den verschiedenen VLANs eventuell überwunden werden können) und der Möglichkeit einer flexiblen Umgestaltung des Netzes abgewogen werden.

Ergänzende Kontrollfragen:

- Sind die eingesetzten Netzkomponenten VLAN-fähig?
- Wurde das Netz geeignet logisch segmentiert?
- Sind die eingesetzten Netzkomponenten bezüglich der VLAN-Funktionalität interoperabel?
- Ist der Remote-Zugang der aktiven Netzkomponenten vor unberechtigter Administration geschützt?
- Wurden die Anforderungen bzgl. Verfügbarkeit, Vertraulichkeit und Integrität ermittelt und berücksichtigt?

M 5.63 Einsatz von GnuPG oder PGP

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator, Benutzer

GNU Privacy Guard (GnuPG) und Pretty Good Privacy (PGP) sind weit verbreitete Programme, mit denen Nachrichten und Dateien ver- und entschlüsselt sowie mit einer digitalen Signatur (auch elektronische Unterschrift genannt) versehen werden können. Beide Tools implementieren Funktionen, die im OpenPGP-Standard (RFC 2440) definiert sind. Durch Verschlüsselung kann die Vertraulichkeit von Informationen geschützt werden, mit digitalen Signaturen kann überprüft werden, ob eine Datei bzw. eine Nachricht authentisch ist und nicht manipuliert wurde. Sowohl mit GnuPG als auch mit PGP können weiterhin die Aufgaben des Schlüsselmanagements, wie z. B. Hinzufügen und Entfernen von Schlüsseln, wahrgenommen werden.

Verschlüsselung und digitale Signatur

Bei GnuPG und PGP werden symmetrische und asymmetrische kryptographische Verfahren eingesetzt. Symmetrische, wie AES und IDEA, dienen zur Datenverschlüsselung, asymmetrische wie ElGamal, RSA und DSA/DSS zum Schlüsselmanagement bzw. zur Signaturbildung.

Beide Tools erzeugen und verwenden öffentliche und private Schlüssel in so genannten Schlüsselpaaren. Zu jedem privaten Schlüssel gibt es genau einen öffentlichen Schlüssel. Es ist praktisch ausgeschlossen, nur mit Kenntnis des öffentlichen Schlüssels den privaten Schlüssel zu errechnen. Eine Nachricht, die mit einem öffentlichen Schlüssel verschlüsselt bzw. mit dem privaten Schlüssel signiert wurde, kann nur mit dem zugehörigen privaten Schlüssel entschlüsselt bzw. mit dem öffentlichen Schlüssel des Absenders verifiziert werden. Der öffentliche Schlüssel kann jedem bekannt gemacht werden. Er dient dazu, Nachrichten an den Besitzer des privaten Schlüssels zu verschlüsseln.

Zum Nachweis von unautorisierten Manipulationen und somit zum Schutz vor Veränderungen einer Nachricht berechnet GnuPG bzw. PGP unter Zuhilfenahme des privaten Schlüssels des Absenders einen Prüfcode über die Nachricht, die digitale Signatur. Jeder Kommunikationspartner kann mit Hilfe des öffentlichen Schlüssels des Absenders der Nachricht feststellen, ob der am Ende der Nachricht stehende Prüfcode zu der erhaltenen Nachricht passt oder ob die Nachricht unautorisiert verändert wurde.

Auf technischer Ebene findet aus Sicherheitsgründen in der Regel eine Trennung zwischen den Schlüsseln für digitale Signaturen und den Schlüsseln für Verschlüsselung statt. Dies ist für den Benutzer meist transparent.

erst signieren, dann verschlüsseln

Empfehlenswert beim Einsatz von GnuPG oder PGP ist die Kombination der beiden zuvor beschriebenen Funktionalitäten. Nachrichten bzw. Dateien sollten standardmäßig zunächst mit dem privaten Schlüssel des Absenders signiert und anschließend mit dem öffentlichen Schlüssel des Empfängers verschlüsselt werden, um einen höchstmöglichen Schutz zu erreichen.

Versionen

Sowohl GnuPG als auch PGP stehen für die gängigsten Rechnerplattformen (Unix, GNU/Linux, Microsoft Windows) zur Verfügung. Von PGP gibt es auch Versionen für MacOS. Bei GnuPG handelt es sich um Freie Software/Open Source, die derzeit aktuelle Version ist 1.2.3.

Gängige Versionen von PGP sind 2.6.3i, und 5.x bis 8.x. Die Versionen ab 5.x sind mit einer graphischen Benutzeroberfläche ausgestattet, aber nicht vollständig abwärtskompatibel zu den Vorgängerversionen.

verwendete PGP-Version möglichst abstimmen

Aufgrund der fehlenden Abwärtskompatibilität ist es empfehlenswert, vor dem Austausch von verschlüsselten Nachrichten nachzufragen, welche PGP-Version von den Kommunikationspartnern verwendet wird. Die nach wie vor weit verbreitete Version 2.6.3i ist kommandozeilenorientiert, kann aber mit Zusatzprogrammen in graphische Benutzeroberflächen und E-Mail-Clients eingebunden werden. PGP kann über verschiedene Quellen bezogen werden, u. a. Freeware-Versionen von diversen WWW-, FTP- oder E-Mail-Servern.

Auch untereinander sind GnuPG und PGP derzeit nicht vollständig interoperabel. Ursache hierfür sind einerseits Software-Patente (der von einigen PGP-Versionen standardmäßig verwendete Algorithmus IDEA ist patentiert) und andererseits kleine Abweichungen vom OpenPGP-Standard. Mit dem Auslaufen des RSA-Patents ist jedoch eine wesentliche Hürde weggefallen. RSA wird von GnuPG ab der Version 1.0.3 unterstützt.

OpenPGP-kompatible Schlüssel verwenden

Um diese Probleme zu umgehen, sollte - wenn möglich - nur eines der beiden Tools eingesetzt werden. Falls dies nicht möglich ist, sollten ausschließlich OpenPGP-kompatible Schlüssel verwendet werden. Auf diese Weise wird auch sichergestellt, dass die Kommunikationspartner mit Triple-DES über einen gemeinsamen symmetrischen Algorithmus verfügen. Das oben beschriebene Interoperabilitätsproblem durch die Verwendung von IDEA tritt dann nicht auf. Näheres hierzu findet sich in der Liste der häufig gestellten Fragen und Antworten auf der WWW-Seite des GnuPG-Projekts *www.gnupg.org und www.gnupg.de*.

Ab der Version 5 von PGP wurde die umstrittene Funktion *Corporate Message Recovery* (CMR) eingeführt. CMR bietet die Möglichkeit, Dateien oder Nachrichten, die von einer Person für eine Zweite verschlüsselt wurden, gleichzeitig für eine dritte Person entschlüsselbar zu machen. Die Verwendung eines solchen "Drittschlüssels" kann durch die Konfiguration vom Administrator zwingend vorgegeben werden.

Die PGP-Version 7 enthält zwei weitere Funktionen, mit denen unter Umständen Sicherheitsfunktionen unterlaufen werden können. Zum einen wurde ein Server-basierter Wiederherstellungsmechanismus für Schlüssel eingeführt, mit dem ein Benutzer Schlüssel weiterverwenden kann, wenn er beispielsweise die zugehörige Passphrase vergessen hat. Die andere Funktion ist das *Passphrase Caching*, bei dem die Passphrase zwischengespeichert wird, damit diese beim Wechsel zwischen verschiedenen PGP-Teilsystemen nicht jedes Mal neu durch den Benutzer eingegeben werden muss. Einen vergleichbaren Mechanismus gibt es auch in der Version 2.6.3i, bei der die

Passphrase in einer Umgebungsvariable gespeichert werden kann. Dieser Mechanismus sollte nicht verwendet werden.

Insbesondere beim Einsatz von GnuPG oder PGP unter Betriebssystemen der Windows-Familie ist zu beachten, dass die Sicherheitsmechanismen dieser Tools durch die Ausnutzung von Sicherheitsmängeln des Betriebssystems möglicherweiser unterlaufen werden können.

Sichere Installation und Bedienung

Einarbeitung erforderlich

Bei GnuPG und PGP werden zwar als sicher anerkannte kryptographische Verfahren eingesetzt, durch falsche Konfiguration oder Fehlbedienung kann es aber zu einer Abschwächung des Sicherheitsniveaus kommen. Die Installation und Konfiguration inklusive der Schlüsselgenerierung ist bei GnuPG und PGP wie bei den meisten komplexeren Kryptoprodukten nicht ganz einfach. Damit sich keine Bedienungsfehler einschleichen können, ist die Einarbeitung in das jeweilige Produkt und in einige kryptographische Grundbegriffe notwendig.

Mitarbeiter in die Verwendung und Bedienung einweisen

Daher sollte sich in Organisationen ein Mitarbeiter in den Umgang mit dem Tool einarbeiten und als Ansprechpartner zur Verfügung stehen. Dieser sollte dann die anderen Benutzer in die sichere Bedienung von GnuPG bzw. PGP einweisen, insbesondere sollten Verschlüsselung, Signatur und Schlüsselmanagement intensiv geübt werden, bevor ein Benutzer das Programm verwendet. Weiterhin ist es empfehlenswert, dass innerhalb einzelner Organisationen eine einheitliche Programmversion verwendet wird, um die zuvor beschriebenen Kompatibilitätsprobleme zu vermeiden. Sowohl zu GnuPG als auch zu PGP gehört eine umfangreiche Dokumentation, die vor der Verwendung gelesen werden sollte. Da erfahrungsgemäß nicht alle Benutzer die Geduld aufbringen, diese zu lesen, empfiehlt es sich, eine schriftliche Einweisung auszuarbeiten, die auf die Organisationseigenheiten angepasst ist.

Falls Benutzer Fragen zu GnuPG oder PGP haben, die über die mitgelieferte Dokumentation hinausgehen, gibt es diverse Möglichkeiten:

- Zunächst gibt es im Internet eine Sammlung der häufigsten Fragen und Antworten (Frequently Asked Questions - FAQ) zu GnuPG (z. B. unter *www.gnupg.org*) und PGP (z. B. unter *www.pgpi.org* bzw. *www.pgp.com*) sowie deutschsprachige Anleitungen und Ausführungen.
- Über Newsgruppen wie *alt.security.pgp*, *de.comp.security*, *sci.crypt* oder Mailinglisten ist es sehr schnell möglich, Antworten zu Problemen zu bekommen.
- Es gibt mehrere Bücher zu PGP.

Schlüsselgenerierung

Jeder Benutzer erzeugt bei GnuPG und PGP sein "Schlüsselpaar" selbst. Hierbei sollten folgende Punkte beachtet werden:

Schlüssellänge

- Bei der Generierung der DSA/DSS- bzw. RSA-Schlüssel können verschiedene Schlüssellängen gewählt werden. Hierbei ist zu beachten, dass mit der Schlüssellänge die Entzifferungsresistenz zunimmt, aber auch die Performance sinkt. Als Schlüssellänge sollte daher 1024 Bit gewählt werden.

- Bei der Schlüsselerzeugung muss eine so genannte *Passphrase* (auch *Mantra* genannt) eingegeben werden, die die Datei mit den privaten Schlüsseln vor unbefugtem Zugriff schützt. Wie jedes Passwort sollte auch dieses nicht leicht zu erraten sein. **Passphrase**

  Es kursieren z. B. trojanische Pferde, die gezielt die Datei mit den privaten Schlüsseln (SECRING.*) suchen und an Externe per E-Mail senden. Wenn dann die Passphrase zu einfach gewählt war, bietet sie Brute-Force-Angriffen (automatisiertes Passwortraten) keinen ausreichenden Widerstand. Daher sollte die Passphrase mindestens aus zehn Zeichen bestehen und Sonderzeichen enthalten.

  Trojanische Pferde werden zwar in der Regel von Viren-Schutzprogrammen erkannt, dies setzt jedoch voraus, dass das beim Benutzer installierte Programm (bzw. dessen Datenbasis) hinreichend aktuell ist.

- Zu den öffentlichen Schlüsseln gehört eine Benutzer-ID, die möglichst eindeutig sein sollte und zudem die E-Mail-Adresse enthält, z. B. *benutzer@bsi.bund.de*. **Benutzer-ID**

- Zur Schlüsselgenerierung benötigen GnuPG und PGP möglichst zufällige Startwerte. Die einzelnen Programme und Versionen verwenden unterschiedliche Verfahren, um diese zufälligen Werte zu erzeugen. Beispielsweise wird der Benutzer gebeten, beliebigen Text einzutippen. Hierbei sollte besser "echter" Text eingegeben werden, z. B. kann dieser Absatz abgetippt werden. Einfach auf der Tastatur "herumklimpern" erzeugt meist schlechtere Ergebnisse, da die zeitlichen Abstände zwischen den Tastendrücken u. U. zu kurz und zu regelmäßig sind. **Zufallszahlen**

Schlüsselaufbewahrung

Die privaten Schlüssel werden in der Datei SECRING.* gespeichert. Entscheidend für den sicheren Betrieb ist, dass der Inhalt dieser Datei vertraulich bleibt und vor Manipulationen geschützt wird. Der Zugriff auf diese Datei ist zwar durch die Passphrase geschützt, trotzdem sollte sie nicht auf lokalen Netzen gehalten werden, nicht einmal auf nicht genügend gesicherten Stand-Alone-Systemen. Schlüsselringe (Sammlungen von Schlüsseln) sollten auf Diskette gespeichert werden, die der Benutzer sorgfältig verwahren muss. Der Einsatz von Chipkarten zur Schlüsselspeicherung ist vorzuziehen. **privaten Schlüssel schützen**

Weiterhin sollte eine Sicherungskopie der Datei SECRING.* angelegt, sowie die Passphrase notiert werden. Die Sicherungskopie und die Passphrase sollten sicher und am besten getrennt verwahrt werden, damit nicht durch einen Festplattencrash oder durch Fehlbedienung der private Schlüssel verloren geht. Nachrichten, die mit dem öffentlichen Schlüssel verschlüsselt worden sind, lassen sich in diesem Fall nicht mehr entschlüsseln. **Sicherungskopie anlegen**

Das Aufschreiben und Hinterlegen der Passphrase an einem gesicherten Ort sollten hierbei als kritischer Vorgang betrachtet werden, die ausschließlich der Notfallvorsorge dienen. Die abgeschlossene Schublade eines Schreibtisches oder ähnlich "sichere" Orte können **keinesfalls** als Aufbewahrungsort für den geheimen Schlüssel oder für die Passphrase empfohlen werden. **Passphrase an gesichertem Ort hinterlegen**

Revocation Certificate

Nach der Schlüsselgenerierung sollte ein so genanntes *Revocation Certificate* erzeugt und ausgedruckt oder auf einer Diskette gespeichert werden. Damit kann der öffentliche Schlüssel widerrufen werden, wenn die Passphrase vergessen wird oder der private Schlüssel aus anderen Gründen nicht mehr zur Verfügung steht. Das *Revocation Certificate* sollte sicher verwahrt werden, damit der öffentliche Schlüssel nicht unberechtigt widerrufen werden kann.

Schlüsselverteilung

Damit ein Empfänger die digitale Signatur eines Senders einer Datei überprüfen kann bzw. damit der Sender eine Nachricht für einen bestimmten Empfänger verschlüsseln kann, benötigt er den öffentlichen Schlüssel seines Kommunikationspartners. Diesen kann er auf verschiedene Weisen erhalten, z. B. per Attachment einer E-Mail oder von einem WWW-Server, er muss sich aber davon überzeugen, dass dieser Schlüssel wirklich zu der angegebenen Person gehört. Für eine kryptographisch abgesicherte Zuordnung einer Person zu ihrem öffentlichen Schlüssel werden Zertifikate verwendet, die ein vertrauenswürdiger Dritter vergibt.

Beglaubigung von Zertifikaten

Bei GnuPG und PGP kann jeder Benutzer die öffentlichen Schlüssel anderer Personen mit Zertifikaten beglaubigen. Ein Benutzer sollte einen öffentlichen Schlüssel aber nur dann zertifizieren, wenn er die Identität des Schlüsselinhabers kennt oder überprüft hat und der öffentliche Schlüssel persönlich übergeben wurde.

Fingerprints

Alternativ kann die Echtheit eines öffentlichen Schlüssels auch über den so genannten *Fingerprint* verifiziert werden. Hierbei wird eine Zahlenfolge (Hashwert) aus dem öffentlichen Schlüssel berechnet und an diesen angehängt. Nach Übersendung eines öffentlichen Schlüssels kann nun mit dem Absender diese Zahlenfolge, z. B. telefonisch, verglichen werden, um nach der Bestätigung des Fingerprints den übersandten öffentlichen Schlüssel zu zertifizieren.

Zertifizierungshierarchie - Web of Trust - Internet-Keyserver

Prinzipiell können GnuPG und PGP sowohl in einer Zertifizierungshierarchie als auch in einem *Web of Trust* eingesetzt werden. Beim *Web of Trust* wird auf die Zertifikate anderer Benutzer vertraut, in einer Zertifizierungshierarchie beglaubigen vertrauenswürdige Dritte, so genannte Zertifizierungsstellen, die Schlüssel aller ihrer Benutzer auf zuverlässige und nachvollziehbare Weise.

Zertifizierungshierarchie aufbauen

In einem Unternehmen oder einer Behörde sollte im Intranet eine Zertifizierungshierarchie aufgebaut werden. Der Betreuer sollte alle Schlüssel für seinen Organisationsbereich bzw. für die gesamte Organisation zertifizieren. Die zertifizierten öffentlichen Schlüssel sollten im Intranet auf einem Server allen Mitarbeitern zugänglich sein, der Zugriff auf diesen Bereich sollte dabei ausschließlich *lesend* (Read-only) sein. Die Methode des *Web of Trust* sollte nur für die private Kommunikation benutzt werden.

Im Internet können öffentliche Schlüssel auf so genannten Keyservern eingestellt werden. Diese dürfen aber keinesfalls mit Zertifizierungsstellen verwechselt werden. Keyserver nehmen Schlüssel von überall in Empfang und verteilen sie auf Anfrage weiter. Es sollte klar sein, dass Schlüssel, die man von einem Keyserver erhält, von diesem in keiner Weise überprüft wurden.

Um die Echtheit eines öffentlichen Schlüssels, der auf einem Keyserver eingestellt wurde, nachzuprüfen, sollte dies mit Hilfe des bereits erwähnten Fingerprints durchgeführt werden.

Eigensignatur des öffentlichen Schlüssels

Durch die Selbstsignatur des öffentlichen Schlüssels wird nur die Benutzer-ID als Teil eines öffentlichen Schlüssels von GnuPG bzw. PGP unterschrieben. Mit Hilfe dieser Selbstsignatur ist es möglich, einen Denial-of-Service-Angriff (siehe G 5.28 *Verhinderung von Diensten*) zu entdecken, dieser kann jedoch durch die Selbstsignatur des öffentlichen Schlüssels nicht verhindert werden. Da die Benutzer-ID eines öffentlichen Schlüssels nicht verschlüsselt ist, kann sie verfälscht werden. Dies hätte zur Folge, dass bei Verwendung dieses "verfälschten" Schlüssels, die verschlüsselten E-Mails den Eigentümer dieses Schlüssels nicht mehr erreichen, da sie an eine andere E-Mail-Adresse umgeleitet werden. Die Vertraulichkeit der verschlüsselten Nachricht wird hierdurch nicht gefährdet, da das Entschlüsseln der Nachricht ausschließlich mit dem privaten Schlüssel erfolgen kann.

Key Recovery

Falls die zur Verschlüsselung benutzten Schlüssel verloren gehen, sind im Allgemeinen auch die damit geschützten Daten verloren. In den kommerziellen Versionen ab 5.0 bietet PGP Funktionen zur Datenwiedergewinnung für solche Fälle an. Diese Funktionen werden auch als Key Recovery bezeichnet. Diese Funktionalität kann durch Wiederherstellung gespeicherter, verschlüsselter Daten einem Datenverlust vorbeugen, wenn ein Schlüssel oder das Zugriffspaßwort verloren ging.

Fehlerhafte Programmversionen vermeiden

Bei älteren Versionen von PGP sind Fehler in der ADK-Implementierung (Additional Decryption Key) bekannt geworden, die für Angriffe ausgenutzt werden können. Hiervon sind insbesondere die PGP-Versionen vor 6.5.8 betroffen. Es sollte daher eine hinreichend aktuelle Version eingesetzt werden, bei der möglichst alle bekannt gewordenen sicherheitsrelevanten Fehler beseitigt sind. GnuPG ignoriert grundsätzlich alle ADKs.

Wenn die Wiedergewinnungsfunktion von PGP genutzt werden soll, müssen ein oder zwei zusätzliche Schlüssel (ADK, Additional Decryption Keys) erzeugt werden. Bei der Schlüsselgenerierung werden diese "Nachschlüssel" an die neu erzeugten Schlüssel angebunden und alle Daten, die mit den neuen Schlüsseln verschlüsselt werden, enthalten zusätzlich eine Verschlüsselung des Sitzungsschlüssels mit den ADKs. So ist es im Notfall möglich, die Daten unter Verwendung dieser ADKs, ohne Nutzung des Originalschlüssels zu entschlüsseln. Damit bietet PGP die Funktion *Message Recovery* ohne zentrale Speicherung der Wiederherstellungsinformationen.

Die Nutzung des Key Recovery kann durch entsprechende Voreinstellungen der Clients erzwungen werden, so dass diese Funktionalität nicht von den einzelnen Benutzern unterlaufen werden kann. Allerdings hängt dann die Sicherheit der gesamten Verschlüsselung von der Vertraulichkeit der ADKs ab. Sind diese offen gelegt, können alle Daten mit ihnen entschlüsselt werden.

ADKs besonders sorgfältig schützen

Um einem Missbrauch dieser höchst sensitiven Funktion vorzubeugen, ist es unabdingbar, dass die ADKs durch ein besonders sorgfältig ausgewähltes, sicher verwahrtes Passwort geschützt werden. Zusätzlich können ab der PGP-Version 6.0 Schlüssel auch in Teile aufgeteilt werden, so dass zu ihrer Nutzung mehrere Personen gemeinsam aktiv werden müssen. Diese Form der Vier-Augen-Kontrolle sollte bei Einsatz von ADKs unbedingt genutzt werden. Als weiterer Schutz kann vorgesehen werden, dass Benutzer jedes Mal gewarnt werden, wenn sie Daten mit einem Schlüssel verschlüsseln, an den ADKs angebunden werden.

Vor- und Nachteile abwägen

Ehe PGP mit Key Recovery eingesetzt wird, sollten die Vor- und Nachteile gegeneinander abgewogen werden. Auf der einen Seite wird zwar einem Datenverlust durch Verlust des Schlüssels vorgebeugt, auf der anderen Seite entsteht ein zentraler Schwachpunkt des Verschlüsselungssystems. Diese Funktion sollte daher nur dann genutzt werden, wenn PGP zur Verschlüsselung gespeicherter Daten eingesetzt wird. Bei einer Nutzung rein für die Kommunikationssicherung kann bei einem Schlüsselverlust auch einfach erneut die E-Mail angefordert werden. Es sollte auch geprüft werden, ob als Alternative die Hinterlegung des Passworts an einer sicheren Stelle in einem geschlossenen Umschlag und die Erstellung von Sicherheitskopien der privaten Schlüsseldateien nicht zu bevorzugen wäre.

Key Reconstruction

Frage/Antwort-Kombinationen

Die Version 7 von PGP bietet eine weitere Möglichkeit, Problemen durch verloren gegangene Schlüssel, beispielsweise durch vergessene Passphrase, vorzubeugen. Hierzu wird der Schlüssel in mehrere Teile aufgespalten, überschlüsselt und auf einem Wiederherstellungs-Server abgespeichert. Bei der Hinterlegung legt der Benutzer fünf Frage/Antwort-Kombinationen fest. Mindestens drei der fünf Fragen muss der Benutzer korrekt beantworten, um seinen Schlüssel wiederherstellen zu können.

Sicherungskopie der privaten Schlüsseldateien bevorzugen

Bei dieser Funktion besteht die Gefahr, dass Benutzer Fragen festlegen, deren Antworten durch Dritte erraten oder ermittelt werden können, beispielsweise Namen von Verwandten oder Geburtsdaten. Als Folge können u. U. Dritte unberechtigt auf Schlüssel des Benutzers zugreifen. Da sich die Qualität der Frage/Antwort-Kombinationen in der Regel auch nicht überprüfen lässt, sollte diese Funktion nicht genutzt werden. Stattdessen wird empfohlen, eine Sicherheitskopie der privaten Schlüsseldateien auf einem Datenträger anzufertigen und den Datenträger an einem abgesicherten Ort zu verwahren. Auch die zugehörige Passphrase ist in einem geschlossenen Umschlag zu hinterlegen (siehe M 2.22 *Hinterlegen des Passwortes*).

Single Sign-On

Passphrase Caching

Unter den Bezeichnungen *Single Sign-On* und *Passphrase Caching* bietet PGP ab der Version 7 einen Mechanismus an, die vom Benutzer eingegebene Passphrase zwischenzuspeichern, damit der Benutzer sie nicht bei jeder Aktion neu eingeben muss. Hierdurch besteht die Gefahr, dass unberechtigte Personen mit der Identität des Benutzers Dokumente ver- oder entschlüsseln bzw. digital signieren können, wenn der Benutzer kurzzeitig seinen Arbeitsplatz verlässt.

Rechner beim Verlassen des Arbeitsplatzes sperren

Falls die Funktion *Passphrase Caching* von PGP genutzt werden soll, muss daher auf jeden Fall sichergestellt sein, dass der Rechner des Benutzers auch bei kurzzeitigem Verlassen des Arbeitsplatzes unmittelbar gesperrt wird. Dies kann beispielsweise mit der Funktion Arbeitsstation sperren von Windows NT erfolgen, sofern ein starkes Benutzerpasswort vergeben ist, oder mit Hilfe einer Chipkartenlösung zur Benutzer-Authentisierung. In allen anderen Fällen sollte im Dialogfeld *PGP Options* die Option *Do not cache passphrase* aktiviert werden.

Ergänzende Kontrollfragen:

- Werden die Benutzer im Umgang mit GnuPG bzw. PGP geschult?
- Werden Daten und Schlüssel getrennt aufbewahrt?
- Werden Sicherungskopien der privaten Schlüssel angelegt? Werden diese an einem gesicherten Ort aufbewahrt?

M 5.64 Secure Shell

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Ohne spezielle Erweiterungen bieten die Protokolle *telnet* und *ftp* nur rudimentäre Mechanismen zur Authentisierung. In der Regel wird eine einfache Abfrage von Benutzer-Kennung und Passwort durchgeführt, die dann - ebenso wie die Nutzdaten - im Klartext gesendet werden. Die Vertraulichkeit der Authentisierungs- und Nutzdaten ist also nicht gesichert. Die verwandten Protokolle *rsh*, *rlogin* und *rcp*, die oft unter der Bezeichnung r-Dienste zusammengefasst werden, weisen ähnliche Sicherheitsmängel auf.

Secure Shell (*ssh*) kann als Ersatz für die r-Dienste genutzt werden, wobei umfangreiche Funktionen zur sicheren Authentisierung und zur Wahrung von Vertraulichkeit und Integrität zum Einsatz kommen. Hierzu wird ein hybrides Verschlüsselungsverfahren, also eine Kombination aus asymmetrischer und symmetrischer Verschlüsselung, verwendet. Angesiedelt ist die Secure Shell auf Schicht 7 (Anwendungsschicht) des ISO/OSI-Referenzmodells, allerdings können auch andere Protokolle wie das *X11*-Protokoll, das von der graphischen Oberfläche X-Windows verwendet wird, über *ssh* transportiert werden.

Derzeit basiert Secure Shell auf drei Protokollen, die aufeinander aufbauen und für die jeweils ein Internet-Draft existiert.

- Das unterste Protokoll ist das *Transport Layer Protocol*. Dieses Protokoll leistet den Großteil der Sicherungsfunktionen von *ssh*, nämlich Authentisierung auf Host-Ebene, Verschlüsselung und Schutz der Datenintegrität. Die kryptographischen Algorithmen sind zwischen den Kommunikationspartnern aushandelbar.
- Das mittlere Protokoll ist das *User Authentication Protocol*. Dies erlaubt die Authentisierung auf Benutzer-Ebene, wobei auch hier das Verfahren ausgehandelt werden kann. Wenn zur Authentisierung eine einfache Übertragung von Benutzer-Kennung und Passwort verwendet wird, so ist die Vertraulichkeit dieser Informationen gegenüber dem Kommunikationsweg durch das darunterliegende *Transport Layer Protocol* gesichert. Empfohlen wird jedoch die Authentisierung durch ein Public-Key-Verfahren.
- Das *Connection Protocol* baut auf den beiden vorhergehenden Protokollen auf und erlaubt den Aufbau von mehreren logischen Nutzkanälen. Die Daten auf diesen Nutzkanälen werden gemeinsam über eine einzelne abgesicherte Secure Shell-Verbindung übertragen.

Für alle gängigen Unix-Betriebssysteme existieren Implementierungen sowohl von *ssh*-Clients als auch von *ssh*-Servern. Darüber hinaus gibt es *ssh*-Clients unter anderem für 32 Bit Windows, OS/2, Macintosh und als Java-Applet.

Grundsätzlich ist der Einsatz von Secure Shell zu empfehlen, wenn die Funktionalitäten der r-Dienste über Kommunikationskanäle genutzt werden, die nicht ausreichend gegen Kompromittierung und/oder Manipulation gesichert

sind (z. B. über das Internet). Im folgenden werden einige Hinweise für den sicheren Einsatz von *ssh* gegeben.

Von besonderer Bedeutung ist die Gefährdung durch so genannte *man-in-the-middle*-Attacken. Hierbei filtert der Angreifer den gesamten Verkehr zwischen den Kommunikationspartnern und reicht gefälschte öffentliche Schlüssel weiter. Ist es den Kommunikationspartnern nicht möglich, die öffentlichen Schlüssel zu prüfen, kann der Angreifer den gesamten Verkehr lesen und manipulieren, indem er die Daten jeweils selbst entschlüsselt, dann liest bzw. modifiziert und schließlich mit einem anderen Schlüssel verschlüsselt und weiterleitet. Dies kann mit Hilfe eines geeigneten Schlüssel-/Zertifikatmanagements verhindert werden. Beim praktischen Einsatz von Secure Shell wird jedoch oft eine Kompromisslösung angewandt, die den Einsatz von *ssh* ohne jede zusätzliche Infrastruktur erlaubt. Dabei wird bei einem Verbindungsaufbau zu einem Host, dessen öffentlicher Schlüssel noch nicht bekannt ist, dieser über das unsichere Netz gesendet und in einer lokalen Datenbank abgelegt. Bei allen nachfolgenden Verbindungen mit diesem Host kann dessen öffentlicher Schlüssel dann anhand der lokalen Datenbank überprüft werden. Im Rahmen des Sicherheitskonzeptes muss geklärt werden, ob dieses Verfahren, das eine reduzierte Sicherheit gegenüber *man-in-the-middle*-Angriffen bietet, für die vorliegende Anwendung ausreichend ist.

In den Internet-Drafts sind kryptographische Verfahren festgelegt, die von den Secure Shell-Implementierungen zur Verfügung gestellt werden müssen. Optional können jedoch zusätzliche kryptographische Algorithmen implementiert werden. Die tatsächlich benutzten Verfahren werden beim Verbindungsaufbau ausgehandelt. Durch Wahl geeigneter Client- und Server-Programme und durch entsprechende Konfiguration ist sicherzustellen, dass sich *ssh*-Client und *ssh*-Server auf qualifizierte kryptographische Algorithmen einigen, die den Sicherheitsanforderungen genügen.

Wenn *ssh* zum Einsatz kommt, sollten nach Möglichkeit alle anderen Protokolle, deren Funktionalität durch Secure Shell abgedeckt wird, also z. B. die r-Dienste und *telnet*, vollständig abgeschaltet werden, damit die Sicherheitsmaßnahmen nicht umgangen werden können. Dies setzt allerdings voraus, dass alle Kommunikationspartner über geeignete Implementierungen verfügen.

Von älteren Implementierungen von *ssh* sind sicherheitsrelevante Programmfehler bekannt. Es sollte daher eine Version verwendet werden, bei der solche Mängel beseitigt sind. Die Kompatibilität zwischen Implementierungen, deren Programmversionen sich stark unterscheiden, ist unter Umständen problematisch. Ein Mischbetrieb sollte deshalb möglichst vermieden werden.

Zu beachten ist, dass beim Einsatz von *ssh* über Firewalls eine inhaltssensitive Kontrolle des Datenstroms nicht mehr möglich ist.

Ergänzende Kontrollfragen:

- Werden r-Dienste oder ähnliche Protokolle über unsichere Kommunikationskanäle genutzt?
- Wie ist bei der Nutzung von Secure Shell die Verifizierung von öffentlichen Host-Schlüsseln geregelt (z. B. organisatorische Maßnahmen)?
- Wird eine Version von Secure Shell genutzt, bei der alle bekannten Sicherheitsmängel behoben sind?

M 5.65 Einsatz von S-HTTP

Diese Maßnahme ist mit Version 2006 entfallen.

M 5.66 Verwendung von SSL

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Das bei der WWW-Nutzung am häufigsten verwendete Sicherheitsprotokoll ist SSL ("Secure Socket Layer"). SSL ist von Netscape entwickelt worden und wird von allen aktuelleren Browsern unterstützt. Mit SSL können Verbindungen abgesichert werden

- durch Verschlüsselung der Verbindungsinhalte,
- durch Überprüfung der Vollständigkeit und Korrektheit der übertragenen Daten,
- durch Prüfung der Identität des Servers und
- optional durch Prüfung der Identität der Client-Seite.

Bei SSL wird eine Verbindung zwischen dem Browser eines Benutzers und dem Server eines Anbieters aufgebaut, über die zunächst die Zertifikate mit den öffentlichen Schlüsseln ausgetauscht werden. Anschließend wird geschützt durch das asymmetrische Verschlüsselungsverfahren RSA ein symmetrischer Schlüssel sicher ausgetauscht. Für die Verschlüsselung der eigentlichen Datenübertragung wird nun ein symmetrisches Verfahren benutzt, da dies große Datenmengen schneller verschlüsseln kann. Bei jeder Transaktion wird ein anderer symmetrischer Schlüssel als "Session Key" ausgehandelt, mit dem dann die Verbindung verschlüsselt wird.

https

Ein Benutzer kann WWW-Seiten, die eine SSL-gesicherte Datenübertragung ermöglichen, beispielsweise daran erkennen, dass die Adresse um ein "s" erweitert ist (https://www...), dass am unteren Bildschirmrand im Netscape Navigator der sonst unterbrochene Schlüssel geschlossen ist oder dass im Internet Explorer das Vorhängeschloss geschlossen statt offen ist.

Die Nutzung von SSL ist nicht auf HTTP-Clients und -Server beschränkt. Auch Anwendungen wie Telnet oder FTP können SSL zur sicheren Kommunikation nutzen. Allerdings setzt dies voraus, dass die betreffenden Clients und Server jeweils dafür angepasst werden.

SSL besteht aus zwei Schichten. Auf der oberen Schicht arbeitet das SSL Handshake Protokoll. Dieses dient dem Client und dem Server dazu, sich gegenseitig zu identifizieren und zu authentisieren sowie dazu, für den anschließenden Datenverkehr einen Schlüssel und einen Verschlüsselungsalgorithmus auszuhandeln. Die untere Schicht, das SSL Record Protokoll, das die Schnittstelle zur TCP-Schicht bildet, ver- und entschlüsselt den eigentlichen Datenverkehr. Da SSL für den Zugriff auf TCP auf der Socket-Schnittstelle aufsetzt und diese durch eine sicherheitserweiterte Version ersetzt, ist sie auch für andere Dienste verwendbar. SSL läuft dadurch auch transparent im Hintergrund jedes Internet-Dienstes ab. Die Benutzer müssen nur bei Wahl eines Zertifikates aktiv werden. Ihnen fehlt somit - im Gegensatz zu S-HTTP - die Möglichkeit, die Sicherheitsfunktionen zu konfigurieren und ihren speziellen Sicherheitserfordernissen anzupassen. Dagegen mag SSL für

Nutzer komfortabler erscheinen, die sich nicht bei jeder Web-Anfrage mit der Konfiguration von Sicherheitsfunktionen aufhalten wollen.

Version 3 oder höher einsetzen

SSL sollte nur ab Version 3 eingesetzt werden, da hier durch die zusätzliche Server-Authentikation keine "Man-in-the-Middle"-Angriffe wie bei SSLv2 mehr möglich sind.

Schlüssellänge

Bei SSL können verschiedene kryptographische Algorithmen mit verschiedenen Schlüssellängen eingesetzt werden, so z. B. RC2 oder RC4 mit 40 oder 128 Bit Schlüssellänge, DES mit 56 Bit Schlüssellänge, Tripel-DES mit 112 Bit Schlüssellänge, IDEA mit 128 Bit Schlüssellänge und als Hashfunktionen z. B. MD5 oder SHA-1 (siehe hierzu auch M 3.23 *Einführung in kryptographische Grundbegriffe*). Beim Verbindungsaufbau müssen sich Client und Server auf die in der Sitzung verwendeten Verfahren einigen.

mindestens 80 Bit Schlüssellänge

In Browsern US-amerikanischer Hersteller sind aufgrund der US-Exportrestriktionen teilweise nur Verschlüsselungsverfahren mit extrem kurzen Schlüssellängen (40 Bit) integriert. Diese halten Brute-Force-Angriffen, d. h. Angriffen durch einfaches Ausprobieren aller möglichen Schlüssel, nicht lange stand. Bei einem geringen Schutzbedarf der übertragenen Daten kann diese kurze Schlüssellänge ausreichend sein und schützt zumindest vor Gelegenheitstätern. Ansonsten sollte auf Browser-Versionen zurückgegriffen werden, die Verschlüsselungsverfahren mit mindestens 80 Bit Schlüssellänge anbieten. Inzwischen sind internationale Versionen der gängigen Browser verfügbar, die 128 Bit Schlüssellänge unterstützen.

Alternativ kann auf Zusatzprodukte einheimischer Hersteller zurückgegriffen werden, die ebenfalls innerhalb von Standard-Browsern die Benutzung längerer Schlüssel ermöglichen. Hierzu kann auch Public Domain Software wie SSLeay oder OpenSSL eingesetzt werden.

Zertifikate

Ein schwieriges Problem bei der Datenkommunikation über offene Netze ist die Überprüfung der Identität der Kommunikationspartner, da man sich nicht darauf verlassen kann, dass Namensangaben korrekt sind. Bei SSL erfolgt die Überprüfung der Identität des Kommunikationspartners über so genannte Zertifikate. Zertifikate enthalten deren öffentliche Schlüssel sowie eine Bestätigung einer weiteren Instanz über die korrekte Zuordnung des öffentlichen Schlüssels zu dessen "Besitzer", hier also ein Server oder Client. Der Wert eines Zertifikates hängt also nicht zuletzt davon ab, wie vertrauenswürdig diese Bestätigungsinstanz (auch Trustcenter oder Zertifizierungsstelle genannt) ist. Die Echtheit des Zertifikates lässt sich wiederum mit dem öffentlichen Schlüssel der Bestätigungsinstanz überprüfen.

Bei SSL sind drei Varianten von Zertifikaten zu unterscheiden:

- Benutzerzertifikate, die für eine Client-Authentisierung benötigt werden,
- Zertifikate von Zertifizierungsstellen, wobei manche Zertifizierungsstellen mehrere Zertifikate haben, je nach der zugrundegelegten Sicherheitspolitik, und
- Zertifikate von Software-Herstellern bzw. Betreibern von Webseite

Sicherheitspolitik der Zertifizierungsstellen prüfen

Alle Browser enthalten bereits bei der Installation SSL-Zertifikate einiger Zertifizierungsstellen. Diese Zertifizierungsstellen haben sehr unterschiedliche Sicherheitsleitlinien und Bedingungen, unter denen sie Zertifikate erteilen. Daher sollten zunächst alle Zertifikate ausgeschaltet und erst dann wieder aktiviert werden, wenn man sich davon überzeugt hat, dass deren Sicherheitspolitik den eigenen Sicherheitsbedürfnissen genügt.

bei neuen Zertifikaten Fingerprints überprüfen

Bei der Aufnahme eines neuen Zertifikates sollte darauf geachtet werden, dieses erst nach Überprüfung des "Fingerprints" zu aktivieren. Der Fingerprint ist eine hexadezimale Zahl, die zusammen mit dem Zertifikat übermittelt wird. Zusätzlich sollte sie auf einem anderen Weg übermittelt und verglichen werden, da diese die Korrektheit des Zertifikats sicherstellen soll.

Betreiber von WWW-Servern, die mit den Besuchern ihrer WWW-Seiten sicherheitsrelevante Daten austauschen wollen, sollten hierzu einen kryptographisch abgesicherten Weg anbieten, also z. B. SSL.

Hinweis: Sind die Benutzer durch eine Firewall vor aktiven Inhalten und Computer-Viren geschützt, so müssen sie bei der Verwendung von SSL eigene Schutzmaßnahmen gegen diese Gefährdungen treffen, wie z. B. in M 4.33 *Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung* bzw. M 5.69 *Schutz vor aktiven Inhalten* beschrieben.

Ergänzende Kontrollfragen:

- Verträgt sich die Nutzung von SSL mit den vorhandenen Sicherheitsleitlinien für die Firewall bzw. für die Nutzung von WWW-Diensten?
- Wissen die Benutzer, was bei der Nutzung von SSL zu beachten ist?

M 5.67 Verwendung eines Zeitstempel-Dienstes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Die im Header einer E-Mail eingetragenen Zeitinformationen können relativ einfach manipuliert werden. Ist es erforderlich, den exakten Absende- oder Empfangszeitpunkt einer E-Mail zu kennen, muss ein Zeitstempeldienst benutzt werden. Ein Zeitstempel ist ein Zeiteintrag von einer neutralen Stelle, der nicht mehr zu verfälschen ist. Er wird von einem Zeitstempel-Server entweder vollautomatisch, d. h. transparent für den Benutzer, oder auf Anforderung durch den Absender aufgebracht.

Ein Zeitstempel besteht aus einem Zeitstempel-Zertifikat, in dem das aktuelle Datum und die aktuelle Uhrzeit sowie die Identität des Zeitstempel-Dienstes selbst dokumentiert werden, sowie aus einer digitalen Signatur über E-Mail und Zertifikat. Hiermit dokumentiert und bestätigt der Zeitstempel die Existenz einer bestimmten Nachricht mit einem bestimmten Inhalt zu einem bestimmten Zeitpunkt. Die Sicherstellung der Authentizität der E-Mail durch den Zeitstempel setzt voraus, dass der Absender seinerseits die E-Mail digital signiert hat.

Ein Zeitstempel-Dienst kann sowohl in einem internen Netz als auch im Internet angeboten und genutzt werden. Er nimmt als Server im Internet/Intranet signierte Dateien oder auch nur deren Signaturen entgegen und versieht diese mit einem synchronisierten Zeitstempel. Alles zusammen wird vom Zeitstempel-Dienst wiederum signiert und wahlweise an den Empfänger weitergeleitet oder auch zurück an den Absender geschickt.

M 5.68 Einsatz von Verschlüsselungsverfahren zur Netzkommunikation

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Gefahr durch Abhören, Manipulation oder Wiedereinspeisung

Kommunikationsnetze transportieren Daten zwischen IT-Systemen. Dabei werden die Daten selten über eine dedizierte Kommunikationsleitung zwischen den an der Kommunikation beteiligten Partnern übertragen. Vielmehr werden die Daten über viele Zwischenstationen geleitet. Je nach Kommunikationsmedium und verwendeter Technik können die Daten von den Zwischenstationen unberechtigt abgehört werden, oder auch von im jeweiligen Vermittlungsnetz angesiedelten Dritten (z. B. bei der Verwendung des Ethernet-Protokolls ohne Punkt-zu-Punkt-Vernetzung). Da die zu übertragenden Daten nicht von unberechtigten Dritten abgehört, verändert oder zur späteren Wiedereinspeisung in das Netz (Replay-Attacke) benutzt werden sollen, muss ein geeigneter Mechanismus eingesetzt werden, der dies verhindert. Verschlüsselung der Daten mit - wenn nötig - gegenseitiger Authentisierung der Kommunikationspartner kann diese Gefahr (je nach Stärke des gewählten Verschlüsselungsverfahrens sowie der Sicherheit der verwendeten Schlüssel) reduzieren (siehe auch Baustein B 1.7 *Kryptokonzept*).

Verschlüsselung auf unterschiedlichen Ebenen

In der Regel kommunizieren Anwendungen miteinander, um anwendungsbezogene Informationen auszutauschen. Die Verschlüsselung der Daten kann nun auf mehreren Ebenen geschehen:

- Auf Applikationsebene: Die kommunizierenden Applikationen müssen dabei jeweils über die entsprechenden Ver- und Entschlüsselungsmechanismen verfügen.
- Auf Betriebssystemebene: Die Verschlüsselung wird vom lokalen Betriebssystem durchgeführt. Jegliche Kommunikation über das Netz wird automatisch oder auf Anforderung verschlüsselt.
- Auf Netzkoppelelementebene: Die Verschlüsselung findet zwischen den Netzkoppelelementen (z. B. Router) statt.

Applikationsebene

Die einzelnen Mechanismen besitzen spezifische Vor- und Nachteile. Die Verschlüsselung auf Applikationsebene hat den Vorteil, dass die Verschlüsselung vollständig der Kontrolle der jeweiligen Applikation unterliegt. Ein Nachteil ist, dass zur verschlüsselten Kommunikation nur eine mit demselben Verschlüsselungsmechanismus ausgestattete Partnerapplikation in Frage kommt. Weiterhin können entsprechende Authentisierungsmechanismen zwischen den beiden Partnerapplikationen zur Anwendung kommen.

Betriebssystemebene

Im Gegensatz dazu findet die Verschlüsselung im Fall der Verschlüsselung auf Betriebssystemebene transparent für jede Applikation statt. Jede Applikation kann mit jeder anderen Applikation verschlüsselt kommunizieren, sofern das Betriebssystem, unter dem die Partnerapplikation abläuft, über den Verschlüsselungsmechanismus verfügt. Nachteilig wirkt sich hier aus, dass bei einer Authentisierung lediglich die Rechner gegenseitig authentisiert werden können, und nicht die jeweiligen Partnerapplikationen.

verschlüsselnde Netzkoppelelemente

Der Einsatz von verschlüsselnden Netzkoppelelementen besitzt den Vorteil, dass applikations- und rechnerseitig keine Verschlüsselungsmechanismen vorhanden sein müssen; die Verschlüsselung ist auch hier transparent für die Kommunikationspartner. Allerdings findet die Kommunikation auf der Strecke bis zum ersten verschlüsselnden Netzkoppelelement unverschlüsselt statt und birgt damit ein Restrisiko. Authentisierung ist hier nur zwischen den Koppelelementen möglich. Die eigentlichen Kommunikationspartner werden hier nicht authentisiert.

sensitive Daten verschlüsseln

Werden sensitive Daten über ein Netz (auch innerhalb des Intranets) übertragen, empfiehlt sich der Einsatz von Verschlüsselungsmechanismen. Bieten die eingesetzten Applikationen keinen eigenen Verschlüsselungsmechanismus an oder wird das angebotene Verfahren als zu schwach eingestuft, so sollte von der Möglichkeit der betriebssystemseitigen Verschlüsselung Gebrauch gemacht werden. Hier bieten sich z. B. Verfahren wie SSL an, die zur transparenten Verschlüsselung auf Betriebssystemebene entworfen wurden. Je nach Sicherheitspolitik können auch verschlüsselnde Netzkoppelelemente eingesetzt werden, etwa um ein virtuelles privates Netz (VPN) mit einem Kommunikationspartner über das Internet zu realisieren (Entsprechende Softwaremechanismen sind in der Regel auch in Firewall-Systemen (siehe Baustein B 3.301 *Sicherheitsgateway (Firewall)*) verfügbar.).

umfangreiche Planung

Beim Einsatz von verschlüsselter Kommunikation und gegenseitiger Authentisierung sind umfangreiche Planungen im Rahmen der Sicherheitspolitik eines Unternehmens bzw. einer Behörde nötig. Im Rahmen der hier angesprochenen Kommunikationsverschlüsselungen sind insbesondere folgende Punkte zu beachten:

- Welche Verfahren sollen zur Verschlüsselung benutzt werden bzw. werden angeboten (z. B. in Routern)?
- Unterstützen/Nutzen die eingesetzten Verschlüsselungsmechanismen existierende oder geplante Standards (IPSec, IPv4, IPv6, IKE)?
- Sind gemäß der Sicherheitspolitik ausreichend starke Verfahren und entsprechend lange Schlüssel gewählt worden?
- Werden die Schlüssel sicher aufbewahrt?
- Werden die Schlüssel in einer sicheren Umgebung erzeugt, und gelangen sie auf sicherem Weg zum notwendigen Einsatzpunkt (Rechner, Softwarekomponente)?
- Sind Schlüssel-Recovery-Mechanismen nötig?

Bei der Nutzung von Zertifikaten zur Authentisierung von Kommunikationspartnern sind hier ähnliche Fragestellungen zu beachten.

M 5.69 Schutz vor aktiven Inhalten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Bis vor kurzem galten Firewalls als der Schutz schlechthin vor Angriffen aus dem Internet auf das eigene Netz. Sie stellten sicher, dass aus dem Internet heraus kein Verbindungsaufbau in das interne Netz möglich war und interne Nutzer problemlos auf Informationen im Internet zugreifen konnten. Aufgrund der immer größeren Verbreitung von so genannten aktiven Inhalten auf WWW-Seiten hat sich diese Situation allerdings geändert. Informationen aus dem Internet werden nicht mehr nur betrachtet, sondern teilweise wird beim Betrachten auch fremder Programmcode ausgeführt. Momentan ist hiermit Java, ActiveX und Javascript gemeint, künftig könnten auch noch weitere hinzukommen. Auch ist über so genannte Plug-Ins das Starten anderer Programme aus dem Browser heraus möglich, teilweise sogar automatisch aus einer HTML-Seite heraus. Je nach Art dieser Programme ist mit ihrem Ausführen eventuell ein Sicherheitsrisiko verbunden.

Um ein internes Netz vor Missbrauch durch aktive Inhalte aus dem Internet zu schützen, sind aus heutiger Sicht mehrere Vorgehensweisen denkbar, die im folgenden anhand von Java, ActiveX und Javascript vorgestellt werden.

Verbieten von aktiven Inhalten auf der Firewall

Auch heute noch kann man sehr gut auf das Internet zugreifen, ohne wirklich aktive Inhalte zu benötigen. Dies ist die sicherste und deshalb empfohlene Methode für den Zugriff auf das Internet, da hiermit weiterhin die Firewall die Hauptkontrolle übernehmen kann. Um die Entgegennahme von aktiven Inhalten zu verhindern, benötigt man auf dem Application Gateway einen Proxy, der HTML-Seiten auf aktive Inhalte untersucht. Findet er diese, müssen sie aus der Seite herausgefiltert werden. Es gibt eine Reihe von Application Gateways, die diese Funktionalität bieten (siehe M 2.75 *Geeignete Auswahl eines Application-Level-Gateways*).

Es muss allerdings davon ausgegangen werden, dass diese Lösung, obwohl sie die sicherste ist, in Zukunft eine immer geringere Akzeptanz finden wird, da die Anzahl derjenigen Seiten zunimmt, wo der aktive Inhalt die eigentliche Information enthält. Wird der aktive Inhalt herausgefiltert, kann der interne Benutzer nicht mehr auf diese Information zugreifen.

Hinweis: Auch in E-Mails können aktive Inhalte versteckt sein, daher sollten auch diese daraufhin überprüft werden. Da verschlüsselte Kommunikation nicht auf aktive Inhalte überprüft werden kann, dürfen bei zentraler Filterung SSL-basierte WWW-Zugriffe nicht erlaubt werden.

Verbieten von aktiven Inhalten im WWW-Browser

Bei zentral administrierten Arbeitsplatzrechnern ist es denkbar, die Rechte der einzelnen Benutzer so weit einzuschränken, dass diese die Sicherheitseinstellungen ihres WWW-Browsers nicht mehr ändern können. Diese könnten dann so konfiguriert werden, dass aktive Inhalte nicht ausgeführt werden. Hierbei kann dann auch auf dem Application Gateway auf die Filterung nach

aktiven Inhalten verzichtet werden, da aktive Inhalte unter diesen Umständen im internen Netz keinen Schaden mehr anrichten können.

Eine andere Lösung ist, für den Zugriff auf das Internet nur bestimmte WWW-Browser zuzulassen. So gibt es nicht nur den Netscape Communicator und den Internet Explorer, sondern auch andere Browser, die keine Möglichkeiten zum Ausführen von aktiven Inhalten haben.

Zum einen könnte die Verwendung solcher Browser durch eine entsprechende Verwaltung der Arbeitsplatzrechner sichergestellt werden. Hierbei müssen aber die Betriebssysteme der Arbeitsplatzrechner eine zuverlässige Rollentrennung zwischen Benutzer und Administrator bieten, damit vom Administrator voreingestellte Konfigurationen von den Benutzern nicht rückgängig gemacht werden können. Bei Betriebssystemen wie Windows 3.1 und Windows 95 sind daher zusätzliche Sicherheitsvorkehrungen notwendig.

Zum anderen könnte der Proxy auf der Firewall so eingerichtet werden, dass nur Internet-Zugriffe einer vorgegebenen Browser-Software erlaubt sind. Hierbei ist allerdings zu berücksichtigen, dass die Sicherheit dieser Variante von der Kennung der verwendeten WWW-Browser abhängt. Mit einem Hex-Editor sollte ein versierter Benutzer keine Schwierigkeiten haben, einen WWW-Browser seiner Wahl so abzuändern, dass dieser die gewünschte Kennung hat.

Sensibilisierung der Benutzer

Es ist auch denkbar, die Verantwortung ganz in die Hände der Benutzer zu legen. Die aktiven Inhalte sollten im WWW-Browser im Regelfall abgeschaltet sein, die Benutzer haben aber die Erlaubnis, unter bestimmten Umständen auch aktive Inhalte auszuführen. Dies könnte z. B. der Fall sein, wenn sie auf das WWW-Informationsangebot eines bekannten Herstellers ohne aktive Inhalte nicht mehr zugreifen können.

Insbesondere ActiveX erlaubt mit seinen verschiedenen Sicherheitseinstellungen, das Ausführen von ActiveX auf bestimmte WWW-Server zu beschränken, so dass der Benutzer nicht dauernd seine Einstellungen ändern muss.

Es ist aber zu bezweifeln, dass ein Benutzer wirklich immer wieder die Sicherheitseinstellungen seines WWW-Browsers ändert, wenn er auf eine andere WWW-Seite wechselt, wo ihn z. B. ein Link vom "bekannten Hersteller" hingeführt haben könnte. Außerdem kann eine einzelne Web-Seite auf einem "sicheren" Rechner auch weitere Web-Seiten laden, die sich auf "unsicheren" Rechnern befinden. Darüber hinaus sind Angriffe im Internet möglich, bei denen ein Benutzer gar nicht die WWW-Seite bekommt, die er angefordert hat (siehe z. B. G 5.48 *IP-Spoofing* und G 5.78 *DNS-Spoofing*).

Filterung bestimmter aktiver Inhalte

In der letzten Zeit sind Programme entwickelt worden, die analog zu Computer-Virensuchprogrammen aktive Inhalte daraufhin untersuchen, ob darin sicherheitsgefährdender Code enthalten ist. Dies ist für die Benutzer eine sehr akzeptable Lösung, da diese dann auf alle ungefährlichen aktiven Inhalte zugreifen können.

Es stellt sich allerdings die Frage, ob solche Programme wirklich einen Schutz bieten. So kann beispielsweise ein Virensuchprogramm nicht vor trojanischen Pferden schützen, und solche können natürlich auch beträchtlichen Schaden anrichten.

Ausführen aktiver Inhalte in einer geschützten Umgebung

Java und Javascript sind so in den WWW-Browsern implementiert, dass diese in einer so genannten Sandbox ausgeführt werden. Wurde diese Sandbox richtig implementiert, so kann der aktive Inhalt nicht auf Daten außerhalb dieser Sandbox zugreifen. Zwar sind noch immer so genannte Verfügbarkeitsattacken (Denial of Service: DOS) möglich, aber die Vertraulichkeit und Integrität anderer Daten ist nicht gefährdet. Dieses Sandbox-Verfahren kann noch weiter ausgedehnt werden.

Hierfür bieten sich zwei Verfahren an:

1. Auf einem Betriebssystem mit Rollentrennung kann der WWW-Browser unter der Kennung eines Benutzers mit minimalen Rechten laufen. Dadurch können aktive Inhalte keinen Schaden anrichten, falls die Rechteprüfung korrekt funktioniert.

   Auf einem Unix-Rechner ist es z. B. möglich, einen WWW-Browser in einer *change-root*-Umgebung zu starten, in der der WWW-Browser nur noch Zugriff auf ein eingeschränktes Dateisystem hat. Sollte ein aktiver Inhalt Schaden anrichten, so kann er dies nur innerhalb dieser eingeschränkten Umgebung. Damit ein Benutzer von seinem Arbeitsplatzrechner aus arbeiten kann, muss der WWW-Browser auf diesem angezeigt werden, was beispielsweise über X-Windows möglich wäre. Auch mit Windows NT ist ein solcher Aufbau möglich.

2. Es gibt neuerdings Proxies, die dem Arbeitsplatzrechner das Ausführen von Java-Applets abnehmen, d. h. das Java-Applet wird auf dem Proxy ausgeführt, aber auf dem Arbeitsplatzrechner angezeigt. Verglichen mit dem ersten Verfahren stellt dieser Ansatz einen wesentlich schonenderen Umgang mit der verfügbaren Netzbandbreite dar.

Empfehlung:

1. Aktive Inhalte in Form von ActiveX sollten, wenn überhaupt, nur dann ausgeführt werden, wenn sie aus einer vertrauenswürdigen Quelle kommen, d. h. wenn sie signiert sind, diese Signatur auch verifiziert wurde und der Signierer vertrauenswürdig ist.

2. Java und Javascript sollten, wenn überhaupt, nur dann erlaubt werden, wenn diese aus einer vertrauenswürdigen Quelle kommen, oder aber, wenn obige Sicherheitsmaßnahmen nachprüfbar umgesetzt worden sind.

3. Es wird empfohlen, aktive Inhalte nicht nur von den WWW-Browsern kapseln zu lassen, sondern auch von einem dafür geeigneten Betriebssystem zusätzlich einzuschränken.

M 5.70 Adreßumsetzung - NAT (Network Address Translation)

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Network Address Translation (NAT) ist ein Mechanismus, bei dem eine aktive Netzkomponente (in der Regel ein Router) bei der Weiterleitung eines Paketes die IP-Adresse des Paketes verändert. Der Router speichert in einer Tabelle die Zuordnung der internen Adresse und des internen Quell-Ports zur externen Adresse, Zielport und dem Port, den der Router selbst für das veränderte Paket gewählt hat und setzt die Antwortpakete entsprechend um.

NAT kann zu verschiedenen Zwecken verwendet werden:

- NAT kann verhindern, dass anhand der IP-Adressen im lokalen Netz auf dessen Struktur rückgeschlossen wird, denn vom externen Netz aus ist nur die IP-Adresse des NAT-Gateways sichtbar. Dies verhindert gleichzeitig, dass Angreifer von außen direkt einzelne Rechner im internen Netz attackieren können.
- Im lokalen Netz werden oft mehr IP-Adressen benötigt, als offiziell registriert sind. Bei Verwendung eines NAT-Gateways wird für jedes Netz nur eine einzige offizielle IP-Adresse zwingend benötigt, die internen Adressen können beliebig gewählt werden.

  Beim Aufbau eines internen Netzes sollten interne Adressen unbedingt nur aus den Bereichen gewählt werden, die offiziell für solche Zwecke vorgesehen sind (siehe RFC 1918 - *Address Allocation for Private Internets*). Diese Bereiche sind:

  - 10.0.0.0 - 10.255.255.255 (8-Bit Netzmaske)
  - 172.16.0.0 - 172.31.255.255 (12-Bit Netzmaske)
  - 192.168.0.0 - 192.168.255.255 (16-Bit Netzmaske)

  Diese Adressen werden im "allgemeinen Internet" nicht geroutet und müssen daher am Gateway zum Internet in eine offiziell zugeteilte IP-Adresse umgesetzt werden.
- Gelegentlich wurden beim Aufbau eines internen Netzes einfach beliebige IP-Adressen verwendet. Beim Anschluss eines solchen Netzes an das Internet können diese bisher verwendeten IP-Adressen dann oft nicht benutzt werden, da der betreffende Adressbereich an andere Institutionen vergeben wurde. Um nicht alle Rechner neu konfigurieren zu müssen, kann eine Adressumsetzung von den internen zu den offiziell registrierten externen Adressen sinnvoll sein. Allerdings werden in diesem Fall oft Probleme bei der Namensauflösung eintreten und die Rechner, denen die intern verwendeten Adressen im Internet zugeordnet sind, werden aus dem internen Netz nicht erreichbar sein.

  Auch bei einem Wechsel des Internet-Providers kann dieser Fall eintreten.
- Beim Zusammenschluss zweier Netze, bei denen IP-Adressen aus den Bereichen des RFC-1918 gewählt wurden, kann ebenfalls eine

Adressumsetzung notwendig werden, wenn in beiden Netzen dieselben Adressen verwendet wurden.

Eine Umsetzung der internen in eine oder mehrere offiziell registrierte IP-Adressen und umgekehrt erfolgt über eine Adressumsetzungskomponente. Auch Proxies verfügen über eine implizite Adressumsetzung, da der Proxy extern nur seine offizielle Adresse verwendet und die Datenpakete an die jeweiligen internen Rechner weiterleitet.

Eine Adressumsetzung durch Router oder dedizierte Paketfilter kann entweder statisch oder dynamisch geschehen. Die statische Adressumsetzung ist einfach und schnell. Es wird jeder internen Adresse genau eine externe zugeordnet. Hierzu wird natürlich für jede interne Adresse genau eine externe benötigt.

Häufiger findet die dynamische Adressumsetzung Verwendung, insbesondere wenn die Anzahl der internen IP-Adressen größer ist als die der extern sichtbaren ist sie Voraussetzung. Im Router oder Paketfilter wird eine Zuordnungstabelle geführt, in der die internen Adressen mit dazugehöriger Portnummer eines Pakets einer externen Adresse mit neuer Portnummer zugeordnet wird. Häufig wird nach außen hin nur eine IP-Adresse sichtbar gemacht, die über die Portnummer-Zuordnung alle internen IP-Adressen verbirgt.

Eine Folge der dynamischen Adressumsetzung ist, dass ein Verbindungsaufbau zu einem internen Rechner aus dem Internet normalerweise nicht möglich ist. Soll dies doch möglich sein, so muss das Sicherheitsgateway "Destination NAT" bzw. "Port Forwarding" beherrschen (siehe unten).

Bestimmte Dienste müssen bei Adressumsetzung besonders behandelt werden (z. B. traceroute oder ftp).

Zugriff von außen bei NAT

Für einen Verbindungsaufbau von außen (z. B. bei Anfragen an einen Web-Server) werden am NAT-Gateway alle Pakete, die an einen bestimmten Port gerichtet sind, umgesetzt und an einen entsprechenden Port des Servers weitergeleitet. Dieser Mechanismus wird auch als "Destination NAT" oder "Port-Forwarding" bezeichnet. Mit den Antwortpaketen des Servers verfährt das NAT-Gateway analog.

Ergänzende Kontrollfragen:

- Welche IP-Adressen werden im internen Netz verwendet?
- Wird NAT eingesetzt?
- Wird Port-Forwarding eingesetzt?

M 5.71 Intrusion Detection und Intrusion Response Systeme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Eine der wesentlichen Aufgaben eines Firewall-Administrators ist es, die anfallenden Protokolldaten zu analysieren, um dadurch Angriffe zeitnah erkennen zu können. Aufgrund der Fülle der Daten und der Vielzahl und Komplexität der verschiedenen Angriffsmöglichkeiten entsteht dadurch ein beträchtlicher Arbeitsaufwand. Intrusion Detection (ID) und Intrusion Response (IR) Systeme können hierbei helfen.

Ziel eines ID-Systems muss es sein, einen durchschnittlichen Administrator soweit zu unterstützen, dass dieser auch ohne tief greifende Kenntnisse im Bereich Internet-Sicherheit in der Lage ist, einen Angriff in einer großen Anzahl von Protokolldaten zu erkennen. IR-Systeme dagegen dienen dazu, automatisch Gegenmaßnahmen einzuleiten, sobald ein Angriff erkannt wurde.

Im Idealfall verfügen diese Programme über ebenso viel Informationen wie ein guter Administrator und sind daher in der Lage, in beliebigen Protokolldaten nicht nur einen Angriff zu erkennen, sondern auch noch Aussagen über die Stärke der Bedrohung und die notwendigen Gegenmaßnahmen zu machen. Zur Zeit ist dies allerdings noch ein Gebiet, welches intensiv erforscht wird, so dass wesentliche Verbesserungen an den vorhandenen Programmen jederzeit möglich sind.

Intrusion Detection Systeme lassen sich im wesentlichen in zwei Klassen einteilen: Signaturanalyse und Anomalie-Erkennung.

Die Signaturanalyse beruht auf der Annahme, dass sich viele Angriffe anhand einer bestimmten Abfolge von Protokolldaten erkennen lassen. Ein Beispiel ist das so genannte Portscanning. Als Vorarbeit für einen Angriff wird zunächst festgestellt, welche Dienste auf dem angegriffenen Rechner ansprechbar sind, d. h. zu welchen TCP-Ports eine Verbindung aufgebaut werden kann. Hierzu wird mit Hilfe eines Programms ein Verbindungsaufbaupaket nacheinander an alle TCP-Ports geschickt. Erfolgt ein Verbindungsaufbau, ist dort ein Dienst installiert und kann angegriffen werden. Die entsprechende Signatur, also Erkennungsmerkmal, dieses Angriffs ist einfach: Verbindungsaufbaupakete, die nacheinander an alle TCP-Ports geschickt werden.

Es zeigen sich aber auch sofort die Probleme bei dieser Art der Angriffserkennung: In welcher Reihenfolge müssen die Ports angesprochen werden und in welchen zeitlichen Abständen, damit ein Angriff von einem normalen Betrieb unterschieden werden kann? Aktuelle Portscanning-Programme arbeiten so, dass nicht nacheinander Port 1, Port 2 bis Port n angesprochen werden, sondern dies in zufälliger Reihenfolge erfolgt. Auch können die Pakete nicht direkt nacheinander verschickt werden, sondern in zufälligen Zeitabständen (z. B. 1 s, 100 ms, 333 ms, 5 s ...). Dies macht die Erstellung einer Signatur schwierig.

Eine subtile Variante des Portscanning besteht darin, einzelne Pakete von verschiedenen Quelladressen zu senden. In Verbindung mit der oben aufgezeigten zeitlich versetzten Initiierung der Pakete ist die Wahrscheinlichkeit gegenwärtig sehr hoch, dass ein solcher Angriff unerkannt bleibt.

Bei der Anomalie-Erkennung geht man andererseits davon aus, dass sich das normale Verhalten der Nutzer oder Rechner statistisch erfassen lässt und wertet Abweichungen hiervon als Angriff. Ein Beispiel hierfür ist der Zeitraum, in dem eine Benutzerin normalerweise an ihrem Rechner angemeldet ist. Arbeitet sie z. B. fast immer Montags bis Freitags in der Zeit von 8.00 Uhr bis 17.00 Uhr mit Abweichungen von maximal 2 Stunden, so kann eine Aktivität am Samstag oder um 24.00 Uhr als Angriff gewertet werden. Das Problem bei der Anomalie-Erkennung ist die Festlegung des normalen Verhaltens. Hierfür lassen sich zwar mit Hilfe von Schwellwerten oder Wahrscheinlichkeitsbetrachtungen einige Aussagen machen. Ob es sinnvoll ist, eine Aktivität des Benutzers A am Montag um 19.10 Uhr sofort als Angriff zu bewerten, erscheint fraglich. Auch ändert sich das normale Verhalten eines Benutzers in Regel, so dass eine Anpassung vorgenommen werden muss. Wer aber sagt dem ID-System, dass diese Verhaltensänderung regulär ist und kein Angriff?

Des weiteren ist eine Unterteilung der ID-Systeme nach der Art der Datenaufnahme sinnvoll. Diese kann entweder mit Hilfe eines dedizierten Sniffers irgendwo im Netz erfolgen (Netzbasiertes ID-System), oder Teil der normalen Protokollierungsfunktionalität auf einem der angeschlossenen Rechner (Hostbasierte ID-Systeme) sein. Beides hat Vor- und Nachteile. Die netzbasierten Systeme haben zwar die Möglichkeit, einen umfassenden Angriff, der gleichzeitig verschiedene Rechner betrifft, leichter zu erkennen. Es ist aber erheblich schwieriger, komplexe Angriffe (z. B. über weitere Zwischenstationen) auf einen Rechner zu erkennen. Darüber hinaus können netzbasierte Systeme keine verschlüsselten Daten analysieren. Für die hostbasierten ID-Systeme gilt andererseits, dass für ihren Einsatz u. U. umfangreiche Änderungen an den Protokollierungsfunktionen der Rechner notwendig sind.

Da auch bei der automatischen Auswertung von Protokollinformationen die Datenschutzbestimmungen oder Personalvereinbarungen beachtet werden müssen, kann es unter Umständen notwendig werden, diese Daten pseudonymisiert abzulegen.

Vor der Kopplung von ID-, IR-System und Firewall sollten folgende Aspekte beachtet werden:

- Ist es möglich, gezielt einen Angriff auf die Firewall zu initiieren, der vom ID-System irrtümlich als echter Angriff gewertet wird? Eine daraufhin vom IR-System ausgelöste Sperrung bestimmter Dienste über die Firewall kann erhebliche Konsequenzen auf die Verfügbarkeit haben.
- Die Interaktion zwischen ID-, IR-System und Firewall sollte hinreichend transparent dokumentiert sein. Nur so ist es möglich, zu jedem Zeitpunkt abzuschätzen, von wem die Firewall administriert wird: vom IR-System

oder vom Administrationspersonal. Im Zweifelsfall sollten Entscheidungen des Administrationspersonals Vorrang haben.

Um Angriffe gegen ein ID-System selbst auszuschließen, sollten diese vom Netz her weitestgehend unsichtbar sein. Einfachste Maßnahme ist die Zuweisung einer IP-Adresse, die im Internet nicht geroutet wird. Empfohlen sei weiterhin die Deaktivierung des Protokolls ARP für das entsprechende Interface, so dass weder auf ARP- noch auf IP-Pakete reagiert wird

M 5.72 Deaktivieren nicht benötigter Netzdienste

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um auf einem Unix-System alle nicht benötigten Netz-Dienste zu deaktivieren, ist folgendermaßen vorzugehen:

Für den Start von Netzdiensten gibt es unter Unix zwei Möglichkeiten: über den Serverdienst *inetd*, der in der Datei */etc/inetd.conf* konfiguriert wird, und über die Startup-Dateien, die sich in */etc/rc.d/init.d* bzw. */etc/init.d* befinden. Zum Abschalten nicht benötigter Dienste in der Datei */etc/inetd.conf* muss die jeweilige Zeile mit # auskommentiert werden. Bei einer Standardinstallation sind in der Regel mehr Dienste konfiguriert als nötig sind. Darunter befinden sich immer wieder Dienste, die eine Gefährdung darstellen können. Daher sollten so wenig Dienste wie möglich freigeschaltet werden, also nur die Dienste, die auf dem jeweiligen System unabdingbar benötigt werden (siehe auch M 4.95 *Minimales Betriebssystem* und M 4.97 *Ein Dienst pro Server*).

Die Dienste, die durch die Startup-Dateien initiiert werden, werden über Links aus den Unterverzeichnissen */etc/rc**X**.d* oder */etc/rc.d/rc**X**.d* referenziert, wobei ***X*** für das jeweilige Unix-Runlevel steht, in dem die Startup-Datei aufgerufen wird. Zum Deaktivieren der nicht benötigten Dienste können die nicht benötigten Dienste in ein Unterverzeichnis verschoben werden, damit man sie bei Bedarf wieder aktivieren kann. Dies kann z. B. wie folgt aussehen:

cd rc3.d; mkdir .s; mv S85sendmail .s/

Die aktuell aktiven Dienste können mit dem Befehl *netstat -a* identifiziert werden.

Ergänzende Kontrollfragen:

- Sind die Änderungen an den Startup-Dateien dokumentiert worden?
- Wer darf auf einem Unix-System Dienste hinzufügen?
- Wird nach jedem Update von Anwendungsprogrammen und Betriebssystembestandteilen mit *netstat -a* überprüft, welche Dienste auf Netzverbindung warten?

M 5.73 Sicherer Betrieb eines Faxservers

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Fax-Poststelle

Der sichere Betrieb eines Faxservers setzt voraus, dass sowohl die lokale Kommunikation als auch die Kommunikation auf Seiten des öffentlichen Netzes abgesichert wird. Eingehende Faxsendungen nimmt der Faxserver von anderen Faxservern oder Faxgeräten entgegen und leitet sie, wenn die Funktion des automatischen Fax-Routing aktiviert ist, an die angeschlossenen Benutzer weiter. Ausgehende Faxsendungen der angeschlossenen Benutzer werden vom Faxserver entgegengenommen und an den Empfänger weitergeleitet. Der Faxserver muss zudem sicherstellen, dass lokale Faxsendungen, d. h. Faxsendungen von einem Arbeitsplatz zu einem anderen innerhalb der gleichen Organisation(seinheit), nur intern und nicht über das öffentliche Netz weitergeleitet werden.

Test und Dokumentation der Konfiguration

Zum sicheren Betrieb eines Faxservers ist es u. a. erforderlich, dass nach der Beschaffung und Installation die Konfiguration des Betriebssystems und der Faxserver-Applikation ausgiebig getestet wird. Auf evtl. auftretende Fehlermeldungen ist - soweit dies möglich ist - mit Änderungen an der Konfiguration zu reagieren. An die Testphase sollte sich ein Pilotversuch anschließen. Erst wenn der Faxserver auch in dieser Phase fehlerfrei arbeitet, sollte die Freigabe für den Wirkbetrieb erfolgen. Die Konfigurationsparameter sollten, ebenso wie alle Änderungen an der Konfiguration, sorgfältig dokumentiert werden.

Löschung von Faxdaten

Faxserver speichern alle eingehenden und ausgehenden Faxsendungen. Die Dauer der Speicherung hängt von den Leistungsmerkmalen der Faxserver-Applikation und der Konfiguration ab. So ist es z. B. möglich, dass ausgehende Faxsendungen nur bis zur Erledigung des Sendeauftrages zwischengespeichert und dann gelöscht werden. Ebenso kann es sein, dass eingehende Faxsendungen nur bis zur Weiterleitung an den Empfänger zwischengespeichert werden und anschließend die Löschung erfolgt. Denkbar ist aber auch, dass grundsätzlich alle ein- und ausgehenden Faxsendungen auf dem Faxserver solange gespeichert werden, bis die Löschung durch den jeweiligen Benutzer oder durch die Fax-Poststelle bzw. den Administrator erfolgt. Die Löschung kann bei einigen Faxservern auch automatisch nach einer gewissen Zeitspanne erfolgen. So können z. B. alle Faxsendungen, die älter als 3 Monate sind, automatisch gelöscht werden. In Abhängigkeit vom Einsatzkonzept sind Regelungen für die Löschung von Faxdaten auf dem Faxserver zu treffen. Gleichzeitig ist zu regeln, wo und in welchem Umfang eine Archivierung von Faxdaten zu erfolgen hat. Generell sollten Faxdaten nicht länger als unbedingt nötig auf dem Faxserver verbleiben.

gesicherte Aufstellung des Faxservers

Es muss ausgeschlossen werden, dass Unbefugte auf Faxsendungen zugreifen können. Daher muss zunächst der Faxserver physikalisch gegen unbefugten Zugriff gesichert werden. Dies kann nur durch die gesicherte Aufstellung des Servers in einem Serverraum oder einem Serverschrank erfolgen (siehe Baustein B 2.4 *Serverraum* und Baustein B 2.7 *Schutzschränke*).

Zuständigkeiten für die Administration

Um den störungsfreien Betrieb des Faxservers sicherzustellen, ist zudem festzulegen, wer für die Administration der Hardware-Komponenten, des Betriebssystems und der Faxserver-Applikation zuständig ist. Es sollte eine Fax-Poststelle eingerichtet werden (siehe auch M 2.180 *Einrichten einer Fax-Poststelle*). Das Administrationspersonal und das in der Fax-Poststelle eingesetzte Personal sind im Umgang mit dem Betriebssystem und der Faxserver-Applikation zu schulen. Um Störungen des Betriebs durch Fehlbedienungen zu vermeiden, sind weiterhin auch die Benutzer im Umgang mit der Faxclient-Applikation zu schulen.

Vergabe von Berechtigungen auf Faxservern

Auf Faxservern können oftmals an Benutzer und Benutzergruppen folgende Berechtigungen für eingehende Faxsendungen vergeben werden:

- lesen,
- weiterleiten,
- löschen.

Für ausgehende Faxsendungen können oftmals folgende Rechte vergeben werden:

- senden,
- anhalten,
- löschen,
- ändern der Sendeoptionen.

Die Berechtigungen sind gemäß den Festlegungen in der Faxsicherheitsleitlinie zu vergeben (siehe auch M 2.178 *Erstellung einer Sicherheitsleitlinie für die Faxnutzung*).

Vergabe von Zugriffsrechten

Sofern nicht durch technische Maßnahmen sichergestellt wird, dass Faxsendungen sofort weitergeleitet werden, ist zudem durch die Vergabe entsprechender Zugriffsrechte sicherzustellen, dass nur berechtigte Benutzer auf die entsprechenden "Postfächer" auf dem Server zugreifen können.

Generell sollte ein Zugriff auf temporäre Bereiche, in denen die Faxserver-Applikation Faxsendungen vor Abgang bzw. vor Verteilung an den Empfänger zwischenspeichert, nur privilegierten Benutzern (Administratoren, Fax-Poststelle) vorbehalten bleiben.

Regelmäßig sind die Verbindungen des Faxservers mit der Telekommunikationsanlage bzw. mit dem öffentlichen Telefonnetz auf Funktion zu überprüfen. Sofern der Faxserver mit internen Kommunikationssystemen, wie z. B. einem E-Mail-System oder einem Workflow-System, zusammenarbeitet, ist ebenfalls regelmäßig die Funktion dieser Verbindungen zu überprüfen.

Prüfung des freien Festplattenplatzes

Außerdem muss regelmäßig geprüft werden, ob der für die Speicherung von Faxsendungen zur Verfügung stehende Festplattenplatz noch ausreichend ist (siehe auch M 5.75 *Schutz vor Überlastung des Faxservers*). Bei erschöpftem Festplattenplatz können keine weiteren Faxsendungen mehr empfangen oder versandt werden.

Auswertung der Protokolle

Die Aktivitäten des Faxservers sind gemäß den Festlegungen in der Faxsicherheitsleitlinie zu protokollieren und die Protokolle sind regelmäßig zu kontrol-

lieren (siehe auch M 2.64 *Kontrolle der Protokolldateien* und M 5.25 *Nutzung von Sende- und Empfangsprotokollen*). Bei der Festlegung von Umfang und Inhalt der Protokollierung ist auf eine frühzeitige Beteiligung des Personal- bzw. Betriebsrates zu achten.

Vorbehalte gegen den Einsatz eines Faxservers bestehen häufig aufgrund der Tatsache, dass dabei ein IT-System, das in das LAN integriert ist, über das öffentliche Telekommunikationsnetz erreicht werden kann.

Durch sorgfältige Auswahl und Konfiguration von Kommunikationskarten, Betriebssystem und Faxserver-Applikation sowie durch eine sichere netztopologische Anordnung des Servers kann die Gefahr eines Einbruchs in das Netz bzw. in den Faxserver bis auf ein geringes Restrisiko minimiert werden.

Deaktivierung nicht benötigter Leistungsmerkmale

Beim Einsatz von aktiven ISDN-Karten sollten Leistungsmerkmale, die nicht zum Empfang und Senden von Faxen notwendig sind, deaktivert werden (siehe M 4.59 *Deaktivieren nicht benötigter ISDN-Karten-Funktionalitäten*).

Sofern dedizierte Faxkarten zum Einsatz kommen, sind auch zunächst die entsprechenden Leistungsmerkmale genau zu untersuchen. Auch hier gilt, dass nicht benötigte Merkmale - soweit dies möglich ist - abzuschalten sind.

ein Dienst pro Server

Der Faxserver sollte keine anderen Dienste als den Fax-Dienst anbieten. Insbesondere sollte ein Faxserver nicht gleichzeitig als Daten-, Drucker-, E-Mail- oder Internet-Server bzw. als Remote-Access-Rechner verwendet werden. Um einem Einbruch über das Telekommunikationsnetz entgegenzuwirken, muss das Betriebssystem so "schlank" wie möglich installiert werden. Dies bedeutet, dass auf die Installation von für den Betrieb nicht zwingend notwendigen Diensten und Protokollen verzichtet wird. Hierzu ein Beispiel: Wenn auf einem Faxserver der Telnet-Dienst nicht gestartet ist, kann auch kein entsprechender Angriff zum Erfolg führen. Bei der Festlegung der benötigten Dienste und Protokolle darf nie vergessen werden, dass Gefährdungen häufig erst durch die Kombination von verschiedenen Diensten und Protokollen entstehen.

Anordnung des Faxservers im Netz

Die sichere netztopologische Anordnung des Faxservers ist unter anderem davon abhängig, ob und ggf. welche Art von Firewall in der Organisation im Einsatz ist.

Ein Faxserver hat jeweils mindestens eine Schnittstelle zum Telekommunikationsnetz und zum LAN. Die Anordnung des Faxservers im Netz sollte so erfolgen, dass im Falle eines erfolgreichen Angriffs auf den Faxserver nicht in das gesamte Netz eingebrochen werden kann. Andererseits sollte es auch nicht möglich sein, den Faxserver von innerhalb des Netzes aus erfolgreich zu attackieren. Denkbar wäre hier z. B. ein Angriff eines Außentäters aus dem Internet. Gelingt solch ein Angriff, so ist der Täter in der Lage, über den Faxserver der angegriffenen Organisation das Versenden von Faxen zu veranlassen. Dies kostet Gebühren und, was ggf. noch schlimmer ist, führt unter Umständen zu Ansehensverlust. Auch ist ein Angreifer im Falle eines erfolgreichen Angriffs in der Lage, unbefugt Kenntnis von den auf dem Faxserver (zwischen-) gespeicherten Faxsendungen zu nehmen. Angriffe eines Innentäters über das LAN sind in vergleichbarer Weise denkbar.

Da ein Faxserver meistens nicht die einzige IT-Komponente mit Anschluss an ein externes Netz ist, ist in der Regel zum Schutz des internen Netzes ohnehin eine Abschottung gegenüber externen Netzen vorhanden (siehe auch Baustein B 3.301 *Sicherheitsgateway (Firewall)*).

Anordnung bei vorhandener Firewall

Sofern als Internet-Firewall ein Screened Subnet (Konfiguration 1 aus M 2.73 *Auswahl geeigneter Grundstrukturen für Sicherheitsgateways*) vorhanden ist, sollte der Faxserver zwischen dem inneren Paketfilter und dem Application Gateway (siehe Abbildung 1) eingebunden werden. Die Schutzwirkung gegenüber Angriffen aus dem unsicheren Netz ist durch den Application Gateway und den äußeren Paketfilter hinreichend groß. Gegen Angriffe aus dem internen Netz wird der Faxserver durch den inneren Paketfilter geschützt.

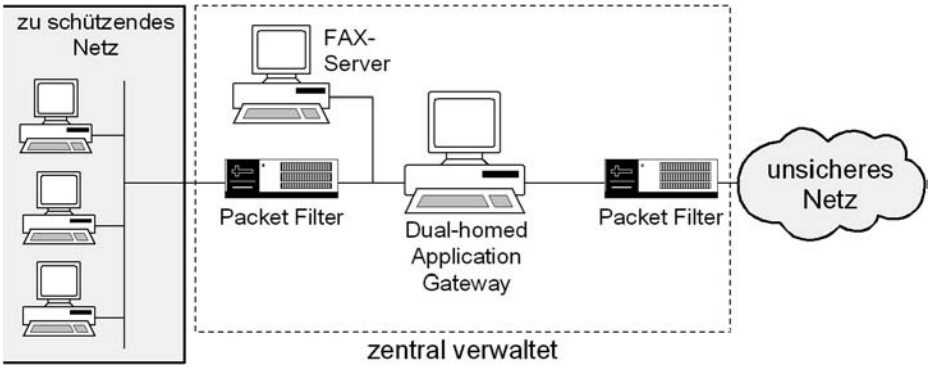


Abbildung: Einbindung eines Faxservers in ein Firewall-System

Anordnung ohne geeignete Firewall

Bei allen anderen Firewall-Kombinationen, insbesondere solchen mit nur einem Paketfilter, oder wenn bisher keine Firewall vorhanden ist, sollte der Faxserver direkt in das sichere Netz eingebunden werden. Sofern das entstehende Restrisiko aufgrund des Schutzbedarfs als nicht tragbar angesehen wird, muss entweder eine Absicherung mittels eigenem Paketfilter erfolgen, oder die Telekommunikationsanlage muss so konfiguriert werden, dass nur abgehende Verbindungen zulässig sind. Für eingehende Faxsendungen muss in diesem Fall ein herkömmliches Faxgerät oder ein Stand-alone-System mit entsprechender Faxapplikation eingesetzt werden, mit der Folge, dass eingehende Faxsendungen nur manuell an die Empfänger verteilt werden können.

Ergänzende Kontrollfragen:

- Ist die Konfiguration des Faxservers dokumentiert?
- Wird diese Dokumentation bei Änderungen der Konfiguration angepasst?
- Werden Faxdaten auf dem Faxserver regelmäßig gelöscht?
- Ist den Benutzern bekannt, nach welchen Regeln diese Löschungen erfolgen?
- Wer ist für die Auswertung der anfallenden Protokolldaten zuständig?

M 5.74 Pflege der Faxserver-Adressbücher und der Verteillisten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Fax-Poststelle

Die meisten Faxserver bieten sowohl zentrale als auch individuelle Adressbücher an. Zentrale Adressbücher stehen allen Benutzern eines Faxservers zur Verfügung und sollten zentral durch die Fax-Poststelle gepflegt werden. Individuelle Adressbücher können von jedem Benutzer erstellt werden, stehen aber in der Regel auch nur dem Ersteller zur Verfügung.

Schutz vor Manipulation

In besonderem Maße sind die zentralen Adressbücher gegen unbefugte Veränderung zu schützen. Dazu sind entweder über die Faxserver-Applikation oder - sofern dies nicht möglich ist - mit Mitteln des Betriebssystems die Berechtigungen so zu vergeben, dass nur die Fax-Poststelle die zentralen Adressbücher verändern kann.

regelmäßige Überprüfung der zentralen Adressbücher

Regelmäßig sollte durch die Fax-Poststelle die Integrität und Aktualität der zentralen Adressbücher überprüft werden. Die meisten Faxserver lassen es zu, mehrere Empfänger in den Adressbüchern zu Gruppen zusammenzufassen. Sofern es einem Angreifer gelingt, solche Gruppen zu manipulieren, können er oder andere Unbefugte Kenntnis von vertraulichen Faxsendungen erhalten. Die Fax-Poststelle sollte daher auch die Zuordnung von Empfängern zu den einzelnen Gruppen regelmäßig auf Aktualität überprüfen. Sofern in einer Organisation zwischen den Arbeitsplätzen Daten über den Faxserver per Fax ausgetauscht werden, müssen durch die Fax-Poststelle auch interne Adressbücher aktuell gehalten werden.

Außerdem sind die Benutzer zur regelmäßigen Kontrolle der von ihnen benutzten Einträge zu verpflichten. Dies gilt sowohl für zentrale als auch für individuelle Adressbücher.

regelmäßige Überprüfung der Verteillisten

Durch den Faxserver werden Verteillisten dazu benutzt, um eingehende Faxsendungen an die Empfänger weiterzuleiten. Falsche Zuordnungen in den Verteillisten können dazu führen, dass Unbefugte Kenntnis von Faxsendungen mit vertraulichem Inhalt erhalten. Die Verteillisten sollten daher von der Fax-Poststelle regelmäßig auf Aktualität und Integrität überprüft werden.

Um die Pflege von Adressbüchern und Verteillisten zu gewährleisten, muss die Fax-Poststelle über das Ausscheiden von Mitarbeitern informiert werden.

Damit durchgeführte Administrationsarbeiten nachvollzogen werden können, sollten die Eintragungen und Veränderungen an den zentralen Adressbüchern und an den Verteillisten dokumentiert werden.

Ergänzende Kontrollfragen:

- Wie häufig wird die Integrität und Aktualität der Adressbücher und Verteillisten überprüft?
- Wie erfährt die Fax-Poststelle vom Ausscheiden von Mitarbeitern?

M 5.75 Schutz vor Überlastung des Faxservers

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Fax-Poststelle

Ein Faxserver kann sowohl durch eingehende als auch durch ausgehende Faxsendungen überlastet werden. Eine Überlastung des Faxservers kann dazu führen, dass zeitweilig keine weiteren Faxsendungen mehr empfangen oder versandt werden können. Es ist auch denkbar, dass im Falle der Überlastung das Betriebssystem oder die Faxserver-Applikation abstürzt und der Faxserver vorübergehend gar nicht mehr verfügbar ist.

Eine Art der Überlastung des Faxservers liegt vor, wenn alle Kanäle, die durch die Kommunikationskarten bereitgestellt werden, durch eingehende und ausgehende Faxsendungen blockiert werden. Folge ist, dass weitere Faxe erst dann wieder empfangen oder gesendet werden können, wenn ein Kanal frei wird. Dieser Effekt tritt auch auf, wenn alle von der Telekommunikationsgesellschaft zur Verfügung gestellten Leitungen durch eingehende und ausgehende Faxsendungen belegt werden.

Beschaffung geeigneter Komponenten

Vor der Beschaffung eines oder mehrerer Faxserver ist zunächst das voraussichtliche Faxvolumen abzuschätzen. Sodann sind ausreichend leistungsfähige Komponenten zu beschaffen. Außerdem sollte darauf geachtet werden, dass genügend Telekommunikationsleitungen zur Verfügung stehen.

Außerdem sollten die Protokolle des Faxservers regelmäßig kontrolliert werden, um feststellen zu können, ob der Server zu bestimmten Zeiten überlastet oder die Grenze der Belastbarkeit erreicht wird.

zeitversetztes Senden

Eine Überlastung des Faxservers kann dadurch erfolgen, dass intern versucht wird, eine große Anzahl von Faxen zu versenden. Unter ungünstigen Umständen kann dies zum Absturz der Faxserver-Applikation oder des Betriebssystems führen. Auslöser kann z. B. eine sehr große Anzahl von Serienfax-Sendungen sein. Es sollte daher schon in der Test- oder in der Pilotierungsphase versucht werden, die Belastungsgrenze zu ermitteln. Um diese Belastungsgrenze nicht zu überschreiten, sollte den Benutzern z. B. mittels geeigneter Dienstanweisung der maximale Umfang einer Serien-Faxsendung vorgegeben werden. Umfangreiche Serien-Faxsendungen sind dann auf mehrere Sendungen aufzuteilen. Zu Zeiten hoher Belastung des Faxservers sollte durch eine entsprechende Dienstanweisung oder durch eine entsprechende Vergabe von Berechtigungen am Faxserver sichergestellt werden, dass Faxe nur in dringenden Fällen gesendet werden. Sinnvoll kann auch die Vorgabe sein, Faxe möglichst nur zeitversetzt in der Nacht zu senden, was zudem noch Gebühren spart.

Absprache mit dem Absender

Wenn festgestellt wird, dass der Faxserver immer durch die gleichen Senderrufnummern mittels einer entsprechenden Anzahl von Faxsendungen zu ganz bestimmten Zeiten blockiert wird, ist zunächst zu ermitteln, wer die Absender sind und um welche Art von Faxsendungen es sich handelt. Sofern die Faxsendungen von der Organisation benötigt werden, kann versucht werden, mit den Absendern Zeiten auszuhandeln, in denen problemlos Faxsendungen entgegengenommen werden können. Sofern die Faxsendungen nicht benötigt werden (z. B. nicht angeforderte Werbe-Faxsendungen), kann versucht

werden, die Absenderrufnummern über die Faxserver-Applikation oder über die Telekommunikationsanlage zu sperren. Dies ist aber nur möglich, sofern die Absenderkennung (CSID= Caller Sender Identification) nicht verschleiert bzw. bei Verwendung von ISDN die Rufnummernübermittlung seitens des Absenders nicht unterdrückt wurde. Sofern die Faxnummer des Absenders nicht zu ermitteln sind, bleibt nur noch die Möglichkeit, die vorhandenen Kapazitäten - wie oben beschrieben - zu erweitern.

ausreichend freien Festplattenplatz sicherstellen

Problematisch kann auch die Festplattenkapazität eines Faxservers sein. Dabei ist die Gefahr, die Festplattenkapazität durch einen Angriff von außen gezielt zu erschöpfen, eher gering. Eine gefaxte DIN A4 Seite ist ca. 70 kB groß. Geht man von heute üblichen Festplattengrößen von mehreren Gigabyte aus, so ist auch angesichts der anfallenden Gebühren ein entsprechender Angriff eher unwahrscheinlich. Grundsätzlich werden alle eingehenden und ausgehenden Faxsendungen auf der Festplatte des Faxservers (zwischen-) gespeichert. Der weitere Ablauf hängt dann von der Faxserver-Applikation und ggf. auch von der Konfiguration ab. So ist z. B. denkbar, dass alle Faxsendungen dauerhaft auf der Festplatte des Faxservers gespeichert bzw. archiviert werden. Bei dieser Betriebsart kann - abhängig vom Faxvolumen - sehr schnell die Festplattenkapazität erschöpft werden. Es sollte in diesem Fall sichergestellt werden, dass Ausgangs-Faxsendungen und bereits gelesene Eingangs-Faxsendungen möglichst zeitnah auf externe Datenträger archiviert und auf dem Faxserver gelöscht werden. Dazu sollte der den Benutzern auf dem Faxserver zur Verfügung gestellte Speicherplatz begrenzt werden. Außerdem sollte z. B. durch Dienstanweisung sichergestellt werden, dass Faxsendungen, die nicht mehr benötigt werden, zu löschen sind. Dies gilt insbesondere für unverlangt erhaltene Werbe-Faxsendungen. Durch die Fax-Poststelle ist regelmäßig der freie Speicherplatz auf der Festplatte des Faxservers zu überprüfen.

Ergänzende Kontrollfragen:

- Zu welchen Zeiten erfolgt eine hohe Auslastung des Faxservers?
- Gibt es Dienstanweisungen, wonach zu Zeiten hoher Belastung Faxe nur in dringenden Fällen gesendet werden dürfen?
- Wird darauf verzichtet, Faxdaten dauerhaft auf dem Faxserver zu archivieren?

M 5.76 Einsatz geeigneter Tunnel-Protokolle für die RAS-Kommunikation

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement-Team

Verantwortlich für Umsetzung: Administrator

Absicherung der RAS-Kommunikation

Wird über Remote Access auf ein LAN zugegriffen, so geschieht dies über eine Datenverbindung, an deren Bereitstellung meist externe Dritte beteiligt sind. So wird beispielsweise bei der Nutzung der direkten Einwahl (Direct Dial-In) das Netz des Telekommunikationsanbieters benutzt. Geschieht der Verbindungsaufbau über das Internet, so werden die Daten über die Netze der beteiligten Internetdienstanbieter (und ggf. deren Kooperationspartner) geleitet. Da über eine RAS-Verbindung (Remote Access Service) die direkte Anbindung des RAS-Clients in ein LAN erfolgt, muss der zur Datenübertragung benutzte Netzpfad so abgesichert werden, dass die Sicherheit der Daten (Vertraulichkeit, Integrität, Authentizität) gewährleistet ist. Die Absicherung wird durch das Verschlüsseln und das Signieren der ausgetauschten Datenpakete erreicht, nachdem die Kommunikationspartner authentisiert wurden (siehe auch M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*). Im RAS-Umfeld haben sich verschiedene Verfahren und Mechanismen zur Absicherung der Kommunikationsverbindung (z. B. Tunneling, siehe unten) herausgebildet.

Die Wahl des Verfahrens, das zur Absicherung einer RAS-Verbindung zu benutzen ist, hängt von verschiedenen Faktoren ab, u. A.

- von den Sicherheitsanforderungen an die Stärke der Verfahren (hierdurch werden beispielsweise die Schlüssellängen bestimmt),
- von den auf Protokollebene einsetzbaren Verfahren (siehe unten),
- von den durch die RAS-Hard- und Software unterstützten Verfahren.

Generell gilt:

- Das RAS-Produkt bietet in der Regel eine Auswahl von unterstützten Standardverfahren zur Kommunikationsabsicherung an. Hier sollte eine möglichst breite Unterstützung von Verfahren angestrebt werden.
- Die zum Datentransport benutzten Protokolle bieten selbst schon Sicherheitsmechanismen an. Diese können vom RAS-Produkt genutzt werden. Alternativ kann das RAS-Produkt auch eigene Verfahren anbieten.

Die Sicherheitsmechanismen basieren auf unterschiedlichen kryptographischen Verfahren. Die Maßnahme M 3.23 *Einführung in kryptographische Grundbegriffe* enthält eine kurze Einführung in kryptographische Grundbegriffe.

Verschlüsseln von Protokollverbindungen: Tunneling

Wird eine verschlüsselte Datenverbindung zwischen zwei Kommunikationspartnern aufgebaut, so realisiert diese Verbindung einen "sicheren Kanal". Durch diesen Kanal können beliebige Daten sicher mit dem zugrunde liegenden Kommunikationsprotokoll (beispielsweise IP) übertragen werden. Stellen die übertragenen Daten selbst die Datenpakete eines Kommunikationsproto

kolls dar, so spricht man auch von einem "Tunnel". Das Protokoll, das verwendet wird, um die Daten zu verschlüsseln, durch den Tunnel zu übertragen und die Verbindung zu verwalten, wird auch als Tunnel-Protokoll bezeichnet. Bei Tunnel-Protokollen kann unterschieden werden,

- auf welchem Transport-Protokoll sie aufbauen und welcher Protokoll-Schicht (OSI-Layer) sie zuzuordnen sind (siehe auch M 4.90 *Einsatz von kryptographischen Verfahren auf den verschiedenen Schichten des ISO/OSI-Referenzmodells*),
- welche Protokolle über die Tunnel-Verbindung übertragen werden können,
- welche kryptographischen Verfahren zur Realisierung des Tunnels unterstützt werden,
- ob die Endpunkte des Tunnels authentisiert werden und
- ob über eine Verbindung des benutzten Transport-Protokolls der Aufbau mehrerer paralleler Tunnel möglich ist.

Das Tunnel-Protokoll ist im Wesentlichen zuständig für

- Verwaltung des bzw. der Tunnel: Aufbau, Aufrechterhaltung und Abbau,
- Aushandeln der zu verwendenden kryptographischen Verfahren für die Realisierung des Tunnels: Schlüsselaustauschverfahren, Verschlüsselungsverfahren und Signaturverfahren,
- Ver- und Entpacken der Datenpakete der durch den Tunnel übertragbaren Protokolle sowie
- Ver- und Entschlüsseln der Datenpakete.

Im RAS-Umfeld haben sich folgende Tunnel-Protokolle etabliert:

- die Schicht-2-Protokolle:
  - PPTP (Point to Point Tunneling Protocol) und
  - L2TP (Layer 2 Tunneling Protocol: Das L2TP ist eine Kombination von PPTP und dem von der Firma Cisco entworfenen Protokoll L2F (Layer 2 Forwarding), welches PPP-Pakete (Point to Point Protocol) von einem PPP-Server über eine WAN-Verbindung an einen L2F-fähigen Router weiterleitet, der diese dann entpackt und in ein Netz einspeist.
- die Schicht-3-Spezifikation IPsec (Internet Protocol Security).

Die Protokolle besitzen die aus der folgenden Tabelle ersichtlichen Charakteristika.

Tunnel-Protokoll	Schicht	Transportierte Protokolle	Benötigtes darunter liegendes Protokoll	Anzahl der unterstützten Tunnel	Tunnel Authentisierung
PPTP	2	IP, IPX, NetBEUI	IP	1	Nein
L2TP	2	IP, IPX, NetBEUI	IP, X.25, Frame Relay, ATM	mehrere	Ja
IPsec	3	IP	IP	1	Ja

Tabelle: Protokolle

Alle Protokolle sind durch die Verwendung von kryptographischen Verfahren in der Lage, gesicherte Verbindungen in ein LAN über ein unsicheres Vermittlungsnetz herzustellen. Dabei werden die Vertraulichkeit und die Integrität der Daten geschützt. Je nach Protokoll ist der Aufbau von einer oder mehreren Tunnel-Verbindungen möglich.

Tunneling auf Schicht 2: PPTP und L2TP

Die Tunnel-Protokolle der Schicht 2 können beide die gebräuchlichsten Protokolle tunneln, unterscheiden sich aber darin, über welche darunter liegenden Protokolle das Tunneling möglich ist: PPTP kann nur über ein IP-basiertes Netz übertragen werden, wohingegen L2TP auch über verschiedene WAN-Protokolle übertragen werden kann und somit eine größere Flexibilität bietet. Die nachfolgende Abbildung veranschaulicht, wie Pakete einer Applikation von PPTP über eine PPP-Verbindung verpackt werden. Wie aus obiger Tabelle zu ersehen ist, können über das modernere L2TP-Protokoll auch mehrere unabhängige Tunnel (z. B. mit unterschiedlichen Qualitätszusicherungen) erzeugt werden. Bei der Authentisierung von Benutzern und bei der Verschlüsselung kommen bei beiden Protokollen die Sicherheitsmechanismen der darunter liegenden PPP-Verbindung zum Tragen.

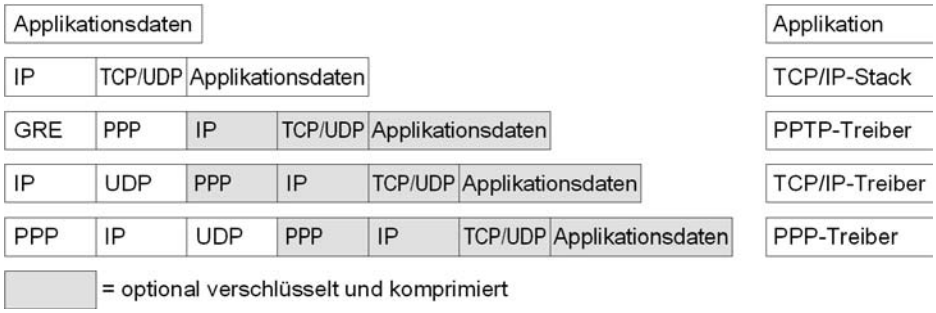


Abbildung: Verpackung von Applikationsdaten beim Protokoll PPTP

Sicherheitsmechanismen des PPP-Protokolls

1. Benutzer-Authentisierung

   Die meisten Implementierungen des PPP-Protokolls unterstützen die folgenden Standardverfahren zur Authentisierung von Benutzern (siehe auch M 5.50 *Authentisierung mittels PAP/CHAP*):

   - Password Authentication Protocol (PAP): Der PPP-Server verlangt vom PPP-Client die Übertragung eines Benutzernamens und eines Passwortes. Beide Informationen werden hier im Klartext übertragen. Dieser Mechanismus ist unsicher, und kann auch nicht gegen so genannte "Replay"-Attacken schützen, bei der ein Unberechtigter die abgehörten Daten später noch einmal sendet. Von der Verwendung des PAP-Authentisierungsprotokolls muss daher abgeraten werden.
   - Challenge-Handshake Authentication Protocol (CHAP): der PPP-Server sendet an den PPP-Client eine so genannte "challenge", bestehend aus einer Sitzungskennung und einer zufälligen Buchstabenfolge, dem "challenge string". Der Client sendet als Antwort den Benutzernamen im Klartext, sowie den MD5-Hashwert der Kombination aus Sitzungskennung, "challenge string", Benutzerpasswort. Hier wird insbesondere das Passwort nicht im Klartext übertragen. Durch die Verwendung der zufälligen Buchstabenfolge kann das Protokoll vor "Replay"-Attacken schützen.

2. Datenverschlüsselung und Schlüsselmanagement

   In der Initialisierungsphase des PPP-Protokolls werden zwischen Client und Server die zu verwendenden Verfahren zur Datenverschlüsselung (und Kompression) ausgehandelt. Generell kann hier jedes Verfahren zum Einsatz kommen, solange Client und Server über eine entsprechende Implementation verfügen. Beim Aushandeln der Verfahren ist darauf zu achten, dass Client und Server jeweils so konfiguriert sind, dass nur die in den IT-Sicherheitsrichtlinien vorgesehenen Verfahren akzeptiert werden. Ebenso ist auszuschließen, dass die unverschlüsselte Kommunikation als Rückfallvariante gewählt wird, wenn zwischen Client und Server kein kompatibles Verfahren ausgehandelt werden konnte. Auch das explizite Aushandeln der unverschlüsselten Kommunikation muss unterbunden werden.

Tunneling auf Schicht 3: IPsec

Während die Schicht-2-Protokolle von den Sicherheitsmechanismen des zugrunde liegenden PPP-Protokolls Gebrauch machen, werden durch die Schicht-3-Spezifikation IPsec eigene Sicherheitsverfahren und -mechanismen festgelegt. Eine Einschränkung von IPsec ist, dass lediglich IP-basierte Kommunikation unterstützt wird. Dies ist jedoch in den meisten Fällen kein starker Nachteil, da heute die meisten Betriebssysteme und Anwendungen auf IP-basierte Kommunikation zurückgreifen.

In Bezug auf die Sicherheitsanforderungen stellt sich IPsec wie folgt dar:

- Benutzer-Authentisierung

  Tunnel-Protokolle auf Schicht 3 gehen davon aus, dass die Authentisierung der Tunnel-Endpunkte schon vor Aufbau des Tunnels durchgeführt wurde und bieten keine eigenen Mechanismen an. Die einzige Ausnahme bildet hier das IPsec IKE-Verfahren (Internet Key Exchange, früher ISAKMP/Oakley), dass eine gegenseitige Authentisierung der Tunnel-Endpunkte auf Applikationsebene erlaubt. Eine Authentisierung auf Benutzer-Ebene ist damit jedoch nicht möglich. Da ein Schicht-3-Protokoll aber seinerseits über ein Schicht-2-Protokoll übertragen wird, kann hier grundsätzlich von den Sicherheitsmechanismen beider Protokollschichten Gebrauch gemacht werden. Im RAS-Einsatz müssen sogar die Mechanismen zur Benutzer-Authentisierung des darunter liegenden Schicht-2-Protokolls genutzt werden, da sonst ein unberechtigter Dritter den Sicherheitsmechanismus - zum Beispiel durch physikalischen Zugriff auf den Client - unterlaufen kann.

- Datenverschlüsselung

  Der Standard IPsec schreibt vor, dass IPsec-konforme Implementationen mindestens die Verschlüsselungsverfahren DES und Tripel-DES, sowie die Hashfunktionen MD5 und SHA-1 zur Verfügung stellen müssen. Es spricht jedoch nichts dagegen, dass hier andere Verfahren zum Einsatz kommen können. Allerdings ist man in diesem Fall darauf angewiesen, dass das gleiche Verfahren auch dem Kommunikationspartner zur Verfügung steht. Generell sollten nur allgemein anerkannte und etablierte Verfahren eingesetzt werden. Die Schlüssellänge für symmetrische Verschlüsselungsverfahren sollte mindestens 80 Bit betragen.

- Schlüsselmanagement

  IPsec kennt mehrere Verfahren zum Generieren, Austauschen und Verwalten von Schlüsseln. Beim "Manual IPsec" Verfahren erfolgt kein automatisches Schlüsselmanagement. In der Regel wird hier der Schlüssel von den Kommunikationspartnern über einen gesicherten Kanal (z. B. Kurier, verschlüsselte E-Mail) ausgetauscht. Das Intervall für das regelmäßige Wechseln des Schlüssels ist hier weitaus größer als bei den automatischen Verfahren, wie das schon erwähnte IKE (ISAKMP/Oakley), oder das von der Firma Sun Microsystems stammende SKIP. Beide letztgenannten Verfahren verwalten die zertifizierten Schlüssel automatisch.

Bei der Wahl der eingesetzten RAS-Hard- und Software sollte darauf geachtet werden, dass möglichst mehrere verschiedene und etablierte Verschlüsselungsverfahren unterstützt werden. Dadurch erhöht sich die Wahrscheinlichkeit, dass zwischen Client und Server geeignete Verfahren ausgehandelt werden können.

Beispiele:

- Zur Verwendung der MPPE-Datenverschlüsselung unter Windows NT ist beim RAS-Client die Option "Nur Microsoft-verschlüsselte Echtheitsbestätigungen annehmen" bei den Eigenschaften einer DFÜ-Netzwerk-

Verbindung unter der Registrierkarte "Sicherheit" einzustellen und die Option "Datenverschlüsselung erforderlich" zu aktivieren. Von der Nutzung der Option "Aktuellen Benutzernamen und Kennwort verwenden" wird abgeraten.

- Unter Windows NT ist zum Aufbau einer PPTP-Verbindung über eine Internetverbindung auf dem RAS-Client das Protokoll VPN-Adapter (RASPPTPM) zu installieren. Dies geschieht über den Dialog *Systemsteuerung, Netzwerk, Protokolle*. Für die VPN-Verbindung muss ein eigener Eintrag im DFÜ-Netzwerk angelegt werden. Dabei wird, anstelle einer Telefonnummer, die IP-Adresse des entfernten RAS-Servers eingetragen. Im Feld "wählen mit" ist der VPN-Adapter auszuwählen. Nach dem erfolgreichen Verbindungsaufbau mit einem ISP wird danach die VPN-Verbindung über diese bestehende Internetverbindung aufgebaut. Der Aufbau kann auch automatisiert durch ein Skript erfolgen, welches dann für die ISP-Verbindung eingerichtet wird.
- Unter Windows 2000 kann die Nutzung der IPsec-basierten Datenverschlüsselung in den Eigenschaften des TCP/IP-Protokolls (unter *Netzwerkeigenschaften, Adapter-Eigenschaften, Protokolle*) aktiviert werden. Hierzu sind auf der Karte "Optionen" die Eigenschaften des Eintrags "IP-Sicherheit" zu verändern. Die Option "IP-Sicherheitsrichtlinien verwenden" muss aktiviert und die gewünschte Sicherheitsrichtlinie auswählt werden.

Ergänzende Kontrollfragen:

- Auf welcher Protokollebene soll das Tunneln ermöglicht werden?
- Über welche Protokolle muss das Tunnel-Protokoll abgewickelt werden?
- Welche Protokolle müssen durch den Tunnel transportiert werden?
- Ist eine Authentisierung der Tunnelendpunkte notwendig?

M 5.77 Bildung von Teilnetzen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

IT-Systeme in Behörden und Unternehmen sind typischerweise in lokale Netze (LANs) integriert, die ihrerseits wieder mit anderen Netzen verbunden sind. Allein aus technischen Gründen ist es bei mittleren und größeren Netzen meist erforderlich, ein LAN in mehrere Teilnetze aufzuteilen, beispielsweise weil die Anzahl der IT-Systeme pro Teilnetz oder die Gesamtlänge der Verkabelung beschränkt ist.

Die Bildung von Teilnetzen ist jedoch auch aus Gründen der IT-Sicherheit empfehlenswert. Einerseits können sensitive Daten auf bestimmte Bereiche innerhalb des LANs begrenzt werden (Vertraulichkeit), andererseits kann verhindert werden, dass Störungen in oder Angriffe auf ein Teilnetz die Funktionsfähigkeit anderer Teilnetze beeinträchtigen (Integrität und Verfügbarkeit).

Schutzbedarf berücksichtigen

Zunächst ist festzulegen, welche IT-Systeme jeweils in einem gemeinsamen Teilnetz betrieben werden sollen. Es wird empfohlen, dabei auf die Ergebnisse der Schutzbedarfsfeststellung zurückzugreifen und wie folgt vorzugehen:

Sensitive Daten auf Teilnetze begrenzen

- Alle IT-Systeme und Kommunikationsverbindungen in einem Teilnetz sollten in Bezug auf den Grundwert Vertraulichkeit den gleichen Schutzbedarf haben. Hierdurch wird erreicht, dass sensitive Daten möglichst auf speziell geschützte Teilnetze begrenzt werden. Entsprechend erforderliche Schutzmaßnahmen können auf diese Teilnetze konzentriert werden.

hochverfügbare Systeme isolieren

- IT-Systeme und Kommunikationsverbindungen mit einem hohen oder sehr hohen Schutzbedarf in Bezug auf Verfügbarkeit oder Integrität sollten möglichst jeweils in einem eigenen Teilnetz betrieben werden. Hierdurch wird erreicht, dass der ordnungsgemäße Betrieb dieser Komponenten bei Störungen in anderen Teilnetzen nicht beeinträchtigt wird. Weiterhin können dadurch Störungen schneller eingegrenzt und behoben werden.

Der zweite Schritt besteht in der Auswahl geeigneter Komponenten für die Kopplung der gebildeten Teilnetze. Empfehlungen hierzu finden sich in der Maßnahme M 5.13 *Geeigneter Einsatz von Elementen zur Netzkopplung*.

Einsatz von Firewalls prüfen

Insbesondere für die Anbindung von Teilnetzen, die Komponenten mit sehr hohem Schutzbedarf enthalten, sollte der Einsatz von Firewalls in Erwägung gezogen werden. Hierdurch wird eine gezielte und sichere Steuerung des Datenflusses in das betroffene Teilnetz hinein bzw. aus dem Teilnetz heraus ermöglicht.

Die folgende Grafik zeigt ein Beispiel, wie die Gesamtstruktur eines LANs aussehen kann, nachdem ein Teilnetz mit hohem Schutzbedarf durch eine zusätzliche Firewall vom restlichen Teilnetz abgetrennt wurde. Zur Vereinfachung sind die beiden Firewalls als ein Symbol dargestellt, sie setzen sich jedoch in der Regel aus mehreren Komponenten (Paketfilter, Application Gateway) zusammen.

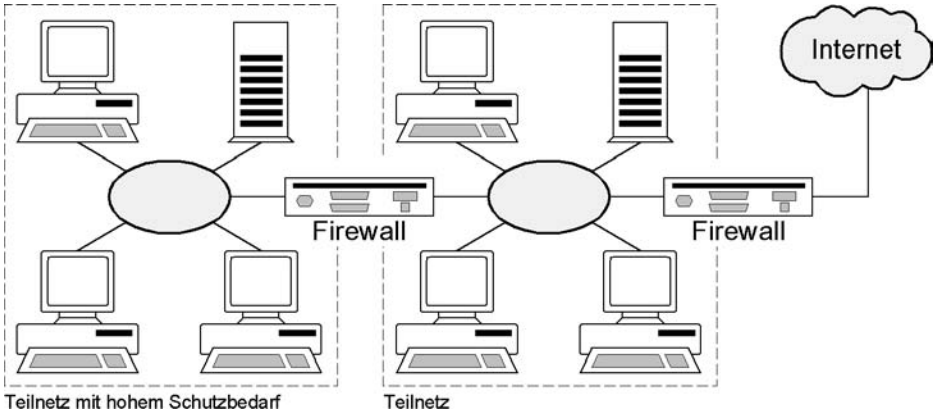


Abbildung: Beispiel einer Gesamtstruktur eines LANs

Empfehlungen für die technische Realisierung der Segmentierung im LAN sind in den Maßnahmen

- M 5.61 *Geeignete physikalische Segmentierung* und
- M 5.62 *Geeignete logische Segmentierung*

enthalten.

Ergänzende Kontrollfragen:

- Gibt es IT-Systeme oder Kommunikationsverbindungen mit unterschiedlichem Schutzbedarf?
- Ist das lokale Netz gemäß den Ergebnissen der Schutzbedarfsfeststellung in mehrere Teilnetze aufgeteilt worden?
- Werden für die Kopplung der Teilnetze geeignete Koppelelemente verwendet?

M 5.78 Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Bei der Mobil-Kommunikation müssen die mobilen Kommunikationspartner aus technischen Gründen geortet werden können, um erreichbar zu sein. Sofern sie selbst eine Verbindung aufbauen, geben sie ebenfalls - im Zuge des Verbindungsaufbaus - Informationen über ihren Standort ab. Diese Standortinformationen könnten durch den Netz- oder Dienstbetreiber - aber eventuell auch von Dritten - zur Bildung personen- oder gerätebezogener "Bewegungsprofile" verwendet werden.

Wird die Erstellung von Bewegungsprofilen bei der Nutzung von Mobiltelefonen als Gefährdung angesehen, dann sollten, falls umsetzbar, die Mobiltelefone und auch die SIM-Karten häufiger unter den Mitarbeitern getauscht werden. So wird eine Zuordnung der Geräte und Karten zu einem bestimmten Nutzer zumindest erschwert.

Soll der Aufenthaltsort zu bestimmten Zeiten unentdeckt bleiben, hilft nur ein Ausschalten des Mobiltelefons. Um ganz sicher zu sein, sollte der Akku entfernt werden.

M 5.79 Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Im GSM-Netz können den beteiligten Kommunikationspartnern die jeweiligen Rufnummern signalisiert werden. Ob dies tatsächlich der Fall ist, hängt von der technischen Ausstattung und der Konfiguration seitens der Mobiltelefone bzw. der Netzbetreiber ab.

Am Mobiltelefon kann mit der Funktion Rufnummernunterdrückung (für den nächsten bzw. alle weiteren Anrufe) verhindert werden, dass die eigene Rufnummer an den Angerufenen weitergeleitet wird. Diese Option ist in den Menüs der Mobiltelefone oft unter Bezeichnungen wie "Inkognito" oder "Anonym" zu finden.

Die Rufnummernweitergabe kann auch über den Netzbetreiber kontinuierlich verhindert werden.

Einen gewissen Schutz gegen die Zuordnung von Rufnummern zu bestimmten Personen gewährt der Austausch von Mobiltelefonen und SIM-Karten. Damit ist keine dauerhafte Zuordnung zwischen Benutzer und Rufnummer bzw. Gerät und Nutzer möglich. Die Zuordnung z. B. zu einer Behörde oder einem Unternehmen bleibt aber bestehen.

Veröffentlichung der Telefonnummer

Außer über die Signalisierung der Rufnummer kann die Mobiltelefonnummer einer bestimmten Person auch über öffentliche Telefonbücher ermittelt werden, wenn sie dort eingetragen ist. Beim Abschluss eines Mobilfunk-Vertrages sollte daher genau überlegt werden, ob bzw. in welcher Form eine Eintragung in öffentliche Telefonbücher sinnvoll ist. Ähnliches gilt für die Veröffentlichung der Rufnummer in internen Telefonbüchern und für deren Weitergabe bei diversen Datenerfassungen (Formulare, Gewinnspiele, etc.).

M 5.80 Schutz vor Abhören der Raumgespräche über Mobiltelefone

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Das Abhören von Raumgesprächen mittels Mobiltelefonen kann nur dann sicher ausgeschlossen werden, wenn die Mitnahme von Mobiltelefonen in den zu schützenden Raum verhindert wird. Wenn die IT-Sicherheitspolitik einer Behörde oder eines Unternehmens es nicht zulässt, dass Mobiltelefone mitgebracht werden, muss an allen Eingängen deutlich darauf hingewiesen werden. Ohne entsprechende Kontrollen ist ein einfacher Hinweis aber meist wirkungslos.

Das Ausschalten des Mobiltelefons reicht als Schutz nicht aus, da im Manipulationsfall ein unbemerktes Einschalten über die Funkstrecke nicht mit hinreichender Sicherheit ausgeschlossen werden kann. Eine solche ungewollte Inbetriebnahme ließe sich allein durch das Entfernen des Akkus unterbinden.

Mobiltelefon-Detektoren

Mobiltelefon-Detektoren sind Geräte, die erkennen, wenn in einem abgegrenzten Bereich ein oder mehrere Mobiltelefone in den Sendebetrieb (Gesprächsverbindungsaufbau) gehen.

passiven Detektoren

Auf dem Markt sind zur Zeit passive Warngeräte verfügbar, die Mobiltelefone melden, die sich im Sendebetrieb befinden. Der Wirkungsbereich der Geräte kann so eingestellt werden, dass er auf den zu überwachenden Bereich beschränkt ist. Es wird empfohlen, bei einem entsprechenden Schutzbedarf solche Warngeräte zu installieren und diese bei Gesprächen mit sensitivem oder vertraulichem Inhalt zu aktivieren.

Die passiven Detektoren können jedoch keine Mobiltelefone erkennen, die im Ruhe-Betrieb (Standby) sind. Damit diese Mobiltelefone ebenfalls erkannt (aufgespürt) werden, ist ein aktiver Sendeteil für den Detektor notwendig. Mit Hilfe dieses Sendeteils wird das Mobiltelefon aufgefordert, in den Sendebetrieb zu gehen. Ist das Mobiltelefon im Sendebetrieb, kann es dann mit einem Detektor erkannt werden.

aktive Detektoren

Sinnvoll sind diese aktiven Detektoren für Besprechungen mit sensitiven Inhalten. Mit Hilfe dieser Geräte lassen sich so alle eingeschalteten Mobiltelefone detektieren. Später eingeschaltete Mobiltelefone müssen sich bei der Basisstation anmelden und können bei diesem Einbuchungsvorgang ebenfalls detektiert werden. Weiterhin wird auf die Einsatzmöglichkeit von Störsendern hingewiesen, die in einem räumlich abgegrenzten Bereich den Funkbetrieb derart stören, dass dort kein Mobilfunkempfang möglich ist.

Derzeit können nur passive Mobiltelefon-Detektoren empfohlen werden. Aktive Detektoren sind zwar ebenfalls sinnvoll, ihr Einsatz kann aber in Deutschland nicht empfohlen werden, da sie keine Betriebsgenehmigung für die Bundesrepublik Deutschland besitzen. Gleiches gilt für Sender, die den Mobilfunkbetrieb stören, sie sind ebenfalls in der Bundesrepublik Deutschland nicht zugelassen.

M 5.81 Sichere Datenübertragung über Mobiltelefone

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Benutzer

Mobiltelefone werden normalerweise für die Sprachübertragung eingesetzt, es können aber auch Daten und Faxe damit übertragen werden. Für einige dieser Dienste wird zusätzliches Zubehör benötigt.

Kurzmitteilungen

Mit dem Kurznachrichtendienst (Short Message Service - SMS) lassen sich Texte mit maximal 160 Zeichen von einem Mobiltelefon zum anderen oder auch an E-Mail-Adressen senden. Die Übertragung von Kurzmitteilungen erfolgt immer über die Kurzmitteilungs-Zentrale, die die Nachrichten an den jeweiligen Empfänger weiterleitet.

Speicherplatz ist begrenzt

Kurzmitteilungen werden im Mobiltelefon gespeichert, solange Speicherplatz verfügbar ist. Wenn kein ausreichender Speicherplatz mehr frei ist, können keine weiteren Kurzmitteilungen empfangen werden. Der Netzbetreiber versucht nur über einen begrenzten Zeitraum, weitere Nachrichten abzusetzen. Wenn nicht rechtzeitig Speicherplatz freigemacht wird, werden die Kurzmitteilungen beim Netzbetreiber gelöscht.

Teilweise kann auch über das Mobiltelefon der Zeitraum, über den Kurzmitteilungen beim Netzbetreiber zwischengespeichert werden, verändert werden. Die Voreinstellung liegt im Allgemeinen zwischen 24 und 48 Stunden. Wenn der Vertrag mit dem Netzbetreiber es nicht vorsieht, kann hierüber allerdings der Speicherungszeitraum nicht erhöht werden. Er sollte auch nicht verringert werden.

Um Kurzmitteilungen verschicken zu können, muss die Rufnummer der Kurzmitteilungs-Zentrale (SMS-Gateway) über das entsprechende Menü am Mobiltelefon voreingestellt werden. Meist ist dies schon auf der SIM-Karte vom Netzbetreiber vorkonfiguriert worden.

SMS-Spam

Im Internet gibt es diverse WWW-Angebote, über die mit minimalen Kosten Kurzmitteilungen versandt werden können. Es ist ohne großen Aufwand möglich, auf diese Weise eine große Anzahl von SMS-Nachrichten an ein Mobiltelefon zu senden. Die Auswirkungen von SMS-Spam sind wie bei E-Mail (siehe auch G 5.75 *Überlastung durch eingehende E-Mails*). Die Mailbox bzw. der Speicherplatz reicht nicht aus und ernsthafte Anfragen kommen nicht durch. Darüber hinaus entstehen dem Benutzer (evtl. hohe) Kosten. Hiergegen hilft nur, im Vorfeld die eigene Rufnummer nicht zu breit zu streuen, also z. B. auf den Eintrag in Telefonbücher zu verzichten, bzw. im Schadensfall eine Zeit lang auf SMS zu verzichten.

Identifikation des Absenders bei SMS unzuverlässig

Eine Identifikation des Absenders ist bei SMS nicht zuverlässig möglich. Sie erfolgt maximal über die Rufnummer des Absenders und diese wird je nach Netzbetreiber bzw. Konfiguration des Mobiltelefons nicht immer mitübertragen. Beim Versand von Kurzmitteilungen über das Internet erfolgt im Allgemeinen überhaupt keine eindeutige Identifizierung. Dies sollte allen Benutzern klar sein, um die Echtheit einer Nachricht richtig einschätzen zu können. Eine Nachricht der Art "Aufgrund einer Umstellung benötigen wir

Ihre ec-PIN. Bitte senden Sie diese an die angegebene Rufnummer. Ihre Bank" sollte nicht ernst genommen werden. Je nach Inhalt einer empfangenen Kurzmitteilung ist es sinnvoll nachzufragen, ob diese wirklich vom angegebenen Absender stammt.

Es passiert immer wieder, dass SMS-Nachrichten beim falschen Empfänger landen, weil eine falsche Rufnummer angegeben oder ein falscher Eintrag aus dem Telefonbuch als Empfänger ausgewählt wurde. Auch wenn die Displays der Mobiltelefone klein sind, sollten die Empfängerangaben vor dem Absenden überprüft werden.

Faxe

Über Mobiltelefone können auch Faxe über SMS ins Festnetz versendet werden. Es können auch Faxe empfangen werden, wenn diese den Restriktionen der SMS-Übertragung genügen, insbesondere also lediglich einen kurzen Text enthalten. Darüber hinaus können Faxe auch über ein mit dem Mobiltelefon gekoppeltes IT-System (z. B. Notebook) gesendet und empfangen werden.

Bei der Fax-Nutzung ist ähnlich wie bei herkömmlichen Faxgeräten (siehe Baustein B 3.402 *Faxgerät*) zu beachten, dass

- der Speicherplatz des Mobiltelefons durch empfangene Faxe überlastet werden kann,
- es je nach Bedeutung von Faxen erforderlich sein kann, davon Kopien anzufertigen, was beim Mobiltelefon unter Umständen schwierig ist,
- es sinnvoll sein kann, die Rufnummern von bestimmten Faxempfängern bzw. Absendern zu sperren,
- nach dem Faxversand nachzufragen, ob dieses lesbar angekommen ist,
- nach dem Faxempfang nachzufragen, ob dieses wirklich vom angegebenen Absender stammt,
- ab und zu die programmierten Zieladressen zu kontrollieren.

E-Mail

Über Mobiltelefone können neben Kurzmitteilungen auch E-Mails empfangen und verschickt werden. E-Mails sind wie Kurzmitteilungen häufig auf 160 Zeichen begrenzt. Wenn dieser Service vom Netzbetreiber eingerichtet worden ist, erhält das Mobiltelefon eine eigene E-Mail-Adresse.

Bei einigen Netzbetreibern können E-Mail-Dienste mit anderen Diensten kombiniert werden. So können eingehende E-Mails von einem Sprachcomputer vorgelesen werden, an ein Faxgerät oder eine andere E-Mail-Adresse weitergeleitet werden. Ausgehende E-Mails können ins Mobiltelefon gesprochen und als Audiodatei (WAV-Datei) versandt werden.

Wie Kurzmitteilungen und Faxe können auch E-Mails schnell den vorhandenen Speicherplatz ausschöpfen. Je nach Vertrag mit dem Netzbetreiber kann bei der E-Mail-Nutzung außerdem nur eine begrenzte Anzahl von E-Mails pro Monat gesendet oder empfangen werden.

Potentielle Sicherheitsprobleme und Maßnahmen bei der Nutzung von E-Mail sind in Baustein B 5.3 *E-Mail* beschrieben. Dabei ist zu beachten, dass die E-Mail-Funktionalität bei Mobiltelefonen stark eingeschränkt ist gegenüber anderen E-Mail-Anwendungen. Ebenso wie SMS ist E-Mail hier eher für die Übermittlung kurzer und kurzlebiger Nachrichten gedacht. Sicherheitsmaßnahmen wie Verschlüsselung oder Signatur sind hierbei nicht möglich (außer über zusätzliche Module oder spezielle Geräte).

Die Übergänge zwischen den verschiedenen Nachrichtenarten wie SMS, Fax und E-Mail sind relativ fließend. Die Unterschiede liegen für die Benutzer im Allgemeinen nicht in der Art der Dateneingabe, sondern im Übertragungsformat. Hier können vom Netzbetreiber auch weitere Formate wie X.400 oder Paging angeboten werden.

Datenübertragung

Wenn das Mobiltelefon mit einem weiteren IT-System (z. B. einem Notebook oder einem Organizer) gekoppelt wird, können auch größere Datenmengen übertragen werden. Dabei kann die Kopplung auf verschiedene Arten erfolgen, je nachdem, welche Techniken die beiden Geräte unterstützen.

Einsteckkarte: Eine Einsteckkarte (PC-Card, PCMCIA) ist die konventionelle Lösung zur Verbindung von Mobiltelefon und Notebook. Die meisten Einsteckkarten können allerdings nur an Mobiltelefone eines bestimmten Herstellers angeschlossen werden.

Softmodem: Bei dieser Lösung wird statt einer Einsteckkarte eine spezielle Software auf dem Notebook installiert. Das Mobiltelefon wird dann einfach über die serielle Schnittstelle mit dem Notebook verbunden. Diese Lösung ist meist preiswerter als eine Einsteckkarte.

Infrarot: Über eine Infrarot-Schnittstelle können Daten auch ohne Kabel vom Mobiltelefon zu einem IT-System (z. B. Laptop oder Organizer) übertragen werden. Dazu muss sowohl das Mobiltelefon als auch das IT-System IrDA unterstützen. IrDA (Infrared Data Association) ist ein weltweiter Standard für die Datenübertragung über Infrarot.

Bluetooth: Bluetooth ist ein neuerer Standard, nach dem Geräte per Funk über kurze Entfernungen miteinander Daten austauschen können. Die Bluetooth-Technik nutzt das frei verfügbare Funknetz ISM (Industrial Scientific Medical), das mit 2,45 GHz arbeitet.

Datenübertragung verschlüsseln

Bei der Datenübertragung z. B. von einem Laptop über GSM sollten die übertragenen Daten vorher auf dem Endgerät verschlüsselt werden. Hierzu gibt es eine Vielzahl von Programmen, die dies einfach ermöglichen. Die Verschlüsselung vor der Übertragung sichert die Informationen auf der gesamten Strecke zwischen Absender und Empfänger. Dies geht über die Absicherung der Luftschnittstelle zwischen Mobiltelefon und Basisstation, wie sie bei GSM Standard ist, hinaus. Weiterhin können die Nachrichten dann auch digital signiert werden. Wie adäquate kryptographische Verfahren und Systeme ausgewählt und eingesetzt werden können, ist in Baustein B 1.7 *Kryptokonzept* beschrieben.

Daten nachladen

Im Internet finden sich diverse Anbieter, über die zusätzliche Klingeltöne, Displaysymbole oder Ähnliches für die verschiedenen Mobiltelefone

heruntergeladen werden können. Hier sollte aber beachtet werden, dass das Aufspielen solcher Daten unter Umständen die Geräte auch funktionsuntüchtig machen kann.

Regelung der Datenübertragung

Die Datenübertragung sollte in allen Organisationen klar geregelt sein. Alle Datenübertragungseinrichtungen sollten genehmigt sein und deren Nutzung klaren Regelungen unterliegen (siehe auch M 2.204 *Verhinderung ungesicherter Netzzugänge*).

Damit durch die Datenübertragung über GSM-Schnittstellen keine Sicherheitslücken entstehen, sollte diese restriktiv gehandhabt werden. So sollten bei IT-Systemen, auf denen sensitive Daten verarbeitet werden, keine Mobilfunkkarten zugelassen werden. Dies gilt ebenso bei allen IT-Systemen, die an einem Rechner-Netz angebunden sind, damit hier nicht der Schutz durch eine Firewall unterhöhlt werden kann.

M 5.82 Sicherer Einsatz von SAMBA

Verantwortlich für Initiierung: Leiter IT, Administrator

Verantwortlich für Umsetzung: Administrator

SAMBA ist ein freies Programmpaket für Unix-Betriebssysteme, das unter anderem Datei-, Druck- und Authentisierungsdienste über das SMB (Server Message Block) bzw. CIFS (Common Internet File System) Protokoll zur Verfügung stellt. Wichtigste Beispiele für SMB/CIFS-Clients sind sicherlich die Betriebssysteme der Microsoft Windows-Familie. Hierdurch ist es beispielsweise möglich, dass Windows 9x- oder Windows NT-Rechner direkt auf freigegebene Dateien auf einem Unix-Server zugreifen können. Ein Umweg über die Protokolle FTP oder NFS und die Installation zusätzlicher Software auf Client-Seite entfallen. In der aktuellen Version bildet SAMBA eine ganze Reihe der Funktionen eines Windows NT Servers nach, sodass ein Unix-System mit SAMBA in vielen Fällen einen solchen Server ersetzen kann.

Falls in der Behörde bzw. im Unternehmen SAMBA zum Einsatz kommt, sollten folgende Empfehlungen berücksichtigt werden:

fehlerbereinigte Version einsetzen

In älteren Versionen von SAMBA sind Programmfehler entdeckt worden, die unter Umständen zu Sicherheitslücken führen können. Es sollte eine aktuellere Version verwendet werden, in der möglichst alle bekannten sicherheitsrelevanten Fehler beseitigt wurden.

sorgfältige Konfiguration

Die Datei *smb.conf* ermöglicht eine äußerst flexible und detaillierte Konfiguration des SAMBA-Servers. Dies bedingt jedoch gleichzeitig eine gewisse Komplexität. Vor dem Einsatz von SAMBA sollte daher die Dokumentation gründlich gelesen werden. Die Konfiguration ist sorgfältig zu planen, zu dokumentieren und durch entsprechende Parameter in der Datei *smb.conf* umzusetzen. Eine umfangreiche Beschreibung der einzelnen Parameter kann beispielsweise durch den Befehl *man smb.conf* angezeigt werden. Bei Änderungen an der Konfiguration ist anhand der Dokumentation und durch entsprechende Tests sicherzustellen, dass die Konfigurationsänderung nicht zu unerwünschten Seiteneffekten führt.

Die folgenden Parameter sind in Bezug auf mögliche Sicherheitsrisiken besonders problematisch. Sie sollten daher nur nach gründlicher Prüfung aller möglichen Auswirkungen auf die IT-Sicherheit des Servers verwendet werden:

[...] command	postexec
add user script	preexec / exec
delete user script	root postexec
fake oplocks	root preexec
ldap [...]	smbrun
panic action	unix password sync
passwd program	

Mit Hilfe des Programms *testparm* kann geprüft werden, ob die Einstellungen in der Datei *smb.conf* zulässig sind. Selbstverständlich kann hierdurch **keine** Aussage darüber gemacht werden, ob die Einstellungen den gewünschten

Effekt oder sicherheitsrelevante Auswirkungen haben. Die Erstellung und Wartung der Datei *smb.conf* kann auch durch graphische Oberflächen unterstützt werden, beispielsweise durch das Samba Web Administration Tool (SWAT), das im Lieferumfang des SAMBA-Pakets enthalten ist.

"security=share" vermeiden

SAMBA bietet derzeit vier verschiedene Verfahren zur Authentisierung von Clients. Bei der Einstellung *security = user* prüft der SAMBA-Server, ob der Client eine gültige Kombination aus Benutzer-Kennung und Passwort übermittelt. Bei *security = server* oder *security = domain* überlässt er diese Prüfung einem oder mehreren anderen SMB/CIFS-Servern, die über den Parameter *password server* spezifiziert werden und denen er vertraut. Dagegen wird bei der Verwendung von *security = share* lediglich eine einfache Passwortprüfung durchgeführt, der Client muss keine Benutzer-Kennung übermitteln. Dieses Verfahren ist erheblich schwächer als die Authentisierung über Benutzer-Kennung und Passwort und sollte nur angewandt werden, wenn die Daten auf dem SAMBA-Server nicht geschützt werden müssen. Als Beispiel sei ein Server mit schreibgeschütztem Datenträger und öffentlich zugänglichen Daten genannt. Zweckmäßigerweise wird hier vollständig auf eine Authentisierung verzichtet, was am einfachsten über die Einstellung *security = share* realisierbar ist.

verschlüsselte Passwörter verwenden

Bei der Authentisierung von Clients können Klartext-Passwörter oder verschlüsselte Passwörter verwendet werden. Da Klartext-Passwörter mit Hilfe von frei zugänglichen Tools beim Transport über das Netz leicht abgehört werden können, sollten grundsätzlich nur verschlüsselte Passwörter zum Einsatz kommen. Auf Seite der Clients werden verschlüsselte Passwörter z. B. von Windows 95 mit installiertem SMB-Update, Windows 98, Windows NT 4.0 und Windows 2000 unterstützt. In der Datei *smb.conf* des SAMBA-Servers werden verschlüsselte Passwörter durch den Parameter *encrypt passwords = yes* aktiviert. Anders als Klartext-Passwörter kann ein SAMBA-Server verschlüsselte Passwörter nicht mit Hilfe der Authentisierungsmechanismen des darunter liegenden Unix-Betriebssystems (die z. B. auf */etc/passwd* oder */etc/shadow* zurückgreifen) überprüfen. Daher ist eine zusätzliche Passwortdatei erforderlich, die über den Parameter *smb passwd file* spezifiziert wird. Diese Datei enthält die verschlüsselten Passwörter und ist vor unberechtigtem Zugriff sorgfältig zu schützen.

Steuerung der Zugriffsrechte

Die Rechte eines Benutzers beim Zugriff auf Verzeichnisse und Dateien über SAMBA ergeben sich einerseits aus den Einstellungen in der Datei *smb.conf* und andererseits aus den Zugriffsrechten des Dateisystems, auf dem die freigegebenen Daten vorgehalten werden. Auch hier ist durch sorgfältige Konfiguration sicherzustellen, dass Zugriffsrechte in konsistenter Weise vergeben werden. Anders als bei Windows NT Servern mit NTFS-Laufwerken ist es beim Einsatz von SAMBA nicht immer sinnvoll, die Zugriffsrechte ausschließlich über das Dateisystem zu vergeben. Der Grund ist, dass gängige Unix-Dateisysteme ein anderes Sicherheitsmodell (Permissions und Ownership) implementieren als NTFS. Abhängig vom konkreten Anwendungsfall ist daher zu prüfen, ob bestimmte übergeordnete Zugriffsbeschränkungen besser über die Datei *smb.conf* konfiguriert werden können. Hierzu wird auf die Parameter *(in)valid users* und *read/write list* verwiesen.

Die folgenden Parameter führen möglicherweise dazu, dass Zugriffsbeschränkungen umgangen werden können:

admin users
force group / group
force user
guest account
hosts equiv
username / users / user
username map

Bei Verwendung dieser Parameter sollten die möglichen Auswirkungen auf die Sicherheit daher genau geprüft werden.

symbolische Links prüfen

Symbolische Links in freigegebenen Verzeichnissen können dazu führen, dass Clients unberechtigten Zugriff auf Dateien *außerhalb* des freigegebenen Bereiches erhalten. Es wird empfohlen, dies durch den Parameter *wide links = no* zu verhindern. Zu beachten ist jedoch, dass dieser Parameter zu einer Verminderung des Durchsatzes führen kann, da die zusätzlich erforderlichen Prüfungen Rechenzeit beanspruchen. Falls es hierdurch zu einer Beeinträchtigung des Betriebes kommt, kann versuchsweise der Parameter *getwd cache = yes* gesetzt werden. Als Alternative zur Prüfung symbolischer Links kann auch überlegt werden, den Parameter *root directory = <pfad>* zu verwenden. Zugriffe auf Verzeichnisse und Dateien außerhalb von *<pfad>* werden damit ausgeschlossen. Dabei müssen jedoch alle zur Ausführung von SAMBA erforderlichen Dateien in Unterverzeichnisse von *<pfad>* kopiert werden, unter anderem auch die Passwortdateien.

Zugriffsrechte auf [netlogon]

Auf dem Server können über die Freigabe *[netlogon]* unter anderem Anmeldeskripten für Clients bereitgestellt werden. Benutzer sollten keinesfalls in der Lage sein, Dateien in dieser Freigabe zu modifizieren. Es wird empfohlen, *writeable = no* und *guest ok = no* bzw. äquivalente Parameter für diese Freigabe zu setzen.

sichere Voreinstellungen

Die folgenden Parameter sind voreingestellt und sollten nicht verändert werden, da anderenfalls der ordnungsgemäße und sichere Betrieb beeinträchtigt werden kann:

kernel oplocks = <automatisch>
locking = yes
magic [...] = <deaktiviert>
map to guest = Never
passwd chat debug = no
password level = 0
share modes = yes
use rhosts = no

Optionaler Einsatz von SSL zum Schutz der Kommunikation

Wenn Dienste eines SAMBA-Servers über größere Netze genutzt werden, die nicht vollständig der eigenen Kontrolle unterliegen, sollte überlegt werden, die Kommunikationsverbindungen durch den Einsatz kryptographischer Verfahren zu schützen. Dies bietet sich insbesondere an, wenn aus zwingenden Gründen Klartext-Passwörter verwendet werden müssen. Die Absicherung kann durch entsprechende Hardware- oder Software-Komponenten erfolgen. Besondere Unterstützung bietet SAMBA für den Einsatz von SSL

an. Hierzu muss auf dem SAMBA-Server ein SSL-Programmpaket, in der Regel das freie SSLeay, installiert werden. Client-seitig ist eine SSL-Proxy-Software erforderlich, die für Windows NT- und Unix-Clients kostenlos verfügbar ist. Windows 9x-Clients können den SSL-Proxy eines Windows NT- oder Unix-Clients in ihrem Subnetz mitbenutzen. Erste Schritte der Konfiguration stellen - falls noch nicht vorhanden - die Einrichtung einer Certification Authority (CA) und die Generierung von Schlüsselpaaren und Zertifikaten für den Server und die Clients dar. Die entsprechenden Vorgehensweisen sind in der Dokumentation von SSLeay erläutert. Um SSL auf dem SAMBA-Server zu aktivieren, sind in der Datei *smb.conf* mindestens die Parameter *ssl = yes* und *ssl server cert = <pfad>* zu setzen. Falls der private Schlüssel des Servers nicht in der gleichen Datei wie das Server-Zertifikat abgelegt ist, wird außerdem der Parameter *ssl server key = <pfad>* benötigt. Es wird empfohlen, die Überprüfung von Server- und Client-Zertifikaten zu aktivieren. Dies erfordert die Parameter *ssl require clientcert = yes* und *ssl require servercert = yes*, sowie *ssl CA certDir = <pfad>* oder *ssl CA certFile = <pfad>*. Für jeden Client, auf dem ein SSL-Proxy zum Einsatz kommt, sind das Schlüsselpaar und das Zertifikat dieses Clients in ein geschütztes Verzeichnis zu kopieren. Die Pfade dieser Dateien und der Name des SAMBA-Servers werden dem SSL-Proxy beim Start als Parameter übergeben. Anschließend können die Clients die gewünschten SMB/CIFS-Dienste vom jeweiligen SSL-Proxy abrufen. Der Proxy leitet die Anfragen - geschützt durch das SSL-Protokoll - an den eigentlichen SAMBA-Server weiter. Deshalb werden die Dienste aus Sicht der Clients scheinbar vom SSL-Proxy anstatt vom SAMBA-Server bereitgestellt.

Konfiguration der Clients

Falls aus zwingenden Gründen Klartext-Passwörter verwendet werden müssen, kann dies auf Clients mit den Betriebssystemen Windows 9x, Windows NT 4.0 oder Windows 2000 durch bestimmte Registry-Einträge erzwungen werden. Erforderlich ist dies beispielsweise bei Windows NT 4.0 mit Service Pack 3 oder höher, da diese Betriebssystemversion ohne Anpassung der Registry die Übertragung von Klartext-Passworten auch dann verweigert, wenn der Server keine verschlüsselten Passwörter unterstützt. Der Client kann sich anderenfalls also nicht erfolgreich am Server anmelden. Zu beachten ist jedoch, dass bei Verwendung von Klartext-Passwörtern auf jeden Fall zusätzliche Schutzmaßnahmen für die Kommunikationsverbindungen (z. B. VPN oder SSL) erforderlich sind.

Sogar mit erfolgter Registry-Anpassung ist die Anmeldung eines Windows NT 4.0 Clients an einem Server mit Klartext-Passwörtern problematisch. Der Benutzer wird in diesem Fall nämlich bei jeder Verbindungsanfrage erneut nach dem Passwort gefragt, was bei Nutzung verschiedener Ressourcen auf dem Server sehr störend sein kann. Dies ist ein weiterer Grund, auf die Verwendung von Klartext-Passwörtern möglichst vollständig zu verzichten.

Weitere Empfehlungen zur sicheren Konfiguration der Clients finden sich in der Maßnahme M 5.38 *Sichere Einbindung von DOS-PCs in ein Unix-Netz* und in den Bausteinen B 3.205 *Client unter Windows NT* und B 3.206 *Client unter Windows 95*.

Ergänzende Kontrollfragen:

- Werden Änderungen an der SAMBA-Konfiguration dokumentiert und vor dem Einsatz im Wirkbetrieb getestet?
- Werden verschlüsselte Passwörter verwendet?
- Werden Schreibzugriffe auf die Freigabe *[netlogon]* unterbunden?

M 5.83 Sichere Anbindung eines externen Netzes mit Linux FreeS/WAN

Verantwortlich für Initiierung: Leiter IT, Administrator

Verantwortlich für Umsetzung: Administrator

Absicherung durch ein Virtuelles Privates Netz

In vielen Institutionen besteht die Anforderung, die lokalen Netze, die an den einzelnen Standorten installiert sind, miteinander zu verbinden. Dies erfolgt in den meisten Fällen über gemietete Leitungen oder öffentliche Netze, die nicht der Kontrolle der Institution unterliegen. Hier besteht z. B. die Gefahr, dass die übertragenen Daten abgehört oder manipuliert werden oder dass sich ein Angreifer als berechtigter Kommunikationspartner ausgibt (Maskerade). Diesen Gefährdungen kann durch den Einsatz eines so genannten *Virtuellen Privaten Netzes* (VPN) entgegengewirkt werden. Mit Hilfe kryptographischer Verfahren können dabei die Integrität und Vertraulichkeit der Daten geschützt und die Kommunikationspartner sicher authentisiert werden. *Linux FreeS/WAN* ist ein freies Programmpaket für das Betriebssystem Linux, mit dessen Hilfe ein zum IPSEC-Standard konformes VPN aufgebaut werden kann.

Planung

Anforderungen festlegen und Dokumentation lesen

In der Planungsphase sollte als Erstes ermittelt werden, welche Anforderungen das Produkt, das für den Schutz der Kommunikationsverbindung verwendet werden soll, erfüllen muss. Hierzu gehört beispielsweise, ob es mit bestimmten bereits vorhandenen Komponenten zusammenarbeiten muss oder ob außer TCP/IP noch andere Protokolle transportiert werden müssen. Anschließend sollte die Dokumentation von FreeS/WAN durchgearbeitet und für die Entscheidung herangezogen werden, ob dieses Programmpaket für die vorliegende Aufgabenstellung geeignet ist. Wenn dies der Fall ist, sollte festgelegt und dokumentiert werden, welche Funktionalitäten von FreeS/WAN wofür genutzt werden sollen und wie es in die vorhandene Netzstruktur eingefügt werden soll.

Installation

unnötige Dienste und Programmpakete vermeiden

FreeS/WAN läuft auf dem freien Betriebssystem Linux und greift in den IP-Protokollstapel des Kernels ein. Es wird empfohlen, FreeS/WAN auf nur für diesen Zweck konfigurierten PCs zu betreiben und - abgesehen von eventuell erforderlichen Routing-Funktionen - keine anderen Dienste auf diesen PCs zu aktivieren (siehe auch M 4.97 *Ein Dienst pro Server*). Insbesondere sollten sie keine Firewall-Funktionen wahrnehmen, sondern unabhängig vom Firewall-System sein. Für die Installation des Betriebssystems sollte auf eine Linux-Distribution zurückgegriffen werden, bei der FreeS/WAN bereits enthalten ist. Dies erleichtert die Installation erheblich, da anderenfalls in der Regel auch der Linux-Kernel neu kompiliert werden muss. Hierzu wird auf die Dokumentation von FreeS/WAN verwiesen. Weiterhin sollten von der Linux-Distribution nur die unbedingt erforderlichen Programmpakete installiert werden.

Konfiguration

zwei LANs über das Internet verbinden

FreeS/WAN implementiert eine ganze Reihe verschiedener Funktionalitäten, die in IPSEC definiert sind. Durch entsprechende Konfiguration ist es daher möglich, dieses Programmpaket in vielen verschiedenen Umgebungen für unterschiedlichste Anwendungsgebiete einzusetzen. Im Folgenden wird anhand eines Beispiels erläutert, wie FreeS/WAN dazu verwendet werden kann, die Kommunikation zwischen zwei lokalen Netzen über das Internet abzusichern. Hierzu wird folgende Anordnung von Komponenten in den Netzen betrachtet:

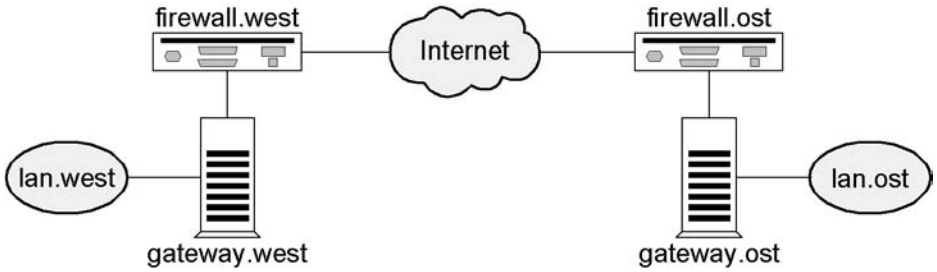


Abbildung: Komponenten in den Netzen

Die beiden Standorte *west* und *east* einer Institution verfügen beide über eine Anbindung an das Internet. Auf beiden Seiten kommt dabei ein **mehrstufiges Firewall-System** zum Einsatz, das zur Vereinfachung jedoch in der Abbildung jeweils nur durch ein einzelnes Symbol dargestellt ist. *gateway.west* und *gateway.east* sind IT-Systeme unter dem Betriebssystem Linux, die mit Hilfe von FreeS/WAN als Gateways für die lokalen Netze *lan.west* und *lan.east* dienen sollen. Die Gateways haben jeweils zwei Netzwerkkarten, über die sie mit den Firewall-Systemen und den lokalen Netzen verbunden sind. Ziel ist, dass alle IT-Systeme in *lan.west* und *lan.east* sicher miteinander kommunizieren können. Die Absicherung der Kommunikation soll für diese IT-Systeme transparent sein.

automatischer Schlüsselaustausch über RSA

Wichtig ist die Auswahl eines geeigneten Verfahrens für das Schlüsselmanagement. Es wird empfohlen, automatischen Schlüsselaustausch über Public-Key-Verfahren (RSA) zu verwenden. Dies bietet verglichen mit den übrigen von FreeS/WAN unterstützten Verfahren das höchste Sicherheitsniveau. Der erste Schritt der Konfiguration besteht daher in der Erzeugung von RSA-Schlüsselpaaren für die beiden Gateways. Dies kann beispielsweise über das Kommando *ipsec rsasigkey* erfolgen. Die Schlüssel sollten mindestens 768 Bit lang sein. Wie in der Dokumentation vermerkt, dürfen die so erzeugten Schlüssel nur für Signaturen, **nicht** für Verschlüsselung verwendet werden. Innerhalb des Programmpakets FreeS/WAN ist dies gewährleistet. Die Ausgabe des Kommandos *ipsec rsasigkey* enthält jeweils den öffentlichen und den privaten RSA-Schlüssel. Entscheidend für die Sicherheit des VPN ist, dass der private Schlüssel **auf keinen Fall** kompromittiert werden darf (siehe auch M 2.46 *Geeignetes Schlüsselmanagement*).

Der private Schlüssel wird in der Datei */etc/ipsec.secrets* auf dem Gateway abgelegt, Ownership und Permissions sind wie folgt zu setzen:

-rw------- root root /etc/ipsec.secrets

Einstellungen in /etc/ipsec.conf

Der öffentliche Schlüssel dagegen wird in die Datei */etc/ipsec.conf* eingetragen (siehe unten). In dieser Datei werden auch alle anderen Einstellungen für FreeS/WAN vorgenommen. Das Format ist so angelegt, dass auf beiden Gateways möglichst die gleiche Datei verwendet werden kann. Die Konfiguration erfolgt in mehreren Abschnitten, in denen jeweils Einstellungen in der Form *Parameter = Wert* vorgenommen werden. Die Parameter, die eine Unterscheidung zwischen den beiden Gateways erfordern, tragen jeweils das vorangestellte Schlüsselwort *left* bzw. *right*. Die jeweilige Instanz von FreeS/WAN erkennt anhand der IP-Adresse selbständig, welcher der beiden Parameter für sie gültig ist. In der Regel unterscheiden sich die auf den beiden Gateways gespeicherten Versionen der Datei */etc/ipsec.conf* daher höchstens beim Parameter *interfaces*, beispielsweise weil auf einer Seite Ethernet und auf der anderen Seite Token Ring verwendet wird. Für das betrachtete Beispiel werden nachfolgend Empfehlungen zur Konfiguration in der Datei */etc/ipsec.conf* vorgestellt.

Abschnitt config setup

In diesem Abschnitt werden allgemeine, nicht verbindungsspezifische Einstellungen vorgenommen.

interfaces = ipsec0=eth0

Zunächst ist mit dem Parameter *interfaces* festzulegen, über welche Netzschnittstellen gesicherte Verbindungen aufgebaut werden sollen. Über alle anderen Schnittstellen werden keine verschlüsselten Pakete gesendet. In dem oben dargestellten Beispiel wird die Verbindung zur Firewall jeweils durch die Schnittstelle *eth0* des Gateways hergestellt.

forwardcontrol = yes

Wird der Parameter *forwardcontrol* auf den Wert *yes* gesetzt, so schaltet FreeS/WAN die Weiterleitung von IP-Paketen selbständig ein oder aus, wenn IPSEC aktiviert bzw. deaktiviert wird. Dies wird empfohlen, da hierdurch verhindert wird, dass Pakete unverschlüsselt übertragen werden, wenn das VPN nicht verfügbar ist. Beim Hochfahren des Linux-Systems sollte sichergestellt sein, dass die Weiterleitung von IP-Paketen ausgeschaltet wird, bevor die Netzschnittstellen aktiviert werden. Wie diese Einstellung vorgenommen wird, hängt von der verwendeten Linux-Distribution ab.

dumpdir =

Der Parameter *dumpdir* sollte auf einen leeren Wert gesetzt werden, damit die Komponenten von FreeS/WAN im Falle eines Programmfehlers keine Speicherabbilder (core dumps) erzeugen. Anderenfalls besteht die Gefahr, dass Unbefugte diesen Speicherabbildern z. B. geheime Schlüssel entnehmen können.

plutoload = %search
plutostart = %search

Der Daemon *pluto* ist Bestandteil des Pakets FreeS/WAN und dient dem automatischen Schlüsselmanagement. Mit den Parameter *plutoload* und *plutostart* wird festgelegt, welche Verbindungen beim Start automatisch in die Datenbank von *pluto* geladen bzw. aktiviert werden. Es ist zweckmäßig, diese Parameter jeweils auf den speziellen Wert *%search* zu setzen. Dadurch werden diejenigen Verbindungen geladen bzw. aktiviert, die durch den Parameter *auto* entsprechend gekennzeichnet sind.

Abschnitt conn west-east

In diesem Abschnitt werden Einstellungen vorgenommen, die speziell für eine bestimmte Verbindung, beispielsweise *west-east*, gelten.

type = tunnel

Mit Hilfe des Parameters *type* wird der Betriebsmodus für diese Verbindung festgelegt. Da im vorliegenden Fall der Netzverkehr zwischen zwei lokalen Netzen über Gateways abgesichert werden soll, muss zwingend der Modus *tunnel* verwendet werden. Der Modus *transport* ist nur bei Host-zu-Host-Kommunikation, *passthrough* nur bei manuellem Schlüsselmanagement zulässig.

auto = start

Sind die Parameter *plutoload* bzw. *plutostart* auf den speziellen Wert *%search* gesetzt, dann legt der Parameter *auto* für die vorliegende Verbindung fest, ob sie beim Start automatisch in die Datenbank von *pluto* geladen bzw. aktiviert wird. Im Beispiel soll die Verbindung direkt aktiviert werden, daher wird der Parameter *auto* auf den Wert *start* gesetzt.

auth = esp

Der Parameter *auth* legt fest, mit welchem der beiden IPSEC-Funktionalitäten, *Encapsulating Security Payload* (ESP) oder *Authentication Header* (AH), die Authentisierung stattfindet. Im vorliegenden Fall kann sowohl die Verschlüsselung als auch die Authentisierung mit ESP erfolgen. Dies ist die Standardeinstellung.

authby = rsasig

Es wird empfohlen, die Authentisierung mit Hilfe von digitalen Signaturen über den RSA-Algorithmus durchzuführen (Einstellung *rsasig*). Dies bietet gegenüber dem Verfahren "shared secrets" (Einstellung *secret*) eine höhere Sicherheit und eine vereinfachte Administration.

pfs = yes

pfs steht für *Perfect Forward Secrecy* und bedeutet, dass Nachrichten, die in der Vergangenheit ausgetauscht wurden, selbst bei Bekanntwerden der privaten Schlüssel der beiden Gateways nicht kompromittiert werden. (Die Sicherheit zukünftiger Verbindungen kann dagegen nicht mehr gewährleistet werden.) Der Standardwert *yes* ist die empfohlene Einstellung für diesen Parameter.

keyingtries = 0

Der Parameter *keyingtries* legt die maximale Anzahl der Versuche fest, die entsprechende Verbindung aufzubauen oder zu aktualisieren. Es wird empfohlen, den speziellen Wert *0* einzustellen, d. h. die Anzahl der Versuche ist nicht begrenzt. Der voreingestellte Wert *3* für den Parameter *keyingtries* ist für die meisten Anwendungen unzureichend.

left = <IP-Adresse von gateway.west>
right = <IP-Adresse von gateway.east>

Mit Hilfe der Parameter *left* und *right* werden die IP-Adressen der beiden beteiligten Gateways eingestellt. Es wird empfohlen, die IP-Adressen numerisch einzutragen und nicht auf den speziellen Wert *%defaultroute* zurückzugreifen. Durch Vergleich mit den IP-Adressen, die den entsprechenden Netzschnittstellen des IT-Systems zugewiesen sind, erkennt FreeS/WAN, welche von beiden Rollen (*left* oder *right*) dieses IT-System übernimmt.

leftnexthop = <IP-Adresse von firewall.west>
rightnexthop = <IP-Adresse von firewall.east>

Als Wert für die Parameter *leftnexthop* und *rightnexthop* ist jeweils die IP-Adresse derjenigen Komponente einzutragen, die die Pakete über das unsichere Netz weiterleitet. Im vorliegenden Beispiel ist diese Komponente Bestandteil des Firewall-Systems. Je nach Segmentierung und Anordnung der aktiven Netzkomponenten im lokalen Netz ist hier jedoch in vielen Fällen der nächstliegende Router auf der Strecke zur Internet-Firewall einzutragen.

leftsubnet = <Subnetz/Maske von lan.west>
rightsubnet = <Subnetz/Maske von lan.east>

Durch diese beiden Parameter wird festgelegt, welche beiden Subnetze gesichert miteinander kommunizieren sollen. Im vorliegenden Beispiel sind dies die lokalen Netze *lan.west* bzw. *lan.east*. Die Werte sind in der Form *Subnetz/Maske* einzutragen, beispielsweise *10.10.0.0/16*.

leftid = @gateway.west
rightid = @gateway.east

Über die Parameter *leftid* und *rightid* werden Namen für die beiden Gateways vergeben, die für die Authentisierung erforderlich sind. Es wird empfohlen, die Namen in Form von DNS-Namen mit vorangestelltem "@"-Zeichen festzulegen. Hierdurch wird verhindert, dass FreeS/WAN die DNS-Namen vor der Verwendung durch eine Anfrage beim DNS-Server in IP-Adressen umwandelt.

leftrsasigkey = <öffentlicher RSA-Schlüssel von gateway.west>
rightrsasigkey = <öffentlicher RSA-Schlüssel von gateway.east>

Mit Hilfe dieser beiden Parameter werden die öffentlichen Schlüssel der Gateways festgelegt. Die entsprechenden geheimen Schlüssel sind dagegen in die Datei */etc/ipsec.secrets* auf dem jeweiligen Gateway einzutragen.

Routing

Für die Weiterleitung von IP-Paketen verwendet FreeS/WAN die Routing-Tabellen des darunter liegenden Linux. Mit Hilfe des Kommandos *route* müssen daher auf beiden Gateways Regeln erzeugt werden, so dass Pakete für

das lokale bzw. entfernte Netz über die entsprechende Netzwerkkarte weitergeleitet werden.

Fernadministration eines Gateways

gateway.west und *gateway.east* können in der vorgestellten Konfiguration nicht über das VPN kommunizieren. Der sichere Tunnel transportiert nur Daten zwischen *lan.west* und *lan.east*. Dies ist aus Sicherheitsgründen erwünscht, es sei denn, eines der beiden Gateways soll von der jeweils anderen Seite aus administriert werden. In diesem Fall ist in der Datei *ipsec.conf* eine weitere Verbindung einzurichten. Diese zusätzliche Verbindung unterscheidet sich von der Verbindung *west-east* dadurch, dass der Parameter *leftsubnet* fehlt (wenn *gateway.west* von *lan.east* aus fernadministriert werden soll) bzw. *rightsubnet* fehlt (wenn *gateway.east* von *lan.west* aus fernadministriert werden soll).

Firewall-Einstellungen

firewall.west und *firewall.east* sollten so konfiguriert werden, dass zwischen den beiden Gateways die verschlüsselten Nutzpakete und die erforderlichen Managementpakete ausgetauscht werden können. Im vorliegenden Beispiel sind dafür folgende Regeln erforderlich:

- IP-Pakete mit Protokollnummer 50 von *gateway.west* nach *gateway.east* und umgekehrt sind erlaubt.
- UDP-Pakete, Port 500 von *gateway.west* nach *gateway.east* und umgekehrt sind erlaubt.

Falls abweichend vom Beispiel für den Parameter *auth* der Wert *ah* eingestellt wurde, müssen IP-Pakete mit Protokollnummer 51 durchgelassen werden. Jede andere Kommunikation mit dem Gateway oder dem lokalen Netz muss vom jeweiligen Firewall-System unterbunden werden.

Da das Firewall-System und das Gateway getrennt voneinander realisiert sind, sollten die Parameter *leftfirewall* und *rightfirewall*, sowie *leftupdown* und *rightupdown* nicht verwendet werden.

keine Adressumsetzung für IPSEC-Pakete durchführen

Beim Einsatz von *Network Address Translation* (NAT) ist zu beachten, dass die Adressumsetzung entweder auf einer Komponente zwischen dem Gateway und dem lokalen Netz oder auf dem Gateway selbst erfolgen muss. Die Adressen können im Allgemeinen nicht innerhalb des Firewall-Systems umgesetzt werden. Grund hierfür ist, dass Teile der IP-Pakete beim Einsatz von NAT modifiziert werden, sodass die Integritätsprüfung von IPSEC in der Regel fehlschlägt. NAT darf daher erst "hinter" dem IPSEC-Gateway erfolgen. Falls die Adressumsetzung auf dem gleichen IT-System durchgeführt werden soll, auf dem auch FreeS/WAN betrieben wird, ist zu beachten, dass dadurch die Verarbeitung der IP-Pakete auf diesem IT-System sehr komplex wird. Hinweise hierzu finden sich in der Dokumentation von FreeS/WAN. Übersichtlicher und damit leichter zu administrieren ist es, NAT auf einer separaten Komponente zwischen dem Gateway und dem lokalen Netz vorzunehmen.

Funktionstest des VPN

kein Testbetrieb mit Produktionsdaten

Vor dem Einsatz im Wirkbetrieb sollte geprüft werden, ob das VPN wie gewünscht funktioniert. Anstelle der beiden lokalen Netze sollten während der Testphase nur Testrechner an die Gateways angeschlossen werden. Anderenfalls ist nicht auszuschließen, dass Daten aus dem Wirkbetrieb ungeschützt über das Internet gesendet werden, wenn das VPN nicht auf Anhieb korrekt funktioniert.

Verschlüsselung überprüfen

Geprüft werden sollte, ob die Pakete tatsächlich verschlüsselt werden. Wie in der Dokumentation beschrieben, geschieht dies am einfachsten über die Tools *ping* und *tcpdump*. Mit Hilfe von *ping* lassen sich leicht zu erkennende IP-Pakete erzeugen, und *tcpdump* kann dazu verwendet werden, den daraus von FreeS/WAN generierten Netzverkehr mitzulesen. Zu beachten ist, dass das *ping*-Kommando auf dem Testrechner und nicht auf dem Gateway ausgeführt werden muss. In der vorgestellten Beispiel-Konfiguration schützt das VPN nur den Verkehr zwischen den lokalen Netzen (die in der Testphase durch einen oder mehrere Testrechner ersetzt sind) und nicht den Verkehr von oder zu den Gateways. (Siehe hierzu auch den Abschnitt *Fernadministration eines Gateways*.) Das Kommando *tcpdump* zum Mitlesen des generierten Netzverkehrs kann auf einem beliebigen IT-System zwischen den beiden Gateways ausgeführt werden.

Für den Fall, dass das VPN nicht wie gewünscht funktioniert, beispielsweise dass gar keine Kommunikation möglich ist oder der Netzverkehr nicht verschlüsselt wird, bietet FreeS/WAN umfangreiche Diagnosemöglichkeiten an. Informationen über den Status des Programmpakets erhält man z. B. über den Inhalt der Pseudodatei */proc/net/ipsec_tncfg* und über das Kommando *ipsec look*. Weitere Informationen hierzu finden sich in der Dokumentation von FreeS/WAN.

Ergänzende Kontrollfragen:

- Werden für den Betrieb von FreeS/WAN eigenständige IT-Systeme mit minimaler Installation des Betriebssystems Linux verwendet?
- Ist sichergestellt, dass private RSA-Schlüssel niemals die Gateways verlassen?
- Wird das VPN vor dem Einsatz im Wirkbetrieb auf korrekte Funktion getestet?

M 5.84 Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Der Datenaustausch zwischen Notes-Client und -Server erfolgt über Netzverbindungen. Je nach Notes-System und Netzstruktur werden die Kommunikationspakete, die neben Datenbankinhalten auch Authentisierungsinformationen enthalten können, ungeschützt übertragen. Die Übertragung erfolgt zwar binär im Datenformat des nicht offen gelegten Notes-Protokolls, dies ist jedoch in vielen Fällen kein ausreichender Schutz.

Notes-Client und -Server erlauben jedoch die Nutzung der so genannten Port-Verschlüsselung. Ist diese aktiviert, erfolgt jede Kommunikation über diesen Kommunikationsendpunkt verschlüsselt. Die Port-Verschlüsselung kann am Server aktiviert werden, so dass die Kommunikation mit allen Notes-Clients verschlüsselt erfolgt, oder die Port-Verschlüsselung wird am Client eingeschaltet. Letzteres führt dazu, dass nur die Kommunikation zwischen dem jeweiligen Client und dem Server abgesichert wird, wenn die Port-Verschlüsselung auf dem Server selbst nicht aktiviert ist.

Außerdem wird die Kommunikation nur auf den Ports verschlüsselt, für die die Verschlüsselung aktiviert wurde. Da ein Notes-Server über unterschiedliche Ports (z. B. TCP/IP, SPX, AppleTalk und COM-Ports) Verbindungen entgegen nehmen kann, muss für jeden Port entschieden werden, ob die Verschlüsselung aktiviert werden muss.

Leistungseinbußen berücksichtigen

Bei der Nutzung der Port-Verschlüsselung ist zu berücksichtigen, dass dadurch Performance-Einbußen beim Notes-Server entstehen (nach Aussagen von der Firma LOTUS ca. 10%-15%).

Die Kommunikation mit Web-Clients ist von der Port-Verschlüsselung nicht betroffen. Hier müssen andere Schutzmechanismen zum Einsatz kommen (siehe M 5.86 *Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes*).

Generell können auch andere Mechanismen außerhalb des Notes-Systems zur Kommunikationsabsicherung zum Einsatz kommen, beispielsweise auf Betriebssystemebene oder verschlüsselnde Netzkoppelelemente.

Der Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation ist zu empfehlen. Da dies aber umfangreiche Planungen und weitere Maßnahmen nach sich zieht, ist dies im Rahmen der Sicherheitsrichtlinien der jeweiligen Organisation zu entscheiden.

M 5.85 Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Das Versenden von E-Mail ist oft eine der wichtigsten Kommunikationsmechanismen in einer Büroumgebung. Auch ein Domino Server bietet die Möglichkeit an, E-Mails zu versenden und zu empfangen. Der Versand und Empfang ist dabei sowohl innerhalb des Notes-Systems als auch an und von Personen im Internet möglich. Da der E-Mail-Verkehr auf dem Weg zum Empfänger unter Umständen über eine Vielzahl von Zwischenstationen geleitet wird und die E-Mail-Inhalte dabei im Klartext übertragen werden, sollte eine zusätzliche Absicherung eingesetzt werden, die das Mitlesen oder Verändern verhindern können (siehe auch Baustein B 5.3 *E-Mail*).

Unter Lotus Notes stehen dem Benutzer verschiedene Möglichkeiten zur Absicherung des E-Mail-Verkehrs zur Verfügung:

- Notes-Verschlüsselung und -Signaturen. Diese Mechanismen können jedoch nur mit dem Notes-Client genutzt werden und stehen an der Web-Schnittstelle nicht zur Verfügung.
- S/MIME-Verschlüsselung und -Signaturen. Hierbei werden X.509-Zertifikate genutzt. Der Notes-Client unterstützt zwar S/MIME, bietet die Nutzung jedoch nur für E-Mail-Empfänger an, die als Empfänger für "Internet-Mail" gelten. Ist dies nicht der Fall, so werden die Notes-eigenen Verfahren zur Absicherung verwendet. Über ein entsprechendes Plug-in kann die S/MIME-Nutzung vereinfacht werden. Dies erfordert jedoch die Verteilung und Installation der Software auf allen Clients.

Bei der Nutzung der E-Mail-Absicherung ist folgendes zu berücksichtigen:

- Die Verschlüsselung (bzw. das Signieren) versandter oder entworfener E-Mails muss im Notes-Client (unter "User Preferences/Mail") aktiviert werden.
- Das Verschlüsseln von E-Mails im Offline-Zustand (ohne Server-Verbindung) führt unter Umständen dazu, dass E-Mails unverschlüsselt auf dem Client zwischengespeichert werden (Datei "mail.box"), bis bei der nächsten Serververbindung auf die Schlüssel der Empfänger im Namens- und Adressbuch zugegriffen werden kann. Nur E-Mails, die an Empfänger versandt werden, deren öffentliche Schlüssel im lokalen Benutzeradressbuch vorhanden sind, können sofort verschlüsselt werden.
- Über die Client-lokale Datei "notes.ini" kann der für starke Verschlüsselung (für Empfänger, deren öffentliche Schlüssel länger als 512 Bit sind) benutzte Algorithmus durch die Option "SMIME_Strong_Algorithm" eingestellt werden. Analog kann der Parameter "SMIME_Weak_Algorithm" gesetzt werden. Dies gilt für Empfänger mit Schlüssellängen kleiner 512 Bit. Mögliche Werte für beide Felder sind: RC2_40, RC2_56, RC2_64, RC2_80, RC2_128, RC5_5, RC5_7, RC5_10, RC5_16, DES und

3DES. Falls hierzu keine anderen Randbedingungen vorliegen, sollte 3DES oder RC5_16 verwendet werden.

- Fremde X.509-Zertifikate können nur in das **persönliche** Adressbuch importiert werden (Aktion "Add sender to address book", Option "Include X.509 certificate when encountered" muss aktiviert sein). Die so angelegten Personendokumente können jedoch in das öffentliche Namens- und Adressbuch (NAB) kopiert werden, so dass die Zertifikate auf diesem Weg auch anderen Benutzern zur Verfügung stehen.
- Es ist möglich, mehr als ein X.509-Zertifikat in einer Notes-ID oder für einen Benutzer im NAB zu speichern. Welches dieser Zertifikate beim Signieren oder Verschlüsseln benutzt wird, kann zur Zeit nicht ausgewählt werden.

Web-Zugriff bietet keine eingebaute E-Mail-Verschlüsselung

Wird ein Browser zum Zugriff auf die E-Mail-Datenbank auf einem Notes-Server verwendet, so stehen Verschlüsselung und Signieren beim Versenden von E-Mails nicht zur Verfügung. Hier muss auf externe E-Mail-Programme zurückgegriffen werden, die S/MIME-Unterstützung anbieten. Allerdings muss dann eine Verwaltung der Zertifikate (eigene und Empfänger-Zertifikate) im jeweiligen E-Mail-Programm erfolgen. Dies erfordert in der Regel, dass jeder Benutzer im Umgang mit der Zertifikatsverwaltung geschult wird.

Außerdem kann unter Lotus Notes die E-Mail-Datenbank eines Benutzers verschlüsselt werden. Auf diese Weise werden alle eingehenden E-Mails automatisch bei der Aufnahme in die Datenbank verschlüsselt. Entsprechend können auch versandte E-Mails oder E-Mail-Entwürfe verschlüsselt vorgehalten werden. Die Verschlüsselung eingehender E-Mail muss im Personendokument (auf dem Server) aktiviert werden.

Enthält die E-Mail-Datenbank vor Aktivierung der Verschlüsselung schon E-Mails, so werden diese nicht verschlüsselt. Hierzu müssen die alten E-Mails geöffnet und geschlossen werden.

Geschützte Kommunikation ist generell der ungeschützten vorzuziehen. Daher ist zu überlegen, ob und wie die Nachrichten verschlüsselt und / oder digital signiert werden sollten. In den Sicherheitsrichtlinie für Lotus Notes sollte diese Entscheidung dokumentiert werden.

Schulung der Benutzer

Beim Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail müssen die Benutzer im Umgang mit den Verschlüsselungsprodukten geschult werden.

Ergänzende Kontrollfragen:

- Werden die Benutzer im Umgang mit den Verschlüsselungsprodukten geschult?
- Welche Verschlüsselungsverfahren werden eingesetzt?

M 5.86 Einsatz von Verschlüsselungsverfahren beim Browser-Zugriff auf Lotus Notes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um die Kommunikation zwischen Domino Server und Web-Client abzusichern, kann die Notes-eigene Port-Verschlüsselung (siehe M 5.84 *Einsatz von Verschlüsselungsverfahren für die Lotus Notes Kommunikation*) nicht genutzt werden, da Browser diese Art der Verschlüsselung nicht unterstützen. Mit Secure Socket Layer (SSL) steht jedoch auch für die Web-Schnittstelle ein Verfahren zur Kommunikationsabsicherung zur Verfügung.

Folgendes ist bei der Nutzung der SSL-Verschlüsselung zur Absicherung der Kommunikation zwischen Notes-Server und Browser zu berücksichtigen:

- Damit SSL verwendet werden kann, muss der Domino Server für die Nutzung von SSL konfiguriert werden. Dem Server muss unter anderem ein SSL-Zertifikat ausgestellt werden, mit dem er sich einem Browser gegenüber im Rahmen des SSL-Verbindungsaufbaus authentisiert.
- Auf dem Server muss die Zertifikatsverwaltung ("certsrv.nfs" aus der Vorlage "certsrv.ntf") eingerichtet werden. Mit Hilfe der Zertifikatsverwaltung können die Schlüsseldateien und Zertifikate des Servers verwaltet werden.
- Für die Ausstellung eines Server-SSL-Zertifikates bestehen zwei grundsätzliche Möglichkeiten:

  Generierung der SSL-Zertifikate

  - Durch die Server-Zertifikatsverwaltung wird ein Selbstzertifikat ausgestellt. Diese einfachste Variante hat jedoch den Nachteil, dass dieses Zertifikat in keine Vertrauenshierarchie eingebettet ist.
  - Das SSL-Zertifikat wird durch eine Zertifizierungsstelle erstellt. Als Aussteller kann eine eigene Zertifizierungsstelle in der Behörde bzw. im Unternehmen dienen. Beispielsweise kann aus der Notes-Vorlagendatenbank "csrv50.ntf" eine Notes-Zertifizierungsstelle erstellt und realisiert werden. Alternativ kann auf eine externe Zertifizierungsstelle zurückgegriffen werden. Die Aussagekraft der verschiedenen Zertifikate ist sehr unterschiedlich, hierzu sollte man sich bei den Zertifikatstellen informieren.

  Wird die Notes-Zertifizierungsstelle nicht genutzt, ist auf die Kompatibilität der Zertifikate zu achten, sowie auf die Möglichkeit des Imports von Zertifikaten.
- Damit das Server-Zertifikat durch den Browser geprüft werden kann, muss das so genannte Root-Zertifikat der Zertifizierungsstelle auch in den Browser importiert werden. Dies erfordert in der Regel Benutzeraktivitäten oder eine automatische Verteilung, z. B. bei der Installation der Browser-Software.

  Browser benötigt Root-Zertifikat
- Soll im Rahmen des SSL-Verbindungsaufbaus auch der Web-Client über ein Zertifikat authentisiert werden (siehe auch M 4.124 *Konfiguration der Authentisierungsmechanismen beim Browser-Zugriff auf Lotus Notes),*

  Zertifikate in Browser importieren

müssen alle Benutzer mit einem entsprechenden Zertifikat ausgestattet werden. Das Zertifikat muss in die Zertifikatsdatenbank des Browsers importiert werden. Auch hier muss der Benutzer unter Umständen selbst aktiv werden, was entsprechendes Know-How voraussetzt. Zusätzlich muss sichergestellt sein, dass mindestens die Version 3 des SSL-Protokolls verwendet wird, da frühere Versionen keine Client-Authentisierung unterstützen.

kompatible Cipher-Suites

- Damit nach der Initialisierung der SSL-Verbindung die Kommunikationsabsicherung erfolgen kann, müssen Client und Server über kompatible kryptographische Verfahren verfügen (so genannte Cipher-Suites). Insbesondere ist sicherzustellen, dass im Rahmen des SSL-Verbindungsaufbaus die Option "Keine Verschlüsselung" nicht erlaubt ist.

Browser mit starken Krypto-Algorithmen einsetzen

- Sowohl im Web-Server als auch im Browser kann die Auswahl der kryptographischen Verfahren (und deren Schlüssellänge) eingeschränkt werden. Solche Einschränkungen sollten nicht zugelassen werden. Grundsätzlich sollten nur Browser eingesetzt werden, die starke kryptographische Algorithmen verarbeiten können.

Ergänzende Kontrollfragen:

- Sind die Administratoren in der Nutzung der SSL-Verschlüsselung und im Aufbau von Zertifizierungshierarchien geschult?
- Wissen die Benutzer, was bei der Nutzung von SSL zu beachten ist?

M 5.87 Vereinbarung über die Anbindung an Netze Dritter

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Immer mehr Unternehmen und Behörden schließen ihre bisher nach außen abgeschotteten Netze zu Netzverbünden zusammen, so genannten Extranets. Bei der Anbindung des eigenen internen Netzes an Netze Dritter ist es erforderlich, dass eine detaillierte Vereinbarung (Data Connection Agreement - DCA) geschlossen wird, bevor eine Netzanbindung erfolgt. Hierdurch muss genau definiert werden, wer dadurch Zugriff auf das eigene Netz erhält, unter welchen Bedingungen und auf welche Bereiche und Dienste des eigenen Netzes Zugriff gegeben werden soll. Ebenso wichtig ist dabei auch die andere Richtung, also die Frage, wer aus der eigenen Organisation mit welchen Zugriffsrechten und zu welchen Bedingungen Zugriff auf ein Fremdnetz erhalten soll.

Eine solche Vereinbarung sollte folgende Bestandteile umfassen:

Keine Netzkopplung ohne Vereinbarung

- eine Beschreibung dessen, was die Vereinbarung insgesamt umfasst,
- eine Festlegung der Verantwortlichen (Wer trägt die Verantwortung für die Einhaltung der Vertragsbedingungen?),
- die Benennung von Ansprechpartnern sowohl für organisatorische als auch technische Probleme und insbesondere für sicherheitsrelevante Ereignisse,

Wer sind die Ansprechpartner?

- die erforderlichen technischen Informationen, also Festlegungen darüber,
  - welche Dienste (z. B. telnet, ftp, http) zur Verfügung gestellt werden,
  - welche IT-Plattformen, Anwendungen und Datenformate unterstützt werden,
  - welche Verfügbarkeit zu gewährleisten ist (Performance, maximale Ausfallrate),
  - wer was protokollieren darf bzw. muss, wo die Protokolldaten abgelegt werden und wer auf die Protokolldaten zugreifen darf (dies kann insbesondere in Notsituationen wichtig sein),
  - inwieweit ein regelmäßiger Austausch von Protokolldaten erfolgen soll,
  - welche Sicherheitsmaßnahmen gewährleistet werden müssen,
- eine Vertraulichkeitsvereinbarung (Non-Disclosure-Agreement), d. h. eine Vereinbarung darüber, dass Informationen, die einer der Beteiligten im Rahmen der Zusammenarbeit erhalten hat, nicht an Außenstehende weitergegeben werden,
- eine Haftungs- bzw. Schadensersatzregelung (hierin sollten unter anderem die Bedingungen für die Trennung der Netzanbindung, Haftung bei Computenviren oder Hackerangriffen, Vertragsstrafen bei nicht erfüllter Leistung bzw. Haftungsübernahme bei Inanspruchnahme für fremde Inhalte geklärt sein),

Haftungsregelung

- eine Regelung über Auskunftspflichten bei aufgetretenen Sicherheitslücken,
- eine Festlegung, welche Daten zu welchen Zwecken genutzt werden dürfen (z. B. bei der Weiterverwendung von Arbeitsergebnissen),
- eine Beschreibung, inwieweit weitere Vertragspartner in die Vereinbarung eingebunden werden, z. B. durch gemeinsame Nutzung von Applikationen oder als Dienstleister für einen der Vertragspartner,
- die Laufzeit der Vereinbarung (Technik entwickelt sich schnell weiter, d. h. auch die Vereinbarungen über deren Nutzung müssen ständig angepasst werden).

Beteilung aller Verantwortlichen

Die Vereinbarung sollte durch die Personen abgeschlossen werden, die auch für deren Einhaltung die Verantwortung tragen. Dafür ist zunächst zu klären, wer die Verantwortung für die Netzanbindung tragen sollte, da hier üblicherweise unterschiedliche Bereiche eines Unternehmens bzw. einer Behörde involviert sind. Sinnvollerweise sollte hierzu ein Team gebildet werden, bei dem zumindest der IT-Sicherheitsbeauftragte, der IT-Leiter, der Fachverantwortliche und der Datenschutzbeauftragte beteiligt sind. Bei kritischen Entscheidungen, z. B. ob die Verbindung wegen Problemen zeitweise getrennt werden soll, sollten **alle** oben genannten Personen beteiligt werden, da sich deren Interessen erfahrungsgemäß stark voneinander unterscheiden können.

Nie mit Sicherheitsmängeln starten!

Bevor eine Netzanbindung aktiviert wird, sollten alle Sicherheitsmängel auf beiden Seiten ausgeräumt worden sein. Hier sollte auch ein Weg gefunden werden, sich von dem IT-Sicherheitsniveau seiner Partner zu überzeugen, beispielsweise durch Basis-Sicherheitschecks oder Stichproben vor Ort. Auf keinen Fall darf die Beseitigung von Sicherheitslücken in den Echtbetrieb verschoben werden, da die Erfahrung lehrt, dass diese niedriger priorisiert werden als reine Verfügbarkeitsprobleme.

Wer nutzt die Netze sonst noch?

Dritten sollten nur die Dienste zur Verfügung gestellt werden, die zum einen vertraglich vereinbart worden sind und zum anderen unbedingt erforderlich sind. Auf welche Bereiche des eigenen Netzes Dritten Zugriff gewährt wird, muss abhängig gemacht werden von der Art der bestehenden Beziehungen zwischen den Kommunikationspartnern und vom Vertrauen in die Kommunikationspartner. Bei ausländischen Partnern müssen unbedingt deren nationale Gesetze berücksichtigt werden, z. B. in den Bereichen Kryptographie bzw. Urheberrecht.

Incident Handling

Falls durch die Netzanbindung Sicherheitsprobleme auftreten, muss klar definiert sein, wer wann die Verbindung trennen darf, wer darüber zu informieren ist und welche Eskalationsschritte vorzusehen sind.

Ergänzende Kontrollfragen:

- Gibt es bei jeder Art der Netzkopplung mit Dritten Vereinbarungen über die zugrunde gelegten Rahmenbedingungen?
- Unterliegen diese Vereinbarungen einer Fortschreibung, so dass auch veränderte Rahmenbedingungen erfasst werden?

M 5.88 Vereinbarung über Datenaustausch mit Dritten

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement

Vereinbarung zum Datenaustausch schützt vor Problemen

Ein Datenaustausch mit anderen Unternehmen und Behörden kann z. B. über Datenträgeraustausch oder E-Mail erfolgen. Neben den Sicherheitsmaßnahmen, die bereits beim sporadischen Datenaustausch zu beachten sind, sollten bei einem regelmäßigen Datenaustausch mit festen Kommunikationspartnern Vereinbarungen getroffen werden, um diesen möglichst reibungslos zu gestalten.

Eine solche Vereinbarung sollte folgende Bestandteile umfassen:

Wer sind die Ansprechpartner?

- Benennung von Ansprechpartnern sowohl für organisatorische als auch technische Probleme und insbesondere für sicherheitsrelevante Ereignisse,

Datenformate festlegen

- die erforderlichen technischen Informationen, also Festlegungen darüber,
  - welche Anwendungen und Datenformate unterstützt werden,
  - welche Verfügbarkeit zu gewährleisten ist, also wie häufig beispielsweise die E-Mail zu lesen und wie schnell sie zu beantworten ist,

Schutz der Daten beim Transport

- welche Sicherheitsmaßnahmen beim Datenaustausch gewährleistet werden müssen, also z. B.
  - dass die Daten vor und nach dem Austausch auf Computer-Viren zu überprüfen sind,
  - wie die Daten vor Transportschäden und unbefugtem Zugriff zu schützen sind (verschlossene Behältnisse, Checksummen, Verschlüsselung),
  - wie das Schlüsselmanagement geregelt ist,
  - dass die Daten auf der Senderseite frühestens nach der Bestätigung des korrekten Empfangs gelöscht werden dürfen, falls eine Löschung erforderlich ist,
- eine Vertraulichkeitsvereinbarung (Non-Disclosure-Agreement), d. h. eine Vereinbarung darüber, dass Informationen, die einer der Beteiligten im Rahmen der Zusammenarbeit erhalten hat, nicht an Außenstehende weitergegeben werden,

Wer darf was mit den Daten machen?

- eine Festlegung, welche Daten zu welchen Zwecken genutzt werden dürfen (z. B. bei der Weiterverwendung von Arbeitsergebnissen),
- eine Verpflichtung auf die Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen, also z. B. Datenschutz- und Urheberrechtsgesetze bzw. Lizenzregelungen.

Weitere Punkte, die in eine solche Vereinbarung aufgenommen werden sollten, finden sich in M 2.45 *Regelung des Datenträgeraustausches* und M 2.119 *Regelung für den Einsatz von E-Mail*.

Ergänzende Kontrollfragen:

- Gibt es bei festen Kommunikationspartnern Vereinbarungen über die zugrunde gelegten Rahmenbedingungen?
- Unterliegen diese Vereinbarungen einer Fortschreibung, so dass auch veränderte Rahmenbedingungen erfasst werden?

M 5.89 Konfiguration des sicheren Kanals unter Windows 2000/XP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Zwischen Rechnern einer Windows 2000 Domäne müssen administrative Daten ausgetauscht werden. So tauschen beispielsweise Domänen-Controller einer Domäne Verwaltungsdaten aus. Generell werden dabei sensitive Daten transportiert und müssen daher abgesichert übertragen werden. Schon unter Windows NT stand dafür der so genannte *Sichere Kanal* (englisch *Secure Channel*) zur Verfügung. Auch unter Windows 2000/XP wird dieser Mechanismus genutzt und muss entsprechend den Sicherheitsanforderungen und den lokalen Gegebenheiten konfiguriert werden. Hierbei werden als Sicherheitsmechanismen die Authentisierung der beiden Kommunikationspartner, Verschlüsselung zur Wahrung der Vertraulichkeit und Signaturen zur Absicherung der Integrität eingesetzt.

Die Konfiguration des sicheren Kanals erfolgt über Gruppenrichtlinien. Bei deren Konfiguration ist Folgendes zu berücksichtigen:

Authentisierung

- Die gegenseitige Authentisierung ist immer gewährleistet, Verschlüsselung und Signatur können jedoch unabhängig voneinander gefordert werden. Unterstützt der Kommunikationspartner die geforderte Absicherung nicht, wird diese nicht eingesetzt. Die Kommunikation erfolgt dann ungesichert.

Verschlüsselung oder Signatur

- Verschlüsselung oder Signatur können als notwendige Voraussetzung für die Kommunikationsaufnahme spezifiziert werden. Unterstützt der Kommunikationspartner die Absicherung nicht, wird keine Kommunikation aufgebaut. Dies kann z. B. zur Folge haben, dass sich Clients nicht an einer Domäne anmelden können. Diese Option sollte nur aktiviert werden, wenn alle Rechner einer Domäne und alle Rechner aller vertrauten Domänen das Verschlüsseln und Signieren unterstützen.

Stärke des Sitzungsschlüssels

- Die Stärke des zur Verschlüsselung erzeugten Sitzungsschlüssels lässt sich vom Windows NT Niveau auf das Windows 2000 Niveau erhöhen. Von dieser Option darf jedoch nur Gebrauch gemacht werden, wenn alle Rechner einer Domäne und alle Rechner aller vertrauten Domänen ausschließlich unter Windows 2000/XP betrieben werden. Ist sie aktiviert, können sich Rechner, auf denen andere Betriebssysteme installiert sind, nicht mehr an der Domäne anmelden.

Die für die Konfiguration relevanten Gruppenrichtlinienparameter sind:

- Secure Channel: Digitally encrypt secure channel data (when possible)
- Secure Channel: Digitally sign secure channel data (when possible)
- Secure Channel: Digitally encrypt or sign secure channel data (always)
- Secure Channel: Require strong (Windows 2000 or later) session key

Diese Parameter finden sich unter Computer *Settings/Windows Settings/ Security Settings/Local Policies/Security Options*.

Wenn sich neben Rechnern mit dem Betriebssystem Windows 2000/XP auch Rechner mit anderen Betriebssystemen im Netz befinden, sollten nur die beiden ersten Optionen aktiviert werden. Verfügen hingegen alle Rechner im Netz über Windows 2000/XP, so sollten alle Optionen aktiviert werden.

M 5.90 Einsatz von IPSec unter Windows 2000/XP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Zur Absicherung der Kommunikation bietet Windows 2000/XP eine IPSec-konforme Implementierung an. IPSec ist ein internationaler Standard, der die kryptographische Absicherung IP-basierter Kommunikation erlaubt und folgende Funktionen umfasst:

- Gegenseitige Authentisierung der Kommunikationsendpunkte **Authentizität**
- Sicherung der Integrität der übertragenen Daten durch digitale Signaturen **Integrität**
- Sicherung der Vertraulichkeit der übertragenen Daten oder des gesamten IP-Datenpaketes durch Verschlüsselung (Tunnel-Modus) **Vertraulichkeit**

Jede IPSec-konforme Komponente muss mindestens folgende Sicherungsverfahren implementieren:

- Zur Wahrung der Integrität müssen mindestens die Hashverfahren MD5 und SHA-1 implementiert sein.
- Zur Wahrung der Vertraulichkeit müssen mindestens die Verschlüsselungsverfahren DES und Tripel-DES implementiert sein.

Damit neben der Integrität und Vertraulichkeit der übertragenen Daten auch sichergestellt werden kann, dass die Daten zwischen den korrekten Kommunikationspartnern ausgetauscht werden, müssen sich diese authentisieren. Die Windows 2000/XP Implementierung erlaubt folgende Verfahren zur Authentisierung der Kommunikationsendpunkte:

- Es kann das Kerberos-Protokoll eingesetzt werden. Hierbei findet die normale Windows 2000 Authentisierung statt. Dieses Verfahren beruht auf symmetrischen Schlüsseln, die zur Verschlüsselung der so genannten Kerberos-Tickets eingesetzt werden. **Kerberos**
- Es können X.509-Zertifikate eingesetzt werden. Hierbei erfolgt die Authentisierung - basierend auf asymmetrischen Schlüsseln - auf Grund der Zertifikatsinformationen. In der Regel wird ein so genanntes Challenge-Response-Verfahren eingesetzt, das überprüft, ob der zu authentisierende Benutzer im Besitz des korrekten privaten Schlüssels ist. **X.509-Zertifikat**
- Es wird ein so genanntes *Pre-shared Secret* benutzt. Hierbei erfolgt die Authentisierung durch einen geheimen Schlüssel (d. h. Passwort), der vorher zwischen den Kommunikationspartnern ausgetauscht wurde. Der Austausch muss über einen sicheren Kanal erfolgt sein, so dass der geheime Schlüssel nur den beiden Kommunikationspartnern bekannt ist. **Pre-shared Secret**

Im Rahmen des ersten IPSec-Verbindungsaufbaus werden zunächst die nachfolgend zu benutzenden Algorithmen und Verfahren zur Authentisierung, Integritätssicherung und Wahrung der Vertraulichkeit zwischen den Kommunikationspartnern ausgehandelt und in der so genannten *Security Association* (SA) gespeichert. Diese in der SA gespeicherten Parameter werden dann für alle zukünftigen Kommunikationsverbindungen benutzt, bis die Gültigkeit der SA-Parameter erlischt und die Verfahren neu ausgehandelt werden. Dies erfolgt in der Regel vollautomatisch durch die Komponenten der IPSec-Implementierung.

Master- und Session-Key

Für die eigentliche Verschlüsselung müssen Schlüssel - der so genannte Master- und Session-Key (Sitzungsschlüssel) - generiert werden. In der Regel wird dabei der Master-Key, von dem alle weiteren Schlüssel abgeleitet werden, pro Verbindung nur einmal erzeugt, der Session-Key hingegen periodisch mehrfach. Es besteht die Möglichkeit, auch den Master-Key periodisch neu zu erzeugen, was jedoch eine erneute Authentisierung der Kommunikationspartner erfordert. In der Regel erfolgt die erneute Authentisierung automatisch durch die Komponenten der IPSec-Implementierung, so dass dadurch im Wesentlichen die Performance beeinflusst wird.

IPSec-Policies

Zur Steuerung der IPSec-basierten Kommunikation bietet Windows 2000/XP so genannte IPSec-Richtlinien (IPSec-Policies) an, die angeben, welche IPSec-Parameter für eine Verbindung zu benutzen sind. Über verschiedene Richtlinien lässt sich erreichen,

- dass Rechner ausschließlich IPSec-geschützte Verbindungen annehmen,
- dass Rechner IPSec-geschützte Verbindungen beim Kommunikationspartner anfordern, jedoch auch ungeschützte Kommunikation zulassen, falls der Partner kein IPSec-Protokol unterstützt,
- oder dass die IPSec-basierte Kommunikation ausgeschlossen wird.

Windows 2000/XP bietet drei vordefinierte IPSec-Richtlinien an:

- Client (nur Antwort): für Rechner, die nur auf Anforderung des Kommunikationspartners die IPSec-Absicherung aushandeln und ansonsten keine Kommunikationsabsicherung betreiben.
- Server (Sicherheit anfordern): für Rechner, die von ihren Kommunikationspartnern IPSec-geschützte Verbindungen anfordern, jedoch auch Verbindungen ohne Schutz akzeptieren, falls der Kommunikationspartner IPSec nicht unterstützt.
- Server (Sicherheit erforderlich): für Rechner, die ausschließlich IPSec-geschützte Verbindungen aufbauen sollen und ungesicherte Verbindungswünsche ablehnen.

Diese vordefinierten Regeln können im Detail den lokalen Anforderungen angepasst werden. Dabei empfiehlt es sich, eine Kopie anzulegen und die Veränderungen auf der Kopie der Richtlinie durchzuführen. Im Rahmen einer IPSec-Richtlinie werden so genannte Filterregeln genutzt, um unterschiedliche IPSec-Parameter, z. B. in Abhängigkeit vom verwendeten Protokoll, definieren zu können. Beispielsweise kann festgelegt werden, dass HTTP unverschlüsselt ist, FTP dagegen immer verschlüsselt wird.

IPSec wird entweder über Gruppenrichtlinien oder lokal im Eigenschaftsdialog für Netzverbindungen aktiviert. Die Konfiguration der IPSec-Einstellungen erfolgt über die IPSec-Richtlinien mit Hilfe der Microsoft Management Console (MMC).

Generell ist für die Nutzung von IPSec unter Windows 2000/XP Folgendes zu berücksichtigen:

Performance prüfen

- Vor dem Einsatz von IPSec muss geprüft werden, ob die mit der Aktivierung verbundenen Performance-Einbußen toleriert werden können. Unter Umständen sollte über den Einsatz von IPSec-konformen Netzwerkkarten nachgedacht werden, die die Verschlüsselung mit Hardware-Unterstützung durchführen und damit eine bessere Performance erreichen können.

Perfect Forward Secrecy aktivieren

- Zum stärkeren Schutz der Session-Keys sollte die Option *Perfect Forward Secrecy (PFS)* aktiviert sein. Dies stellt sicher, dass bei Kompromittierung eines Session-Keys ausschließlich die mit diesem einzelnen Session-Key verschlüsselten Daten entschlüsselt werden können. Dies wird dadurch erreicht,
  - dass ein Session-Key, der zum Verschlüssen von Daten benutzt wurde, nicht benutzt wird, um weitere Schlüssel zu erzeugen, und
  - dass das Schlüsselausgangsmaterial, das zum Erzeugen eines Session-Keys benutzt wurde, nicht ein weiteres Mal zum Erzeugen eines Session-Keys benutzt wird.

  Dies hat zwar geringe Performance-Einbußen zur Folge, diese fallen in der Regel jedoch nicht ins Gewicht.
- Für Verbindungen mit hohem Schutzbedarf kann auch für den Master-Key die Option PFS aktiviert werden. Dies führt jedoch zu stärkeren Performance-Einbußen als PFS für Session-Keys, da hier jedes Mal eine Authentisierung der Kommunikationspartner durchgeführt werden muss.

Auswahl der Mechanismen

- Im konkreten Fall muss jeweils entschieden werden, welche Mechanismen und Verfahren zur Authentisierung und zur Sicherung der Integrität und Vertraulichkeit im Rahmen der IPSec-Verhandlung während des Verbindungsaufbaus zur Verfügung stehen sollen. Es muss dabei berücksichtigt werden, dass zwischen den Kommunikationspartnern jeweils mindestens ein Verfahren existieren muss, das beide Partner unterstützen.

- Werden eigene IPSec-Richtlinien erstellt, so muss unbedingt immer eine so genannte *Standardantwortregel* definiert werden, die greift, wenn keine andere Filterregel der Richtlinie Anwendung findet. Fehlt diese, so kann es vorkommen, dass keine Verbindung zwischen den Kommunikationspartnern zustande kommt.
- Die Filterregeln einer IPSec-Richtlinie erlauben es, die IPSec-Absicherung z. B. auch an die IP-Adresse des Kommunikationspartners zu binden, so dass die Verschlüsselung in Abhängigkeit vom Kommunikationspartner aktiviert werden kann.
- Wird zur Authentisierung der Kerberos-Mechanismus verwendet, so erfolgt die Authentisierung nicht IPSec-abgesichert, da Kerberos nicht im Rahmen der IPSec-Verbindung abgewickelt wird. Nach Einspielen des Windows 2000 Service Pack 1 kann die IPSec-Absicherung auch für das Kerberos-Protokoll aktiviert werden. Dazu ist jedoch ein Eingriff in die Registry notwendig (siehe dazu auch Microsoft Knowledgebase Artikel Q254728):

  Absicherung der Kerberos-Authentisierung

  Unter *HKEY_LOCAL_MACHINE / SYSTEM / CurrentControlSet / Services / IPSEC* muss der Schlüssel *NoDefaultExempt* vom Typ *REG_DWORD* und dem Wert 1 eingetragen werden.
- Um das korrekte Funktionieren des IPSec-Verbindungsaufbaus und der IPSec-Kommunikation zu prüfen, stellt Windows 2000 das Programm *ipsecmon.exe* und Windows XP das MMC Snap-In *IP-Sicherheitsmonitor* zur Verfügung. Dieses kann zur Eingrenzung der Fehlerquelle benutzt werden, falls Probleme mit IPSec-Verbindungen bestehen. Das Programm ist jedoch relativ einfach aufgebaut, so dass es nur zu einer ersten Ursachenforschung verwendet werden kann.

  Fehlersuche
- IPSec sollte unter anderem in Kombination mit EFS-verschlüsselten Dateien eingesetzt werden, wenn diese auf Servern lagern und abgesichert über das Netz zu einem Client transportiert werden sollen. Außer IPSec kann jedoch auch jeder andere Mechanismus zur Absicherung der Netzkommunikation genutzt werden, um serverseitig gespeicherte EFS-Dateien beim Transport zu schützen.
- Soll die Kommunikation mit einem System, auf dem nicht Windows 2000/XP als Betriebssystem installiert ist, mittels IPSec geschützt werden, so ist die Interoperabilität und das korrekte Funktionieren in einem praktischen Test zu überprüfen. Zwar ist das IPSec-Verfahren standardisiert, im Einzelfall ergeben sich jedoch unter Umständen auch bei standardisierten Verfahren Kompatibilitätsprobleme.

  Interoperabilität mit anderen Systemen prüfen

Es muss jeweils im Einzelfall entschieden werden, ob IPSec zur Kommunikationsabsicherung eingesetzt werden soll. Dies ist schon bei der Planung des Windows 2000/XP Einsatzes zu berücksichtigen.

Ergänzende Kontrollfragen:

- Wurde der Einsatz von IPSec bedarfsgerecht geplant?
- Sind alle Kommunikationspartner identifiziert, für die die Kommunikation mittels IPSec abgesichert werden soll?
- Wurde überprüft, ob der IPSec-Verbindungsaufbau korrekt durchgeführt wird?

M 5.91 Einsatz von Personal Firewalls für Internet-PCs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

kein Ersatz für zentrale Firewall

Die Entwicklung der als Personal Firewalls bezeichneten Produktlinie ist auf die Absicherung der lokalen Ressourcen eines Clients zugeschnitten. Als alleinige Maßnahme für die Absicherung eines Behörden- oder Unternehmensnetzes gegenüber Angriffen aus dem Internet sind Personal Firewalls ungenügend. Der alleinige Einsatz dieser Firewalls bringt folgende Nachteile mit sich:

- Alle ans Internet angeschlossenen Clients müssen gehärtet werden, d. h. die potentiellen Schwachstellen des Betriebssystems müssen behoben werden.
- Wie bei jeder dezentral eingesetzten Software ist das Management und die Auswertung der Protokolldaten der einzelnen Personal Firewalls aufwendig.

Derzeit verfügbare Produkte weisen hier noch einen erheblichen Optimierungsbedarf auf. Vom Hersteller angebotene Sicherheitsprofile bieten hier eine praktikable Konfigurationsmöglichkeit.

Prüfung auf Schadsoftware

Als Ergänzung zu einer zentralen Firewall kann der Einsatz von Personal Firewalls durchaus sinnvoll sein. Prinzipiell ist es z. B. möglich, mit ihnen die Prüfung auf Schadsoftware, die über E-Mail, Java, ActiveX oder ähnliche Mechanismen übertragen werden kann, auf den Clients vorzunehmen. Hierfür können Mechanismen wie Sandboxes zum Einsatz kommen, mit denen der Zugriff von Applikationen, die vom Internet auf das lokale System übertragen werden (Java, ActiveX, etc.), eingeschränkt werden kann. Mit ihnen wird die Aufgabe der Prüfung auf Schadsoftware dezentralisiert und damit das Firewall-System entlastet. Ein weiterer Vorteil liegt darin, dass die Problematik der Filterung von verschlüsselten Daten auf der Firewall umgangen werden kann.

Einsatz auf Internet-PCs

Der Einsatz einer Personal Firewall bietet sich insbesondere bei Internet-PCs an, d. h. auf Computern, die ausschließlich für die Nutzung des Internets bereitgestellt werden und keine Verbindung zum Behörden- bzw. Unternehmensnetz haben. Aufgrund des vielfältigen Funktionsumfangs dieser Produkte und der Komplexität der Technologie muss dabei jedoch eine kompetente Administration sichergestellt sein.

Bei Konfiguration und Betrieb einer Personal Firewall sollten folgende Aspekte berücksichtigt werden:

- Die Filterregeln sollten so restriktiv wie möglich eingestellt werden. Dabei gilt der Grundsatz: *Alles was nicht ausdrücklich erlaubt ist, ist verboten.*
- Um dem Missbrauch von NETBIOS-Funktionen entgegenzuwirken, sollten Zugriffe vom Internet auf die IP-Ports 137 bis 139 und 445 gesperrt werden, falls die verwendete Personal Firewall dies ermöglicht.
- **Konfiguration testen**
  Die Filterregeln der Personal Firewall sollten nach der erstmaligen Konfiguration daraufhin getestet werden, ob die erlaubten Ereignisse zugelassen und unerlaubte Ereignisse unterbunden werden.

- Die korrekte Konfiguration der Filterregeln sollte in sporadischen Abständen überprüft werden, wenn die Installation des Internet-PCs nicht ohnehin regelmäßig gelöscht und anhand eines Festplatten-Abbildes (Images) erneut aufgespielt wird.
- Falls das verwendete Produkt diese Möglichkeit bietet, sollten die Regeln der Personal Firewall auch speziellen Programmen zugeordnet werden. Dadurch kann unter Umständen erkannt und verhindert werden, dass ein anderes als die vorgesehenen Client-Programme Verbindungen zu Rechnern im Internet aufbaut oder annimmt.
- Da viele der Prüfmechanismen einer Personal Firewall auf aktuellen Erkenntnissen beruhen, müssen vom Hersteller veröffentlichte Patches bzw. Updates regelmäßig eingespielt werden. Dabei ist sicherzustellen, dass die dafür erforderlichen Dateien von einer vertrauenswürdigen Quelle, beispielsweise direkt vom Hersteller, bezogen werden.

Patches einspielen

- Die Personal Firewall muss so konfiguriert werden, dass die Benutzer nicht durch eine Vielzahl von Warnmeldungen belästigt werden, die sie nicht interpretieren können.
- Falls das verwendete Produkt diese Möglichkeit bietet, sollten sicherheitsrelevante Ereignisse protokolliert werden. Die Protokolldaten sollten regelmäßig durch fachkundiges Personal ausgewertet werden. Die Hinweise in M 2.110 *Datenschutzaspekte bei der Protokollierung* sind zu beachten.

inkrementelle Konfiguration ...

Einige Produkte verfügen über die Möglichkeit, mit einer sehr restriktiven Grundkonfiguration zu starten und danach die Einstellungen im laufenden Betrieb zu verfeinern. Dabei wird jedes Mal, wenn ein sicherheitsrelevantes Ereignis auftritt, für das bisher noch keine eindeutige Regel existiert, der Benutzer gefragt, ob dieses Ereignis zulässig ist. Ein Beispiel für ein solches sicherheitsrelevantes Ereignis ist der Zugriff eines bestimmten installierten Programms auf das Internet. Auf der Grundlage der Antworten des Benutzers ermittelt die Personal Firewall Schritt für Schritt die gewünschte Konfiguration, z. B. die Filterregeln.

... hat Vor- und Nachteile

Der Vorteil dieser inkrementellen Konfiguration ist, dass dadurch die Komplexität der Administration reduziert werden kann. Nachteilig ist jedoch, dass Benutzer in der Regel nicht ohne weiteres beurteilen können, ob ein bestimmtes Ereignis zulässig ist oder nicht. Die inkrementelle Konfiguration der Personal Firewall kann daher nur dann empfohlen werden, wenn den Benutzern entweder präzise Vorgaben gemacht werden, wie sie auf Rückfragen des Programms antworten sollen oder wenn dies unter Anleitung eines Administrators, z. B. durch telefonische Rückfragen, erfolgt.

Personal Firewalls werden inzwischen von einer Vielzahl von Herstellern angeboten. Zum Teil ist der Einsatz für private Anwender sogar kostenlos. Im kommerziellen oder behördlichen Umfeld müssen jedoch in der Regel Lizenzen erworben werden. Personal Firewalls werden häufig in Fachzeitschriften getestet. Die Ergebnisse dieser Tests können bei der Auswahl eines für den vorliegenden Einsatzzweck geeigneten Produkts helfen.

Ergänzende Kontrollfragen:

- Existiert ein Konzept für den Einsatz von Personal Firewalls?
- Werden vom Hersteller veröffentlichte Patches bzw. Updates zur Behebung sicherheitsrelevanter Schwachstellen installiert?

M 5.92 Sichere Internet-Anbindung von Internet-PCs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Für den ordnungsgemäßen Betrieb eines Internet-PCs ist die sichere Anbindung an das Internet aufgrund des speziellen Einsatzszenarios besonders wichtig. Die Internet-Anbindung sollte daher sorgfältig geplant werden. Dabei sollten folgende Teilaspekte berücksichtigt werden:

Auswahl eines geeigneten Internet Service Providers (ISP)

Die Anbindung an das Internet geschieht über einen ISP, der die für die Nutzung des Internets notwendige Technik und Dienstleistungen zur Verfügung stellt. Die Anbieter am Markt unterscheiden sich dabei in Bezug auf Umfang, Qualität und Preis der Dienstleistungen. Die Auswahl eines geeigneten ISPs muss anhand der Anforderungen an die Internet-Anbindung getroffen werden:

- Bietet der ISP die gewünschte Verbindungstechnik, d. h. Modem, ISDN, DSL usw., an?
- Erfüllt der ISP die Anforderungen an die minimale bzw. durchschnittliche Bandbreite und die Verfügbarkeit des Internet-Zugangs? Hierzu sollten auch Testberichte in Fachzeitschriften zu Rate gezogen werden.

Bandbreite und Verfügbarkeit

- Bietet der ISP die benötigten Zusatzdienstleistungen an, z. B. für E-Mail oder News, oder soll hierfür auf einen weiteren Dienstleister zurückgegriffen werden?
- Stellt der ISP die erforderlichen IT-Sicherheitsmechanismen für die angebotenen Dienstleistungen bereit? Werden beispielsweise Proxy-Server für WWW und FTP zur Verfügung gestellt und kann E-Mail auch SSL-geschützt abgeholt werden?

IT-Sicherheitsmechanismen

- Macht der ISP Angaben zum Umgang mit personenbezogenen Daten oder mit Informationen über die Behörde bzw. das Unternehmen? Decken sich diese Angaben mit den eigenen Anforderungen an den Datenschutz?
- ISPs bieten unterschiedliche Preismodelle für die Internet-Anbindung an. Beispielsweise kann zwischen pauschalen, zeitabhängigen und volumenabhängigen Gebühren unterschieden werden. Ist das Preismodell für den Einsatzzweck des Internet-PCs geeignet?
- Anhand der Anforderungen an die Verfügbarkeit der Internet-Anbindung sollte geprüft werden, ob es erforderlich ist, aus Redundanzgründen Verträge mit zwei oder sogar mehr Providern abzuschließen.

redundante Provider

Weitere Empfehlungen zur geeigneten Auswahl eines Internet Service Providers finden sich in Maßnahme M 2.176 *Geeignete Auswahl eines Internet Service Providers*.

Beschaffung geeigneter Netzkomponenten für die Internet-Anbindung

Je nachdem, ob mit der Internet-Anbindung nur ein einzelner Internet-PCs oder ein ganzer Pool solcher Internet-PCs versorgt werden soll, ergeben sich unterschiedliche Anforderungen an die hierfür erforderlichen Hardware-

Komponenten. Bei der Beschaffung sollten die folgenden Aspekte berücksichtigt werden:

einzelner Internet-PC

- Falls ein einzelner Internet-PC an das Internet angebunden werden soll, kommt in vielen Fällen ein Modem oder eine ISDN-Karte zum Einsatz. Kompatibilitätsprobleme zwischen diesen Geräten und dem Einwahl-Server beim ISP treten inzwischen nur noch selten auf. Modems und ISDN-Karten sind sehr preiswert und lassen sich bei technischem Defekt schnell ersetzen. Falls erhöhte Anforderungen an die Verfügbarkeit bestehen, sollten Ersatzgeräte vorgehalten werden.

Internet-PC-Pool

- Falls ein Internet-PC-Pool versorgt werden soll oder falls aus anderen Gründen hohe Bandbreiten benötigt werden, kommen häufig spezielle Router, z. B. DSL-Router, für die Internet-Anbindung zum Einsatz. Falls die Geräte nicht vom ISP zur Verfügung gestellt werden, ist eine präzise Abstimmung erforderlich, um Kompatibilitätsprobleme zu vermeiden. Bei erhöhten Verfügbarkeitsanforderungen sollte geprüft werden, ob der ISP entsprechende Dienstleistungen anbietet, beispielsweise Austausch des Routers innerhalb einer vorgegebenen Zeitspanne, Vorhalten eines Ersatzgerätes, usw.

Sichere Konfiguration und Betrieb der Internet-Anbindung

Für den sicheren und ordnungsgemäßen Betrieb der Internet-Anbindung sollten folgende Empfehlungen berücksichtigt werden:

- Alle Konfigurationseinstellungen für die Internet-Anbindung sollten dokumentiert werden, damit sie bei Datenverlust schnell wiederhergestellt und Abweichungen erkannt werden können.

Proxy-Server

- Für Zugriffe über die Protokolle HTTP und FTP sollten möglichst so genannte Proxy-Server verwendet werden. Diese Proxy-Server leiten Anfragen von Clients als "Stellvertreter" an den gewünschten HTTP- bzw. FTP-Server weiter. Dadurch ergibt sich unter anderem der Vorteil, dass restriktivere Regeln auf evtl. eingesetzten Paketfiltern konfiguriert werden können. ISP betreiben in der Regel entsprechende Proxy-Server.

Schutz vor DNS-Spoofing

- Server beim ISP oder im Internet, die öfter genutzt werden, beispielsweise E-Mail-Server, Proxy-Server usw., sollten immer über ihre IP-Adresse angesprochen werden. Diese IP-Adressen sollten in allen betroffenen Komponenten fest eingestellt werden. Dadurch verringert sich die Gefahr durch so genannte DNS-Spoofing-Angriffe.
- Falls ein Internet-Zugang mit dynamischen IP-Adressen genutzt wird, sollte ab und zu die Verbindung getrennt werden, damit dem Client bei der nächsten Einwahl eine neue IP-Adresse zugeordnet wird. Dies ist besonders wichtig bei pauschalen Gebühren ("flat rate"). Durch solche Wechsel der IP-Adresse werden gezielte Angriffe erschwert.
- Voreingestellte Passwörter, z. B. für die Einwahl beim Internet Service Provider, müssen geändert werden. Empfehlungen hierzu finden sich in M 2.11 *Regelung des Passwortgebrauchs*.

- Der Zugriff auf die Konfigurationsdateien für die Internet-Anbindung sollte auf die zuständigen Administratoren beschränkt werden, wenn das verwendete Betriebssystem dies zulässt.
- Falls die verwendete Kommunikations-Software oder die eingesetzten Modem-, ISDN- oder DSL-Geräte Funktionen zur Fernsteuerung bieten, müssen diese deaktiviert oder gut geschützt werden.
- Falls die Internet-Anbindung durch Einwahl erfolgt, sollten die Rufnummern für die Einwahl beim ISP fest eingetragen werden.
- Das Modem bzw. die ISDN-Komponente sollte die Verbindung unterbrechen, wenn der Benutzer sich abmeldet bzw. die Internet-Anwendung beendet.

Verbindung bei Sitzungsende trennen

- Falls für die Authentisierung bei der Einwahl beim Internet Service Provider zwischen dem PAP- und dem CHAP-Verfahren gewählt werden kann, sollte besser CHAP genutzt werden. Dadurch wird vermieden, dass die Authentisierungsdaten im Klartext übertragen werden (siehe auch M 5.50 *Authentisierung mittels PAP/CHAP*).
- Alle nicht benötigten Funktionen, wie z. B. das Aktivieren der Kommunikationsverbindung von außen, müssen abgeschaltet werden. Eingehende Anrufe dürfen nicht angenommen werden.
- Die verwendeten Zieladressen und die eingestellten Parameter sollten gelegentlich kontrolliert werden (siehe auch M 5.29 *Gelegentliche Kontrolle programmierter Zieladressen und Protokolle*).

Ergänzende Kontrollfragen:

- Erfüllt der Internet Service Provider die Anforderungen an die Verfügbarkeit des Internet-Zugangs?
- Wurden alle Konfigurationseinstellungen für die Internet-Anbindung dokumentiert?

M 5.93 Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsbeauftragter

Verantwortlich für Umsetzung: Administrator

Das World Wide Web (WWW) ist sicherlich einer der wichtigsten Dienste, die im Internet angeboten werden. Neben dem reinen Abrufen von Informationen dient es heute auch als Plattform für interaktive Angebote, wie z. B. im E-Business und E-Government. Auf Internet-PCs wird daher in den meisten Fällen ein Browser, d. h. ein Client-Programm für die Nutzung von WWW-Angeboten, benötigt. Populäre WWW-Browser sind z. B. *Netscape Navigator*, *Microsoft Internet Explorer* und *Opera*.

Die Browser-Technologie hat sich rasant weiterentwickelt. Von der ursprünglichen Funktion, Text und Bilder aus dem Internet zu laden und anzuzeigen, haben sich WWW-Browser zu universellen Frontends für netzbasierte Anwendungen entwickelt. Browser können eine Vielzahl unterschiedlicher Medienformate anzeigen und abspielen und dienen außerdem als Ablaufumgebung für Programme und Skripten, so genannten aktiven Inhalten. Zu letzteren gehören unter anderem die Technologien *Java*, *Javascript* und *ActiveX*. Der Funktionsumfang moderner Browser kann durch so genannte *Plug-Ins* zusätzlich erweitert werden.

Diese Vielzahl von Funktionen bringt komplexe Konfigurationsmöglichkeiten und potentielle Sicherheitsprobleme mit sich. Die nachfolgenden Empfehlungen zur Konfiguration von Browsern beim Einsatz von Internet-PCs sollen diesen IT-Sicherheitsaspekten Rechnung tragen.

Installation

nicht jedes Plug-In installieren

Die Grundsatzempfehlung, nur benötigte Software-Komponenten zu installieren, gilt für WWW-Browser ganz besonders, speziell für die zahlreichen verfügbaren Plug-Ins. Diese dienen meist dazu, bestimmte Medienformate, z. B. Videos oder Radioprogramme, anzuzeigen oder abzuspielen. Dabei besteht die grundsätzliche Gefahr, dass durch Design- oder Implementierungsfehler in den Plug-Ins beim Aufruf entsprechender Webseiten unerwünschte Aktionen ausgelöst werden, z. B. Manipulation oder Kompromittierung lokaler Daten. Es sollten daher nur die Plug-Ins installiert werden, die für die tägliche Arbeit auch wirklich erforderlich sind.

Software-Schwachstellen sind nicht nur in Plug-Ins, sondern vielfach auch in Browsern selbst bekannt geworden. Diese Schwachstellen können dazu ausgenutzt werden, Sicherheitsmechanismen zu umgehen oder anderweitig Schäden auszulösen. Browser-Hersteller veröffentlichen daher häufig Patches, Updates oder Anleitungen zur Behebung dieser Sicherheitslücken. Die Administration sollte sich daher regelmäßig auf den Webseiten des jeweiligen Browser-Herstellers über aktuelle Sicherheitslücken informieren und evtl. bereitgestellte Updates bzw. Patches installieren (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*).

Ein weiteres Problemfeld ist der Aufruf externer Programme aus dem Browser heraus. Die meisten Browser bieten die Möglichkeit, Dateien nach dem

Download direkt mit dem zugeordneten Anwendungsprogramm zu öffnen oder zu starten. Da die heruntergeladenen Dateien oft aus unbekannten Quellen stammen, besteht die Gefahr, dass beim Öffnen oder Starten unerwünschte Aktionen ausgelöst werden. Ursache können dabei z. B. Pufferüberläufe in den Anwendungsprogrammen oder schädliche, in die Dateien eingebettete Makros sein. Um das Risiko zu minimieren, sollten auf einem Internet-PC daher so wenig Anwendungsprogramme wie möglich installiert werden. Zur Anzeige von Fremdformaten, z. B. Word- oder Excel-Dateien, sollten möglichst Viewer-Programme verwendet werden, die die Ausführung von Makros nicht unterstützen.

Alle installierten Software-Komponenten, wie z. B. Plug-Ins, Patches, Updates und Viewer-Programme, sollten ausschließlich aus vertrauenswürdigen Quellen bezogen werden, beispielsweise direkt vom Hersteller oder offiziellen Spiegel-Servern.

Konfiguration

Die verbreiteten WWW-Browser haben komplexe Konfigurationsmöglichkeiten. Viele Optionen haben Auswirkungen auf den sicheren Betrieb des Browsers und damit auch auf die IT-Sicherheit des Internet-PCs. Nach einer Standard-Installation entsprechen die Browser-Einstellungen in der Regel nicht den IT-Sicherheitsanforderungen. Die einzelnen Konfigurationseinstellungen sollten daher systematisch überprüft und ggf. angepasst werden. Grundlage hierfür sind die Vorgaben im Einsatzkonzept und in den Richtlinien für Internet-PCs (siehe Maßnahmen M 2.234 *Konzeption von Internet-PCs* und M 2.235 *Richtlinien für die Nutzung von Internet-PCs*). Die folgenden Empfehlungen sollten bei der Konfiguration berücksichtigt werden.

Proxy-Server eintragen

Wenn der Internet Service Provider (ISP) einen Proxy-Server anbietet, sollte dieser auch genutzt werden. Hierzu müssen im Browser die IP-Adresse und die Port-Nummer des Proxy-Servers eingetragen werden. Bei einigen Browsern müssen diese Informationen für jeden unterstützten Dienst separat angegeben werden. Proxy-Server unterstützten in der Regel mindestens die Dienste HTTP, HTTPS und FTP. Die benötigten IP-Adressen und Port-Nummern sollten den Informationen des ISPs entnommen oder dort erfragt werden.

aktive Inhalte vermeiden

Unter *aktiven Inhalten* sind Computerprogramme zu verstehen, die in Internet-Seiten enthalten sind oder beim Betrachten einer Internet-Seite automatisiert nachgeladen werden. Ausgeführt werden diese Computerprogramme auf dem Computer des Internet-Nutzers entweder vom jeweiligen WWW-Browser oder von dem darunter liegenden Betriebssystem. Wichtige Beispiele für aktive Inhalte sind die Technologien *Javascript*, *Java* und *ActiveX*. Wie bei jedem Computerprogramm besteht bei aktiven Inhalten die Gefahr, dass von dem Programmcode nicht nur sinnvolle Aktionen durchgeführt werden, sondern auch unerwünschte oder sogar schädliche Aktionen. Aktive Inhalte können also beispielsweise Viren transportieren oder Trojanische Pferde darstellen. Die Browser enthalten zwar einige Sicherheitsfunktionen zum Schutz vor schädlichen aktiven Inhalten, in der Vergangenheit sind jedoch zahlreiche Software-Schwachstellen bekannt geworden, die zum Aushebeln dieser Sicherheitsfunktionen ausgenutzt werden können (siehe auch M 5.69 *Schutz vor aktiven Inhalten*).

In den gängigen Browsern kann eingestellt werden, wie mit aktiven Inhalten umgegangen werden soll. Aus den oben genannten Gründen sollte die Ausführung aktiver Inhalte nur dann im Browser freigeschaltet werden, wenn dies im Einsatzkonzept bzw. in den Richtlinien für Internet-PCs ausdrücklich vorgesehen ist. In diesem Fall sollten nur die Technologien aktiviert werden, die für die tägliche Arbeit benötigt werden, z. B. Javascript.

keine Passwörter abspeichern

Einige Browser bieten die Möglichkeit, persönliche Informationen oder Passwörter abzuspeichern, damit diese automatisch in WWW-Formulare eingetragen bzw. als Authentisierungsdaten an den WWW-Server gesendet werden können und somit nicht jedes Mal eingetippt werden müssen. Der Internet Explorer bietet dies z. B. unter dem Stichwort *AutoVervollständigen* an. Diese Funktion sollte nicht verwendet werden, da sonst die Gefahr besteht, dass unbeabsichtigt Passwörter, persönliche Informationen oder Informationen über die Behörde bzw. das Unternehmen weitergegeben werden.

anonymer FTP-Zugriff

Auch für den Zugriff auf FTP-Server bieten einige Browser die Möglichkeit an, automatisch Benutzernamen und Passwörter zu übermitteln. Damit nicht unbeabsichtigt Passwörter an Dritte weitergegeben werden, sollte der Browser so konfiguriert werden, dass standardmäßig nur anonyme Anmeldungen erfolgen.

Dateien nicht automatisch öffnen!

Bei einigen Browsern kann konfiguriert werden, ob heruntergeladene Dateien automatisch geöffnet oder gespeichert werden sollen oder ob der Benutzer gefragt werden soll. Damit Dateien nicht versehentlich geöffnet oder gestartet werden, sollte diese Option auf *Speichern* oder *Benutzer fragen* eingestellt werden.

Mit Hilfe so genannter *Cookies* können WWW-Server auf dem Internet-PC Daten hinterlegen und später wieder abrufen. Diese Funktion wird häufig für virtuelle Warenkörbe bei Internet-Shops benötigt. Aus Sicht der IT-Sicherheit sind Cookies weitgehend unproblematisch. Allerdings lassen sich mit Hilfe von Cookies auch Profile über das Verhalten von Benutzern erstellen, so dass es u. U. aus Gründen des Datenschutzes wünschenswert ist, das Abspeichern von Cookies zu deaktivieren. Gängige Browser können auch so konfiguriert werden, dass der Benutzer gefragt wird, wenn ein WWW-Server versucht, ein Cookie zu setzen. Je nachdem, welche WWW-Angebote typischerweise genutzt werden, wird der Benutzer dadurch jedoch durch eine Vielzahl von Dialogfenstern belästigt und bei der Arbeit behindert. Es muss daher anhand des konkreten Anwendungsfalls entschieden werden, wie bei der Nutzung von Internet-PCs mit Cookies umgegangen wird.

SSL/TLS (Secure Sockets Layer/Transport Layer Security) sind Protokolle, mit denen die Kommunikation zwischen WWW-Server und WWW-Browser kryptographisch geschützt werden kann. Die Absicherung durch SSL/TLS sollte immer genutzt werden, wenn sie Server-seitig angeboten wird. Dies ist besonders wichtig bei der Übertragung personenbezogener Daten, beispielsweise wenn E-Mails vom Server abgeholt werden.

Für die Authentisierung der Kommunikationspartner können Zertifikate eingesetzt werden, in der Praxis werden meist jedoch nur SSL-Zertifikate für WWW-Server ausgestellt. Falls zusätzlich eine Authentisierung des Clients

erforderlich ist, erfolgt diese meist auf andere Weise, z. B. mit Hilfe von Benutzername und Passwort (siehe auch M 5.66 *Verwendung von SSL*).

SSL-Zertifikate überprüfen

Die Echtheit eines SSL-Zertifikats kann die Browser-Software meist anhand der digitalen Signatur einer Zertifizierungsstelle überprüfen. Die Zertifikate einiger etablierter Zertifizierungsstellen werden bei den gängigen Browsern mitgeliefert. Einige Server-Betreiber greifen jedoch auf andere Zertifizierungsstellen zurück, so dass die Echtheit des SSL-Zertifikats nicht direkt überprüft werden kann. Falls häufig auf einen solchen WWW-Server zugegriffen werden muss, sollte das Zertifikat der entsprechenden Zertifizierungsstelle in den Browser importiert werden, wenn es verfügbar ist. Um die Echtheit dieses Zertifikats sicherzustellen, sollte vor dem Import der so genannte *Fingerprint* auf einem unabhängigen Weg, z. B. via Fax, Telefon oder E-Mail, übermittelt und verglichen werden. Nur dann können Benutzer davon ausgehen, dass der Server tatsächlich zu dem gewünschten Betreiber gehört.

Um die Angriffs- und Missbrauchsmöglichkeiten bei WWW-Browsern zu minimieren, sollten grundsätzlich nur die Funktionen aktiviert werden, die zur Erledigung der Fachaufgabe benötigt werden.

Betrieb

Daten und Programme sollten von möglichst vertrauenswürdigen Quellen heruntergeladen werden. Hierfür bieten sich z. B. das Internet-Angebot des Herstellers bzw. Herausgebers der Informationen oder offizielle Spiegelserver ("Mirrors") an. Dateien und Programme aus dem Internet sollten auf Computer-Viren geprüft werden, wenn das entsprechende Dateiformat befallen werden kann. Dateien und Programme sollten daher nach dem Download nicht automatisch aus dem Browser heraus geöffnet bzw. gestartet, sondern zunächst abgespeichert werden.

Cookies regelmäßig entfernen

Wie bereits oben erläutert, können Cookies auch dazu verwendet werden, Profile über das Verhalten von Benutzern zu erstellen. Falls das Speichern von Cookies grundsätzlich erlaubt wird, sollten sie daher regelmäßig gelöscht werden. Dies geschieht entweder aus dem Browser heraus oder durch Löschen der entsprechenden Datei, in der die Cookies gespeichert werden. Im Internet sind eine Reihe von Shareware-Tools verfügbar, mit denen die Verwaltung gespeicherter Cookies möglich ist.

Achtung: Cache kann vertrauliche Daten enthalten!

Der *Cache* eines Browsers dient dazu, WWW-Seiten lokal zwischenzuspeichern, damit sie nicht neu aus dem Internet geladen werden müssen, wenn der Benutzer sie noch einmal aufruft. Dies verkürzt die Antwortzeiten bei der WWW-Nutzung. Besonders beim "Einkauf über das Internet" werden oftmals vertrauliche Informationen, z. B. Kreditkartennummern, übertragen. Diese Informationen werden unter Umständen im Cache des Browsers zwischengespeichert. Dadurch besteht die Gefahr, dass diese Informationen unberechtigterweise aus dem Cache ausgelesen und missbraucht werden. Falls der Zugang zum Internet-PC nicht wirksam geschützt ist, sollte der Cache des Browsers daher nach der Übertragung von vertraulichen Informationen gelöscht werden. Alternativ kann die Cache-Funktion auch bei der Konfiguration vollständig deaktiviert werden.

Ergänzende Kontrollfragen:

- Werden alle Software-Komponenten aus vertrauenswürdigen Quellen bezogen?
- Ist die Ausführung aktiver Inhalte entsprechend den Vorgaben in den Richtlinien für den Internet-PC konfiguriert?
- Werden heruntergeladene Dateien mit einem Viren-Schutzprogramm geprüft, bevor sie geöffnet bzw. gestartet werden?

M 5.94 Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsbeauftragter

Verantwortlich für Umsetzung: Administrator

E-Mail ist einer der wichtigsten Intranet- und Internet-Dienste. In der modernen Bürokommunikation wird E-Mail als Ergänzung, teilweise auch als Ersatz für die klassischen Kommunikationswege, wie Telefon, Telefax, Brief und Fernschreiber, verwendet. Eine erhebliche Aufwertung hat der E-Mail-Verkehr auch durch die Möglichkeit erfahren, Dateien in Form von *Attachments* zu transportieren. Dadurch wird E-Mail vielfach auch als Groupware-Lösung benutzt, beispielweise wenn mehrere Kommunikationspartner nacheinander an einem Dokument arbeiten.

Webmail-Dienste als Alternative

Auf technischer Ebene gibt es unterschiedliche Verfahren, E-Mail zu nutzen. Eine Möglichkeit ist die Verwendung von Webmail-Diensten, wie sie von mehreren Dienstleistern im Internet angeboten werden, z. B. Web.de oder gmx. Diese Angebote stellen dem Benutzer alle benötigten Funktionen zum Empfangen, Lesen, Verfassen, Senden und Verwalten von E-Mails über eine WWW-Schnittstelle zur Verfügung. Die Nutzung geschieht somit - wie jedes andere WWW-Angebot - über einen Browser. Die Vorteile von Webmail-Diensten sind,

- dass neben dem Browser keine weiteren Software-Komponenten auf dem Client installiert werden müssen und
- dass der Benutzer daher für die Nutzung von E-Mail nicht an einen bestimmten Computer oder Ort gebunden ist.

Nachteilig ist jedoch, dass die Sicherheit der E-Mail-Nutzung weitgehend in der Hand des Webmail-Providers liegt. Empfehlungen zur sicheren Nutzung von Webmail finden sich in Maßnahme M 5.96 *Sichere Nutzung von Webmail*.

POP3, IMAP und SMTP

Das klassische Verfahren für die Nutzung von E-Mail ist die Verwendung eines entsprechenden Client-Programms, beispielsweise Microsoft Outlook, Outlook Express, Netscape Messenger oder KMail. Um eingehende E-Mail vom Provider abzuholen, wird meist das Protokoll POP3 (Post Office Protocol Version 3) oder IMAP (Internet Message Access Protocol) verwendet. Ausgehende E-Mail wird mit Hilfe des Protokolls SMTP (Simple Mail Transfer Protocol) versendet. Hierzu müssen bei der Konfiguration des Client-Programms die Adressen der Server für ausgehende und eingehende E-Mails eingetragen werden. Es wird empfohlen, die IP-Adressen dieser Server beim Provider zu erfragen und fest im Client-Programm einzustellen.

Absicherung durch TLS/SSL

Bevor eingehende E-Mail vom Provider zum Client übertragen werden kann, muss sich der Client in der Regel beim E-Mail-Server authentisieren. Diese Authentisierung geschieht meist durch ein Passwort, das im Klartext an den jeweiligen Server übermittelt wird, wenn keine zusätzlichen Sicherheitsmaßnahmen eingesetzt werden. Dadurch besteht die Gefahr, dass das Passwort beim Transport über das Internet mitgelesen und anschließend missbraucht wird. Um dies zu verhindern, sollte die gesamte Kommunikation mit dem E-Mail-Server mit Hilfe von TLS/SSL verschlüsselt werden. Dies schützt

auch die E-Mails bei der Übertragung vor Kompromittierung und Manipulation. Die Möglichkeit, den Zugriff über POP3 oder IMAP mit Hilfe von TLS/SSL abzusichern, bieten inzwischen viele Provider an (siehe auch RFC 2595).

Sicheres E-Mail-Passwort

Das Passwort für den Zugriff auf den E-Mail-Server beim Provider sollte ausreichend lang und nicht leicht zu erraten sein, damit Unbefugte nicht auf die E-Mail zugreifen können. Es sollte außerdem regelmäßig gewechselt werden. Die Frage, ob das E-Mail-Passwort auf dem Internet-PC abgespeichert werden darf oder ob es bei jedem Zugriff neu eingegeben werden muss, kann nicht allgemein beantwortet werden. Dies hängt davon ab, wie viele Authentisierungsprozesse der Benutzer insgesamt durchlaufen muss (Anmeldung am Client, Einwahl beim ISP, usw.) und wie groß die Gefahr durch missbräuchliche Nutzung eingeschätzt wird. Weitere Empfehlungen zu Passwörtern sind in Maßnahme M 2.11 *Regelung des Passwortgebrauchs* aufgeführt.

E-Mails im Text- oder RTF-Format erstellen

Einige E-Mail-Clients bieten die Möglichkeit, E-Mails im HTML- oder Rich Text Format (RTF) zu erstellen. Beim HTML-Format besteht das Problem, dass darin auch aktive Inhalte, z. B. Javascript, und Verweise auf andere Objekte im Internet enthalten sein können. Dies hat schon mehrfach zu Sicherheitsproblemen geführt. Daher sollten keine E-Mails im HTML-Format versendet werden. Falls unbedingt Formatierungselemente, wie z. B. Schriftart und Farbe, benötigt werden, ist stattdessen das RTF-Format zu verwenden. Die Client-Programme sollten daher so konfiguriert werden, dass sie E-Mails im reinen Text-Format oder im RTF-Format erstellen und versenden.

Umgang mit E-Mails im HTML-Format

Für eingehende HTML-formatierte E-Mails sollte der Client so konfiguriert werden, dass er bei der Anzeige solcher E-Mails keine aktiven Inhalte ausführt. Einige E-Mail-Clients zeigen HTML-formatierte E-Mails nicht selbst an, sondern starten einen externen Viewer oder Browser. In diesem Fall sollte ein Viewer bzw. Browser verwendet werden, der keine aktiven Inhalte ausführt. Außerdem sollte sichergestellt sein, dass beim Lesen der E-Mail keine Zugriffe auf andere Objekte im Internet erfolgen, beispielsweise indem die Internet-Verbindung vorher getrennt wird. Alternativ können HTML-formatierte E-Mails auch mit einem reinen Text-Editor geöffnet werden. Aufgrund der enthaltenen Steuerelemente (*Tags*) lässt sich der Inhalt dabei jedoch meist schwer lesen.

Vorschau-Funktion deaktivieren

Einige Client-Programme bieten eine Vorschau-Funktion für E-Mails an. Dabei wird der Inhalt einer ausgewählten E-Mail angezeigt, ohne dass sie explizit vom Benutzer geöffnet wurde. Dadurch besteht die Gefahr, dass schädliche Inhalte in E-Mails unbeabsichtigt ausgeführt werden. Die Vorschau-Funktion sollte daher deaktiviert werden.

Attachments mit Viren-Schutzprogramm prüfen

Attachments, d. h. Dateien, die als Anlage zum eigentlichen Text in der E-Mail enthalten sind, sind ein beliebtes Transportmedium für Computer-Viren, Würmer und andere Schadprogramme. Die im E-Mail-Programm angezeigte Dateinamenserweiterung (*.jpg*, *.exe*, usw.) stimmt außerdem nicht immer mit dem tatsächlichen Dateityp überein. Es gibt Techniken, mit denen in bestimmten Client-Programmen die tatsächliche Dateinamenserweiterung verborgen werden kann. Attachments in eingehenden E-Mails sollten daher grundsätzlich mit Misstrauen behandelt werden, insbesondere wenn die Übersendung nicht abgesprochen oder der Absender unbekannt ist. Vor dem

Öffnen bzw. Starten sollten Attachments abgespeichert und mit einem Viren-Schutzprogramm geprüft werden.

Vorsicht bei merkwürdigen E-Mails oder Attachments

Ausführbare Dateien und Dateien, die Änderungen an der Systemkonfiguration vornehmen können, beispielsweise *.exe*, *.vbs*, *.reg* unter Windows oder Shell-Skripten unter Linux, sollten nicht ohne Zustimmung der Administration gestartet werden. Vorsicht ist auch bei Attachments geboten, die offenbar keinen Bezug zur üblichen Geschäftsbeziehung mit dem Absender haben, z. B. Erotik-Angebote vom Steuerberater, oder wenn die E-Mail in einer anderen Sprache als sonst verfasst ist. Bei solchen Auffälligkeiten sollten die eventuell enthaltenen Attachments zunächst nicht geöffnet, sondern die Administration oder der IT-Sicherheitsbeauftragte verständigt werden. Zur Klärung kann auch beim Absender nachgefragt werden, was es mit den Attachments auf sich hat.

nicht Makro-fähige Viewer verwenden

Unter Windows sollten möglichst nur solche Programme als Standardapplikationen konfiguriert werden, die keine Makros bzw. eingebetteten Skripten ausführen können. Für die meisten verbreiteten Dokumenten- bzw. Dateitypen, z. B. Word- oder Excel-Dateien, sind entsprechende Viewer verfügbar. Auf die Installation der vollwertigen Anwendungsprogramme, beispielsweise Microsoft Office, sollte nach Möglichkeit ganz verzichtet werden. Anstelle der Default-Einstellung *Zusammenführen* sollte für den Dateityp *.reg* ein Editor als Standardapplikation konfiguriert werden. Anderenfalls werden die in der Datei enthaltenen Registry-Einträge bei einem Doppelklick oder bei einem anderweitig ausgelösten Öffnen der Datei in die Registry des Internet-PCs eingetragen. Durch diese Konfigurationsänderung können u. a. Sicherheitseinstellungen ungewollt deaktiviert werden. Die Standardapplikation für Dateitypen kann vom Explorer aus über das Dialogfeld *Ansicht* | *Optionen* | *Dateitypen* geändert werden.

Verschlüsselung und digitale Signaturen

Auch via E-Mail werden in vielen Fällen Informationen übertragen, deren Vertraulichkeit und Integrität beim Transport vom Sender zum Empfänger geschützt werden müssen. Hierfür können Verschlüsselung und digitale Signaturen eingesetzt werden. Problematisch ist dabei, dass sich unterschiedliche Verfahren, wie S/MIME, GnuPG bzw. PGP und MailTrusT, für die kryptographische Absicherung von E-Mail etabliert haben, die gar nicht oder nur teilweise interoperabel sind. Bevor Verschlüsselung oder digitale Signatur für E-Mails eingesetzt werden kann, muss daher eine Abstimmung mit den Kommunikationspartnern darüber erfolgen, welches oder welche Verfahren verwendet werden (siehe auch M 5.63 *Einsatz von GnuPG oder PGP*). Die hierzu benötigten Software-Komponenten werden häufig als Plug-Ins für gängige E-Mail-Programme angeboten. Falls mehrere verschiedene Plug-Ins zur E-Mail-Verschlüsselung verwendet werden sollen, ist darauf zu achten, dass keine technischen Probleme dadurch entstehen, dass diese in das gleiche E-Mail-Programm installiert werden.

Lese- und Empfangsbestätigungen

Beim Empfang bzw. beim Lesen eingehender Nachrichten bieten gängige E-Mail-Programme die Möglichkeit, Empfangs- oder Lesebestätigungen anzufordern. Für eine Empfangsbestätigung muss der Server des Empfängers den DSN-Standard (Delivery Service Notification) unterstützen, für eine Lesebestätigung muss der E-Mail-Client den MDN-Standard (Message Disposition Notification) unterstützen. Abhängig vom E-Mail-Client kann dieser so einge-

stellt werden, dass er eine Bestätigungsanforderung immer, nie oder nur bei bestimmten Absender(kreisen) beantwortet.

Aus Sicht der IT-Sicherheit sind solche Bestätigungsnachrichten in der Regel unproblematisch. Im Zusammenhang mit Werbe-E-Mails, die unspezifisch an eine große Anzahl von E-Mail-Adressen versendet werden, kann diese Funktion jedoch unerwünscht sein. Dem Absender wird dadurch signalisiert, dass die jeweilige E-Mail-Adresse existiert und ggf. auch dass die Werbe-E-Mail gelesen wurde.

Vorsicht bei automatischer E-Mail-Weiterleitung

Eingehende oder ausgehende E-Mails können bei einigen E-Mail-Clients auf Wunsch automatisch an einen festgelegten E-Mail-Empfänger oder eine Verteilerliste gesendet werden, beispielsweise als BCC (Blind Carbon Copy). Beim Netscape Messenger 4.7 findet sich diese Funktion z. B. unter *Einstellungen | Mail & Diskussionsforen | Kopien und Ordner | BCC an andere*. Diese Funktion sollte nur verwendet werden, wenn sichergestellt ist, dass alle Personen, die auf die dort eingetragene E-Mail-Adresse zugreifen können, alle eingehenden bzw. ausgehenden E-Mails lesen dürfen. Anderenfalls besteht die Gefahr, dass vertrauliche Informationen ungewollt an Dritte weitergegeben werden.

Bei einigen Versionen des Betriebssystems Windows wird das Client-Programm Outlook Express mitgeliefert. Falls dieses Programm nicht benötigt wird, z. B. weil ein anderes Client-Programm eingesetzt oder ein Webmail-Dienst genutzt wird, sollte Outlook Express deinstalliert werden.

Für alle auf dem Internet-PC installieren Software-Komponenten muss sichergestellt sein, dass alle verfügbaren sicherheitsrelevanten Patches und Updates zeitnah eingespielt werden.

Ergänzende Kontrollfragen:

- Wird das Passwort für den Zugriff auf den E-Mail-Server regelmäßig gewechselt?
- Werden E-Mails entweder im reinen Text- oder im RTF-Format erstellt und versendet?
- Werden Attachments in eingehenden E-Mails mit einem Viren-Schutzprogramm geprüft, bevor sie geöffnet oder gestartet werden?

M 5.95 Sicherer E-Commerce bei der Nutzung von Internet-PCs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsbeauftragter

Verantwortlich für Umsetzung: Administrator

Das Internet wird heute nicht nur zur Informationsgewinnung und Kommunikation, sondern auch intensiv als Plattform für die Abwicklung von Geschäfts- oder Verwaltungsvorgängen genutzt. Beispiele hierfür sind Online-Bestellungen, Konto- oder Wertpapiertransaktionen und E-Government-Anwendungen.

höhere Sicherheitsanforderungen

E-Commerce- und E-Government-Anwendungen haben in der Regel höhere Sicherheitsanforderungen als die reine Informationsgewinnung über das World Wide Web. Insbesondere muss sichergestellt werden, dass Online-Transaktionen und -Bestellungen bei der Verarbeitung auf dem Internet-PC und bei der Übertragung über das Internet nicht manipuliert werden. Falls ein Internet-PC auch für E-Commerce oder E-Government-Anwendungen genutzt wird, sollten daher die nachfolgenden Empfehlungen berücksichtigt werden.

Datenschutz und Sicherheit beim Anbieter berücksichtigen

Bevor eine Geschäftsbeziehung mit einem Anbieter über das Internet aufgenommen wird, sollte geprüft werden, ob dessen Grundsätze in Bezug auf Datenschutz und Datensicherheit mit den eigenen Anforderungen vereinbar sind. Der Anbieter sollte hierzu Informationen auf dem Webserver bereitstellen.

Schutz vor Schadprogrammen

Zum Schutz vor Computer-Viren, Trojanischen Pferden und anderen Schadprogrammen muss ein Viren-Schutzprogramm installiert werden, dessen Datenbank regelmäßig aktualisiert wird. Weitere Empfehlungen hierzu finden sich in Baustein B 1.6 *Computer-Viren-Schutzkonzept* und Maßnahme M 4.3 *Regelmäßiger Einsatz eines Viren-Schutzprogramms*.

regelmäßige Datensicherung

Die für die E-Commerce- bzw. E-Government-Anwendungen erforderlichen Datenbestände und Konfigurationseinstellungen müssen regelmäßig gesichert werden (siehe auch M 6.79 *Datensicherung beim Einsatz von Internet-PCs*). Andernfalls besteht die Gefahr, dass die Anwendung beim Ausfall des Internet-PCs oder bei versehentlicher Löschung nicht zeitnah wiederhergestellt oder getätigte (Trans)aktionen nicht nachvollzogen werden können.

Patches und Updates einspielen

Falls für die Anwendung spezielle Software-Komponenten, z. B. Online-Banking-Programme, benötigt werden, sollten diese ausschließlich von vertrauenswürdigen Quellen bezogen werden, möglichst direkt vom Anbieter bzw. Hersteller. Für diese Software-Komponenten muss regelmäßig geprüft werden, ob sicherheitsrelevante Patches oder Updates existieren. Diese müssen eingespielt werden. Software und Updates sind vor der Installation auf Schadprogramme zu prüfen.

fester Benutzer bei regelmäßiger Nutzung

Falls ein Internet-PC regelmäßig für E-Commerce- oder E-Government-Anwendungen genutzt wird, sollte er einem festen Benutzer zugeordnet und ausschließlich für diese Anwendungen verwendet werden. Anderenfalls besteht die Gefahr, dass später nicht nachvollziehbar ist, welcher Benutzer eine bestimmte Aktion vorgenommen hat.

Bei vielen Anwendungen im E-Commerce und E-Government wird der WWW-Browser als Client-Programm verwendet. Als Schutzmechanismus für

die Übertragung kommt dabei in der Regel das TLS/SSL-Protokoll zum Einsatz. Dabei werden Vertraulichkeit und Integrität der Daten mit Hilfe kryptographischer Verfahren geschützt. Eine TLS/SSL-Verbindung erkennt man im Browser daran, dass die Adresse (URL) mit *https:* statt mit *http:* beginnt, und bei den gängigen Browsern auch an einem besonderen Symbol, z. B. einem geschlossenen Schloss.

TLS/SSL-Protokoll nutzen

Webbasierte E-Commerce- und E-Government-Anwendungen sollten ausschließlich über TLS/SSL genutzt werden. Der Anbieter sollte die gesamte Web-Anwendung über TLS/SSL bereitstellen. Es ist darauf zu achten, dass ein Browser verwendet wird, der starke kryptographische Verfahren unterstützt, insbesondere 128 Bit Schlüssellänge. Dies ist bei einigen älteren Browsern aufgrund von Export-Restriktionen nicht der Fall.

Server-Zertifikate sporadisch überprüfen

Für die Authentisierung des WWW-Servers kommen beim TLS/SSL-Protokoll Zertifikate zum Einsatz. Bei der Nutzung von E-Commerce- oder E-Government-Anwendungen über TLS/SSL sollten die Benutzer sporadisch überprüfen, ob das Server-Zertifikat gültig ist und ob sie tatsächlich mit dem gewünschten Server verbunden sind. Hierzu ist es erforderlich, dass die Benutzer für die Bedienung des WWW-Browsers geschult werden und ihnen Hinweise zur Verfügung gestellt werden, wie sie die Überprüfung bei der konkreten Installation und Konfiguration vornehmen.

Ergänzende Kontrollfragen:

- Wird ein Viren-Schutzprogramm eingesetzt und dessen Datenbank regelmäßig aktualisiert?
- Werden die Daten der E-Commerce- bzw. E-Government-Anwendung regelmäßig gesichert?
- Wird ein Browser verwendet, der starke Verschlüsselung unterstützt?

M 5.96 Sichere Nutzung von Webmail

Verantwortlich für Initiierung: Administrator, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer, Administrator

Nicht jede Institution betreibt einen eigenen Mailserver, sondern nutzt die entsprechenden Dienstleistungen von externen Anbietern. Dabei ist Webmail eine einfache, benutzerfreundliche Variante, um über die Webserver der Anbieter auf Maildienste zuzugreifen. Mit Webmail werden alle Internet-basierten E-Mail-Dienste bezeichnet, bei denen zur Benutzung nur ein Browser als Client und eine Internet-Anbindung benötigt wird. Dazu gehören z. B. die Angebote von Web.de, Freenet.de oder gmx.de. Webbasierte E-Mail-Dienste erlauben den Zugriff auf E-Mails unabhängig vom Ort und Provider.

Bei der ersten Anmeldung bei einem Webmail-Dienstleister müssen in der Regel Name und Adresse des Benutzers, die gewünschte E-Mail-Adresse und ein Zugangspasswort angegeben werden. Einige Anbieter verlangen eine schriftliche Bestätigung der Anmeldung. Das gewählte Passwort dient bei nachfolgenden Anmeldungen zur Authentisierung. Der Benutzer erhält dann ein oder mehrere E-Mail-Adressen sowie ein Benutzerkonto, über das E-Mail empfangen, weiterverarbeitet und gesendet werden kann.

Es gibt eine Vielzahl von Anbietern von Webmaildiensten, viele davon bieten ihre Dienstleistungen sogar kostenlos an. Es ist zu beachten, dass diese sich nicht nur im Funktionsumfang unterscheiden (z. B. Postfachgröße, Fax, SMS, Spamfilter, etc.), sondern auch das Sicherheitsniveau stark variieren kann, bis hin zu gravierenden Sicherheitslücken.

Bei der Auswahl eines Dienstleisters sollte daher sorgfältig vorgegangen werden. Wichtig sind insbesondere die folgenden Punkte:

- **Geschäftsbedingungen**
  Die Allgemeinen Geschäftsbedingungen (AGBs) sollten zunächst einmal überhaupt auffindbar und abrufbar sein, außerdem sollten sie verständlich sein und keinen unakzeptablen Bedingungen enthalten. Letzteres heißt u. a., dass der Datenschutz gewährleistet sein sollte. Der Kunde sollte also nicht der Weitergabe seiner personenbezogenen Daten zustimmen müssen, was häufig in Werbeflut resultiert. Ebenso sollten gravierende Änderungen der Dienstleistungen und Kostenstrukturen rechtzeitig angekündigt werden, damit die Kunden reagieren können (z. B. Posteingänge umleiten, Postfächer sichern).
- **Erreichbarkeit**
  Bei Vielreisenden ist ein weltweiter Zugriff auf die Postfächer wichtig. Außerdem sollte generell getestet werden, wie lange der Versand bzw. Empfang von E-Mails dauert.
- **Service**
  Neben der Benutzerfreundlichkeit des Angebotes sollte auch untersucht werden, ob Onlinehilfen, FAQs oder andere Dokumentation vorhanden ist. Außerdem sollte die Erreichbarkeit und Kompetenz des Supportteams hinterfragt werden (per E-Mail, Telefon oder Fax).
- **Sicherheit**
  Bei der Bewertung der Sicherheit des Angebotes sollten die technischen und organisatorischen Sicherheitsvorkehrungen betrachtet werden:
  - Es sollte möglich sein, über eine verschlüsselte Verbindung auf das Benutzerkonto zuzugreifen, z. B. über SSL.

- Die E-Mail sollte verschlüsselt bzw. digital signiert werden können.
- Es ist zu hinterfragen, ob eine Prüfung der Identität von Neukunden stattfindet, ob es beispielsweise möglich ist, sich unter falschem Namen oder falscher Adresse anzumelden oder sich fehlleitende E-Mailadressen wie *support@...* auszusuchen. Die Identität des Kunden sollte postalisch geprüft werden.

Identitätsprüfung der Kunden

- Jeder kann einmal ein Passwort vergessen. Trotzdem ist es kein gutes Zeichen, sondern falsch verstandene Benutzerfreundlichkeit, wenn man bei der Hotline ohne große Nachfragen ein neues Passwort erhält. Hier müssen vernünftige Sicherheitsüberprüfungen eingebaut sein.

Sicherheitsmechanismen bei vergessenem Passwort

- Für den Zugriff auf die Webmail-Dienste sollten keine aktiven Inhalte akzeptiert werden müssen (Java, JavaScript, ActiveX).
- Eine Virenprüfung der ein- und ausgehenden E-Mail sollte selbstverständlich sein.
- Spamfilterung sollte möglich sein.

Auch bei der Nutzung von Webmail-Diensten sind einige Punkte zu beachten:

- Das Passwort für den Zugriff auf die Webmail-Dienste sollte geeignet gewählt sein, also lang genug (mindestens 8 Stellen) und kompliziert genug (Zahlen, Buchstaben und Sonderzeichen). Das Passwort sollte regelmäßig gewechselt werden. Es darf auf keinen Fall auf dem PC abgespeichert oder am PC aufbewahrt werden. Weitere Hinweise zur Passwortauswahl finden sich in M 2.11 *Regelung des Passwortgebrauchs*.

sicherer Passwortgebrauch

- Für den Zugriff auf das Benutzerkonto sollte SSL benutzt werden.
- E-Mail sollte möglichst verschlüsselt bzw. digital signiert werden. Hierzu ist in der Regel eine Abstimmung mit dem Empfänger darüber erforderlich, welche kryptographischen Verfahren und Programme hierfür auf beiden Seiten zur Verfügung stehen.
- Auch wenn der Anbieter Virenschutz verspricht, sollten Dateianhänge außerdem auf dem eigenen Rechner auf Viren überprüft werden.
- Eingehende E-Mails sollten regelmäßig gelesen werden. Wichtige E-Mails sollten lokal gespeichert werden. Außerdem sollten die Postfächer regelmäßig aufgeräumt werden, also lokal bereits gespeicherte oder unwichtige E-Mails gelöscht werden. Darüber hinaus sollten die Postfächer regelmäßig auf lokale Datenträger gespeichert werden, aber auch die lokal gespeicherten E-Mails sorgfältig gesichert werden.

Postfächer regelmäßig aufräumen

- Der Webmail-Dienst sollte immer über den Log-Out-Button oder ähnliche Mechanismen verlassen werden, damit keine anderen Benutzer des lokalen PCs auf die Webmail zugreifen können.

HTML-formatierte E-Mails können Sicherheitsprobleme verursachen (siehe G 5.103 *Missbrauch von Webmail*). Es sollte vermieden werden, HTML-formatierte E-Mails oder solche mit aktiven Inhalten zu versenden. Der Provider sollte die Möglichkeit anbieten, dass eventuell in eingehender E-Mail enthaltene aktive Inhalte herausgefiltert werden. Außerdem sollten E-Mail-

Clients gewählt werden, bei denen HTML-formatierte E-Mails als solche zu erkennen sind, damit der Benutzer diese nicht unbewusst öffnet.

Ergänzende Kontrollfrage:

- Gibt es Regelungen für die Nutzung von Webmail-Diensten?

M 5.97 Absicherung der Kommunikation mit Novell eDirectory

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Der Datenaustausch zwischen eDirectory-Client und -Server erfolgt über Netzverbindungen. Je nach eDirectory-System und Netzstruktur werden die Kommunikationspakete, die neben Verzeichnisinhalten unter Umständen auch Authentisierungsinformationen enthalten können, ungeschützt übertragen.

Dabei können abhängig vom installiertem Betriebssystem unterschiedliche Netzprotokolle zum Einsatz kommen. So kann ein Zugriff auf eDirectory sowohl über das Novell-eigene NDAP erfolgen, das auf dem *Netware Core Protocol* (NCP) aufsetzt, als auch über das standardisierte Protokoll LDAP. Der Transport der Daten erfolgt dabei für NDAP über IP- oder IPX-Netze und für LDAP ausschließlich über IP-Netze.

NDAP-Zugriffe nur im Intranet zulassen

Die Benutzer-Authentisierung beim Zugriff über NDAP erfolgt nach einem proprietären Verfahren, das keine Authentisierungsdaten direkt über das Netz transportiert. Die Kommunikation zwischen Client und Server wird jedoch bei Verwendung von NDAP nicht grundsätzlich verschlüsselt, es ist die Angelegenheit des eingesetzten (NDAP-Clients, die Verschlüsselung der Kommunikation zu sicherzustellen. Daher sollte der Zugriff auf eDirectory über dieses Protokoll nur innerhalb des Intranets möglich sein.

externe Zugriffe durch VPN absichern

Soll von außen über NDAP auf einen eDirectory-Server zugegriffen werden, so ist eine entsprechende Absicherung der Kommunikationsverbindung zwischen Client und Server zu realisieren, die die Vertraulichkeit der übertragenen Daten hinreichend schützt. Dies kann z. B. durch Verwendung eines *Virtuellen Privaten Netzes* (VPN) erreicht werden.

Der Zugriff auf eDirectory über LDAP bietet spezielle Möglichkeiten zur Verschlüsselung (Einsatz von SSL) aber auch spezielle Risiken (Einrichtung des anonymen Zugriffs). Auf diese Sicherheitsaspekte wird in Maßnahme M 4.158 *Einrichten des LDAP-Zugriffs auf Novell eDirectory* eingegangen.

Weiterhin können Administratoren über einen Fernzugang auf das System zugreifen. Ein Beispiel hierfür ist das Novell-eigene Werkzeug *iMonitor*, mit dem über einen Browser auf Daten des Systemmonitors zugegriffen werden kann (siehe M 4.160 *Überwachen von Novell eDirectory*).

Monitor-Zugriff beschränken und schützen

Da die im iMonitor verfügbaren Daten wesentliche Einblicke in den Aufbau und die Konfiguration einer eDirectory-Installation geben, muss auch dieser indirekte Zugang zum eDirectory abgesichert werden. Es sollte deshalb nur autorisierten Benutzern möglich sein, über HTTP auf den iMonitor zuzugreifen. Die Übertragung sollte außerdem durch TLS/SSL geschützt werden (siehe M 5.66 *Verwendung von SSL*).

Beispiel: Steht ein eDirectory-Server für den LDAP-Zugriff von außen innerhalb des Screened-Subnet eines Firewall-Systems, so sollte auf diesen Server kein HTTP-Zugriff möglich sein.

Ergänzende Kontrollfragen:

- Werden Zugriffe auf Daten des eDirectory über Außenverbindungen verhindert?
- Von wo ist der Zugriff auf Systemdaten des eDirectory über das Werkzeug *iMonitor* möglich?

M 5.98 Schutz vor Missbrauch kostenpflichtiger Einwahlnummern

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Kostenpflichtige Internet-Angebote werden häufig über die Telefonrechnung abgerechnet, indem die Benutzer über spezielle Einwahl-Programme auf kostenintensive Telefonnummern umgelenkt werden. Dies können beispielsweise 0900er Nummern sein.

Die dafür benutzten Webdialer sind Programme, die auf dem Rechner einen neuen Internetzugang einrichten. Nach dem Download und der Installation auf dem PC wählt sich der Dialer ins Internet ein. Eine zu dieser Zeit bereits bestehende Internetverbindung wird in der Regel zuvor getrennt. (Dies funktioniert allerdings nur über Wählzugänge, nicht jedoch über DSL oder ähnliche Techniken.)

Die kostenpflichtigen Inhalte können dann über diese Verbindung abgerufen werden. Dabei ist die vom Webdialer benutzte Einwahlnummer maßgeblich für die Höhe der anfallenden Kosten. Sowohl pro Einwahl als auch pro Zeiteinheit können hohe Gebühren anfallen.

Was ursprünglich als einfache und anonyme Zahlungsmethode im Internet gedacht war, wird leider in letzter Zeit zunehmend missbraucht, um auf Internet-PCs vom Benutzer unbemerkt solche Webdialer zu installieren. Solche Webdialer können z. B. über Trojanische Pferde oder beim Aufruf einer Webseite unauffällig installiert werden. Sie verursachen dann massiv Kosten, ohne dass die Benutzer dies merken und ohne dass dem eine angemessene Leistung gegenübersteht.

Um sich vor solchen Problemen zu schützen,

- sollten die Benutzer darüber aufgeklärt werden, was Webdialer sind und wie sich solche bösartigen Programme verbreiten,
- zu jedem Internet-PC sollten Einzelverbindungsnachweise vom Telekommunikationsanbieter verlangt werden (Dies ist in Deutschland kostenlos.),
- sollte erwogen werden, "teure" Telefonnummern, wie 0900er Nummern generell oder bestimmte Nummernblöcke, sperren zu lassen,
- sollten aktive Inhalte, insbesondere ActiveX, möglichst deaktiviert werden.

Generell sollten keine Programme installiert werden, die angeblich kostenlose oder schnellere Verbindungen zu Web-Seiten mit dubiosen Inhalten versprechen.

M 5.99 SSL/TLS-Absicherung für Exchange 2000

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

In vielen Einsatzszenarien ist die Verschlüsselung der Übertragungswege zwischen einem Client und einem Exchange 2000 Server sinnvoll oder erforderlich. Dies betrifft besonders die Übertragung sensitiver Daten über nicht vertrauenswürdige Kommunikationswege, wie beispielsweise das Internet. In einer Exchange 2000 Umgebung kann hierfür das SSL- bzw. TLS-Protokoll (siehe auch M 5.66 *Verwendung von SSL* eingesetzt werden. Die Entscheidung über einen optionalen oder erzwungenen Einsatz von SSL/TLS sollte vom Standort der zugreifenden Clients und dem Schutzbedarf der übertragenen Daten abhängig gemacht werden.

Die Verschlüsselung der Übertragungsstrecke ermöglicht auch die Verwendung von schwächeren Authentisierungsmechanismen, wie z. B. die Kennwort-basierte *HTTP Basic Authentisierung*.

Absicherung der Client-Server-Kommunikation

Outlook Web Access

Eines der möglichen Szenarien für den Einsatz von SSL/TLS ergibt sich aus der Zugriffsmöglichkeit auf einen Exchange-Server über *Outlook Web Access* (OWA, siehe dazu auch M 4.164 *Browser-Zugriff auf Exchange 2000*). Die Verschlüsselung der Übertragungswege hat hier zwischen dem Web-Browser und dem IIS-Server zu erfolgen.

Remote Procedure Call

Ist ein Outlook 2000 Client als Exchange-Client konfiguriert, basiert die Kommunikation zwischen Outlook und Exchange auf RPC. Daher ist an dieser Stelle eine Absicherung des Datentransports mit SSL/TLS nicht ohne weiteres möglich. Die Kommunikation kann jedoch mit anderen Mitteln geschützt werden (siehe dazu M 4.162 *Sichere Konfiguration von Exchange 2000 Servern*).

Verwendet Outlook 2000 nur die Internet-Protokolle (POP3, IMAP4, SMTP, NNTP) beim Zugriff auf den Exchange-Server, so kann die Verbindung mit TLS abgesichert werden. Dies gilt generell auch für den Zugriff auf andere E-Mail-Server. Weitere Informationen dazu finden sich ebenfalls in der Maßnahme M 4.162 *Sichere Konfiguration von Exchange 2000 Servern*.

Absicherung der Server-Server-Kommunikation

Verschlüsselung

Die Server-Server-Kommunikation muss dann verschlüsselt werden, wenn sensitive Daten über ungesicherte Netze übertragen werden oder die Authentisierung mittels HTTP Basic Authentisierung stattfindet.

Die zur Verfügung stehenden Verschlüsselungsmechanismen hängen von den verwendeten Exchange-Connectors ab: Ein SMTP-Connector unterstützt die Verschlüsselung mittels TLS, ein X.400- oder ein Routing-Group-Connector dagegen nicht. Insofern ist bei der Wahl das Connectors auch darauf zu achten, welche Verschlüsselungsmechanismen dadurch benutzt werden können.

Ergänzende Kontrollfragen:

- Wurde das Zugriffsprotokoll der E-Mail-Clients auf Exchange 2000 festgelegt?
- Soll die Authentisierung der Clients über Passwörter oder Zertifikate erzielt werden?

M 5.100 Einsatz von Verschlüsselungs- und Signaturverfahren für die Exchange 2000 Kommunikation

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Verschlüsselung und digitale Signaturen dienen dem Schutz der Integrität und Vertraulichkeit sowie auch der Nicht-Abstreitbarkeit elektronisch übermittelter Nachrichten.

Für eine Absicherung der E-Mail-Kommunikation stehen entsprechend dem OSI-Schichtenmodell mehrere mögliche Lösungsansätze zur Verfügung:

- Auf physikalischer Ebene ist eine Linkverschlüsselung denkbar, jedoch im allgemeinen nicht praktikabel.
- Auf Netzebene ist die Einrichtung eines *Virtuellen Privaten Netzes* (*VPN*) möglich. Wegen der hohen Verbreitung des Internet-Protokolls IP wird dabei in der Regel der Standard IPSec verwendet. IPSec erlaubt die Absicherung von IP-Verbindungen zwischen Standorten, zwischen Endgeräten und auch von Endgeräten zu Standorten. Es können sowohl fest vorkonfigurierte Schlüssel (*preshared keys*) als auch Public Key Infrastrukturen (PKI) für das Schlüsselmanagement verwendet werden. Um auf Basis von IPSec eine Absicherung zu erreichen, müssen alle am E-Mail-Routing beteiligten Rechner über IPSec kommunizieren. An den Knotenpunkten liegt die Information jeweils im Klartext vor.

VPN

- Auf Nachrichten-Ebene haben sich in der Praxis die Standards S/MIME und PGP durchgesetzt. Das Schlüsselmanagement von S/MIME setzt den Betrieb einer PKI voraus. PGP setzt dagegen auf ein offenes Schlüsselmanagement und verlangt keinen Aufbau einer zentralen PKI.

S/MIME und PGP

Die Absicherung auf Nachrichten-Ebene wird von Drittherstellern in der Regel als Plug-In-Lösung für einen oder mehrere E-Mail-Clients realisiert. Im Projekt SPHINX werden Produkte verschiedener Hersteller auf übergreifende Interoperabilität untersucht. Weitere Informationen zu SPHINX finden sich auf dem Internet-Angebot des BSI (*http://www.bsi.bund.de*) und M 5.110 *Absicherung von E-Mail mit SPHINX (S/MIME)*.

Auch auf der Ebene des Dateisystems sind Lösungen, z. B. in Form von Shell-Erweiterungen, zur Verschlüsselung und Signatur einzelner Dateien verfügbar. Derart geschützte Dateien können dann als Dateianhänge via E-Mail versendet werden.

Public Key Infrastruktur

Outlook 2000 bietet einen eingebauten Mechanismus zur E-Mail-Verschlüsselung auf Basis von S/MIME. Dieser nutzt die Vertrauensbeziehungen einer Public Key Infrastruktur, die mit Hilfe der eigenen *Windows 2000 Enterprise CA* oder einer fremden CA betrieben werden kann. Die von einer CA selbstsignierten Wurzelzertifikate müssen dem System zur Verfügung stehen. Dazu sollten die als vertrauenswürdig geltenden Wurzelzertifikate zentral über eine Windows 2000 Gruppenrichtlinie konfiguriert werden.

Key Management Services

Als nächster Schritt zur Nutzung von Verschlüsselung und digitaler Signatur in *Outlook 2000* müssen die Benutzer ihre Schlüsselinformationen, bestehend aus dem Zertifikat (signierter öffentlicher Schlüssel) und dem zugehörigen privaten Schlüssel, erhalten. Die *Windows 2000 Enterprise CA* bzw. der Schlüsselverwaltungsdienst *Windows 2000 Key Management Services* (KMS) unterstützen eine organisationsweite Verteilung der Schlüsselpaare.

Hierzu muss zunächst eine *Windows 2000 Enterprise CA* mit wenigstens einem *Enrollment Agent* installiert werden. Danach lässt sich der KMS unter Verwendung eines *Exchange Certificate Templates* betreiben. Der Start des KMS wird innerhalb des *Exchange-Snap-Ins* der *Microsoft Management Console* (MMC) vorgenommen, und zwar unter dem Punkt *Advanced Security* | *Key Manager*.

Corporate or Workgroup Service Option

Weiterhin muss *Outlook 2000* mit der so genannten *Corporate or Workgroup Service Option* in der Organisation installiert sein. Nun lassen sich die Schlüsselinformationen der Benutzer verteilen.

Kennwörter

Standard-Kennwort ändern

Bei der Installation des Schlüsselverwaltungsdienstes wird ein Kennwort zum Starten des KMS generiert. Dabei stehen zwei Möglichkeiten zur Verfügung: das Kennwort ist bei jedem Start der KMS manuell einzugeben oder auf einer Diskette zu speichern, um so einen automatischen Start der KMS zu ermöglichen. Die manuelle Eingabe des Startkennworts wird als die sicherere Methode empfohlen.

Da während der KMS-Installation ein Standard-Kennwort für die spätere Administration festgelegt wird, muss dieses nach der Installation umgehend geändert werden.

Der KMS-Dienst unterstützt das Vier-Augen-Prinzip. Es wird empfohlen, folgende sicherheitsrelevante Aufgaben nur von (mindestens) zwei Administratoren erledigen zu lassen:

- Hinzufügen/Löschen von Administratoren und Modifizieren der Kennwort-Policy,
- Wiederherstellung eines Benutzerschlüssels (key recovery),
- Import/Export von Benutzereinträgen.

Die Anzahl der erforderlichen Administratoren wird im *Exchange System Manager* unter *Key Manager* | *Properties* | *Passwords* festgelegt.

Auswahl geeigneter kryptographischer Algorithmen und Formate

Exchange 2000 bietet in seiner Konfiguration die Möglichkeit, zwischen zwei Formaten für verschlüsselte E-Mails zu wählen: S/MIME oder Exchange 4.0/5.0. Die Wahl des Formats hängt von den zu unterstützenden Clients ab. Beim geplanten Einsatz von *Outlook 2000* (auch *Outlook 98*) sollte das S/MIME-Format ausgewählt werden. *Exchange 2000* erlaubt weiterhin die Wahl eines bevorzugten Verschlüsselungsalgorithmus. Es wird empfohlen, für die Verschlüsselung den 3DES-Algorithmus zu verwenden. Die Einstellungen für das Verschlüsselungsformat und den bevorzugten Verschlüsselungsalgo-

rithmus werden im *Exchange System Manager* unter *Advanced Security* | *Encryption Configuration* | *Properties* | *Algorithms* vorgenommen.

X.509 v3

Der KMS-Dienst kann Benutzerzertifikate in zwei verschiedenen Zertifikatsversionen ausstellen: X.509 v1 und X.509 v3. Die Version 1 ist für die Kompatibilität mit Exchange 4.0 und 5.0 erforderlich. Besteht eine solche Forderung nicht, sollte die Version 3 verwendet werden. Diese Einstellungen finden sich im *Exchange System Manager* unter *Key Manager* | *Properties* | *Enrollment* | *Certificate Version*.

Schlüsselverteilung

manuelle Schlüsselverteilung

Die Schlüsselverteilung läuft generell in mehreren Phasen ab: die Erstellung der Schlüsselpaare und Sicherheitstoken durch einen Administrator, die Zustellung des Sicherheitstokens an die Benutzer und das Importieren der erzeugten Schlüssel durch die Benutzer.

Besonders sicherheitskritisch ist dabei die Zustellung der erzeugten Sicherheitstoken an die Benutzer. Hierfür bestehen zwei Möglichkeiten: Das Sicherheitstoken kann entweder manuell vom Administrator verteilt oder aber automatisch per E-Mail zugestellt werden. Da das Sicherheitstoken in einer E-Mail im Klartext übermittelt wird und somit unter Umständen von einem Angreifer mitgelesen werden kann, wird empfohlen, die standardmäßig eingestellte manuelle Verteilung beizubehalten.

Sollen die Benutzer über die Ausstellung des Sicherheitstokens automatisch benachrichtigt, das Sicherheitstoken selbst jedoch nicht automatisch in einer E-Mail übermittelt werden, wird folgende Vorgehensweise empfohlen: Die automatische Zustellung wird zwar aktiviert, aber die Vorlage für die automatische E-Mail-Benachrichtigung wird angepasst, indem die Variable *%TOKEN%* entfernt wird. Dies erfolgt im *Exchange System Manager* unter *Key Manager* | *Properties* | *Enrollment* | *Token distribution* | *Customize Message*.

Weitere Sicherheitsvorkehrungen

Um einen sicheren Betrieb zu gewährleisten, sind die folgenden Vorkehrungen zu treffen:

- Absicherung der eingesetzten Komponenten,
- Verwendung von Zertifikatsrückruflisten (Certificate Revocation List - CRL),
- Schulung der Administratoren,
- Schulung der Benutzer (speziell im Umgang mit verschlüsselten bzw. signierten Nachrichten).

Zusätzlich zu den allgemein bekannten Systemkomponenten von *Exchange 2000* müssen noch die Komponenten abgesichert werden, die für den Betrieb von Exchange mit Verschlüsselungs- und Signatur-Funktionalität zuständig sind. Dies sind vor allem die Zertifizierungsinstanz (CA), der *Key Management Service* (KMS) und die KMS-Datenbank (*Exchsrvr \ KMSData \ Kmsmdb.edb*).

Beim Rückruf eines oder mehrerer Benutzerzertifikate spielt die Gültigkeitsdauer der Zertifikatsrückrufliste eine wesentliche Rolle. Es wird empfohlen, die CRL nach einem Rückruf sofort zu veröffentlichen und nicht auf den nächsten eingeplanten Zeitpunkt der Veröffentlichung zu warten. Es ist jedoch zu beachten, dass durch die Veröffentlichung einer neuen CRL die alte Liste nicht ihre Gültigkeit verliert und somit die Clients, die bereits eine gültige CRL besitzen, von der neuen keinen Gebrauch machen werden. Generell empfiehlt es sich daher, die Gültigkeitsdauer von CRLs relativ kurz zu bemessen, so dass die Clients entsprechend häufig ihre CRLs erneuern müssen.

Verschlüsselung der Chat-Kommunikation

Chat ist ein Klartextprotokoll, das die Verschlüsselung über SSL oder TLS nicht unterstützt. Soll diese Kommunikation geschützt werden, so ist der Einsatz eines VPN in Betracht zu ziehen (*Point-to-Point Tunneling-Protokoll* - PPTP, *Layer 2 Tunneling Protocoll* - L2TP, IPSec).

Ergänzende Kontrollfragen:

- Sind die Benutzer im Umgang mit der Verschlüsselungs- und Signaturfunktionalität geschult worden?
- Wurde das Standard-Kennwort geändert?
- Ist der Ablauf der Zustellung der Sicherheitstoken an die Benutzer zweckmäßig festgelegt?

M 5.101 Entfernen nicht benötigter ODBC-Treiber beim IIS-Einsatz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Open Database Connectivity (ODBC) ist eine von Microsoft entwickelte standardisierte Schnittstelle (Application Programming Interface, API), über die eine Anwendung auf eine Reihe von Datenquellen zugreifen kann. Voraussetzung ist, dass es für die Datenquelle einen ODBC-kompatiblen Treiber gibt. Die Anwendung setzt die *Structured Query Language* (SQL) als Standardsprache zum Datenzugriff ein.

Bei einem ODBC-Treiber handelt es sich um eine *Dynamic Link Library* (DLL), die ODBC-Funktionsaufrufe implementiert. Die Anwendung ruft den ODBC-Treiber zum Zugriff auf eine bestimmte Datenquelle auf.

Die ODBC-Schnittstelle definiert

- eine Bibliothek mit ODBC-Funktionsaufrufen, mit denen eine Verbindung zur Datenquelle hergestellt, SQL-Anweisungen ausgeführt und Ergebnisse abgerufen werden,
- eine Standardmethode zur Herstellung einer Verbindung und zur Anmeldung bei der Datenquelle,
- eine auf der X/Open und SQL Access Group (SAG) CAE-Spezifikation (1992) aufbauende SQL-Syntax,
- eine standardisierte Darstellungsweise für Datentypen und
- eine standardisierte Gruppe von Fehlercodes.

Bei ODBC-Datenquellen handelt es sich um die Verknüpfung eines ODBC-Treibers mit einer Datenbank. Diese ODBC-Datenquellen werden mit Hilfe des ODBC-Datenquellen-Administrators eingerichtet.

Einige Anwendungen installieren ODBC-Datenquellen für Beispiel-datenbanken und/oder unbenutzte ODBC/OLE-DB Datenbanktreiber. Um einen unerwünschten Zugriff über diese ODBC-Datenquellen bzw. Treiber zu verhindern, sollten alle nicht benötigten Datenquellen und Treiber entfernt werden. Hierzu ist der ODBC-Datenquellen-Administrator aus der Systemsteuerung zu verwenden.

Ergänzende Kontrollfrage:

- Wurden alle nicht benötigten ODBC-Datenquellen und Treiber entfernt?

M 5.102 Installation von URL-Filtern beim IIS-Einsatz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Uniform Resource Locators (URLs) werden im Internet eingesetzt, um Objekte, z. B. Dokumente und HTML-Seiten, zu spezifizieren. Dadurch kann beispielsweise ein Browser auf eine bestimmte Web-Seite auf einem IIS zugreifen.

URL-Angriff

Das Ziel eines URL-Angriffs kann die Beeinträchtigung der Verfügbarkeit des Web-Servers sein. Dies wird z. B. durch überlange URLs, die einen Puffer-Überlauf verursachen, erreicht. Bei einem anderen URL-Angriff versucht ein Angreifer, die URL so zu verändern, dass er zusätzliche Rechte erhält und z. B. auf Verzeichnisse außerhalb des *Webroot*-Verzeichnisses oder auf Systemdateien zugreifen kann.

Um beispielsweise aus dem *Webroot*-Verzeichnis auszubrechen, werden so genannte UNICODE-Zeichen in der URL verwendet. Bei der englischen Version des IIS stellen die Zeichenfolgen *%c0%af* und *%c1%9c* die Zeichen "/" und "\" in UNICODE dar und ermöglichen einen Zugriff auf das nächst höhere Verzeichnis.

Durch die Installation von URL-Filtern kann die Sicherheit eines Web-Servers erhöht werden, da die Möglichkeit besteht, bestimmte Zeichenfolgen oder URLs mit Überlänge zu erkennen. Dies ist als zusätzliche Maßnahme zur Installation von aktuellen Patches und Hotfixes anzusehen, durch die z. B. ein Ausbruch aus dem *Webroot*-Verzeichnis unter Verwendung von UNICODE Zeichen verhindert wird.

Auf dem Markt werden URL-Filter von Microsoft aber auch von Drittherstellern angeboten. Ein Beispiel ist das *URLScan Security Tool* von Microsoft (*http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32571*). In dem Produkt *SecureIIS* von der Firma eEye ist ebenfalls ein URL-Filter enthalten (*http://www.eeye.com/html/Products/SecureIIS/index.html*).

Ergänzende Kontrollfrage:

- Wurde ein URL-Filter installiert?

M 5.103 Entfernen sämtlicher Netzwerkfreigaben beim IIS-Einsatz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Netz- und Administrationsfreigaben

C$, D$ und Admin$

Ein besonderes Sicherheitsrisiko bilden Netz- und Administrationsfreigaben auf dem Server. Über die Administrationsfreigaben, z. B. *C$, D$* und *Admin$,* besteht für einen Administrator die Möglichkeit, über das Netz auf den Server zuzugreifen. Diese Freigaben werden standardmäßig eingerichtet und bieten einen Angriffspunkt für Brute-Force-Attacken.

Es ist sicherzustellen, dass keine Freigaben auf dem IIS bestehen. Zur Kontrolle ist der Befehl *net share* in der Kommandozeile zu starten.

Zusätzlich sind die Administrationsfreigaben (*C$, D$, Admin$*) zu entfernen. Hierfür sind folgende Einträge in der Registrierung anzupassen:

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	CurrentControlSet\Services\LanmanServer\Parameters
Name	AutoShareServer
Type	REG_DWORD
Wert	0

Hinweis: Sollte dieser Eintrag nicht bestehen, so ist er mit dem Wert 0 hinzuzufügen. Anschließend ist das System neu zu starten.

Tabelle: Registrierungseinträge für Netz- und Administrationsfreigaben

Beschränken des Netzzugriffs für Anonymous (IPC$ NullSession)

IPC$

Windows NT/2000 erlaubt es, dass ein nicht authentisierter Benutzer Informationen über die Windows NT/2000 Domäne mit Hilfe von *net use* oder geeigneten Tools gewinnt. Mittels

net use \\Zielsystem\ipc$ "" /user:""

kann eine so genannte *NullSession* (über TCP-Port 139) aufgebaut werden. Diese ermöglicht es, Zugriff auf User-ID-Listen, Gruppenlisten, Account-Namen und auf die Ereignisanzeige (nur Application- und System-Logs, keine Sicherheits-Logs) zu erhalten oder Benutzer-Informationen über den Benutzer-Manager für Domänen zu verändern. Seit Windows NT SP3 kann der NullSession-Zugriff etwas eingeschränkt werden. Folgende Änderungen sollten in der Registrierung durchgeführt werden:

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	CurrentControlSet\Control\LSA
Name	RestrictAnonymous
Type	REG_DWORD
Wert	1

Tabelle: Registrierungseinträge bei Restrict Anonymus

RestrictAnonymous kann unter Windows NT die Werte 0 und 1 haben. Unter Windows 2000 sind die Werte 0 bis 2 möglich. Die Werte haben folgende Bedeutung:

0 Keine Einschränkung

1 Aufzählungen aus der SAM-Datenbank werden nicht erlaubt

2 Kein Zugriff ohne ausdrückliche Anonymous-Erlaubnis

Hinweis: Die NullSession-Verbindung ist dadurch weiterhin möglich, aber die Abfragemöglichkeiten werden beschränkt (Abfragen wie *sid2user* funktionieren weiterhin). Eine komplette Abhilfe ist nur durch das Deaktivieren von NetBIOS oder durch Blocken von Port 139 (am Router, Firewall) möglich.

Ergänzende Kontrollfrage:

- Wurden alle Netzfreigaben entfernt?

M 5.104 Konfiguration des TCP/IP-Filters beim IIS-Einsatz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Ein Informationsserver sollte nur die Informationen zur Verfügung stellen, die erforderlich bzw. gewünscht sind. Aus diesem Grund ist ein TCP/IP-Filter zu konfigurieren, der die zugelassenen Dienste und Protokolle beschränkt. Die Konfiguration des TCP/IP-Filters erfolgt durch die Spezifikation, welche Ports auf jedem Netz erlaubt sind.

Unter Windows NT ist der Filter unter *Systemsteuerung* | *Netzwerk* | *Protokolle* | *TCP/IP* | *Eigenschaften* | *Optionen* | *Sicherheit aktivieren* | *Konfigurieren* für den TCP-Anschluss einzustellen.

Unter Windows 2000 ist der Filter unter *Systemsteuerung* | *Netzwerk* | *Eigenschaften Netzwerkverbindung* | *Eigenschaften TCP/IP-Protokoll* | *Erweitert* | *Reiter Optionen* | *Eigenschaften TCP/IP-Filter* einzustellen.

Die Konfiguration sollte wie folgt aussehen:

- TCP/IP-Filter aktivieren (alle Netzkarten)
- Zulassen der TCP-Ports 80, 443 (wenn HTTP über SSL eingesetzt wird) und aller weiteren benötigten Ports
- Die folgende Tabelle zeigt Beispiele für Protokolle und zugehörige Ports:

Protokoll	**Port**	**Beschreibung**
http	80	HyperText Transfer Protocol
ftp	21 control 20 data	File Transfer Protocol
smtp	25	Simple Mail Transfer Protocol
nntp	119	Network News Transfer Protocol
https	443	http über SSL
ftps	990 control 989 data	ftp über SSL
nntps	563	nntp über SSL

Tabelle: Protokolle und zugehörige Ports

Hinweis: Beim passiven FTP werden die Verbindungen sowohl für Kommando- als auch Datenkanal vom Client initiiert. Der Client baut dabei die Datenverbindung zu einem Port >1024 auf. Um den passiven Modus zu ermöglichen, sind folglich alle Ports >1024 freizuschalten. Eine größere Sicherheit für den Web-Server bietet der aktive Modus. Die Initiierung der Datenverbindung erfolgt vom Server, so dass nur die Freigabe des Ports 21 erforderlich ist.

- Keine User Datagram Protocol (UDP) Ports zulassen
- Zulassen der IP-Protokollnummer 6 (TCP)

  IP verwendet Protokollnummern, um empfangene Daten an das richtige Transportprotokoll weiterzuleiten. Die Protokollnummer ist ein einzelnes Byte im IP-Header. Die Protokollnummern sind im gesamten Internet einheitlich und sind im RFC 1700 definiert.

  Hier einige Beispiele:

ip	0	IP	# internet protocol, pseudo protcol number
icmp	1	ICMP	# internet control message protocol
igmp	2	IGMP	# internet group multicast protocol
ggp	3	GGP	# gateway-gateway protocol
tcp	6	TCP	# transmission control protocol
pup	12	PUP	# PARC universal packet protocol
udp	17	UDP	# user datagram protocol
raw	255	RAW	# RAW IP interface

Tabelle: Beispiele von Protokollnummern

Empfängt eine IP-Implementation ein Datenpaket, in dessen Header als Protokollnummer 6 eingetragen ist, so werden diese Daten an das *Transmission Control Protocol* (TCP) weitergeleitet. Ist die Nummer 17, werden die Daten an das UDP weitergeleitet.

Ergänzende Kontrollfrage:

Wurden Protokolle und Dienste durch den TCP/IP-Filter unter Windows NT/2000 beschränkt?

M 5.105 Vorbeugen vor SYN-Attacken auf den IIS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

TCP-Verbindungen werden über einen *Drei-Wege-Handshake* aufgebaut, indem zuerst ein so genanntes SYN-Paket (SYN dient der Synchronisation von *Sequenznummern* beim Verbindungsaufbau) gesendet, darauf mittels eines SYN/ACK-Paketes geantwortet und anschließend wiederum mittels eines ACK-Paketes bestätigt wird. Bei einer SYN-Flooding-Attacke wird dem "Opfer" beim Handshake eine falsche Absenderadresse übermittelt. Das SYN/ACK-Antwortpaket wird also an eine falsche IP-Adresse gesendet. Wenn nach einiger Zeit keine Rückantwort in Form eines ACK-Paketes erfolgt, wird der Verbindungsversuch als erfolglos abgebrochen. Der entscheidende Punkt beim SYN-Flooding besteht darin, diese Zeit bis zum Abbruch (Timeout) dafür zu nutzen, das Opfer mit SYN-Paketen zu überfluten. Das SYN-Flooding kann dadurch ein *Denial of Service* (DoS) auslösen, da der Server für jede halboffene Verbindung Speicher belegt.

Mit dem Befehl *netstat -n -p tcp* werden alle aktuellen Verbindungen eines Rechners aufgelistet.

Wenn sich viele Verbindungen im Status *SYN_RECEIVED* befinden, kann dies ein Hinweis auf einen möglichen Angriff sein. Um diesen Attacken vorzubeugen, sind einige Einstellungen im TCP/IP über die Registrierung vorzunehmen.

"halboffene" Verbindungen schneller abbrechen

Die Information, wie häufig eine Antwort auf eine TCP-Verbindungsanfrage gesendet wird, kann an den Treiber *Tcpip.sys* (ab Windows NT 4.0 SP 2) übergeben werden. Der Registrierungsschlüssel *TcpMaxConnectResponseRetransmissions* steuert das Verhalten.

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	CurrentControlSet\Services\Tcpip\Parameters
Name	TcpMaxConnectResponseRetransmissions
Type	REG_DWORD
Wert	3 (Standard)

Dieser Eintrag legt fest, wie oft eine Erwiderung auf einen versuchten TCP-Verbindungsaufbau wiederholt wird. D. h. es wird festgelegt, wie viele TCP-SYN-ACKs nach Eingang eines TCP-SYN gesendet werden. Die erste Verzögerung liegt bei drei Sekunden, mit jeder neuen Übertragung des TCP-SYN-ACKs wird diese Wartezeit verdoppelt.

Standardmäßig ist der Wert des Registrierungsschlüssels auf 3 gesetzt (höchster Wert). Ein zu niedriger Wert kann bei höheren Laufzeiten einen korrekten Verbindungsaufbau verhindern. Zu empfehlen ist eine Einstellung

von 1 oder 2 in Abhängigkeit von den Eigenschaften des Netzes und der Wahrscheinlichkeit von SYN-Attacken. Die folgende Tabelle zeigt eine Übersicht über mögliche Werte und die damit verbundenen Eigenschaften.

Wert	Abstände der Übertragungs-wiederholungen	Verstrichene Zeit	Kommentar
3	3, 6 und 12 Sekunden	45 Sekunden	Der Versuch gilt nach 24 Sekunden nach der letzten Wiederholung als beendet.
2	3 und 12 Sekunden	21 Sekunden	Der Versuch gilt nach 12 Sekunden nach der letzten Wiederholung als beendet.
1	3 Sekunden	9 Sekunden	Der Versuch gilt nach 6 Sekunden nach der letzten Wiederholung als beendet.
0	Es werden keine SYN-ACKs in Wiederholung gesendet.	Nach drei Sekunden ist der TCP-SYN-Versuch verfallen.	Dieser Wert kann dazu führen, dass korrekte Versuche zum Verbindungsaufbau scheitern, wenn die Laufzeit über ein langsames Netz hin und zurück mehr als drei Sekunden beträgt.

Tabelle 1: Einstellungen des Treibers Tcpip.sys

NetBIOS über TCP/IP

NetBIOS über TCP/IP (NetBT) ist die Netzkomponente, die über den TCP-Anschluss 139 den Microsoft Netzdienst (z. B. Datei- und Druckerfreigaben) zur Verfügung stellt. NetBIOS kann einen Angriffspunkt für eventuelle Attacken darstellen und sollte aus diesem Grund deaktiviert werden. Dazu wird über die Systemsteuerung im Menü *Netzwerk* | *Dienste* die *NetBios-Schnittstelle* entfernt.

Um einen externen Zugriff auf das NetBIOS-Protokoll zu verhindern, sollten die Ports 137 und 139 auf der Firewall zwischen Internet und Web-Server generell gesperrt werden.

Kann auf NetBT nicht verzichtet werden, so ist das Verhalten von NetBT wie folgt in der Registrierung einzustellen (ab Windows NT 4.0 SP 2).

Einstellen der zunehmenden Verbindungsblöcke (*INCREASING CONNECTION BLOCK INCREMENT*)

Die Anzahl der Verbindungsblöcke, die hinzugefügt werden, falls die Anzahl der freien Blöcke unter zwei liegt, wird wie folgt in der Registrierung eingestellt:

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	CurrentControlSet\Services\NetBT\Parameters
Name	BacklogIncrement
Type	REG_DWORD
Wert	3 (Standard)
Bereich	1 bis 20

Der Standardwert 3 kann in der Regel beibehalten werden. Ist der Wert zu hoch, werden viele Systemressourcen benötigt, was hingegen aber die Geschwindigkeit erhöht, mit der die Anschlüsse zur Verfügung gestellt werden.

Einstellen der maximalen Verbindungsblöcke (*MAXIMUM CONNECTION BLOCKS*)

Jeder Verbindungsblock belegt 78 Byte im Arbeitsspeicher. Die Anzahl der maximalen Verbindungsblöcke wird wie folgt in der Registrierung eingestellt:

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	CurrentControlSet\Services\NetBT\Parameters
Name	MaxConnBackLog
Type	REG_DWORD
Wert	1.000 (Standard)
Bereich	1 bis 40.000

Der Standardwert 1.000 kann in der Regel beibehalten werden. Abhängig von der Systemausstattung und der Frequentierung des Servers kann der Wert bis 40.000 erhöht werden.

Einstellen des dynamischen Reserve-Verhaltens

Anwendungen wie ftp-Server und Web-Server verarbeiten die TCP-Anschlussversuche mit Hilfe der Komponente *afd.sys*. Dieser Treiber ist von Microsoft geändert worden, um viele Anschlüsse während der Synchronisation (*SYN_RECEIVED*) zu unterstützen, ohne den Zugriff von einem berechtigten Client zu verweigern.

Diese Einstellungen sind durch den Administrator entsprechend zu konfigurieren.

Hierzu unterstützt die neue Version von *afd.sys* vier Parameter, die in der Registrierung hinterlegt sind. Diese Parameter steuern das dynamische Reserve-Verhalten.

EnableDynamicBacklog ist ein globaler Schalter zum Aktivieren oder Sperren der dynamischen Reserve. Der Standardwert ist 0 (deaktiviert). Diese Einstellung liefert keine Änderung zur vorherigen Version. Bei einem durch SYN-Attacken bedrohten System sollte das dynamische Reserve-Verhalten durch Setzen des Wertes 1 aktiviert werden.

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	CurrentControlSet\Services\AFD\Parameters
Name	EnableDynamicBacklog
Type	REG_DWORD
Wert	1

MinimumDynamicBacklog steuert die Mindestzahl der freien Anschlüsse, die erlaubt werden. Dieser Wert sollte nicht zu groß gewählt werden, denn ein zu großer Wert kann zu Leistungseinbrüchen führen. Es wird empfohlen, den Wert auf 20 einzustellen.

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	CurrentControlSet\Services\AFD\Parameters
Name	MinimumDynamicBacklog
Type	REG_DWORD
Wert	20

MaximumDynamicBacklog steuert die Höchstzahl der freien Anschlüsse und der Anschlüsse, die sich im Synchronisationsmodus (*SYN_RECEIVED*) befinden.

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	CurrentControlSet\Services\AFD\Parameters
Name	MaximumDynamicBacklog
Type	REG_DWORD
Wert	Dieser Wert sollte nicht 5000 pro 32MB RAM übersteigen.

DynamicBacklogGrowthDelta legt die maximale Zahl verfügbarer Verbindungen fest, die eingerichtet werden, wenn das *dynamic backlog feature* ausgelöst wird. Ist der Wert zu groß, kann es zu einem übermäßigen Anwachsen der Zahl freier Verbindungen kommen. Es wird empfohlen, den Wert auf 10 einzustellen.

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	CurrentControlSet\Services\AFD\Parameters
Name	DynamicBacklogGrowthDelta
Type	REG_DWORD
Wert	10

Die aktuelle Version des Treibers (*afd.sys*) ist in den aktuellen Service Packs für Windows NT 4.0 und Windows 2000 enthalten. Weitere Informationen sind bei Microsoft erhältlich.

Ergänzende Kontrollfrage:

Wurden die Einstellungen in der Registry angepasst, um SYN-Attacken vorzubeugen?

M 5.106 Entfernen nicht vertrauenswürdiger Root-Zertifikate beim IIS-Einsatz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

In einer Public-Key-Infrastruktur wird die Sicherheit u. a. durch die zugelassenen Root-Zertifikate bestimmt. Wenn einem solchen Root-Zertifikat vertraut werden soll, muss es im Betriebssystem geladen werden. Zertifikate, denen nicht vertraut wird, sollten aus dem System gelöscht werden.

Die Verwaltung der Zertifikate hängt von den eingesetzten Systemen ab:

IIS 4.0 + Internet Explorer 4 + Windows NT 4 + SP4 oder höher

In diesem Szenario werden alle Root-Zertifikate von der Komponente *schannel.dll* verwaltet. Diese DLL speichert die Daten in der Registrierung. Unter dem in der Tabelle dargestellten Schlüssel befinden sich eine Reihe von registrierten Schlüsseln, einer für jedes vorinstallierte Root-Zertifikat. Jedes Root-Zertifikat hat einen Eintrag namens *Enabled* mit dem Wert *0x1*, wenn dem Zertifikat vertraut wird. Wird dem Zertifikat nicht vertraut, ist der Wert auf *0x0* zu setzen.

Registrierung	
Bereich	HKEY_LOCAL_MACHINE\SYSTEM
Schlüssel	CurrentControlSet\Control\SecurityProviders\ SCHANNEL\CertificationAuthorities
Name	Enabled
Type	REG_DWORD
Wert	0

Die Registrierungseinträge sollten nicht gelöscht werden, da *schannel.dll* die fehlenden Einträge neu erstellen wird.

IIS 4.0 + Internet Explorer 5 + Windows NT 4 + SP4 oder höher

In diesem Szenario sollten die folgenden Schritte ausgeführt und die Root-Zertifikate entsprechend bearbeitet werden:

- Öffnen des Internet Explorer 5
- Extras | Internetoptionen
- Reiter *Inhalt* wählen
- Schaltfläche *Zertifikate* wählen
- Reiter *vertrauenswürdige Stammzertifizierungsstellen* wählen
- Alle nicht vertrauenswürdigen Zertifikate entfernen
- IIS 4.0 stoppen: *net stop iisadmin /j*
- IIS 4.0 starten: *net start w3svc*

Beim IIS 5.0 können die Zertifikate auf zwei unterschiedliche Arten entfernt werden:

IIS 5.0: Entfernen der Zertifikate mittels Internet Explorer

In diesem Szenario sollten die folgenden Schritte ausgeführt und die Root-Zertifikate entsprechend bearbeitet werden:

- Öffnen des Internet Explorer 5
- Extras | Internetoptionen
- Reiter *Inhalt* wählen
- Schaltfläche *Zertifikate* wählen
- Reiter Vertrauenswürdige Stammzertifizierungsstellen wählen
- Alle nicht vertrauenswürdigen Zertifikate entfernen
- IIS 5.0 stoppen: net stop iisadmin /j
- IIS 5.0 starten: *net start w3svc*

IIS 5.0: Entfernen der Zertifikate mittels MMC

In diesem Szenario sollten die folgenden Schritte ausgeführt und die Root-Zertifikate entsprechend bearbeitet werden:

- Öffnen der Microsoft Management Console (MMC)
- Das Snap-in *Zertifikate* hinzufügen
- Das Computerkonto zur Verwaltung auswählen
- Lokalen Computer zur Verwaltung auswählen
- Fertigstellen
- Fenster schließen
- Die Struktur Zertifikate | Vertrauenswürdige Stammzertifizierungsstellen | Zertifikate auswählen
- Alle nicht vertrauenswürdigen Zertifikate entfernen
- IIS 5.0 stoppen: net stop iisadmin /j
- IIS 5.0 starten: *net start w3svc*

Es dürfen keine Microsoft- oder VeriSign-Zertifikate entfernt werden, da diese vom Betriebssystem verwendet werden.

Ergänzende Kontrollfrage:

- Wurden alle nicht vertrauenswürdigen Root-Zertifikate entfernt?

M 5.107 Verwendung von SSL im Apache-Webserver

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Bei der Verwendung von SSL auf dem Apache-Webserver ist eine Reihe sicherheitsrelevanter Einstellungen zu treffen. Die Beispiele in dieser Maßnahme beziehen sich auf das Modul mod_ssl der Version 2.0 des Apache-Webservers.

Kryptoalgorithmen festlegen

Die vom Webserver akzeptierten Versionen des SSL-Protokolls und die von ihm akzeptierten Kryptoalgorithmen können mit den Direktiven *SSLProtocol* und *SSLCipherSuite* festgelegt werden. Dabei sollten die "schwachen" Methoden nach Möglichkeit abgeschaltet werden. Beispielsweise sollten mittels

SSLProtocol ALL -SSLv2

SSLCipherSuite ALL:!NULL

die als unsicher geltenden veralteten SSL-Protokollversionen sowie der "No-Encryption-Modus", bei dem keine Datenverschlüsselung stattfindet, entfernt werden. Dies kann dazu führen, dass mit bestimmten veralteten Clients keine Verbindung möglich ist.

Zertifikate und Schlüssel

Das SSL-Zertifikat für den Apache-Webserver selbst muss dem Apache-Webserver ebenso in einer Datei zur Verfügung gestellt werden wie der zugehörige private Schlüssel. Die Pfade zu diesen Dateien werden mit den Direktiven *SSLCertificateFile* und *SSLCertificateKeyFile* festgelegt.

Der private Schlüssel sollte nicht zusammen mit dem Zertifikat in einer Datei gespeichert werden und die Datei mit dem privaten Schlüssel sollte durch eine Passphrase geschützt sein. Die Datei, in der sich der private Schlüssel des Webservers befindet, muss besonders sorgfältig geschützt werden. Der Lesezugriff für diese Datei sollte auf denjenigen Benutzer beschränkt werden, unter dessen Kennung der Apache-Webserver abläuft.

Durch die Verwendung einer Passphrase für den privaten Schlüssel des Serverzertifikats werden automatische unbeaufsichtigte Neustarts des Servers sehr erschwert, da die Passphrase bei jedem Neustart abgefragt wird. Mit der Direktive *SSLPassPhraseDialog* kann festgelegt werden, auf welche Weise die Passphrase dem Apache-Webserver zur Verfügung gestellt wird. Standardmäßig erfolgt die Eingabe der Passphrase beim Start des Serverprogramms an der Kommandozeile. Da die Direktive *SSLPassPhraseDialog* die Angabe eines Programms erlaubt, als dessen Ausgabe die Passphrase entgegen genommen werden kann, kann eventuell auf diesem Weg eine Lösung erarbeitet werden, die automatische Neustarts in einem bestimmten Rahmen möglich macht. Jede solche Lösung wird jedoch einen Kompromiss zwischen Sicherheit und Bequemlichkeit darstellen.

Die Wurzelzertifikate von Zertifizierungsstellen, die der Server akzeptieren soll, müssen dem Apache-Webserver ebenso in einer Datei zur Verfügung gestellt werden, wie die CRLs (falls diese Option verwendet wird). Die Pfade zu diesen Dateien werden durch entsprechende Direktiven angegeben.

Zugriffsrechte auf Zertifikatsdateien

Für die Dateien bzw. Verzeichnisse, in denen der Apache-Webserver Zertifikate bzw. CRLs erwartet, muss durch Vergabe entsprechender Zugriffsrechte im Dateisystem sichergestellt werden, dass diese Dateien nur von dazu befugten lokalen Benutzern geändert dürfen. Insbesondere darf es der Benutzerkennung, unter der der Apache-Webserver abläuft, nicht möglich sein, diese Dateien zu ändern. Ein lesender Zugriff durch den Apache-Webserver muss jedoch möglich sein.

Ist der private Schlüssel des Webservers nicht durch eine Passphrase geschützt, so muss dies dokumentiert werden. Dies gilt auch, wenn die verwendete Passphrase auf dem Rechner selbst abgelegt wurde. Insbesondere muss in diesem Fall geprüft werden, ob ein solches Vorgehen konform zu den Sicherheitsrichtlinien der Organisation ist.

Ergänzende Kontrollfragen:

- Wie ist der Schutz des privaten Schlüssels des Webservers gewährleistet?
- Sind die Dateien mit dem Serverzertifikat und den anderen benötigten Zertifikaten gegen unbefugten Zugriff, insbesondere gegen unbefugte Veränderung, geschützt?

M 5.108 Kryptographische Absicherung von E-Mail

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Benutzer, Administrator

Damit E-Mails nicht unterwegs verändert oder mitgelesen werden können, sind zusätzliche Maßnahmen erforderlich. Diese gehören oft nicht zum Standardumfang von E-Mail-Systemen, sondern müssen zusätzlich installiert und konfiguriert werden. Dabei kann die Vertraulichkeit von E-Mail durch Verschlüsselung und die Integrität und Authentizität durch digitale Signaturen von E-Mails erreicht werden. Die digitale Signatur stellt dabei sicher, dass die E-Mail vom angegebenen Absender kommt und unverändert ist.

Generell ist die kryptographische Absicherung von E-Mail auf drei Ebenen möglich:

- **Netz-zu-Netz**

  Hierbei wird die Kommunikation von einem Netzübergabepunkt zum anderen abgesichert, z. B. durch den Aufbau eines VPN (Virtual Private Network, siehe dazu auch Baustein B 4.4 *Remote Access*).

  Vorteil: Die vorgegebene Verschlüsselung funktioniert unabhängig von Benutzereingriffen. Statt vielen Benutzern müssen nur einzelne Administratoren geschult werden.

  Nachteile: Es sind keine individuellen Einstellungen möglich, z. B. für digitale Signaturen. Diese Lösung kann außerdem nur für einzelne Gruppen von vorher festgelegten Kommunikationspartnern eingesetzt werden.

  Dies ist eine gute Lösung, wenn Organisationen oder Organisationsteile, die geographisch getrennt sind, häufig über einen sicheren Kanal kommunizieren wollen.

- **Client-zu-Web-/Mailserver: z. B. TLS/SSL, Proxy-Lösung**

  Bei der Proxy-Lösung wird jede Mail auf dem E-Mail-Server ver- bzw. entschlüsselt und im Klartext an den Client weitergeleitet.

  Vorteil: Dies funktioniert unabhängig vom E-Mail-Client. Es ist keine zusätzliche Installation von Kryptoprogrammen bei den E-Mails-Clients erforderlich.

  Nachteile: Bei Proxy-Lösungen kann die Konfiguration aufwendig sein. Bei TLS/SSL-Lösungen kann viel falsch gemacht werden.

- **Client-zu-Client bzw. "Ende zu Ende"**

  Bei der kryptographischen Absicherung von Client-zu-Client werden Funktionalitäten benutzt, die im jeweiligen E-Mail-Client integriert sind oder dort nachträglich installiert werden (z. B. als Plug-In). Bekannte Produkte hierfür sind GnuPG oder PGP. Bei deren Einsatz müssen viele Rahmenbedingungen beachtet werden, damit diese wirklich die Sicherheit bieten, die von ihnen erwartet wird. Was hierzu umzusetzen ist, ist beispielsweise in den folgenden Maßnahmen beschrieben:

  - M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*

- M 5.63 *Einsatz von GnuPG oder PGP*
- M 5.85 *Einsatz von Verschlüsselungsverfahren für Lotus Notes E-Mail*
- M 5.100 *Einsatz von Verschlüsselungs- und Signaturverfahren für die Exchange 2000 Kommunikation*
- M 5.110 *Absicherung von E-Mail mit SPHINX (S/MIME)*

In vielen E-Mail-Clients ist mittlerweile bereits die Möglichkeit zur Verschlüsselung und Digitalen Signatur integriert. Dadurch ergibt sich der Vorteil, dass diese Funktionen ohne Zusatzaufwand benutzt werden können. Der E-Mail-Verkehr innerhalb einer Institution kann damit direkt geschützt werden. Der Nachteil ist, dass dabei manchmal kryptographisch schwache Verfahren oder Implementierungen verwendet werden. Häufig treten auch Inkompatibilitäten mit anderen E-Mail-Clients auf.

Als Alternative gibt es eine Reihe von Plug-Ins, also Programme, die einem vorhandenen E-Mail-Client weitere Funktionalitäten hinzufügen, in diesem Fall also Verschlüsselung und Digitale Signatur. Vorteil: Die Produkte können so ausgewählt werden, dass sie genau auf die Bedingungen und Sicherheitsansprüche innerhalb einer Institution passen. Ein Nachteil ist, dass diese Plug-Ins nicht immer für alle E-Mail-Programme verfügbar sind. Bei Updates des E-Mail-Programms ist unsicher, ob das Plug-In noch funktioniert oder auch dafür ein Update benötigt wird. Es kann passieren, dass diese Verschlüsselungsprogramme inkompatibel mit ähnlichen Programmen auf Empfängerseite sind.

Da die Client-zu-Client-Absicherung immer darauf basiert, dass jedem Benutzer kryptographische Schlüssel zugeordnet werden müssen, ist hierzu ein zentrales Schlüsselmanagement notwendig. Dieses muss unter anderem gewährleisten, dass die Schlüssel regelmäßig gewechselt werden, immer aktuell sind und sicher installiert und gespeichert werden, also nur dem Berechtigten zugänglich sind. Dies zieht natürlich einiges an Aufwand nach sich (siehe auch M 2.46 *Geeignetes Schlüsselmanagement*).

Welche Kriterien (z. B. Funktionalität, Benutzerfreundlichkeit, Interoperabilität, Wirtschaftlichkeit, vorliegende Sicherheitsuntersuchungen) bei der Auswahl eines geeigneten kryptographischen Produktes zu beachten sind, ist in Baustein B 1.7 *Kryptokonzept* beschrieben.

Ergänzende Kontrollfragen:

- Existiert ein Konzept für die kryptographische Absicherung von E-Mail?
- Werden die Benutzer bzw. Administratoren im Umgang mit Krypto-Produkten geschult?
- Welche Verschlüsselungs- bzw. Signaturverfahren werden eingesetzt?

M 5.109 Einsatz eines E-Mail-Scanners auf dem Mailserver

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator

Zur Erhöhung der Sicherheit sollte auf dem zentralen Mailserver ein speicherresidentes Virenschutzprogramm (oft auch E-Mail-Wächter genannt) installiert werden, das sowohl eingehende als auch ausgehende E-Mails, insbesondere deren Anhänge, auf Computer-Viren und andere schädliche Inhalte überprüft.

Ergänzend zur Einrichtung eines E-Mail-Wächters auf dem Mailserver selbst kann auch am Übergang zum Internet ein so genanntes SMTP-Gateway eingerichtet werden, auf dem die Überprüfung der ein- und ausgehenden E-Mails erfolgt. Die Anbindung an das Internet muss dann so realisiert werden, dass sämtliche SMTP-Verbindungen nur über das SMTP-Gateway abgewickelt werden können.

Auch ausgehende E-Mails scannen

Dabei ist es wichtig, auch ausgehende E-Mails zu überprüfen. Einerseits kann so möglicherweise eine Infektion im internen Netz entdeckt werden, bevor größerer Schaden entsteht. Andererseits schützt dies aber auch die Behörde bzw. das Unternehmen vor einem eventuellen Ansehensverlust oder gar Schadensersatzansprüchen, die dadurch entstehen könnten, dass virenverseuchte E-Mails an Geschäftspartner verschickt werden.

Die meisten E-Mail-Wächter bieten umfangreiche Einstellmöglichkeiten im Bezug darauf, was mit "verdächtigen" E-Mails zu tun ist. Beispielsweise können solche E-Mails grundsätzlich gelöscht oder auch auf einem "Quarantäne-Server" zwischengespeichert werden bis feststeht, ob der Inhalt harmlos ist. Eine weitere Möglichkeit ist es, nur eventuell bösartige E-Mail-Anhänge abzutrennen, während die Nachricht selbst mit einem entsprechenden Hinweis an den Empfänger weiter geleitet wird.

Blacklist oder Whitelist

Als mögliche Vorgehensweisen bieten sich ein Ansatz mit "Blacklist" oder ein "Whitelist" an. Bei der "Blacklist" wird eine Liste "verbotener" Dateitypen definiert, die keinesfalls als Anhänge an E-Mails versandt werden dürfen und die auch bei eingehenden E-Mails nicht akzeptiert werden. Ein restriktiverer Ansatz ist die "Whitelist", bei der nur solche Dateitypen als E-Mail-Anhänge zugelassen werden, die auf der festgelegten Liste erlaubter Typen stehen. Bei der Festlegung von Black- oder Whitelists sollte darauf geachtet werden, dass ein vernünftiger Kompromiss zwischen Sicherheit und Funktionalität gefunden wird. Zu laxe Einstellungen führen unter Umständen dazu, dass schädliche Inhalte in das interne Netz gelangen, während zu strenge Einstellungen die Produktivität behindern können.

Gefährliche Datei-Typen auf jeden Fall filtern

Datei-Typen, die im täglichen Arbeitsablauf nicht als Anhänge von E-Mails vorkommen und potentiell gefährliche Inhalte darstellen (z. B. ausführbare Dateien wie *.VBS, *.WSH, *.BAT, *.PIF, *.EXE unter Windows sowie *.SH, *.CSH, *.TCSH, *.PL und ähnliche unter Unix) sollten in jedem Fall zentral blockiert werden.

Da verschlüsselte E-Mails nicht automatisch überprüft werden können, muss auch festgelegt werden, wie mit verschlüsselten E-Mails zu verfahren ist

(siehe hierzu auch Bausteine B 1.6 *Computer-Viren-Schutzkonzept* und B 1.7 *Kryptokonzept*).

Information der Mitarbeiter, Beteiligung der Personalvertretung, Rechtslage beachten

Die Mitarbeiter müssen darüber informiert werden, dass E-Mails automatisch gescannt werden und welche Regeln gelten. Außerdem sollte bei der Entscheidung, E-Mails automatisch auf dem Mailserver zu scannen, die Personalvertretung und der Datenschutzbeauftragte beteiligt werden. Je nach Land und der Art der Organisation (Behörde oder Firma) müssen eventuell auch noch andere Rechtsvorschriften beachtet werden.

Kein Ersatz für lokale Virenscanner

Selbst wenn ein E-Mail-Wächter auf dem Mailserver installiert wurde, sollte keinesfalls auf den Einsatz von Virenscannern auf den Arbeitsplatzrechnern verzichtet werden. Obwohl inzwischen der überwiegende Anteil von Viren und anderen Schadprogrammen per E-Mail verbreitet wird, gibt es doch noch genügend andere Verbreitungsmöglichkeiten für bösartige Programme, beispielsweise nach wie vor über Disketten oder andere Wechselmedien oder über den Dateidownload aus dem Web.

Ergänzende Kontrollfragen:

- Existiert ein umfassender Schutz gegen Computer-Viren, die über E-Mail verbreitet werden?
- Sind die Mitarbeiter darüber informiert, was sie beachten müssen, um einer Verbreitung von Computer-Viren über E-Mail vorzubeugen?

M 5.110 Absicherung von E-Mail mit SPHINX (S/MIME)

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Benutzer, Administrator

Die zunehmende Bedeutung von E-Mail erfordert den Einsatz von Maßnahmen, die eine Vertraulichkeit und Verbindlichkeit gewährleisten. Dies kann durch den breiten Einsatz von Produkten zur Verschlüsselung und digitalen Signatur von E-Mails erreicht werden. Die elektronische Signatur stellt dabei sicher, dass die E-Mail vom angegebenen Absender kommt und unverändert ist. Die Verschlüsselung der Informationen bewirkt, dass nur der rechtmäßige Empfänger die E-Mail lesen kann.

Projekt SPHINX

Zu diesem Zweck wurde vom BSI das Projekt SPHINX initiiert, in dessen Rahmen kryptographische Produkte auf internationalen Standards fortentwickelt wurden. Die Interoperabilität, das bedeutet die fehlerfreie Austauschbarkeit von kryptographisch behandelten Nachrichten, der Produkte verschiedener Hersteller und für verschiedene Plattformen wird quartalsweise durch ein Testlabor untersucht und das Ergebnis veröffentlicht.

Kryptographische Verfahren

kryptographische Algorithmen

Zur Erreichung einer herstellerunabhängigen Interoperabilität kommen bei SPHINX ausschließlich Produkte zum Einsatz, die auf den Industriestandards S/MIME und "MailTrusT" beruhen. Diese Standards nutzen zur Erzeugung sicherer E-Mails eine Kombination unterschiedlicher kryptographischer Verfahren. Als symmetrisches Verfahren wird der Triple-DES-Algorithmus mit 112 Bit Schlüssellänge zur Verschlüsselung der Daten verwendet. Das eingesetzte Public-Key-Verfahren für die elektronische Signatur und zur Verschlüsselung ist der RSA-Algorithmus mit mindestens 1024 Bit Schlüssellänge. SHA-1 ist der empfohlene Hash-Algorithmus, der zur eindeutigen Abbildung der Nachricht auf einen Wert mit definierter Länge verwendet wird.

digitale Zertifikate

Die Zuordnung von kryptographischen Schlüsseln zu Personen wird durch digitale Zertifikate geregelt. Ein Zertifikat ist ein elektronisches Dokument, das im wesentlichen den öffentlichen Schlüssel und den Namen des Schlüsselinhabers enthält. Mit ihrer elektronischen Unterschrift beglaubigt die Zertifizierungsstelle (Trustcenter) die Zuordnung zwischen Schlüssel und Person. Bei SPHINX werden standardisierte Zertifikate gemäß der ITU-Empfehlung X.509 Version 3 verwendet.

Public Key Infrastruktur (PKI)

Das Vertrauen zwischen den Kommunikationspartnern besteht im Kern im Vertrauen auf die digitalen Zertifikate und der Glaubwürdigkeit aller Angaben, die es enthält. Für die öffentliche Verwaltung wurden bereits durch mehrere Trustcenter Zertifikate ausgestellt. Diese Trustcenter werden durch die übergeordnete Wurzelzertifizierungsstelle des BSI überprüft und in der PKI (Public Key Infrastruktur) der öffentlichen Verwaltung zusammengeschlossen. Damit unterliegen alle ausgestellten Zertifikate dem Standard des IT-Grundschutzes in allen Fragen der IT-Sicherheit. Für den Kontakt zum Bürger und zu Firmen wurde die Verwaltungs-PKI in die European Bridge-CA integriert, die unabhängige PKI miteinander vertrauenswürdig verbindet.

Personal-Security-Environment (PSE): Chipkarte und Datei

Eine weitere Anforderung zur Bildung des Vertrauens ist der Schutz des geheimen Schlüssels eines Benutzers. Dazu kann der geheime (oder persönliche)

Schlüssel entweder in einer speziellen Datei oder einer Chipkartegespeichert werden. Im Allgemeinen wird diese Datei bzw. die Chipkarte als Personal-Security-Environment (PSE) bezeichnet, also persönliche Sicherheitsumgebung. PSEs sind kryptographisch geschützt und können nur mittels Passwort zur Benutzung aktiviert werden. Für den sicheren Umgang mit dem Passwort und der Datei bzw. der Chipkarte ist der Eigentümer verantwortlich.

Weitere Informationen finden zu SPHINX und der PKI der öffentlichen Verwaltung finden sich unter:

http://www.bsi.bund.de/fachthem/verwpki/sphinx/index.htm

Sichere Installation und Bedienung

Einarbeitung der IT-Administratoren erforderlich

Bei SPHINX-Produkten handelt es sich in der Regel um sogenannte Plugin-Produkte. Sie ergänzen das vorhandene E-Mail-Produkt mit als sicher anerkannte kryptographische Verfahren.

Durch falsche Konfiguration oder Fehlbedienung kann es aber zu einer Abschwächung des Sicherheitsniveaus kommen.

Die Konfiguration ist bei SPHINX-Produkten wie bei den meisten komplexeren Kryptoprodukten nicht selbsterklärend. Damit sich keine Administrationsfehler einschleichen, ist die Einarbeitung in das genutzte SPHINX-Produkt notwendig. In Unternehmen und Behörden sollte ein Mitarbeiter der IT-Administration in den Umgang mit dem SPHINX-Produkt eingearbeitet werden und als technischer Ansprechpartner zur Verfügung stehen.

Schulung der Benutzer

Um Verständnis für die Anwendung der neuen Funktionalitäten beim Benutzer zu erreichen, ist die Vermittlung von einigen kryptographischen Grundbegriffen notwendig. Die Abläufe zur Beantragung eines Zertifikates und die Bedienung des SPHINX-Produktes sollten geschult werden. In Unternehmen und Behörden sollten ausgewählte Benutzer in den Umgang mit dem SPHINX-Produkt eingearbeitet werden und als Multiplikatoren die weiteren Benutzer im Umgang mit dem Produkt einweisen. Eine Schulung durch den Hersteller bzw. Vertreiber des Produktes ist vorzuziehen. Insbesondere sollte das Erzeugen von signierten und verschlüsselten E-Mails bzw. der Empfang dieser geübt werden, bevor ein Benutzer das Programm verwendet.

homogene Ausstattung mit einem SPHINX-Produkt

Es ist empfehlenswert, dass innerhalb einzelner Organisationen ein einheitliches SPHINX-Produkt, besser noch eine einheitliche Programmversion verwendet wird. Damit können Aufwände bei der Administration, Schulung, Betreuung und Software-Pflege gering gehalten werden.

Dokumentation auf Organisation anpassen

Zu jedem SPHINX-Produkt gehört eine umfangreiche Dokumentation, die vor der Verwendung gelesen werden sollte. Sie sollte vor ihrer Verteilung an die Anwender auf die Eigenheiten der Organisation angepasst werden. Damit lässt sich eine höhere Akzeptanz bei der Produkteinführung erreichen.

Schlüsselaufbewahrung

privaten Schlüssel schützen

Die privaten Schlüssel werden in der Personal-Security-Environment (PSE) abgelegt. Entscheidend für den sicheren Betrieb ist, dass der Inhalt der PSE vertraulich bleibt und vor Manipulationen geschützt wird. Das genutzte Passwort ist nach den in M 2.11 *Regelung des Passwortgebrauchs* beschriebenen Passwortregeln zu bilden und sicher zu verwahren. Eine Weitergabe, unge-

wollt oder wissentlich, befähigt andere Personen im Namen des Eigentümers elektronisch zu unterschreiben.

Ist die PSE eine Datei, so spricht man von einer Soft-PSE. Diese ist durch das Passwort kryptographisch geschützt. Es wird empfohlen, sie nicht auf Netzlaufwerken zu speichern, da sonst weitere Sicherheitsmaßnahmen ergriffen werden müssen. Der Einsatz von Chipkarten zur Schlüsselspeicherung ist vorzuziehen. Aber auch bei Chipkarten muss das verwendete Passwort sicher verwahrt werden. Bei den Chipkarten, die bei SPHINX zum Einsatz kommen, kann keine Kopie angelegt werden.

Soft-PSE: Backup und Passwort an gesichertem Ort aufbewahren

Von der Soft-PSE sollte eine Sicherungskopie angelegt sowie das Passwort notiert werden. Die Sicherungskopie und das Passwort sollten sicher, am besten getrennt verwahrt werden. So kann sichergestellt werden, dass bei einem Festplattencrash oder einer Fehlbedienung die PSE nicht verloren geht. Nachrichten, die verschlüsselt wurden, lassen sich bei Verlust der PSE nicht mehr entschlüsseln.

Das Aufschreiben und Hinterlegen des Passworts an einem gesicherten Ort sollte hierbei als kritischer Vorgang betrachtet werden, der ausschließlich der Notfallvorsorge dient. Die abgeschlossene Schublade eines Schreibtisches oder ähnlich "sichere" Orte können **keinesfalls** als Aufbewahrungsort für die PSE oder das Passwort empfohlen werden.

Schlüsselverteilung

Damit ein Empfänger die elektronische Signatur des Senders einer Datei überprüfen kann bzw. der Sender eine Nachricht für einen bestimmten Empfänger verschlüsseln kann, benötigt er das digitale Zertifikat seines Kommunikationspartners. Dieses kann er auf verschiedene Arten erhalten, z. B. per Anlage einer E-Mail oder von einem speziellen Internet-Server (Verzeichnis), manchmal auch von einem WWW-Server.

SPHINX-Produkte unterstützen den Benutzer bei der Überprüfung der digitalen Zertifikate. Der Benutzer muss bei den meisten Produkten beim ersten Empfang das Zertifikat seines Kommunikationspartners einer E-Mailadresse manuell zuordnen. Neben dem Zertifikat des Kommunikationspartners wird zur automatischen Überprüfung das Zertifikat des ausstellenden Trustcenters benötigt. Die erforderlichen Zertifikate werden meistens als Anlage in der signierten E-Mail mit übertragen. Das Zertifikat der Wurzelzertifizierungsstelle sollte vorhanden oder durch den IT-Service vorinstalliert worden sein.

Damit ein Benutzer in den Besitz eines eigenen Zertifikats gelangt, werden von ihm Zertifikats-Beantragung und Identifikation gefordert. Beides wickelt er in Zusammenarbeit mit der Registrierungsstelle ab. Bei Behörden, Firmen, Organisationen sind diese meist beim Inneren Dienst bzw. Werkschutz zu finden. Trustcenter unterhalten meist Registrierungsstellen in ihren Filialen. Die Registrierungsstelle prüft die Zertifikatsanträge auf Richtigkeit und identifiziert den Benutzer anhand seines Dienst- oder Personalausweis. Werden Chipkarten ausgegeben, so sind sie in der Regel ebenfalls dort zu erhalten. Bei Soft-PSEs erfolgt die Zusendung elektronisch, meistens per E-Mail.

Ergänzende Kontrollfragen:

- Werden die Benutzer im Umgang mit dem SPHINX-Produkt geschult?

- Werden Administratoren auf Konfiguration und Support des SPHINX-Produktes vorbereitet?
- Ist eine Registrierungsstelle eingerichtet und das notwendige Personal auf die Aufgabe vorbereitet?
- Wie ist die sichere Aufbewahrung von Sicherheitskopien der Soft-PSE und des Passwortes geregelt?
- Werden die Benutzer über die Sicherheitsmaßnahmen und die Abläufe unterrichtet?
- Sind die Benutzer über das Verfahren zur Beantragung und Sperrung eines Zertifikates informiert?

M 5.111 Einrichtung von Access Control Lists auf Routern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die vielfältigen Zugriffsmöglichkeiten für die Nutzung und die Administration von Routern und Switches können mit Hilfe von Access Control Lists (ACLs) kontrolliert werden. Der Zugriff kann für einzelne Rechner oder Netze und für die jeweilige Zugriffsmethode festgelegt werden.

Mittels der ACL erfolgt die Festlegung, welche Rechner oder Netze auf den Router oder den Switch über Dienste wie bspw. TELNET, SNMP, HTTP, etc. zugreifen können. Das folgende Beispiel zeigt eine entsprechende ACL eines Cisco-Routers zur Zugriffsbeschränkung für den Dienst TELNET auf das Netzkoppelelement selbst:

access-list 102 permit tcp host 163.183.200.22 any eq 23 log

access-list 102 permit tcp host 163.183.200.24 any eq 23 log

access-list 102 deny ip any any log

Die Festlegung der ACLs muss entsprechend den Vorgaben der Sicherheitsrichtlinie erfolgen. Insbesondere sollte ein generelles Vorgehen für den Fall festgelegt werden, dass keine spezifischen Regeln existieren. In diesem Zusammenhang gibt es grundsätzlich die beiden Ansätze "Was nicht verboten ist, ist erlaubt" (Blacklist) und "Was nicht erlaubt ist, ist verboten" (Whitelist). Bei der Konfiguration sollte generell der restriktivere Whitelist-Ansatz bevorzugt werden, da beim reinen Blacklist-Ansatz nahezu zwangsläufig Lücken bestehen bleiben.

Mit Hilfe von ACLs kann nicht nur der Zugriff auf das Netzkoppelelement selbst, sondern auch der Datenverkehr über das Netzkoppelelement kontrolliert werden. Insbesondere Router werden als Paketfilter in lokalen Netzen und Weitverkehrsnetzen eingesetzt. Der Router kontrolliert in diesem Fall den Datenverkehr pro Interface und Richtung (inbound und outbound) zwischen den angeschlossenen Subnetzen.

Für verbindungsbehaftete Protokolle (beispielsweise TCP) gibt es zudem die Möglichkeit, ACLs zu definieren, die den Status der Verbindung berücksichtigen. Dies erlaubt es, vorzugeben, dass bestimmte Verbindungen nur in einer Richtung durch den Router erlaubt sind (beispielsweise Telnet-Verbindungen "von innen nach außen"). Dabei lässt der Router Pakete in der Gegenrichtung passieren, wenn sie Antwortpakete zu einer bestehenden Verbindung sind, weist jedoch Pakete zurück mit denen ein Verbindungsaufbau in der verbotenen Richtung versucht werden soll.

Verbindungslose Protokolle wie UDP lassen sich nur unzureichend mit einem herkömmlichen Paketfilter absichern. Für diesen Zweck wird deshalb oftmals ein Stateful-Inspection-System verwendet. Dabei führt das System eine Tabelle, in der gespeichert wird, ob und von wo innerhalb einer festgelegten Zeitspanne ein "erlaubtes" Paket (beispielsweise eine DNS-Anfrage) an eine bestimmte Adresse gesendet wurde. Wird innerhalb der festgelegten Zeit ein Paket in der entgegengesetzten Richtung registriert, so wird dies als Antwort

auf die gespeicherte Anfrage interpretiert und durchgelassen. Pakete, zu denen es keine entsprechende Anfrage gibt, werden abgewiesen.

In der Regel werden innerhalb einer ACL mindestens folgende Kriterien ausgewertet:

- Quelladresse (IP-Adresse im IP-Header) des Pakets
- Zieladresse (IP-Adresse im IP-Header) des Pakets
- Verwendetes Protokoll und gegebenenfalls Portnummer (z. B. Port 80/TCP für HTTP oder 25/TCP für SMTP)

Zum Erkennen von Problemen wie beispielsweise Konfigurationsfehlern oder Angriffsversuchen im Netz sind ACLs immer derart zu konfigurieren, dass abgewiesene Zugriffsversuche protokolliert werden. Hierzu ist jedem Eintrag in der ACL das entsprechende Protokoll-Kommando anzufügen. Die Protokolldateien werden so zu einer wertvollen Datenquelle im Umgang mit Problemen und Angriffen im Netz.

Die Erstellung einer ACL muss entsprechend den Vorgaben der Sicherheitsrichtlinie erfolgen. Nach Möglichkeit sollten Vorlagen (Templates) erstellt werden, die immer wieder verwendet werden können und nur gegebenenfalls geringfügig modifiziert werden müssen.

Bei der Nutzung von ACLs muss beachtet werden, dass damit eine gewisse Performance-Einbuße verbunden ist. Meist ist diese zwar selbst bei komplizierteren Regeln vernachlässigbar, wenn aber ein Router bereits mit einer erheblichen Auslastung betrieben wird, dann sollte vor einer Erweiterung der ACLs sicherheitshalber geprüft werden, ob das Gerät die erweiterten Regeln noch verarbeiten kann.

Nachfolgend sind als Beispiel einige Filterregeln anhand eines Auszugs aus einer Access Control List für einen Router des Herstellers Cisco dargestellt. Es wird davon ausgegangen, dass es sich um eine eingehende Zugriffsliste (inbound) handelt. Folgende Dienste sollen eingehend erlaubt, sonstige Verbindungen verboten werden:

- SMTP zum internen MAIL-SERVER
- TELNET zu einem internen TELNET-SERVER
- HTTP zum internen WEB-SERVER
- HTTPS zum internen WEB-SERVER

```
access-list 103 permit tcp any any established
access-list 103 permit tcp any host MAIL-SERVER eq smtp
access-list 103 permit tcp any host TELNET-SERVER eq telnet
access-list 103 permit tcp any host WEB-SERVER eq www
access-list 103 permit tcp any host WEB-SERVER eq 443
access-list 103 deny ip any any log
```

Ergänzende Kontrollfragen:

- Wurde die Einrichtung von Access Control Lists anhand der Sicherheitsrichtlinie durchgeführt?
- Wurde die Funktionalität der Access Control Lists geprüft?
- Werden nicht erlaubte Verbindungen protokolliert?

M 5.112 Sicherheitsaspekte von Routing-Protokollen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Authentisierung

Idealerweise sollten nur Routing-Protokolle eingesetzt werden, die eine sichere Authentisierung der Router beim Austausch von Routing-Informationen unterstützen. Sobald Updates von Routing-Tabellen versendet werden, muss eine Authentisierung des Routers stattfinden, der diese Routing-Updates versendet hat. Damit wird erreicht, dass ein Router nur zuverlässige Routing-Informationen von einer vertrauten Quelle (Router) verarbeitet. Ohne eine Authentisierung beim Austausch von Routing-Informationen wird die Sicherheit des Netzes durch unautorisierte oder absichtlich gefälschte Routing-Updates gefährdet.

Zusätzliche Sicherheit wird durch die Einrichtung von Access Control Lists erreicht, so dass nur definierte IP-Adressen Routing-Informationen austauschen dürfen.

Dynamische Routing-Protokolle sollten ausschließlich in sicheren Netzen verwendet werden. In demilitarisierten Zonen (DMZ) dürfen sie nicht eingesetzt werden. Gelingt es nämlich einem Angreifer, Datenpakete beim Austausch von Routing-Informationen in der DMZ mitzulesen, so kann er daraus Kenntnisse über die interne Netzstruktur erlangen. In demilitarisierten Zonen sollten stattdessen statische Routen eingetragen werden.

Folgende Routing-Protokolle unterstützen die Authentisierung beim Austausch von Routing-Informationen:

- Border Gateway Protocol (BGPv4)
- Open Shortest Path First (OSPFv2)
- Routing Information Protocol in der Version 2 (RIPv2)
- Enhanced Interior Gateway Protocol (EIGRP)
- Intermediate-System-to Intermediate-System (IS-IS)

Die Authentisierung eines Routers, der Routing-Updates versendet, wird durch den Austausch eines Schlüssels (Passwort) erreicht. Dieser Schlüssel muss allen beteiligten Routern bekannt sein. Der Schlüssel wird bei der Konfiguration des Routers vom Administrator festgelegt. Diese Schlüssel sollten regelmäßig geändert werden.

MD5-Authentisierung

Bei den unterschiedlichen Routing-Protokollen wird zwischen der Klartextauthentisierung und der verschlüsselten Authentisierung unterschieden. Es kann nur der Einsatz von Routing-Protokollen empfohlen werden, die eine verschlüsselte Authentisierung unterstützen.

Bei der verschlüsselten Authentisierung wird MD5 verwendet. Statt des eigentlichen Schlüssels wird dabei ein sogenanntes Message-Digest zur Authentisierung versendet. Der Message-Digest wird zwar mit Hilfe des Schlüssels erzeugt, jedoch wird der Schlüssel nicht über das Netz gesendet.

Damit wird verhindert, dass der Schlüssel im Netz mitgelesen werden kann. Sollte die Änderung von Schlüsseln mit Hilfe des SNMP-Protokolls durchgeführt werden, ist darauf zu achten, dass in diesem Fall der Schlüssel im Klartext über das Netz versendet wird.

Folgende Protokolle unterstützen die MD5-Authentisierung:

- Border Gateway Protocol (BGPv4)
- Open Shortest Path First (OSPFv2)
- Routing Information Protocol in der Version 2 (RIPv2)
- Enhanced Interior Gateway Protocol (EIGRP)

Schlüsselverwaltung

Einige Routing-Protokolle bieten eine Verwaltung von Schlüsseln unter Verwendung sogenannter Schlüsselketten an. Eine Schlüsselkette besteht aus einer Reihe von festgelegten Schlüsseln. Diese Schlüssel werden von den Routern im Rotationsverfahren verwendet. Dies verringert die Wahrscheinlichkeit, dass die Schlüssel ausgespäht werden. Der Schlüssel innerhalb einer Schlüsselkette besitzt nur für einen definierten Zeitraum Gültigkeit. Hier ist es wichtig, dass die Router die genaue Uhrzeit besitzen, damit der Schlüssel synchron gewechselt wird. Dies kann durch die Angabe eines internen NTP-Servers erreicht werden. Idealerweise sollte der interne NTP-Server mit einer Funkuhr verbunden sein.

Folgende Protokolle unterstützen die Schlüsselverwaltung:

- Routing Information Protocol in der Version 2 (RIPv2)
- Enhanced Interior Gateway Protocol (EIGRP)

Die folgende Tabelle stellt die unterschiedlichen Merkmale von Routing-Protokollen aus sicherheitstechnischer Sicht in bezug auf die Authentisierung dar:

Protokollname	Authentisierung	Klartext	MD5 Hash	Protokoll RFCs
RIPv1	Nein			RFC 1058
IGRP	Nein			Proprietär (Cisco)
RIPv2	Ja	Ja	Ja	RFC 1723
EIGRP	Ja		Ja	Proprietär (Cisco)
OSPFv2	Ja	Ja	Ja	RFC 2328
IS-IS	Ja	Ja		RFC 1142 (ISO 10589), 1195
BGPv4	Ja		Ja	RFC 1771

Tabelle: Authentisierung bei unterschiedlichen Routing-Protokollen

Ergänzende Kontrollfragen:

- Welche Routing-Protokolle werden eingesetzt?
- Wurden bei der Planung des Einsatzes des Routers die Sicherheitsaspekte der verwendeten Routing-Protokolle berücksichtigt?
- Wurde berücksichtigt, dass in sicherheitsrelevanten Teilnetzen (z. B. DMZ) keine Routing-Protokolle verwendet werden sollen?
- Wurde eine klar abzugrenzende Routing-Domäne definiert?
- Werden Routing-Protokolle eingesetzt, die eine sichere Authentisierung unterstützen?

M 5.113 Einsatz des VTAM Session Management Exit unter z/OS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Verfahrensverantwortlicher, Administrator

Die z/OS-Komponente VTAM (*Virtual Telecommunication Access Method*) bietet die Möglichkeit, den Login-Vorgang durch einen *VTAM Session Management Exit* (*ISTEXCAA*) zusätzlich zu schützen. Dieser *Exit* wird während des Session-Aufbaus und -Abbaus von VTAM aus angesprochen und erlaubt die folgenden Funktionen:

- Session Authorization

  Prüfen und Erlauben/Ablehnen von *Logical Unit Sessions*

- Session Accounting

  Sammeln von *Session-Accounting*-Daten zur späteren Auswertung

- Adjacent SSCP Selection

  Auswahl eines *System Service Control Point* nach definierten Regeln (Routing)

- Unterstützung des Session Takeover im Rahmen von XRF Application Processing

Für die beiden ersten Funktionen wird der *VTAM Session Management Exit* häufig eingesetzt, für die beiden letzten dagegen nur in wenigen Sonderfällen. Der *VTAM Session Management Exit* muss vom Betreiber selbst erstellt oder beschafft werden. Der Hersteller liefert keinen *VTAM Session Management Exit* mit dem Betriebssystem aus.

Für den Einsatz des *VTAM Session Management Exits* sollten die folgenden Empfehlungen beachtet werden.

Hinweise zur Programmierung

Assembler-Kenntnisse

Der *Exit* muss in Assembler programmiert werden. Zudem werden gute Kenntnisse der VTAM-Software vorausgesetzt. Wenn die notwendigen Kenntnisse nicht vorliegen, ist zu überlegen, ob am Markt verfügbare alternative Software-Produkte eingesetzt werden sollten. Diese sind häufig einfacher und sicherer zu installieren.

Performance

Der *Exit* kann die VTAM-Performance erheblich beeinflussen. Deshalb ist darauf zu achten, dass beim Durchlaufen des *Exits* keine zeitaufwendigen Aktivitäten, wie z. B. das Lesen von Dateien, stattfinden.

Definitionen

Alle Definitionen, die der *Exit* während des Betriebs benutzt, sollten dynamisch nachladbar sein, ohne dass Betriebsfunktionen gestoppt werden müssen.

Das Regelwerk (*Policy*) für den *Exit* sollte möglichst extern definierbar sein (keine Definitionen im Programm).

Unterstützte Funktionen

Es sollten mindestens folgende Funktionen im *Exit* unterstützt werden:

- Schreiben eines LOG-Eintrags (*Syslog*)
- Schreiben eines SMF-Records
- Schnittstelle zu WTO (*Write to Operator*) für Abweisungen

Damit ist eine nachträgliche Kontrolle der abgewiesenen Login-Versuche möglich. Als Option können zusätzlich Statistik-Informationen geführt werden, jedoch können diese Informationen auch aus den SMF-Records abgeleitet werden.

Schutz der Sicherheitsregeln

Das Regelwerk (*Policy*) des *Exits* sollte in einer separaten Datei geführt werden, die beim ersten Durchlaufen des *Exits* in den Hauptspeicher geladen wird. Es sollten nur die Mitarbeiter Zugriff auf diese Datei haben, deren Tätigkeit dies erfordert. Dies gilt besonders dann, wenn das Regelwerk des *Exits* in der aktuellen *VTAMLST*-Datei geführt wird. Es ist zu überlegen, ob die Verkettung von verschiedenen *VTAMLST*-Dateien helfen kann, die Sicherheit des Betriebs zu erhöhen. Verschiedene *VTAMLST*-Dateien erlauben unterschiedliche Zugriffsrechte, wobei die verketteten Dateien in Bezug auf die Verarbeitung wie eine Datei behandelt werden. Eine Vertretungsregelung ist vorzusehen.

VTAM Kommandos

Der *VTAM Session Management Exit* kann während des Betriebs durch das *VTAM Modify*-Kommando dynamisch aktiviert bzw. deaktiviert werden. Durch entsprechende RACF-Definitionen ist sicherzustellen, dass nur die Mitarbeiter Zugang zu diesem Kommando haben, deren Tätigkeit dies erfordert. Eine Vertretungsregelung ist vorzusehen.

Einsatz von NetView ALIAS Name Translation

Im *VTAM Session Management Exit* können Funktionen zur *ALIAS Name Translation* eingesetzt werden. Parallel hierzu kann auch die *NetView ALIAS Name Translation Facility* verwendet werden. Letzteres wird durch ein Flag angezeigt. Wenn beides eingesetzt wird, ist darauf zu achten, dass beide Möglichkeiten zur *ALIAS Name Translation* aufeinander abgestimmt und widerspruchsfrei sind. Beispielsweise dürfen keine unterschiedlichen *Aliase* für den selben Namen gesetzt werden.

Ergänzende Kontrollfragen:

- Falls ein *VTAM Session Management Exit* eingesetzt ist, werden dessen Regeln extern definiert?
- Ist das *VTAM Modify*-Kommando durch entsprechende RACF-Profile vor unautorisiertem Zugang geschützt?
- Lassen sich die *Exit*-Regeln dynamisch ohne Betriebsunterbrechung nachladen?

M 5.114 Absicherung der z/OS-Tracefunktionen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Mit Trace-Funktionen können unter z/OS Fehler beim Verbindungsaufbau analysiert werden. Sie können sowohl in VTAM (*Virtual Telecommunication Access Method*), als auch bei TCP/IP benutzt werden. Das GTF (*Generalized Trace Facility*) wird benutzt, um die Trace-Daten zu erfassen und auszuwerten. Darüber hinaus stehen auch die Funktionen NLDM (*Network Logical Data Manager* - eine NetView-Komponente) und ACFTAP (*Advanced Communication Facility Trace Analysis Programm*) für die Auswertung von VTAM-Daten zur Verfügung.

Trace-Funktionen zeigen nicht nur Fehler auf, sondern erlauben auch die Darstellung der übertragenen Daten selbst. Deshalb sind die folgenden Hinweise zu beachten:

Schutz von Trace-Funktionen und GTF

Werden Session-Daten unverschlüsselt übertragen, sind die Passwörter in Klarschrift im Trace lesbar. Zugang zu den Kommandos, die Traces initiieren können, darf deshalb nur den Mitarbeitern gegeben werden, die GTF im Rahmen ihrer Tätigkeit benötigen. Die Zahl dieser Mitarbeiter sollte möglichst klein gehalten werden, um das Risiko von Vertraulichkeitsverletzungen zu minimieren.

Schutz von GTF-Dateien

Die GTF-Auswertungen werden in Dateien gesichert. Diese Dateien müssen so geschützt werden, dass nur die zuständigen Mitarbeiter darauf Zugriff haben (insbesondere *Universal Access=NONE*). Dies gilt auch für Kopien dieser Dateien.

NLDM Traces

Die Trace-Funktion von NLDM sollte normalerweise deaktiviert sein und nur im Bedarfsfall aktiviert werden. Sie sollte nur den zuständigen Mitarbeitern zur Verfügung stehen.

Schutz von ACFTAP

Das Programm ACFTAP sollte so geschützt werden, dass nur die zuständigen Mitarbeiter Zugriff auf dieses Programm haben.

Session-Daten

Um die Passwörter vor unbefugtem Mitlesen bei der Übertragung zu schützen, sollte überlegt werden, die Session-Daten verschlüsselt zu übertragen. Es wird empfohlen, dies mindestens für die Verbindungen der RACF-Administratoren (*Resource Access Control Facility*) vorzusehen.

Ergänzende Kontrollfragen:

- Werden die Session-Daten verschlüsselt übertragen?
- Sind die GTF-Dateien und Kopien davon so geschützt, dass nur entsprechend autorisierte Mitarbeiter Zugriff auf diese Dateien haben?

M 5.115 Integration eines Webservers in ein Sicherheitsgateway

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Die Integration eines Webservers in ein Sicherheitsgateway ist in vielen Fällen kritisch, da ein Webserver oft hohe Anforderungen an die Netz-Bandbreite stellt. Neben der Sicherstellung der Verfügbarkeit ist zum Schutz vor gezielten Angriffen auch die Wahl der richtigen Variante zur Server-Platzierung wichtig, da Webserver auf Grund ihrer hohen "Sichtbarkeit" besonders Angriffen ausgesetzt sind und in Webserver-Programmen in der Vergangenheit oft Sicherheitslücken vorhanden waren.

Im folgenden werden drei Szenarien beschrieben, wie ein Webserver in ein Sicherheitsgateway integriert werden kann:

- Integration ohne Verwendung eines Reverse Proxy
- Integration unter Verwendung eines Reverse Proxy, der die Auslastung des Webservers reduzieren soll.
- Integration unter Verwendung eines Reverse Proxy und mit zusätzlicher Absicherung durch einen weiteren Paketfilter.

In allen drei Fällen wird der Server nicht hinter einem ALG, sondern nur hinter einem Paketfilter aufgestellt, da der ALG den Gesamtdurchsatz des Systems unter Umständen zu stark beeinträchtigen kann. Daher sind die Empfehlungen auch dann anwendbar, wenn nur ein einfaches Sicherheitsgateway (bestehend nur aus einem Paketfilter) eingesetzt wird. Der Webserver sollte in keinem Fall im internen Netz angesiedelt werden.

Spezielle ALGs für Webanwendungen

Bei besonderen Sicherheitsanforderungen kann es trotzdem erforderlich sein, den Webserver mit einem eigenen ALG abzusichern, der den Webserver und darauf betriebene Webanwendungen vor bestimmten Arten von Angriffen (Cross-Site Scripting, Command Injection und ähnliches) schützt. Entsprechende ALGs existieren von verschiedenen Anbietern. Bei komplexeren Webanwendungen wird der Einsatz eines solchen ALG empfohlen.

Webserver ohne Verwendung eines Reverse Proxy

Bestehen keine besonderen Anforderungen an die Sicherheit des Webservers selbst und kann der Server die ankommenden Anfragen problemlos bewältigen, so bietet es sich an, den Webserver in einer eigenen DMZ des externen Paketfilters anzusiedeln.

Durch entsprechende Paketfilterregeln sollte sichergestellt werden, dass der Webserver vor Angriffen von außen so weit wie möglich geschützt wird. Zusätzlich sollte durch weitere Filterregeln dafür gesorgt werden, dass ein Angreifer selbst nach einer erfolgreichen Kompromittierung des Webservers selbst so wenig weiteren Schaden wie möglich anrichten kann. In der folgenden Tabelle sind Empfehlungen zusammengestellt.

Quelle	Ziel	Entscheidung	Bemerkungen
Allgemein			
Webserver	externes Netz und internes Netz	Nur Pakete erlauben, die zu einer Verbindung gehören, die vom anderen Rechner initiiert wurde	Der Webserver antwortet nur auf Anfragen. Eigene Verbindungen brauchen nicht aufgebaut zu werden
Kommunikation des Webservers mit dem Internet			
Externes Netz	Webserver Port 80	erlauben	Port 80 ist der Standardport
Externes Netz	andere Ports des Webservers	verbieten	
Kommunikation des Webservers mit dem internen Netz			
Internes Netz	Webserver Port 80	erlauben	Nutzung des Webservers auch vom internen Netz aus
Internes Netz (gegebenenfalls Einschränkung auf Administrationsnetz)	Webserver Port 22 (SSH)	erlauben	Administration und Datenübertragung erfolgen per SSH und SCP
Internes Netz	andere Ports des Webservers	verbieten	
Protokollierung			
Webserver	Loghost UDP-Port 514	erlauben	Übertragung der Protokolldaten zum Loghost

Dabei wird davon ausgegangen, dass die Administration des Webservers aus dem internen Netz über eine SSH-Verbindung abgewickelt wird und dass die WWW-Daten per SCP auf den Webserver übertragen werden. Weiter wird davon ausgegangen, dass auf dem Webserver kein DNS verwendet wird. Eine Namensauflösung ist zum normalen Betrieb nicht notwendig. Für die Erstellung von Zugriffsstatistiken oder sonstigen Auswertungen kann sie gegebenenfalls später erfolgen. Die auf dem Webserver anfallenden Protokolldaten werden über das Netz an einen eigenen Loghost geschickt (siehe auch M 4.225 *Einsatz eines Protokollierungsservers in einem Sicherheitsgateway*).

Dadurch, dass keine Verbindungen zugelassen werden, die vom Webserver aus initiiert werden, kann beispielsweise ein Angreifer, der den Webserver kompromittiert hat, entscheidend behindert werden. Meist benötigt ein Angreifer nämlich zur Fortsetzung seines Angriffs nach dem Einbruch weitere

Tools, die er von externen Rechnern nachlädt. Wenn dies wegen entsprechender Paketfilterregeln nicht möglich oder deutlich erschwert ist, so brechen weniger geschickte oder entschlossene Angreifer (beispielsweise *Script Kiddies*) den Angriff eventuell sogar ab.

Falls die Administration des Webservers auf andere Weise abgewickelt oder die WWW-Daten auf andere Weise auf den Webserver übertragen werden, so sollten für die jeweils genutzten Protokolle entsprechende Filterregeln umgesetzt werden.

Webserver unter Verwendung eines Reverse Proxy

Im ersten Szenario trägt der Webserver die gesamte Belastung durch eingehende Anfragen. Soll der Webserver von eingehenden Anfragen entlastet werden, kann ein Reverse Proxy eingesetzt werden, der häufig wiederkehrende Anfragen aus seinem Cache beantwortet und so die Belastung des Webservers selbst reduziert.

Zur Erzielung eines möglichst hohen Durchsatzes ist es notwendig, Webserver und Reverse Proxy in der gleichen DMZ aufzustellen. Der Zugriff aus dem nicht-vertrauenswürdigen Netz sollte nur auf den Reverse Proxy gestattet sein, der direkte Zugriff auf den Webserver aus dem nicht-vertrauenswürdigen Netz sollte durch den äußeren Paketfilter unterbunden werden.

Webserver und Reverse Proxy in getrennten DMZs

Reverse Proxies wurden meist nicht primär unter dem Aspekt der Sicherheit entwickelt. Daher sollte gegebenenfalls in Betracht gezogen werden, den Reverse Proxy durch einen weiteren Paketfilter vom Webserver zu trennen. Dies erhöht die Sicherheit für den Webserver, kann aber andererseits zu einer Reduzierung der zur Verfügung stehenden Bandbreite führen.

Auf diese Weise können bei einer etwaigen Kompromittierung des Reverse Proxy unerwünschte Zugriffe vom Reverse Proxy auf den Webserver (z. B. auf Administrationsports) unterbunden werden. Diese Lösung ist in der folgenden Abbildung dargestellt.

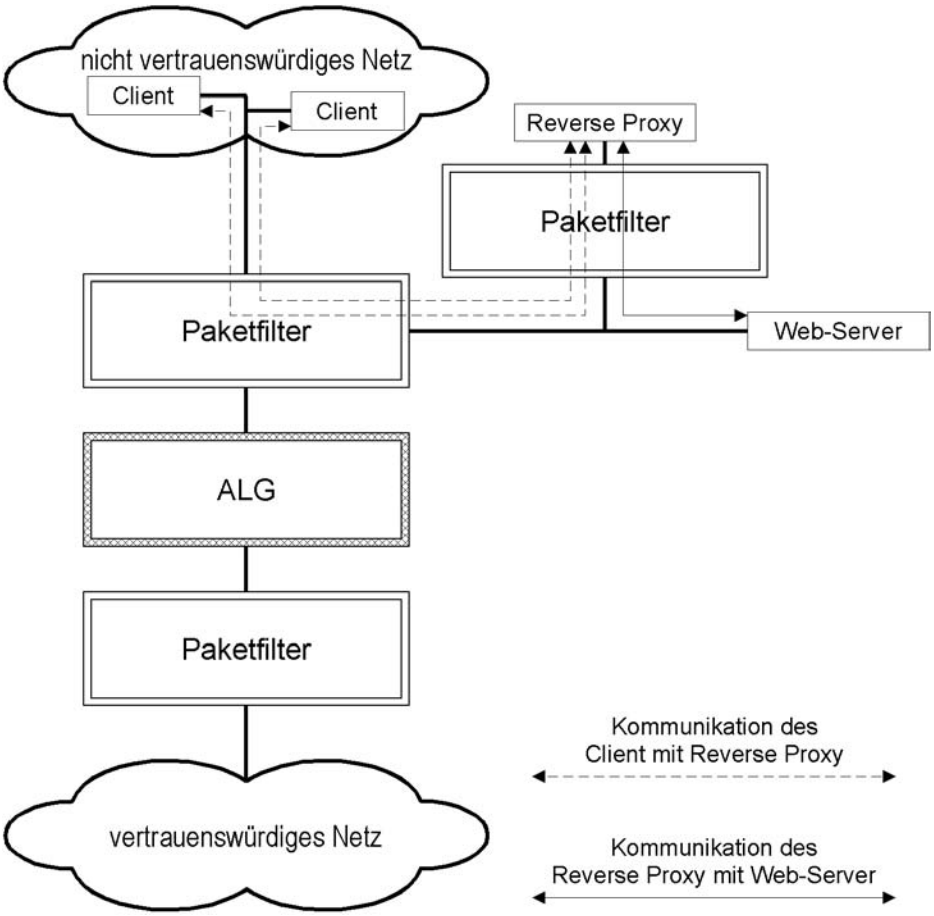


Abbildung 1: Integration eines Webservers unter Verwendung eines (reverse) Caching-Proxy und eines weiteren Paketfilters zur zusätzlichen Absicherung des Webservers

Diese Lösung ist äquivalent dazu, den Reverse Proxy und den Webserver in unterschiedlichen DMZs des äußeren Paketfilters anzusiedeln. Ob die zusätzliche Filterstufe eingesetzt werden soll muss im konkreten Einsatzszenario abgewogen werden.

Ergänzende Kontrollfragen:

- Wie ist der Webserver in das Sicherheitsgateway integriert?
- Wird ein zusätzlicher ALG zum Schutz vor Angriffen auf Webanwendungen eingesetzt?

M 5.116 Integration eines E-Mailservers in ein Sicherheitsgateway

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Bei der Frage der Integration eines E-Mailservers in ein Sicherheitsgateway werden zwei Szenarien betrachtet: Im ersten Fall geht es nur darum, den Dienst E-Mail für ein einzelnes vertrauenswürdiges Netz zur Verfügung zu stellen, im zweiten Fall soll E-Mail für mehrere vertrauenswürdige Netze bereitgestellt werden.

Bei beiden Szenarien werden interne E-Mailserver in den vertrauenswürdigen Netzen betrieben. Ein E-Mailserver innerhalb des vertrauenswürdigen Netzes wird zur Verwaltung der Alias-Datenbank, mit der die Benutzeradressen auf ein einheitliches Format umgesetzt werden können, gegebenenfalls für einen POP- oder IMAP-Daemon oder auch als Gateway zum Übergang in ein anderes Mailsystem (z. B. X.400) eingesetzt. Alle internen Mails werden an diesen Server geschickt und von dort gegebenenfalls über einen externen Mailserver nach außen weitergeleitet.

Die Nutzung eines internen Mailservers ist aus verschiedenen Gründen empfehlenswert:

- E-Mails zwischen Rechnern innerhalb der vertrauenswürdigen Netze verlassen diese Netze nicht, da sie von den jeweiligen internen Mailservern verarbeitet werden.
- Wird der interne Mailserver gleichzeitig als Groupware-Server eingesetzt, so könnte dies zu einer unnötig hohen Belastung des ALG führen.
- Ein Groupware-Server ist auf diese Weise besser vor Angriffen von außen geschützt, da er weiter vom nicht-vertrauenswürdigen Netz entfernt ist.

Es wird allerdings empfohlen, die Mail- bzw. Groupware-Server im internen Netz zusätzlich zumindest durch Paketfilterregeln auch vor unberechtigtem Zugriff aus dem internen Netz geschützt werden. Dies entspricht der Aufstellung des Servers in einer eigenen DMZ des inneren Paketfilters. Bei besonderen Sicherheitsanforderungen im internen Netz sollte dies unbedingt geschehen.

Im Unterschied zum Webserver, bei dem eine Aufstellung "möglichst weit außen" im Sicherheitsgateway empfohlen wird, stellt die hier empfohlene Anordnung für E-Mailserver eine Aufstellung "möglichst weit innen" dar. Der Grund dafür ist, dass auf diese Weise auch bei Ausfall der Internetanbindung immer noch interne E-Mails geschickt werden können.

Anbindung eines einzelnen vertrauenswürdigen Netzes

Soll nur für ein einzelnes vertrauenswürdiges Netz ein Mailserver eingesetzt werden, so genügt der interne Mailserver alleine. Der ALG agiert in diesem Fall als "Smart Host" für den internen Mailserver.

Smart Host

Ein Smart Host ist ein Rechner, über den alle E-Mails eines Netzes geleitet werden. Wenn der ALG als Smart Host für den internen Mailserver konfiguriert ist, so braucht der interne Mailserver für abgehende E-Mails nicht

zu ermitteln, welches der Mailserver der Empfänger-Domain ist, sondern er leitet die E-Mails einfach an den Smart Host weiter, der die Aufgabe übernimmt, den richtigen Empfänger-Mailserver zu ermitteln. Dies kann ebenfalls wieder ein Smart Host (beispielsweise beim Internet-Dienstleister) sein; wenn der ALG als Smart Host für das interne Netz eingesetzt wird, so wird dies normalerweise der Fall sein. Smart Hosts werden auch gelegentlich als Mail-Relays bezeichnet.

Für eintreffende E-Mails agiert der ALG entweder als Mail Exchanger, der alle eingehenden E-Mails von den Absender-Mailservern entgegennimmt und an den internen Mailserver weiterleitet, oder als Smart Host für einen externen Mail-Exchanger.

Anbindung mehrerer vertrauenswürdiger Netze

Wenn ein Sicherheitsgateway für mehrere vertrauenswürdige Netze gemeinsam eingesetzt wird, etwa als gemeinsamer Internet-Zugang für mehrere Standorte einer Organisation, so ist der oben beschriebene einfache Aufbau oft nicht mehr machbar.

Versand und Empfang von E-Mails sollten bei diesem Szenario zweistufig erfolgen: Nach wie vor sollten in den vertrauenswürdigen Netzen eigene Mailserver eingesetzt werden, über die interne E-Mails direkt verschickt werden können. Zusätzlich ist es sinnvoll, einen zentralen Mailserver in der DMZ einzusetzen, der als zentraler Mail Exchanger für die vertrauenswürdigen Netze agiert und über den externe E-Mails abgewickelt werden. Je nach Produkt kann ein solcher E-Mailserver in der DMZ bereits in das ALG integriert sein.

Die folgende Abbildung zeigt einen solchen Aufbau mit zwei vertrauenswürdigen Netzen mit jeweils einem internen Mailserver, die mit einem nicht-vertrauenswürdigen Netz (beispielsweise dem Internet) verbunden sind. Die beiden internen Mailserver sind zuständig für unterschiedliche (Sub-) Domains, d. h. der Mailserver in der DMZ entscheidet, zu welchem internen Mailserver eintreffende E-Mails weitergeleitet werden.

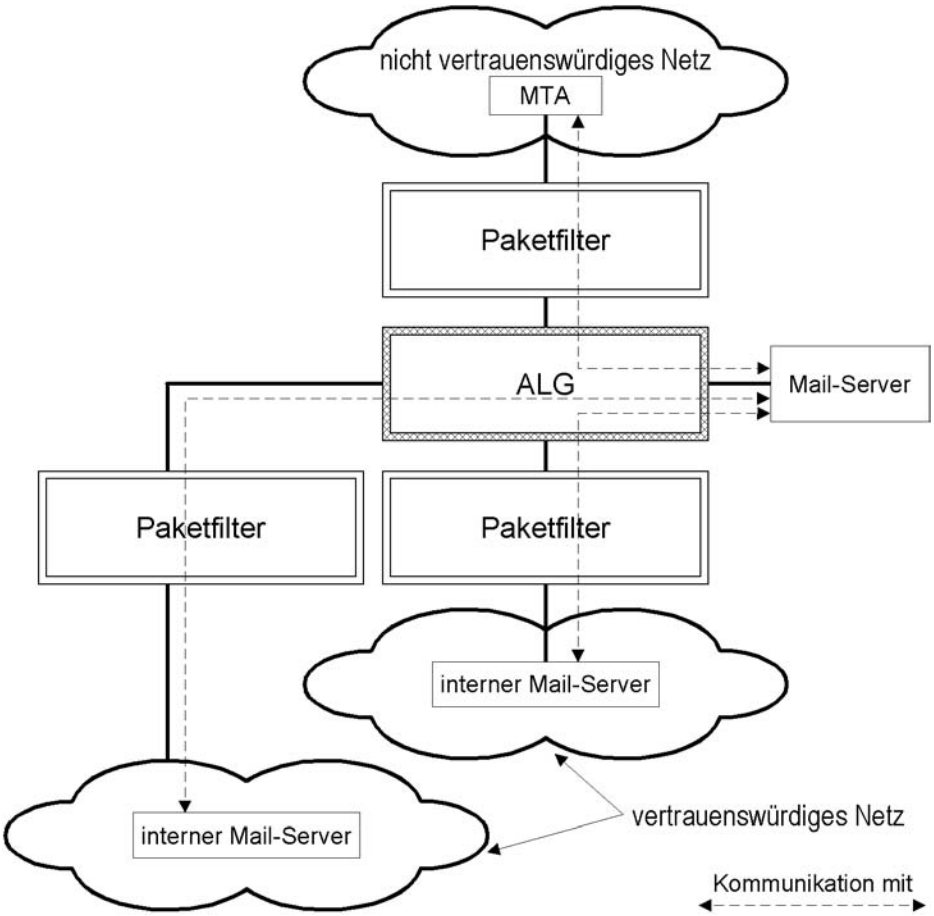


Abbildung 1: Platzierung der internen MTAs und des Mailservers zur Anbindung von zwei vertrauenswürdigen Netzen (an der Schnittstelle des ALG zur DMZ müssen zwei SMTP-Proxies eingerichtet werden, z. B. unter Zuhilfenahme von virtuellen IP-Adressen).

Eingehende externe E-Mails passieren die MTAs wie folgt:

1. MTA im nicht-vertrauenswürdigen Netz (beim Absender oder beim Internet-Dienstleister)
2. MTA in der DMZ. Dieser trifft die Entscheidung, in welches der beiden vertrauenswürdigen Netze (bzw. an welchen MTA) die E-Mail weitergeleitet werden muss.
3. Mailserver im jeweiligen vertrauenswürdigen Netz

Ausgehende E-Mails passieren die MTAs in der umgekehrten Reihenfolge.

E-Mailserver bei einfachen Sicherheitsgateways

Wird nur ein einfaches Sicherheitsgateway bestehend aus einem Paketfilter eingesetzt, so wird empfohlen, den E-Mailserver in einer DMZ des Paketfilters anzusiedeln. Wegen des fehlenden ALGs ist der Schutz des

Mailservers vor einer Kompromittierung von außen dabei geringer. Die Aufstellung in der DMZ bietet im Ausgleich einen etwas höheren Schutz des internen Netzes bei einer Kompromittierung des Mailservers, als wenn der Server direkt im internen Netz angesiedelt würde.

Soll auch bei einem Ausfall der externen (Internet-) Anbindung das Verschicken interner E-Mails noch gewährleistet sein, so kann der E-Mail-Server in das interne Netz verlegt werden und zusätzlich ein Mailserver (MTA) in einer DMZ des Paketfilters angesiedelt werden, der als externer Mail-Exchanger agiert. Diese Lösung stellt eine gewissermaßen eine Mischung aus den oben beschriebenen komplexeren Lösungen dar.

Ergänzende Kontrollfragen:

- Wo ist der E-Mailserver aufgestellt?
- Welche Kommunikationsverbindungen sind zugelassen?

M 5.117 Integration eines Datenbank-Servers in ein Sicherheitsgateway

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Bei der Aufstellung von Datenbank-Servern zum Zugriff aus einem nicht-vertrauenswürdigen Netz sind zwei Haupt-Anwendungsfälle zu unterscheiden:

1. Zugriff auf die Daten der Datenbank über ein Web-Frontend
2. Direkter Zugriff auf die Daten der Datenbank (z. B. mittels SQL)

Beide Anwendungsfälle werden in den folgenden beiden Abschnitten beschrieben:

Zugriff über Web-Frontend

Der Webserver und der Datenbank-Server sollten in unterschiedlichen DMZ stehen, damit bei einer Kompromittierung des Webservers ein Schutz des Datenbank-Servers durch einen Proxy des Application Level Gateways (ALG) besteht. Der Schutz durch den Proxy ist allerdings nur gering, beispielsweise wird der TCP/IP-Stack des Datenbank-Servers geschützt. Zudem können Angriffe auf Basis von TCP/IP-Header-Daten verhindert werden. Falls keine besonderen Sicherheitsanforderungen bestehen, so kann der Server auch in der gleichen DMZ wie der Webserver aufgestellt werden.

Der Aufbau und die Kommunikationsbeziehungen sind in diesem Fall wie folgt:

- Der Zugriff vom Internet aus erfolgt ausschließlich per HTTP oder HTTPS auf den Webserver. Die Zugriffe werden durch das ALG entsprechend abgesichert.
- Eine auf dem Webserver laufende Anwendung setzt die Anfrage in entsprechende Datenbankabfragen um, führt diese Abfragen auf der Datenbank aus und bereitet die Ergebnisse entsprechend auf.
- Die Administration des Datenbankrechners, des Datenbanksystems und die Pflege der Daten in der Datenbank erfolgen über entsprechend abgesicherte Verbindungen aus dem internen Netz.

Diese Verbindungen sind ebenfalls in der folgenden Abbildung dargestellt.

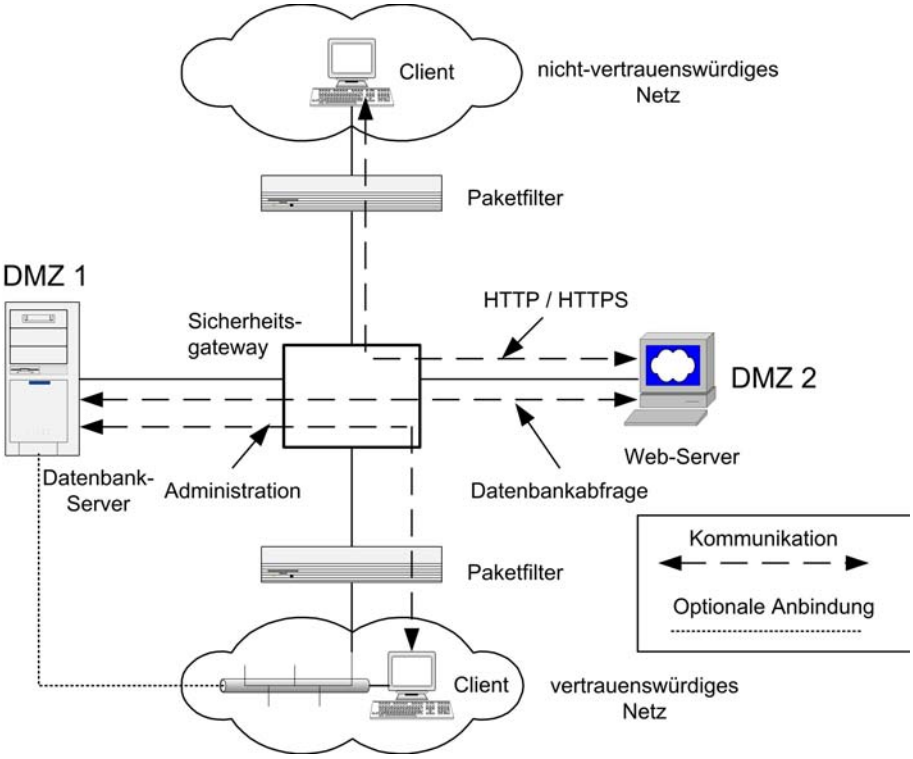


Abbildung 1: Zugriff auf eine Datenbank durch Nutzung eines Web-Frontends

Der Client im nicht-vertrauenswürdigen Netz kann ausschließlich an den Webserver über Webseiten Anfragen stellen, ein direkter Zugriff auf die Datenbank selbst ist nicht möglich.

Bei diesem Aufbau ist es über die Absicherung auf der Transportebene hinaus wichtig, dass die Anwendung auf dem Webserver, welche die Anfragen und Ergebnisse aufbereitet, entsprechend sicher programmiert ist und keine Möglichkeiten für Angriffe auf die Datenbank (beispielsweise SQL Injection) bietet. Falls über das Web-Frontend sogar direkt Datenbankanfragen in der betreffenden Datenbanksprache (beispielsweise SQL) formuliert werden können sollte der Zugriff auf das Web-Frontend nur über HTTPS erfolgen.

Direkter Zugriff

Soll auf die Datenbank direkt aus dem nicht-vertrauenswürdigen Netz heraus zugegriffen werden, so sollte der Server in einer eigenen DMZ aufgestellt werden. Da nur wenige Proxies für Datenbankprotokolle existieren, ist der Einsatz eines TCP- oder UDP-Relays oftmals unumgänglich.

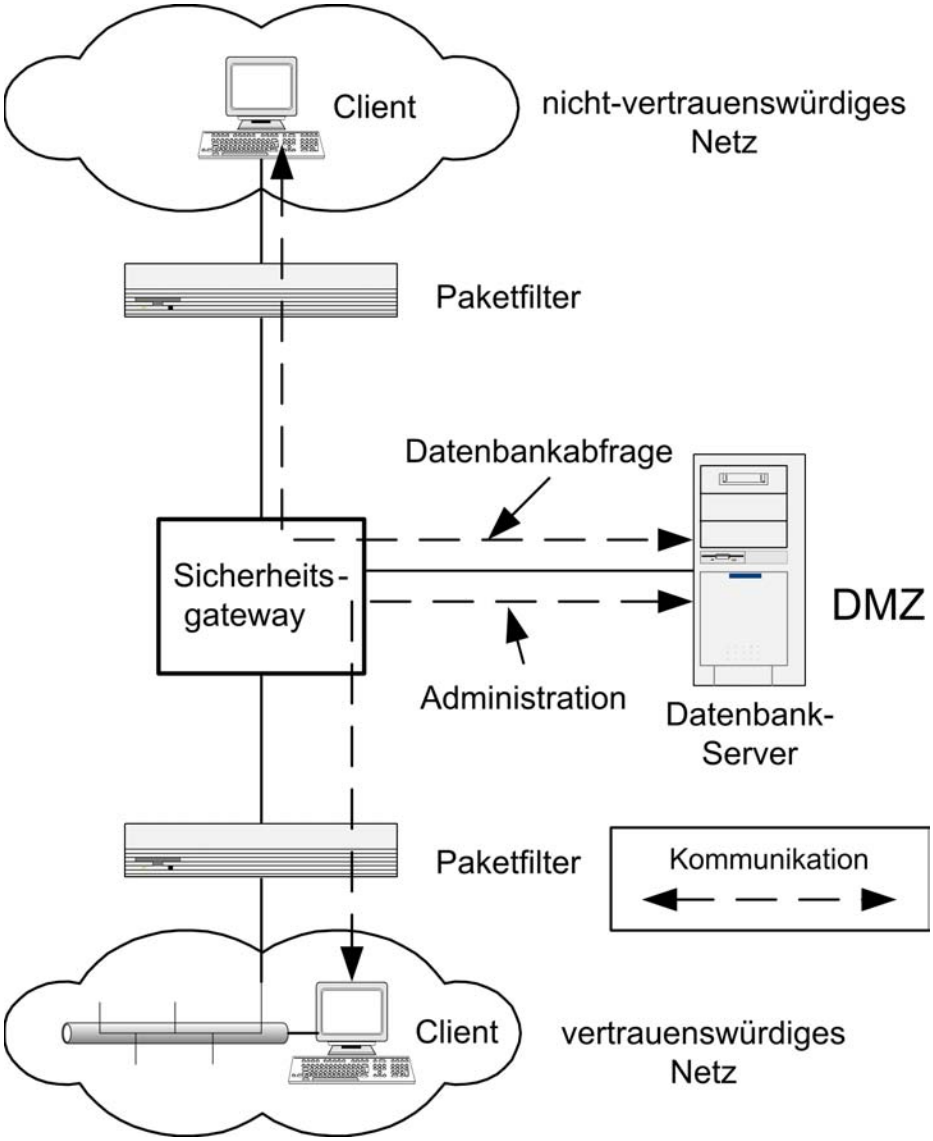


Abbildung 2: Direkter Zugriff auf eine Datenbank

Da sich, wegen der fehlenden Sicherheitsproxies für Datenbankabfrage-Protokolle kaum mittels Sicherheitsproxies kontrollieren lassen, ist die zuerst vorgestellte Lösung mit einem Web-Frontend in der Regel die sichere Variante.

Je nach dem Schutzbedarf der Daten in der Datenbank wird dringend empfohlen, nicht die "Echtdatenbank" für den externen Zugriff freizugeben, sondern nur eine Kopie der Daten auf einer separaten Datenbank, die in entsprechenden Intervallen mit der "Echtdatenbank" synchronisiert wird.

Ergänzende Kontrollfragen:

- Wie werden Datenbankabfragen abgewickelt?
- Falls ein Web-Frontend eingesetzt wird: Sind direkte Datenbankabfragen möglich? Wird der Zugriff über HTTPS abgesichert?
- Falls direkter Datenbankzugriff möglich ist: Wird ein entsprechender Sicherheitsproxy eingesetzt?

M 5.118 Integration eines DNS-Servers in ein Sicherheitsgateway

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator

Der Domain Name Service (DNS) dient zur Umsetzung von Rechnernamen in IP-Adressen und umgekehrt und stellt ferner Informationen über im Netz vorhandene Rechnersysteme zur Verfügung. Diese Informationen sind teilweise für die korrekte Funktion der Internetanbindung erforderlich, beispielsweise Informationen über DNS-Server oder Mail-Exchanger für eine Domain. Andererseits können DNS-Informationen auch von potentiellen Angreifern bei der Vorbereitung von Angriffen ausgenutzt werden. Hat ein Rechner beispielsweise einen Namen wie "mssql01", so kann ein Angreifer daraus schließen, dass es sich vermutlich um einen Rechner mit Microsoft-Betriebssystem handelt, auf dem ein Microsoft SQL-Server läuft.

Trennung wischen internen und öffentlichen Informationen

Bei DNS sollte daher eine Trennung zwischen der Namensauflösung für interne Zwecke und der Namensauflösung "nach außen" eingeführt werden. Interne DNS-Informationen sollten vor dem nicht-vertrauenswürdigen Netz verborgen werden. Rechner im internen Netz sollten selbst dann keinen von außen auflösbaren DNS-Namen erhalten, wenn sie eine "öffentliche" IP-Adresse besitzen. Werden im internen Netz private IP-Adressen aus den Adressbereichen des RFC 1918 verwendet, so müssen diese ohnehin durch einen internen Nameserver aufgelöst werden.

Gerade DNS-Server-Programme waren in der Vergangenheit wegen Sicherheitslücken immer wieder eine Quelle von Problemen. Wegen der besonderen Bedeutung der DNS-Informationen und der erhöhten Anfälligkeit der DNS-Software als Grundlage für Angriffe ist ein besonderer Aufbau notwendig, um DNS-Informationen sicher bereitstellen und nutzen zu können.

DNS-Server in einem dreistufigen Sicherheitsgateway

Für eine sichere Integration von DNS in ein dreistufiges Sicherheitsgateway bietet sich der in der folgenden Abbildung gezeigte Aufbau an, bei dem keine direkte Verbindung zwischen einem Client im vertrauenswürdigen Netz und einem DNS-Server im nicht-vertrauenswürdigen Netz (und umgekehrt) stattfindet. Es werden zwei getrennte DNS-Server eingesetzt:

- Der "öffentliche" DNS-Server, der die extern verfügbaren Informationen enthält, wird in einer DMZ des äußeren Paketfilters angesiedelt. Er ist als "Primary Nameserver" für die Domain des vertrauenswürdigen Netzes eingerichtet und enthält nur die unbedingt notwendigen Informationen, beispielsweise:
  - Name und IP-Adresse des externen Mailservers (MX-Eintrag)
  - Namen und Adressen von Informationsservern, die Informationen für die Öffentlichkeit anbieten. Dabei muss zwischen den Servern, die vor dem ALG angesiedelt sind und denen, die hinter dem ALG angesiedelt sind, unterschieden werden. Bei ersteren muss die Adresse des Servers selbst eingetragen sein, bei letzteren die Adresse des ALG.

- Der "private" DNS-Server wird in einer DMZ des inneren Paketfilters aufgestellt. Er enthält die Informationen über die Rechner des internen Netzes. Für Rechner des internen Netzes wird dieser Server als DNS-Server eingetragen: Alle Clients des vertrauenswürdigen Netzes nutzen ausschließlich den privaten DNS-Server (z. B. bei Unix-Rechnern mittels Einträgen in der Datei /etc/resolv.conf). Benötigt ein Client im vertrauenswürdigen Netz eine DNS-Information aus dem nicht-vertrauenswürdigen Netz, so stellt er die DNS-Anfrage an den privaten DNS-Server. Als "Forwarder" nutzt dieser den öffentlichen DNS-Server für Anfragen, die externe Namen betreffen. Der direkte Zugriff auf den privaten DNS-Server aus dem nicht-vertrauenswürdigen Netz sollte durch Paketfilterregeln unterbunden werden, so dass die DNS-Informationen des vertrauenswürdigen Netzes nur im vertrauenswürdigen Netz sichtbar sind.

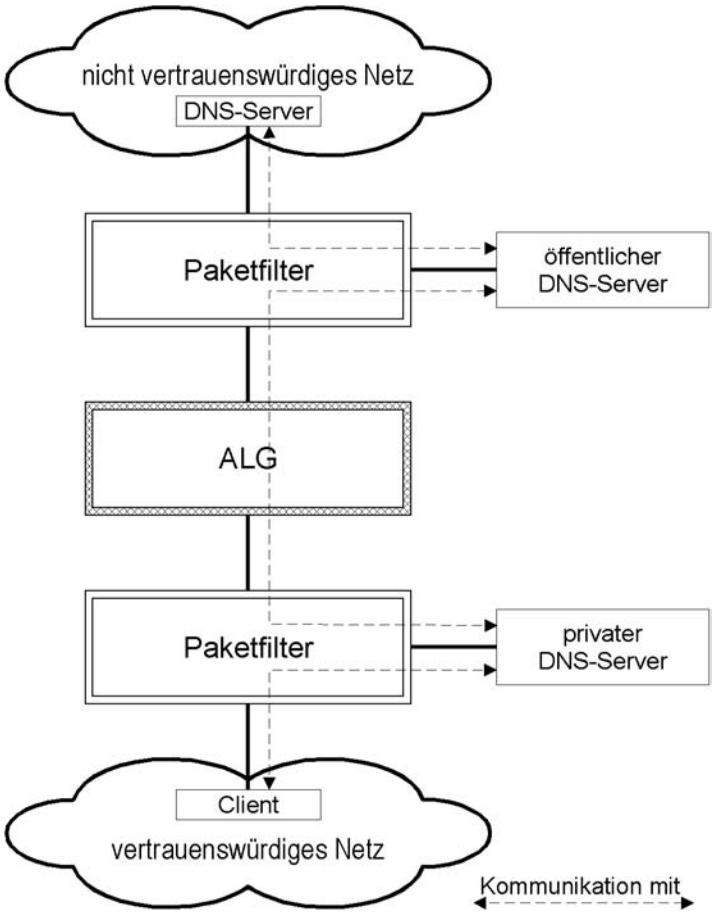


Abbildung 1: Integration der DNS-Server zur sicheren Kommunikation von vertrauenswürdigem und nicht-vertrauenswürdigem Netz

Der eingesetzte Paketfilter muss so konfiguriert werden, dass zwischen den Servern nur der DNS-Dienst gestattet ist, d. h. DNS-Port 53 als (je nach betrachteter Richtung) Quell- bzw. Zielport. Vom öffentlichen DNS-Server sollten keinerlei Verbindungen ins interne Netz zugelassen werden. Die

Administration des Servers sollte über entsprechend abgesicherte Verbindungen (SSH) erfolgen.

In der folgenden Tabelle wird eine mögliche Konfiguration für Zugriffsregelungen beschrieben, die über entsprechende Paketfilterregeln umgesetzt werden kann. Dabei wird davon ausgegangen, dass die Administration der Server über eine SSH-Verbindung aus dem internen Netz erfolgt und dass für DNS als Trägerprotokoll UDP verwendet wird. Protokolldaten werden über Syslog auf einen Logserver übertragen.

Quelle	**Ziel**	**Entscheidung**	**Bemerkungen**
Kommunikation des öffentlichen DNS-Servers mit dem Internet			
Externes Netz	Öffentlicher DNS-Server UDP Port 53	erlauben	DNS-Anfragen und Antworten aus dem öffentlichen Netz
Externes Netz	andere Ports des öffentlichen DNS-Servers	verbieten	
Externer DNS-Server	DNS-Server im Internet, Port 53 TCP und UDP	erlauben	Auflösung von externen Namen durch den DNS-Server
Externer DNS-Server	Alle anderen Verbindungen ins Internet	verbieten	
Kommunikation des externen DNS-Servers mit dem internen Netz			
Externer DNS-Server	Alle Verbind-ungen ins interne Netz	verbieten	
Internes Netz (ggfs. Einschränkung auf Administrationsnetz)	Öffentlicher DNS-Server Port 22 (SSH)	erlauben	Administration und Datenübertragung erfolgen per SSH und SCP
Internes Netz	Alle anderen Zugriffe auf den öffentlichen DNS-Server	verbieten	DNS-Anfragen aus dem internen Netz erfolgen über den internen Server

Tabelle: Konfiguration für Zugriffsregeln

Quelle	Ziel	Entscheidung	Bemerkungen
Kommunikation der beiden DNS-Server untereinander:			
Interner DNS-Server	Öffentlicher DNS-Server UDP Port 53	erlauben	Der interne DNS-Server leitet Anfragen an den öffentlichen Server weiter
Externer DNS-Server	Interner DNS-Server UDP Port 53	erlauben	Der externe DNS-Server löst externe Namen für den internen Server auf
Kommunikation des internen DNS-Servers mit dem internen Netz			
Internes Netz	Interner DNS-Server UDP Port 53	erlauben	DNS-Anfragen aus dem internen Netz erfolgen über den internen Server
Interner DNS-Server, UDP Port 53	Internes Netz	erlauben	DNS-Antworten in das interne Netz
Interner DNS-Server, sonstige Quellports	Internes Netz	verbieten	
Internes Netz (ggfs. Einschränkung auf Administrationsnetz)	Interner DNS-Server Port 22 (SSH)	erlauben	Administration und Datenübertragung erfolgen per SSH und SCP
Protokollierung			
Interner und externer DNS-Server	Loghost UDP-Port 514	erlauben	Übertragung der Protokolldaten zum Loghost

Tabelle: Konfiguration für Zugriffsregeln

DNS-Server in einem einfachen Sicherheitsgateway

Wird nur ein einfaches Sicherheitsgateway (Paketfilter) eingesetzt, so wird empfohlen, trotzdem zwei getrennte DNS-Server einzusetzen. Wenn die beiden DNS-Server in zwei getrennten DMZs des Paketfilters angesiedelt werden, können die selben Regeln eingesetzt werden, wie oben beschrieben.

Ist der Aufwand für die Einrichtung zweier getrennter DMZs zu groß oder können aus technischen Gründen keine zwei getrennten DMZs eingerichtet werden, so kann gegebenenfalls auf einfachere Konstruktionen zurückgegriffen werden. Diese bieten allerdings nur einen geringeren Schutz und es muss daher im Einzelfall abgewogen werden, ob das Sicherheitsniveau noch akzeptabel ist.

Der öffentliche DNS-Server sollte in jedem Fall in einer DMZ des Paketfilters angesiedelt werden. Der interne DNS-Server kann gegebenenfalls im internen Netz stehen.

Wenn nur ein DNS-Server zur Verfügung steht, der sowohl die interne als auch die externe Namensauflösung übernehmen muss, so sollte dieser in einer DMZ des Paketfilters aufgestellt werden. Wenn möglich sollte in diesem Fall das DNS-Server-Programm so konfiguriert werden, dass zwischen Anfragen aus dem internen und solchen aus dem externen Netz unterschieden wird und gegebenenfalls unterschiedliche Daten geliefert werden. Diese Lösung bietet jedoch nur für kleine Netze ohne besondere Anforderungen an die Sicherheit einen ausreichenden Schutz.

Domain-Registrierung bei externem Dienstleister

Bei dieser Alternative werden wichtige DNS-Informationen bei einem externen Dienstleister gespeichert und nicht mehr durch einen eigenen DNS-Server bereitgestellt. Der Unterschied zu den eben beschriebenen Szenarien besteht im Wesentlichen im Wegfall des externen DNS-Servers. DNS-Anfragen aus dem externen Netz nach DNS-Informationen aus dem internen Netz werden nicht an den organisationsinternen DNS-Server, sondern an den DNS-Server des externen Dienstleisters gesendet und von diesem beantwortet. Der interne DNS-Server greift bei Anfragen nach externen DNS-Namen oder IP-Adressen direkt über das Sicherheitsgateway hinweg auf einen DNS-Server im externen Netz zu.

Auch bei dieser Integrationsvariante sollten nur die unbedingt notwendigen DNS-Informationen extern angeboten werden, z. B. Name und IP-Adresse des Mail-Servers und des ALG. Bei besonders unbedenklichen organisationsinternen Nutzern kann der interne DNS-Server auch im internen Netz, anstatt in einer DMZ des inneren Paketfilters betrieben werden, was die Administration des Paketfilters (wenn auch nur in geringem Maße) erleichtert.

Vorteile dieser Variante sind die geringen Investitionskosten und die geringe Komplexität bei der Integration in ein Sicherheitsgateway. Zudem verfügt ein Dienstleister möglicherweise über redundante Systeme, was bei einer organisationsinternen Lösung oftmals nicht der Fall ist.

Ergänzende Kontrollfragen:

- Welche Informationen über das Netz können von extern über DNS abgefragt werden?
- Welche Anordnung der DNS-Server wurde gewählt?
- Welche Kommunikationsverbindungen für die DNS-Server sind zugelassen?

M 5.119 Integration einer Web-Anwendung mit Web-, Applikations- und Datenbank-Server in ein Sicherheitsgateway

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement,

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator,

Zur Bereitstellung einer komplexen Web-Applikation (beispielsweise einer E-Government-Anwendung oder eines Online-Shop) sind aufgrund des erhöhten Schutzbedarfs weitergehende Schutzmaßnahmen notwendig. Im Folgenden wird zu diesem Spezialfall ein Standardaufbau zur Bereitstellung einer Web-Applikation, bestehend aus Webserver, Applikationsserver und Datenbankserver, vorgeschlagen.

Architektur mit zwei ALGs und Paketfiltern

Das Sicherheitsgateway ist so angelegt, dass alle Server durch ein ALG voneinander getrennt sind, um unberechtigte Übergriffe von einem Server auf einen anderen zu unterbinden und eine Kontrolle über die eingesetzten Protokolle zu erhalten. Der Webserver ist sowohl durch einen Paketfilter als auch durch ein ALG abgesichert, um einen höchstmöglichen Schutz vor Angreifern aus dem nicht-vertrauenswürdigem Netz zu bieten.

Der Aufbau wurde so gewählt, dass jeder Server im Anwendungszusammenhang maximal zwei Kommunikationsverbindungen eingehen kann, die jeweils durch entsprechende ALGs abgesichert sind. Die folgende Tabelle stellt die Kommunikationsverbindungen zusammen:

Server	Kommunikation mit	Protokoll	Bemerkung
Webserver	Client aus dem externen Netz	HTTPS	Gegebenenfalls kann die verschlüsselte Verbindung bereits am ALG terminiert werden. Siehe auch M 5.115 Integration eines Webservers in ein Sicherheitsgateway
Webserver	Applikations-Server	Anwendungs-spezifische Protokolle, beispielsweise SOAP, RPC, Corba o.ä.	Für die Protokolle existieren ebenfalls Sicherheitsproxies
Applikations-Server	Datenbank-Server	Datenbank Protokoll	Siehe auch M 5.117 Integration eines Datenbankservers in ein Sicherheitsgateway

Tabelle: Kommunikationsverbindungen

Zusätzlich sind jeweils eventuell noch Zugriffe zur Administration aus dem internen Netz notwendig. Diese müssen auf entsprechende Administrationsrechner beschränkt werden und dürfen nur über entsprechend abgesicherte Protokolle (beispielsweise SSH) abgewickelt werden. Es sollte geprüft werden, ob auf eine physikalische Verbindung zu dem vertrauenswürdigen Netz ganz verzichtet werden kann, um einem Angriff durch Innentäter vorzubauen.

Die folgende Abbildung zeigt noch einmal die oben beschriebene Architektur. Die jeweils zugelassenen Kommunikationsverbindungen sind eingetragen.

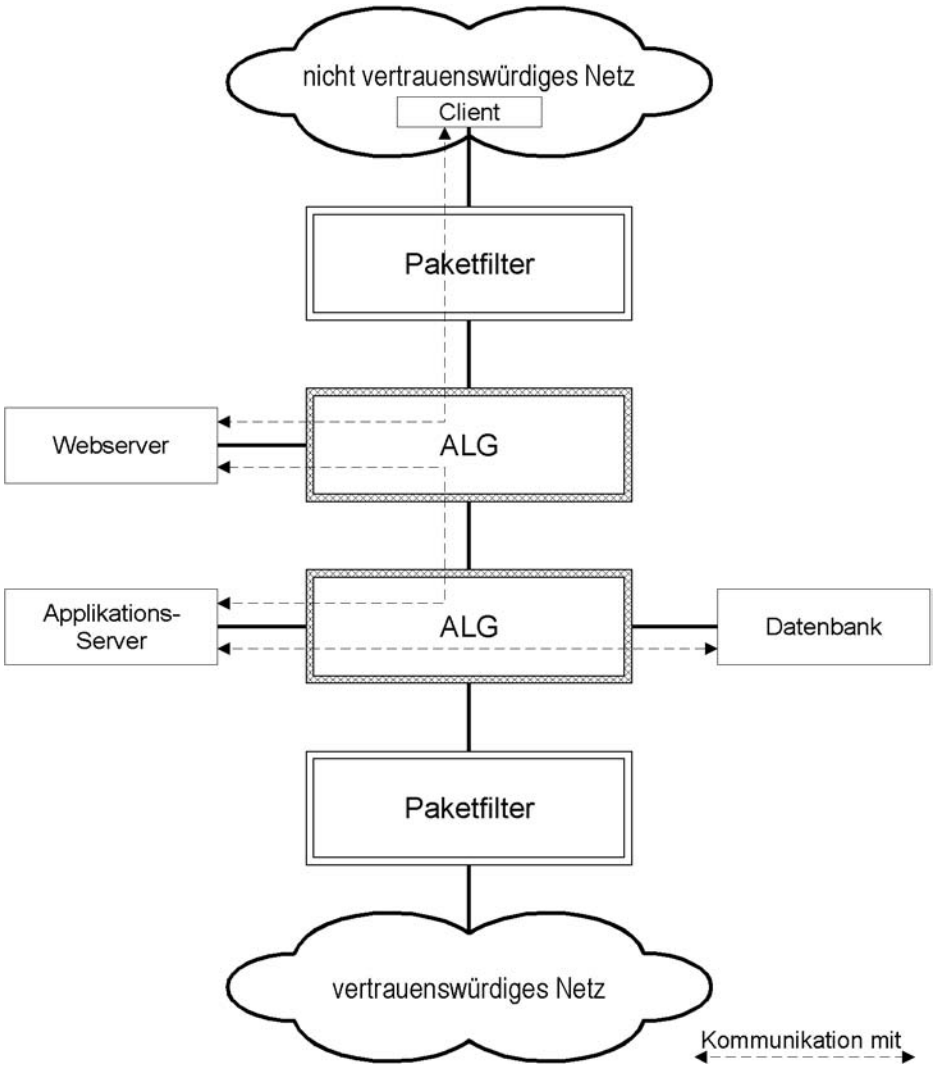


Abbildung 1: Aufbau einer typischen Web-Applikation bestehend aus Webserver, Applikationsserver und Datenbank.

Vereinfachte Architektur ohne ALGs

Falls die Anwendung keine besonderen Sicherheitsanforderungen stellt können eventuell die ALGs wegfallen und der Webserver kann in einer DMZ des äußeren Paketfilters aufgestellt werden, der Applikations- und der Datenbankserver in separaten DMZs des inneren Paketfilters. Die Kommunikationsbeziehungen werden in diesem Fall nur durch entsprechende Paketfilterregeln eingeschränkt.

In diesem Fall besteht allerdings nicht mehr die Möglichkeit zur Kontrolle des Inhalts der Kommunikation. Wird auf ALG zwischen dem Client und dem Webserver verzichtet (Reverse-HTTP-Proxy) können beispielsweise keine HTTP-Anfragen aus dem nicht-vertrauenswürdigen Netz mehr auf Konformität mit der HTTP-Spezifikation überprüft und auf (im jeweiligen Zusammenhang) ungewöhnliche Inhalte getestet werden.

Es wird dringend empfohlen, zumindest für den Zugriff der Clients auf den Webserver ein entsprechendes ALG (Reverse-HTTP-Proxy) einzusetzen.

Die folgende Abbildung zeigt die vereinfachte Architektur mit zwei Paketfiltern. Die Kommunikationsbeziehungen sind wie in der obigen Tabelle beschrieben, nur dass keine protokollspezifischen Sicherheitsproxies eingesetzt werden.

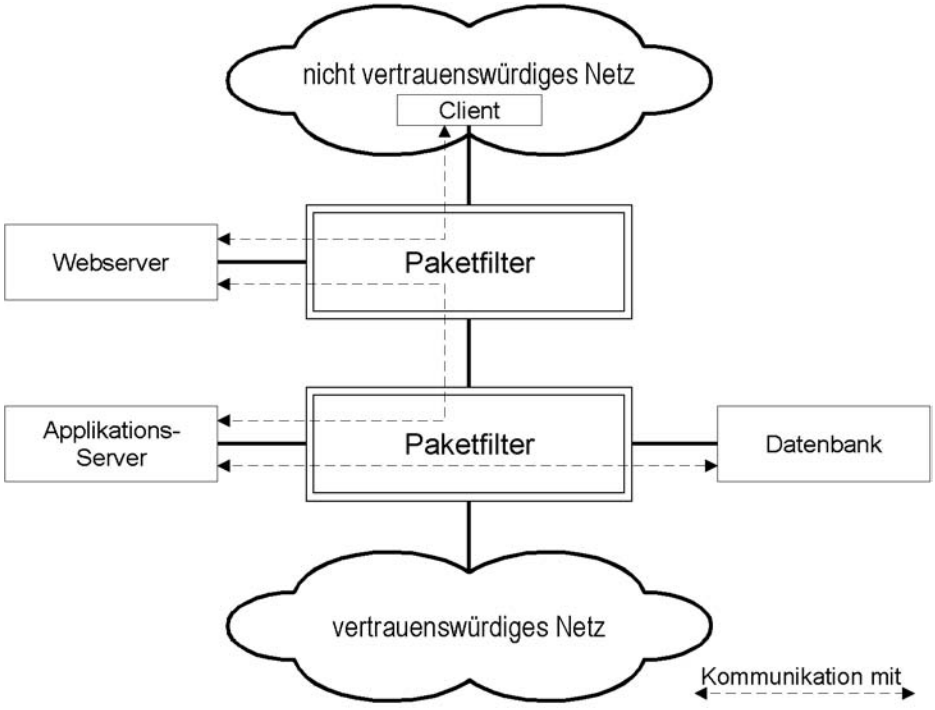


Abbildung 2: Aufbau einer typischen Web-Applikation bestehend aus Webserver, Applikationsserver und Datenbank ohne Verwendung von ALGs

Ob für die jeweils eingesetzte Webapplikation der vereinfachte Aufbau ausreichend ist muss im Einzelfall geklärt werden. Die Entscheidung muss anhand des Schutzbedarfs der verarbeiteten Daten getroffen werden, keinesfalls dürfen ausschließlich Kostenargumente den Ausschlag geben. Die Entscheidung und die Gründe dafür müssen dokumentiert werden und es muss regelmäßig geprüft werden, ob sich die Voraussetzungen nicht geändert haben. Insbesondere bei Änderungen und Erweiterungen der Webanwendung muss sichergestellt sein, dass die Architektur noch den Sicherheitsanforderungen entspricht.

Die folgenden Punkte können bei den Erwägungen als Hinweise dienen:

- Für Webanwendungen, auf die nur aus einem "relativ vertrauenswürdigen Netz" zugegriffen wird, bietet auch der vereinfachte Aufbau meist ein ausreichendes Sicherheitsniveau.
- Handelt es sich bei der Webanwendung um eine Anwendung, auf die über das Internet zugegriffen werden kann oder haben die verarbeiteten Daten einen hohen Schutzbedarf, so sollte mindestens ein Reverse-HTTP-Proxy zur Absicherung des Webservers vor Angriffen aus dem Internet eingesetzt werden.
- Werden auf dem Datenbankserver, der zu der Webapplikation gehört, noch weitere Datenbanken betrieben, so muss auch der Schutzbedarf dieser Daten in die Überlegungen einbezogen werden. In diesem Fall kommt der sicheren und sorgfältigen Konfiguration des Datenbankservers eine besondere Bedeutung zu. In diesem Fall wird der Einsatz eines Sicherheitsproxies für die Datenbankzugriffe dringend empfohlen.

Ergänzende Kontrollfragen:

- Welche Architektur wurde für die Webanwendung gewählt?
- Sind die Entscheidungsgründe dokumentiert und nachvollziehbar?

M 5.120 Behandlung von ICMP am Sicherheitsgateway

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter

Verantwortlich für Umsetzung: Administrator

Das Internet Control Message Protocol (ICMP, spezifiziert in RFC 792) hat als Protokoll der Transportschicht die Aufgabe, Fehler- und Diagnoseinformationen für IP zu transportieren. Es wird intern von IP, TCP oder UDP angestoßen und verarbeitet. ICMP kennt eine Anzahl verschiedener so genannter Nachrichtentypen für verschiedene Zwecke. Neben vielen nützlichen Funktionen gibt es in ICMP einige Nachrichtentypen, mit denen Angreifer sich wichtige Informationen über ein Netz verschaffen können, oder die direkt für Angriffe benutzt werden können (siehe G 5.50 *Missbrauch des ICMP-Protokolls*).

Leider ist jedoch der radikale Ansatz, ICMP grundsätzlich am Sicherheitsgateway zu blockieren, ebenfalls keine befriedigende Lösung, da bestimmte Funktionen dann nicht mehr verfügbar sind. Auf Befehle wie *ping* oder *traceroute* kann zwar in der Regel auf normalen Arbeitsplatzrechnern und Servern verzichtet werden, eine globale Blockierung von ICMP am Sicherheitsgateway kann aber zu Beeinträchtigungen führen, die schwer zu diagnostizieren sind.

Selektive Filterung von ICMP

Daher sollte überlegt werden, sowohl am Sicherheitsgateway als auch gegebenenfalls an einem lokalen Paketfilter auf den einzelnen IT-Systemen eine selektive ICMP-Filterung vorzunehmen, sofern dieser die entsprechenden Möglichkeiten zur Verfügung stellt. Dabei sollten der Einsatzzweck des Rechners (Server oder Arbeitsplatzrechner), der Schutzbedarf und bei einzelnen Rechnern die am Sicherheitsgateway getroffenen Maßnahmen berücksichtigt werden. Beispielsweise kann für das interne Netz eine größere Zahl von Nachrichtentypen zugelassen werden, als für das externe Netz.

Die ICMP-Nachricht *Echo Request* (Nachrichtentyp 8) wird beispielsweise von Programmen wie dem Kommandozeilentool *ping* ausgeschickt und dient dazu herauszufinden, ob ein Rechner prinzipiell erreichbar ist. Der Rechner antwortet darauf mit einem Echo Reply (Nachrichtentyp 0). Werden ICMP Echo Requests aus dem externen Netz ins interne Netz durchgelassen, so kann dies von einem Angreifer ausgenutzt werden, um das interne Netz zu "kartographieren".

Die ICMP-Nachricht *Destination Unreachable* (Nachrichtentyp 3) wird beispielsweise dann erzeugt, wenn ein Rechner oder ein Netz nicht erreichbar ist, und kann dazu missbraucht werden, alle Verbindungen zwischen den beteiligten Rechnern zu unterbrechen. Trotzdem ist gerade die Nachricht Destination Unreachable für das Funktionieren der Protokolle der höheren Schichten wichtig. Beispielsweise ist der Subtyp *"Fragmentation Needed but the Don't Fragment Bit was Set"* (Nachrichtentyp 3, Code 4) wichtig für die Funktion der Ermittlung der maximal möglichen Paketgröße für eine bestimmte Verbindung ("Path MTU Discovery").

Die ICMP-Nachricht *Redirect* (Nachrichtentyp 5) wird ausgesandt, wenn ein Gateway erkennt, dass das Paket direkt an ein anderes Gateway geschickt werden kann, also bisher ein Umweg benutzt wurde. Der kürzere Weg wird

dann in die Routingtabelle des Absenders eingetragen. Dieses kann von Angreifern missbraucht werden, um Routen über eigene Angriffsrechner zu konfigurieren. Daher sollten ICMP-Redirect Nachrichten am Sicherheitsgateway blockiert werden.

Bei den anderen Meldungen ist abzuwägen, ob Informationen, die eventuell nach außen geliefert werden, für einen Angriff missbraucht werden können.

Rechner im internen Netz

Die nachfolgende Tabelle zeigt eine mögliche Einstellung für ein Sicherheitsgateway, welches das interne Netz einer Organisation vom Internet trennt. Diese Einstellungen stellen für die meisten Zwecke einen akzeptablen Kompromiss zwischen Sicherheit und Funktionalität dar:

ICMP Nachricht	Ankommend	Abgehend	Bemerkung
Echo Request (Typ 8)	blockieren	zulassen	
Echo Reply (Typ 0)	zulassen	blockieren	Erlaubt zusammen mit der darüber stehenden Einstellung das "pingen" von innen nach außen, aber nicht umgekehrt
Destination unreachable (Typ 3)	zulassen	zulassen	Eventuell feinere Unterscheidung anhand des Nachrichtencodes treffen
Time exceeded (Typ 11)	zulassen	zulassen	Eventuell ausgehende Nachrichten blockieren
Redirect (Typ 5)	blockieren	blockieren	
Andere Typen	blockieren	blockieren	

Tabelle 1: ICMP für Rechner im internen Netz

Da "pingen" keine besondere Rolle für das Funktionieren eines Netzes spielt, sollte auch bei normalem Schutzbedarf überlegt werden, die Typen Echo Request und Echo Response komplett zu sperren.

Bei höheren Sicherheitsanforderungen sollte die Anzahl der erlaubten abgehenden ICMP-Typen weiter eingeschränkt werden.

"Öffentliche" Server in der DMZ

Für Server, die in einer Demilitarisierten Zone des Sicherheitsgateway aufgestellt sind und die öffentlich zugängliche Dienste anbieten kann es sinnvoll sein, zusätzliche Nachrichtentypen zu erlauben. Der Schutz vor dem "Ausspähen" einer internen Netzstruktur spielt in diesem Fall keine Rolle, da diese Rechner ohnehin von außen erreichbar sein müssen. Die folgende Tabelle kann dafür als Anhaltspunkt dienen:

ICMP Nachricht	Ankommend	Abgehend	Bemerkung
Echo Request und Echo Reply (Typen 0 und 8)	zulassen	zulassen	
Destination unreachable (Typ 3)	zulassen	zulassen	Eventuell feinere Unterscheidung anhand des Nachrichtencodes treffen
Time exceeded (Typ 11)	zulassen	zulassen	
Source Quench (Typ 4)	zulassen	blockieren	
Redirect (Typ 5)	blockieren	blockieren	
Andere Typen	blockieren	blockieren	

Tabelle 2: ICMP für "öffentliche" Server in der DMZ

Komponenten des Sicherheitsgateways

Komponenten des Sicherheitsgateways selbst sollten für den normalen Netzverkehr so transparent wie möglich sein. Daher ist es bei diesen Systemen empfehlenswert, überhaupt keine ICMP-Nachrichten zu generieren, weder selbständig noch als Antwort auf ankommende ICMP-Nachrichten. Es ist sinnvoll, diese Einstellung direkt am jeweiligen System zu treffen, sofern entsprechende Konfigurationsmöglichkeiten vorhanden sind. Anderenfalls sollten entsprechende Pakete am äußeren Paketfilter blockiert werden.

ICMP bei besonderen Sicherheitsanforderungen

Für IT-Systeme und Netze mit besonderen Sicherheitsanforderungen wird empfohlen, sämtliche ICMP-Nachrichten zu blockieren, eventuell mit Ausnahme von Nachrichten des Nachrichtentyps 3, Nachrichtencode 4 ("Fragmentation Needed but the Don't Fragment Bit was Set"). Diese Ausnahme vermeidet Probleme in Verbindung mit der sogenannten "Path MTU Discovery" (Ermittlung der maximal möglichen Paketgröße für eine bestimmte Verbindung).

ICMP im internen Netz

Auch im internen Netz kann es sinnvoll sein, ICMP ganz oder teilweise zu blockieren. An internen Sicherheitsgateways, die ein Netz mit besonderen Sicherheitsanforderungen von einem Netz mit normalem Schutzbedarf trennen wird empfohlen, im Bezug auf ICMP die selben Einstellungen zu wählen, wie sie oben für die Trennung des internen Netzes vom Internet empfohlen werden.

ICMP und Stateful Inspection

Manche Hersteller von Paketfiltern oder Sicherheitsgateways bieten bei Ihren Produkten die Möglichkeit, auch für ICMP eine Art Stateful Inspection

vorzunehmen. Auf Grund seines Einsatzzweckes eignet sich ICMP aber besonders schlecht für Stateful Inspection. Wegen der Fehleranfälligkeit einer entsprechenden Konfiguration und dem vergleichsweise geringen Nutzen wird davon abgeraten, entsprechende Optionen zu aktivieren.

Ergänzende Kontrollfragen:

- Wie wird am Sicherheitsgateway mit ICMP verfahren?
- Welche ICMP-Nachrichten werden von außen nach innen durchgelassen?
- Welche ICMP-Nachrichten werden von innen nach außen durchgelassen?

M 5.121 Sichere Kommunikation von unterwegs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Über mobile Endgeräte wie Laptops oder PDAs soll auch häufig unterwegs auf Daten aus dem Internet oder dem internen Netz einer Institution zugegriffen werden. Dabei werden üblicherweise öffentliche Kommunikationsnetze benutzt. Da weder die Institution noch die mobilen Mitarbeiter großen Einfluss darauf nehmen können, ob die Vertraulichkeit, Integrität und Verfügbarkeit im öffentlichen Kommunikationsnetz gewahrt werden, sind zusätzliche Maßnahmen zum Schutz der Informationen erforderlich.

Generell muss die Datenübertragung zwischen einem mobilen Endgerät und dem LAN einer Institution folgende Sicherheitsanforderungen erfüllen:

- *Sicherstellung der Vertraulichkeit der übertragenen Daten*: es muss durch eine ausreichend sichere Verschlüsselung der Datenübertragung erreicht werden, dass auch durch Abhören der Kommunikation kein Rückschluss auf den Inhalt der Daten möglich ist. Dazu gehört neben einem geeigneten Verschlüsselungsverfahren auch ein angepasstes Schlüsselmanagement mit periodischem Schlüsselwechsel.
- *Sicherstellung der Integrität der übertragenen Daten*: Die eingesetzten Übertragungsprotokolle müssen die Möglichkeit bieten, Veränderungen an den übertragenen Daten zu erkennen und eventuell sogar zu beheben. Solche Veränderungen können beispielsweise durch Übertragungsfehler (technische Probleme) oder durch absichtliche Manipulationen durch einen Angreifer entstehen. Zusätzlich kann der Einsatz digitaler Signaturen sinnvoll sein, um die Datenintegrität sicherzustellen.
- *Sicherstellung der Authentizität der Daten*: bei der Übertragung der Daten muss vertrauenswürdig feststellbar sein, ob die Kommunikation zwischen den richtigen Teilnehmern stattfindet, so dass eine Maskerade oder ein Man-in-the-Middle-Angriff ausgeschlossen werden kann. Zu diesem Zweck muss eine gegenseitige Authentisierung der Kommunikationspartner (beispielsweise über digitale Zertifikate) erfolgen.
- *Sicherstellung der Nachvollziehbarkeit der Datenübertragung*: um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden, die nachträglich feststellen lassen, welche Daten wann an wen übertragen wurden.

Die Stärke der dazu erforderlichen Mechanismen richtet sich dabei nach dem Schutzbedarf der übertragenen Daten. Wie adäquate kryptographische Verfahren und Systeme ausgewählt und eingesetzt werden können, ist in Baustein B 1.7 *Kryptokonzept* beschrieben.

Wenn mit mobilen Endgeräten über öffentliche Netze hinweg auf interne Ressourcen zugegriffen werden soll, so wird der Einsatz eines Virtual Private Network (VPN) dringend empfohlen. Entsprechende Produkte sind von diversen Herstellern und für praktisch alle gebräuchlichen Plattformen verfügbar. Auf Daten oder Systeme mit hohem Schutzbedarf darf nicht ohne entsprechende Sicherungsmaßnahmen zugegriffen werden.

Für den Zugriff auf Internet-Anwendungen, bei denen sensible Daten wie personenbezogene Daten, interne Informationen oder Kontendaten ausgetauscht werden, muss zumindest SSL zur Verschlüsselung genutzt werden (siehe auch M 5.66 *Verwendung von SSL*).

Kopplung mit anderen IT-Systemen

Bei der Nutzung von mobilen Endgeräten wie Laptops oder PDAs sollen häufig auch Daten mit anderen IT-Systemen ausgetauscht werden, etwa mit Geschäftspartnern. Auch zum Zugriff auf das Internet ist häufig die Kopplung mit anderen IT-Systemen erforderlich. Dies kann auf verschiedene Arten erfolgen, je nachdem, welche Techniken die beteiligten Geräte unterstützen, beispielsweise über Infrarot-, Bluetooth-, WLAN- oder GSM-Schnittstellen. Hier müssen zum einen die Übertragungstechniken sicher eingesetzt werden (näheres hierzu findet sich in den entsprechenden IT-Grundschutz-Bausteinen oder anderen Veröffentlichungen des BSI), zum anderen müssen die eigenen IT-Systeme sicher konfiguriert sein. Dazu gehören bei mobilen Clients Sicherheitsmaßnahmen wie z. B. Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall, restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene, lokale Verschlüsselung, etc.

Soll ein mobiles Endgerät an fremde Netze oder an das Internet angeschlossen werden, so sollte das System grundsätzlich über eine Personal Firewall abgesichert werden (siehe auch M 5.91 *Einsatz von Personal Firewalls für Internet-PCs*).

Nutzung fremder IT-Systeme

Bei der Nutzung fremder IT-Systeme, z. B. in Internet-Cafes, oder bei der Kopplung mit fremden IT-Geräten, z. B. zum Austausch von Dateien, sollten sich alle Benutzer darüber im Klaren sein, dass diese als unsichere Systeme eingestuft werden müssen. Es darf auf keinen Fall vorausgesetzt werden, dass diese frei von Schadsoftware (z. B. Computer-Viren oder Trojanische Pferde) sind. Außerdem muss immer darüber nachgedacht werden, ob und wo durch eine Benutzung sensible Informationen gespeichert worden sein können, z. B. in temporären Dateien, im Cache eines Web-Proxys oder im Browser-Cache. Auf Daten oder IT-Systeme mit hohem Schutzbedarf darf nicht von solchen unsicheren Systemen aus zugegriffen werden.

In allen Organisationen sollte klar geregelt sein, auf welche Daten von unterwegs zugegriffen werden darf und auf welche nicht. Vor allem muss allen IT-Benutzern bekannt sein, unter welchen Randbedingungen sie Daten über externe Netze oder direkt mit fremden IT-Systemen austauschen dürfen (siehe auch M 2.217 *Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen* und M 2.218 *Regelung der Mitnahme von Datenträgern und IT-Komponenten*).

Ergänzende Kontrollfragen:

- Werden bei der Datenübertragung die Daten ausreichend geschützt?
- Wird beim Datenaustausch das eigene IT-System ausreichend geschützt?

M 5.122 Sicherer Anschluss von Laptops an lokale Netze

Verantwortlich für Initiierung: Administrator, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer, Administrator

Laptops haben als mobile IT-Geräte ein höheres Gefährdungspotential als stationäre IT-Systeme, die ausschließlich in einer kontrollierten Umgebung betrieben werden. Daher ist es wichtig, festzulegen, welche Regelungen beim Anschluss von Laptops an LANs zu beachten sind, um zu vermeiden, dass dadurch der sichere Betrieb des LANs und anderer damit gekoppelter IT-Systeme beeinträchtigt wird, z. B. durch Schadsoftware.

Wenn ein Laptop nach einem externen Einsatz wieder an das Unternehmens- bzw. Behördennetz angeschlossen werden soll, so ist zunächst durch eine gründliche Überprüfung mit aktuellen Virensignaturen sicherzustellen, dass dieser Laptop nicht infiziert ist.

Sofern Laptops bei mobiler Nutzung direkt an das Internet angeschlossen werden, ist es unabdingbar, sie durch eine restriktiv konfigurierte Personal Firewall gegen Angriffe aus dem Netz zu schützen. Der Virenschutz reicht alleine nicht aus, um alle zu erwartenden Angriffe abzuwehren. Ebenso ist es unbedingt erforderlich, die Software des Laptops auf aktuellem Stand zu halten und notwendige Sicherheitspatches zeitnah einzuspielen. Es ist sinnvoll, vor einem Zugriff auf das Produktivnetz zu überprüfen, ob Personal Firewall, andere Sicherheitsprogramme und Sicherheitspatches auf dem Laptop auf dem aktuellsten Stand sind. Empfehlenswert ist es, über entsprechende Tools diese Prüfungen automatisiert durchzuführen, so dass bei Sicherheitsmängeln der Zugriff auf das interne Netz abgewiesen werden kann.

Die auf dem Laptop installierten Internet-Anwendungsprogramme, vor allem Browser und E-Mail-Client, sollten mit sicheren Einstellungen betrieben werden (siehe hierzu M 5.45 *Sicherheit von WWW-Browsern* und M 5.57 *Sichere Konfiguration der Mail-Clients*). Die Änderung der voreingestellten Optionen durch den Benutzer sollte administrativ unterbunden werden. Zusätzlich könnten Tools eingesetzt werden, die die Funktionalität des Browsers einschränken, so dass dieser in einer Sandbox-ähnlichen Umgebung ausgeführt wird.

Zertifikate/MAC-Adressen

Es muss sichergestellt sein, dass nicht jeder beliebige Laptop sich an ein LAN anmelden kann. Bevor einem Laptop ein Zugriff auf ein LAN gestattet wird, muss dieser sich erfolgreich gegenüber einem Authentikationsserver authentisiert haben.

Um zu überprüfen, welche Geräte grundsätzlich zum Netzzugriff berechtigt sind, können beispielsweise Geräte-Zertifikate oder MAC-Adressen benutzt werden. Zu beachten ist hierbei allerdings, dass MAC-Adressen gefälscht werden können und deshalb nicht als alleiniges Authentisierungskriterium herangezogen werden sollten.

Zugriffsbeschränkungen

Es muss sichergestellt werden, dass ein VPN-Nutzer ausschließlich auf die zur Aufgabenerledigung notwendigen Dienste auf den Servern im LAN zugreifen kann. Dies könnte beispielsweise sichergestellt werden durch eine benutzerbezogene Authentisierung auf Anwendungsebene *und* die Kontrolle des Verkehrs mit Hilfe von Paketfiltern (Paketfilter alleine sind aufgrund der Fälschbarkeit der IP-Adressen nicht ausreichend).

VPN

Zugriffe von einem Laptop von außerhalb auf das interne Netz sollten ausschließlich über VPN gesichert erfolgen. Ermöglicht die Institution einen Abruf von dienstlichen E-Mails über das Internet mittels einer Web-Mail-Lösung, so ist sicherzustellen, dass die E-Mails ausschließlich verschlüsselt vom Server auf das Laptop übertragen werden (z. B. mittels SSL). Allerdings muss hierbei nicht nur der Transportkanal, sondern auch das Endsystem selbst besonders abgesichert werden. Ein Laptop kann kompromittiert werden, wenn neben der VPN-Nutzung gleichzeitig auch noch Standardprotokolle wie z. B. HTTP oder SMTP im Internet genutzt werden. Daher sollten Laptops möglichst so abgesichert werden, dass bei bestehender VPN-Verbindung in das interne Netz keine anderen Verbindungen möglich sind (Split-Tunneling). Dabei muss gewährleistet sein, dass alle abgehenden Datenpakete des Clients in den Tunnel gehen und ausschließlich Datenpakete aus dem Tunnel akzeptiert werden.

Es sollte in diesem Zusammenhang auch darauf geachtet werden, dass neben dem VPN-gesicherten Laptop-Zugriff auf das interne Netz nicht gleichzeitig andere Netzzugriffe möglich sind. Insbesondere darf während der VPN-Zugriffe kein WLAN oder Bluetooth auf dem Laptop aktiv sein.

Der Einsatz von PPTP als VPN-Lösung wird nicht empfohlen, da in PPTP eine Vielzahl von Sicherheitslücken gefunden wurden, unter anderem wegen gravierender kryptographischer Schwachstellen insbesondere in Zusammenhang mit schwachen Passworten.

Ein mobiles IT-System kann leicht in falsche Hände geraten. Die Verbindung in das interne Netz (der Tunnelaufbau) sollte daher nicht automatisiert, sondern erst nach einer Authentisierung erfolgen. Weitere Empfehlungen des BSI zum sicheren Aufbau und Betrieb von VPNs finden sich auf der Webseite www.bsi.bund.de, Stichwort Internet-Sicherheit.

DHCP

Über das Dynamic Host Configuration Protocol (DHCP) werden in IP-basierten Netzen den angeschlossenen Clients automatisch temporäre IP-Adressen sowie Routing- und DNS-Server-Informationen zugewiesen, so dass der Laptop zum Internet-Zugriff nicht mehr vom Benutzer konfiguriert werden muss.

Wenn DHCP aktiviert ist, wird einem IT-System automatisch eine gültige IP-Adresse für das lokale Netz zugewiesen und kann somit auf alle freigegebenen Ordner und Laufwerke zugreifen. Als Abhilfe sollte zum einen DHCP auf dem Laptop deaktiviert werden, wenn es nicht benötigt wird (dann müssen allerdings die IP-Adressen manuell verteilt werden). Zum anderen sollte bei der IP-Adressvergabe zusätzlich über die MAC-Adresse überprüft werden, ob der Client zum Netz zugelassen werden sollte.

Internet-Zugriffe

Es muss geregelt werden, ob Laptops direkt auf das Internet zugreifen dürfen. Der kritische Punkt hierbei ist, dass dabei die institutionseigenen Sicherheitsgateways und Sicherheitsmechanismen umgangen werden, dies also potentiell Sicherheitsprobleme nach sich ziehen kann. Es gibt verschiedene Lösungsmöglichkeiten, die je nach Sicherheitsanforderungen und Einsatzumgebung ausgewählt werden müssen:

- Verbot direkter Internet-Zugriffe: Diese Lösung hat natürlich den Vorteil, dass sie am einfachsten umzusetzen ist. Sie ist allerdings auch die einschränkenste Möglichkeit und wird daher nicht einfach durchzusetzen sein.
- Nutzung verschiedener Benutzerkennungen: Auf Betriebssystem-Ebene sollten in diesem Fall zwei verschiedene Benutzerkennungen genutzt werden, einmal für die allgemeine geschäftliche Nutzung und einmal für Internet-Zugriff. Hierbei sollte die Internet-Kennung nur über minimale Rechte verfügen.
- Nutzung verschiedener Partitionen/Betriebssysteminstallationen: Bei dieser Lösung werden verschiedene Partitionen genutzt, die möglichst stark getrennt sind, beispielsweise durch unterschiedliche Betriebs- und Dateisysteme. Je stärker die Trennung ist, desto höher sind die Hürden, um die Beeinträchtigung der Produktiv-Umgebung durch Schadsoftware aus dem Internet oder ähnliches zu verhindern.
- Virtuelle Maschinen: Hierbei erfolgt die direkte Nutzung des Internets ausschließlich über ein Betriebssystem, das in einer virtuellen Maschine (z. B. User Mode Linux, UML) betrieben wird. Durch die virtuelle Maschine wird der benutzte Browser stärker vom eigentlichen Host-Betriebssystem getrennt, als dies bei einer Nutzung ohne virtuelle Maschine der Fall ist. Allerdings besteht bei dieser Variante das Restrisiko,

dass Schadprogramme - z. B. mit JavaScript erzeugt - mittels Copy&Paste zwischen dem Host-Betriebssystem und dem virtuellen Betriebssystem hin- und herkopiert werden können. Das Host-Betriebssystem könnte sich in diesem Fall bei der nächsten VPN-Einwahl in einem unsicheren Zustand befinden.

- Verwendung von Boot-CDs: Hierbei wird für die Internet-Nutzung von einem schreibgeschützten Medium wie einer CD-ROM eine internetfähige Betriebsumgebung hergestellt, wobei die Nutzbarkeit dadurch eingeschränkt wird, dass notwendige IP-Informationen evtl. von Hand eingetragen werden müssen. Hierzu kann beispielsweise Knoppix verwendet werden, eine komplett von CD lauffähige Zusammenstellung von GNU/Linux-Software (siehe www.knoppix.org).
- Internet-Zugriff nur über VPN (über Intranet über institutionseigenen Sicherheitsgateway ins Intranet). Dies hat den Vorteil, dass gefährliche Inhalte aussortiert werden.

Authentisierung der VPN-Nutzung

Bevor ein VPN aufgebaut wird, sollte die Authentizität des Benutzers mit starken Authentisierungsverfahren sichergestellt werden. Starke Authentisierungsverfahren sind beispielsweise Einmal-Passwort- oder Challenge-Response-Verfahren.

Protokollierung

Die Nutzung der Server-Dienste sollte durch Protokollierung der Zugriffe nachvollziehbar sein. Dabei sollte auch erkennbar sein, ob der Laptop-Zugriff aus dem Unternehmen bzw. der Behörde oder von extern erfolgte.

Temporäre Daten

Es sollte sichergestellt werden, dass alle zwischengespeicherten Authentisierungsinformationen, die den Aufbau eines VPNs ermöglichen, nach dem Ende der VPN-Nutzung automatisch gelöscht werden. Dies gilt sowohl für absichtlich als auch unabsichtlich beendete VPN-Verbindungen. Zusätzlich sollte beispielsweise bei Browser-basierten SSL-VPNs darauf geachtet werden, dass sämtliche Zwischenspeicher deaktiviert werden, damit Authentisierungsinformationen erst gar nicht temporär gespeichert werden und einem Angreifer die Wiederherstellung der VPN-Verbindung erleichtern.

Ergänzende Kontrollfragen:

- Welche Regelungen existieren für den Anschluss von Laptops an interne LANs?
- Ist sichergestellt, dass nur zugelassene Laptops sich an das LAN anmelden können?
- Werden alle Laptop-Zugriffe von außerhalb auf das interne Netz über VPN abgesichert?

M 5.123 Absicherung der Netzwerkkommunikation unter Windows XP

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Administrator

Die Sicherheit einer Windows XP Infrastruktur wird nicht ausschließlich von der sicheren Konfiguration und dem sicheren Betrieb einzelner Systeme bestimmt. Die Gesamtsicherheit hängt auch wesentlich von der Sicherheit in der Netzkommunikation ab, die unter anderem durch die Absicherung der Kommunikationswege (Signaturen, Verschlüsselung) und verwendete Authentisierungsmechanismen bestimmt wird.

Generell gilt, dass nicht verwendete Netzwerkkomponenten (z. B. *Datei- und Druckerfreigabe für Microsoft-Netzwerke*) von existierenden Schnittstellen zu entfernen sind. Die Beurteilung, welche Netzwerkprotokolle entfernt werden sollten, hat anhand konkreter Umstände und im Einzelfall zu erfolgen.

Sicherer Kanal

Die Kommunikation eines Clients mit einem Domain Controller erfolgt über den sog. Sicheren Kanal, der unter anderem für die Übertragung der Authentisierungsdaten verwendet wird. Die Daten des Sicheren Kanals werden mit einem Sitzungsschlüssel verschlüsselt. Das jeweilige Computer-Konto des Clients (automatisch von Windows verwaltet) wird für den Aufbau dieses Kanals verwendet. Die regelmäßigen Änderungen des Kennworts für das Computer-Konto sind daher maßgebend für die Sicherheit des Sicheren Kanals.

Standardmäßig sind die Änderungen des Kennworts für das Computer-Konto aktiviert und sollten nicht durch eine nachträgliche Konfiguration deaktiviert werden (*Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Domänenmitglied: Änderungen von Computerkennwörtern deaktivieren*), da dies zu Sicherheitsproblemen führen kann. Das Maximalalter des Kennworts ist standardmäßig auf 30 Tage voreingestellt (*Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Domänenmitglied: Maximalalter von Computerkennwörtern*) und sollte im Normalfall nicht auf einen größeren Wert geändert werden.

Die Absicherung der Kommunikation mit Domain Controllern ist sehr wichtig, da hier kritische Informationen übertragen werden. Diese Kommunikation muss immer signiert und stark verschlüsselt werden. Eine starke Verschlüsselung mit 128 Bit (*Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Domänenmitglied: Starker Sitzungsschlüssel erforderlich*) sollte daher verwendet werden, wenn auf allen Rechnern der Domäne und aller vertrauten Domänen mindestens Windows 2000 eingesetzt wird. Kommen ältere Betriebssystemversionen zum Einsatz, kann diese Einstellung nicht erfolgen. Die Aktivierung starker Verschlüsselung ist also anhand der konkreten Umstände und im Einzelfall festzulegen.

Signieren und Verschlüsseln der Kommunikation

Alle Daten, die über den Sicheren Kanal übertragen werden, sollten signiert und verschlüsselt werden. Standardmäßig erfolgt dies aber nur dann, wenn beide Kommunikationspartner gleiche Verfahren verwenden. Unterstützt einer der beiden Partner jedoch Verschlüsselung bzw. Signieren nicht, erfolgt die Kommunikation ungeschützt (Richtlinien *Domänenmitglied: Daten des sicheren Kanals digital signieren (wenn möglich)* und *Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln (wenn möglich)* unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen)*. Wird die Richtlinie *Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)* aktiviert, muss die Kommunikation signiert oder verschlüsselt werden. Unterstützen dann beide Partner nicht die gleichen Verfahren, wird keine Verbindung aufgebaut. Diese Option wird für den Einsatz empfohlen, wenn alle Domain Controller der Domäne und aller vertrauten Domänen mindestens Windows NT 4.0 mit Service Pack 4 ausführen.

Das SMB-Protokoll (Server Message Block) unterstützt nicht nur eine gegenseitige Authentisierung, sondern erlaubt auch das Signieren der SMB-Pakete. Durch die Authentisierung und das Signieren werden Man-in-the-Middle-Angriffe verhindert.

Die SMB-Signaturen werden mit folgenden Richtlinien unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* konfiguriert:

- *Microsoft-Netzwerk (Client): Kommunikation digital signieren (wenn Server zustimmt)*,
- *Microsoft-Netzwerk (Client): Kommunikation digital signieren (immer)*,
- *Microsoft-Netzwerk (Server): Kommunikation digital signieren (wenn Client zustimmt)*,
- *Microsoft-Netzwerk (Server): Kommunikation digital signieren (immer)*.

Standardmäßig werden die Signaturen für SMB-Pakete unter Windows XP nicht erzwungen, lediglich die Richtlinie *Microsoft-Netzwerk (Client): Kommunikation digital signieren (wenn Server zustimmt)* ist aktiviert. Nur wenn auf dem SMB-Server beispielsweise das Signieren der Pakete aktiviert wurde, wird die Kommunikation signiert. Es besteht jedoch die Möglichkeit, die Signaturen zu erzwingen. Hierfür sind die restlichen Richtlinien zu aktivieren.

Das Aktivieren der Richtlinien zum Signieren der SMB-Kommunikation kann sich auf die Kompatibilität mit Clients, Diensten und Anwendungen auswirken. Vor der Aktivierung dieser Einstellungen sind daher Kompatibilitätstests erforderlich.

Nicht alle SMB-Server von Drittanbietern unterstützen die Kennwortverschlüsselung während der Authentisierung. Wird im Rahmen des SMB-Protokolls auf einen solchen Server zugegriffen, kann das Kennwort unverschlüsselt übertragen werden, wenn die Richtlinie *Microsoft-Netzwerk (Client): Unverschlüsseltes Kennwort an SMB-Server von Drittanbietern*

senden aktiviert wird. Die Übertragung ungeschützter Kennwörter sollte nicht zugelassen werden, d. h. die genannte Richtlinie darf nicht aktiviert werden.

Windows XP erlaubt das Festlegen der minimalen Sitzungssicherheit für die Kommunikation auf Anwendungsebene (z. B. zwischen RPC-Komponenten). Folgende Optionen können in beiden Richtlinien *Netzwerksicherheit: minimale Sitzungssicherheit für NTLM-SSP-basierte Clients (einschließlich sicherer RPC-Clients)* und *Netzwerksicherheit: minimale Sitzungssicherheit für NTLM-SSP-basierte Server (einschließlich sicherer RPC-Server)* unter *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* gewählt werden:

- Nachrichtenintegrität erfordern,
- Nachrichtenvertraulichkeit erfordern,
- NTLMv2-Sitzungssicherheit erfordern,
- 128-Bit-Verschlüsselung erfordern.

Standardmäßig werden keine Minimaloptionen festgelegt. Wird auf allen Rechnern Windows XP bzw. Windows 2003 mit aktivierter 128-Bit-Verschlüsselung ausgeführt, sind die Optionen für NTLMv2-Authentisierung und 128-Bit-Verschlüsselung zu aktivieren.

Starker Authentisierungsmechanismus

Die Güte des Authentisierungsverfahrens bei Netzwerkanmeldungen spielt ebenfalls eine signifikante Rolle für die Gewährleistung der Sicherheit. Insgesamt können drei Authentisierungsmechanismen verwendet werden: LM, NTLMv1 und NTLMv2. Vor Windows 2000/XP/2003 wurde zunächst das LM-Verfahren und ab Windows NT das NTLM-Verfahren (in zwei Versionen) eingesetzt. Die alten Verfahren haben jedoch Schwächen, so dass aus einem übertragenen Authentisierungswert das Kennwort bestimmt werden kann. Den besten Schutz bietet an dieser Stelle die Version 2 des NTLM Protokolls.

In reinen Windows Netzen (mit NT 4.0 ab SP4/2000/XP/2003) sollte in jedem Fall ausschließlich NTLMv2 als das sicherste verfügbare Verfahren eingesetzt werden. Die älteren Protokolle sollten aufgrund ihrer Schwächen abgelehnt werden. Dazu ist in der zugehörigen Richtlinie *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* | *Netzwerksicherheit: LAN Manager-Authentifizierungsebene* der Wert *Nur NTLMv2-Antworten senden\LM&NTLM verweigern* einzustellen.

Die Speicherung der LAN Manager Hashwerte bei Kennwortänderungen sollte deaktiviert werden. Dies wird durch das Aktivieren der Richtlinie *Computerkonfiguration* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen* |*Netzwerksicherheit: Keine LAN Manager-Hashwerte für nächste Kennwortänderung speichern* erreicht.

Sind noch ältere Systeme im Einsatz (Windows 9x/NT 4.0 vor Service Pack 4), so kann es aus Kompatibilitätsgründen notwendig sein, auch andere Authentisierungsmechanismen zuzulassen, was aus Sicherheitssicht jedoch nicht empfohlen wird. Grundsätzlich wird empfohlen, die älteren Systeme mit Hilfe entsprechender Service Packs zu aktualisieren (Windows NT 4.0 Service Pack 4 oder höher) oder Zusatzsoftware zu verwenden (NTLMv2 ist

zusammen mit dem optionalen Client für Verzeichnisdienste auch unter Windows 95/98 verfügbar).

Anonymer Zugriff

Anonyme Zugänge über das Netzwerk sollten grundsätzlich nicht möglich sein (sogenannte NULL SESSIONS). Unter Windows XP ist es standardmäßig vorgesehen, bestimmte Aktivitäten wie z. B. das Aufzählen von SAM-Konten anonym durchzuführen. Diese Funktionalität ist durch das Aktivieren der Richtlinien *Netzwerkzugriff: Anonyme SID-/Namensübersetzung nicht erlauben*, *Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten nicht erlauben* und *Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten und Freigaben nicht erlauben* (unter *Computereinstellungen* | *Windows-Einstellungen* | *Sicherheitseinstellungen* | *Lokale Richtlinien* | *Sicherheitsoptionen*) explizit zu deaktivieren. Die Richtlinie *Netzwerkzugriff: Die Verwendung von 'Jeder'-Berechtigungen für anonyme Benutzer* ist zu deaktivieren.

Ergänzende Kontrollfragen:

- Wurde gewährleistet, dass auch ältere Clients das NTLMv2 Verfahren zur Authentisierung verwenden (z. B. durch das Einspielen entsprechender Service Packs oder zusätzlicher Software)?
- Wurden die Sicherheitseinstellungen auf die Kompatibilität mit Diensten und Anwendungen getestet?

M 5.124 Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Administrator, Haustechnik

In Besprechungs-, Veranstaltungs- und Schulungsräumen sind einerseits häufig IT-Systeme wie Beamer oder Schulungsrechner fest installiert, andererseits werden dorthin auch mobile IT-Systeme wie Laptops häufig mitgebracht. Dabei ist oft auch gewünscht, dass diese IT-Systeme miteinander, mit dem Internet oder dem institutionsinternen Intranet vernetzt werden können.

Da fremde IT aber zunächst immer als nicht vertrauenswürdig betrachtet werden sollte, sollte eine unkontrollierte Anbindung von durch Besucher mitgebrachten IT-Systemen an interne LANs unterbunden werden. Es sollte auch möglichst keine direkte Kopplung von mitgebrachten und internen IT-Systemen stattfinden. Hierbei sind zumindest alle Sicherheitsmaßnahmen umzusetzen, die in Baustein B 5.2 *Datenträgeraustausch* beschrieben sind.

Grundsätzlich können folgende Zugriffsarten gewünscht sein:

- LAN-Zugriff für alle Raumnutzer, ohne Zugriff auf Internet
- LAN-Zugriff für Mitarbeiter
- Direkter Internet-Zugriff für alle Raumnutzer
- Internet-Zugriff über LAN für alle Raumnutzer
- Internet-Zugriff über LAN für Mitarbeiter

Im folgenden wird beschrieben, wie diese verschiedenen Zugriffsarten zu bewerten und abzusichern sind:

Zugriff auf Intranet

Aus Sicherheitssicht die beste und einfachste Lösung ist es, einen Zugriff aus Besprechungs-, Veranstaltungs- und Schulungsräumen auf interne LANs generell zu unterbinden. Im sichersten Fall sollten gar keine entsprechenden Anschlüsse installiert werden, um auszuschließen, dass Institutionsfremde sich mit dem internen Netz verbinden können.

Dies ist allerdings nicht immer möglich. Wenn eigene Mitarbeiter aus Besprechungs-, Veranstaltungs- und Schulungsräumen auf das Intranet zugreifen können sollen, sind mindestens folgende Maßnahmen zu ergreifen (siehe M 5.122 *Sicherer Anschluss von Laptops an lokale Netze*):

- Der Zugriff auf ein LAN sollte auf hierfür zugelassene IT-Systeme beschränkt werden. Dies sollte beispielsweise über die Prüfung der MAC-Adressen, über rechnergebundene Zertifikate oder über eine Benutzerauthentisierung sichergestellt werden.
- Besprechungs-, Veranstaltungs- und Schulungsräume sollten durch einen restriktiv konfigurierten Paketfilter vom LAN getrennt werden, um unerwünschte Kommunikation unterbinden zu können. Dadurch können unter anderem die Auswirkungen der auf den angeschlossenen Rechnern eventuell vorhandenen Schadsoftware gemindert werden.

- Es muss sichergestellt werden, dass Dritte den Datenverkehr bei der LAN-Nutzung durch Mitarbeiter nicht mitlesen bzw. mitschneiden können. Dies könnte zum einen erfolgen, indem die Infrastruktur so geschaffen wird, dass weitere Rechner den Anschluss des Mitarbeiters nicht mitnutzen können (z. B. durch Verzicht auf Hubs). Zum anderen könnte eine verschlüsselte Kommunikation eingesetzt werden, die erst nach einer entsprechenden Authentisierung des Mitarbeiters aufgebaut werden kann.
- Nach Möglichkeit sollte kein Dynamic Host Configuration Protocol (DHCP) für die Zugänge zum LAN angeboten werden. Angeschlossene Fremdrechner sind somit nicht automatisch in das Netz integriert und müssen von Hand konfiguriert werden (die hauseigenen Rechner müssten in diesem Fall entsprechend vorkonfiguriert sein). Denkbar wäre auch statisches DHCP, dass nur den anhand der MAC-Adresse erkannten, hauseigenen Rechnern die Netzinfrastrukturinformationen zuordnet.

Einrichtung eines Internet-Zugangs

Zunehmend sind in Besprechungs-, Veranstaltungs- und Schulungsräumen aber auch direkte Internet-Zugänge zu finden, z. B. über dedizierte DSL-Zugänge. Die Zugänge werden häufig als Internet-Steckdosen gekennzeichnet. Hierüber können Besucher beispielsweise auf ihr Heimat-Netz zugreifen. Diese Internet-Zugänge dürfen aus Sicherheitsgründen nicht direkt mit dem Intranet verbunden werden, damit der zentrale Sicherheitsgateway nicht umgangen werden kann. Es muss auch ausgeschlossen werden, dass ein Rechner gleichzeitig eine Verbindung zu Intranet und Internet aufbauen kann. In diesem Fall wird die ursprüngliche hardwaremäßige Trennung der beiden Netze aufgehoben. Wenn Besprechungs-, Veranstaltungs- und Schulungsräume mit dem Internet direkt vernetzt werden sollen, sollte der Zugang mit einem Paketfilter abgesichert sein, um die angeschlossenen IT-Systeme Systeme vor Standardangriffen auf Ports zu schützen. Ein einfacher Sicherheitsproxy kann darüber hinaus die angeschlossenen Rechner vor den Gefährdungen durch aktive Inhalte schützen und die Zugriffe auf Web-Seiten im Rahmen der datenschutzrechtlichen Möglichkeiten protokollieren.

Es sollte darauf verzichtet werden, fremden Mitarbeitern einen Zugang zum Internet anzubieten, der das institutionsinterne Netz als Vermittlungsnetz nutzt. Es kann z. B. aufgrund von Konfigurationsfehlern nie ausgeschlossen werden, dass fremde Mitarbeiter sich trotz eingeschränkter Zugriffsmöglichkeiten einen Zugang zu schutzwürdigen Informationen oder Anwendungen verschaffen.

Wenn ein direkter LAN-Zugriff unterbunden ist, kann eigenen Mitarbeiter auch der Zugriff auf das LAN aus Besprechungs-, Veranstaltungs- und Schulungsräumen heraus über ein VPN über das Internet ermöglicht werden (siehe M 5.122 *Sicherer Anschluss von Laptops an lokale Netze*).

Für den Aufbau von WLANs zur Bereitstellung eines Internetzugangs sollten die entsprechenden Sicherheitsmaßnahmen ergriffen werden.

Ergänzende Kontrollfragen:

- Ist sichergestellt, dass aus Besprechungs-, Veranstaltungs- und Schulungsräumen heraus kein unkontrollierter Zugriff auf das LAN möglich ist?

M 5.125 Absicherung der Kommunikation von und zu SAP Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Ein SAP System kommuniziert über das lokale Netz mit SAP Clients, Browsern, Applikationen und anderen SAP Systemen. Auch zwischen den SAP Systemkomponenten findet Datenaustausch statt. In allen Fällen werden Daten übertragen, die geschützt werden müssen. Dies sind nicht nur die Daten, die genutzt werden, um Benutzer zu authentisieren (z. B. Benutzername und Passwort, SSO-Tickets, SAPSSO2-Cookie), sondern auch Geschäftsdaten, die im Rahmen der aufgerufenen Funktionen verarbeitet werden.

Es muss daher entschieden werden, ob und mit welchem Schutzmechanismus die Kommunikation abgesichert wird. Die Kommunikationsmethoden können im Wesentlichen in folgende Klassen unterteilt werden:

- RFC-Kommunikation:

  Hier werden die Daten im Klartext übertragen. Protokolle, die auf RFC aufsetzten, beispielsweise DIAG, das von SAPGui-Clients genutzt wird, komprimieren die Daten. Dies ist jedoch kein Schutzmechanismus. Zudem kann die Kompression ausgeschaltet werden.

- HTTP-basierte Kommunikation:

  Die Daten werden in Klartext-Form übertragen.

- TCP/IP-Kommunikation:

  Die Daten werden in Klartext-Form übertragen.

Bei der Übertragung schützenswerter Daten von und zu SAP Systemen sollten diese verschlüsselt werden. Zum Schutz der Daten können unterschiedliche Verfahren eingesetzt werden. Es ist daher zu entscheiden, welches Verfahren unter Kosten-Nutzen-Aspekten das günstigste ist. Die Entscheidung ist nachvollziehbar zu dokumentieren.

Einsatz von IPSec

IPSec bietet eine generelle Absicherung der Kommunikation auf IP-Ebene: Alle Datenpakete werden verschlüsselt und integritätsgeschützt. Vorteilhaft an diesem Verfahren ist, dass auf SAP System-Ebene keine zusätzlichen Konfigurationen durchzuführen sind, da der IPSec-Schutz auf Betriebssystem-Ebene konfiguriert wird.

Werden SAP Systeme in reinen Windows-Netzen betrieben (Versionen ab Windows 2000), ist IPSec standardmäßig und ohne Mehrkosten (z. B. für Lizenzen) verfügbar. Es entsteht jedoch administrativer Aufwand für die Konfiguration. Weitere Informationen finden sich in M 5.90 *Einsatz von IPSec unter Windows 2000/XP*.

Beim Einsatz von IPSec wird sowohl die Kommunikation des ABAP- als auch des Java-Stacks geschützt.

Einsatz von SNC

Innerhalb des SAP Systems kann die Kommunikation mit SNC (Secure Network Communications) geschützt werden. SNC ist jedoch nur eine standardisierte Schnittstelle, so dass SNC-konforme Schutzbibliotheken (auch SNC-Bibliothek, SNC-Modul oder SNC-Implementierung genannt) zusätzlich erworben, lizenziert und installiert werden müssen.

SNC bietet unterschiedliche Schutzlevel an. Im Wesentlichen wird jedoch Authentisierung und Verschlüsselung angeboten. Je nach SNC-Bibliothek können dabei unterschiedliche Algorithmen eingesetzt werden. SNC bietet eine generelle Absicherung der Kommunikation auf SAP System-Ebene.

Bei der Beschaffung von SNC-Implementierungen ist Folgendes zu berücksichtigen:

- Welche Algorithmen werden angeboten? Es ist auf ausreichend sichere Algorithmen mit ausreichend langen Schlüsseln zu achten. Proprietäre und nicht offen gelegte Verschlüsselungsverfahren sind zu vermeiden.
- Wie ist das Preis- und Lizenzmodell? Für große Unternehmen oder Behörden können hier nicht zu vernachlässigende Kosten entstehen.
- Die Authentisierung erfolgt bei SNC außerhalb des SAP Systems. Wie werden die SNC-Benutzer verwaltet? Müssen die Benutzer über ein separates Werkzeug verwaltet werden oder erfolgt eine Integration in bestehende Verwaltungsstrukturen (z. B. LDAP-Server, Windows Active Directory)?

Von SAP sind SNC-Implementierungen kostenfrei verfügbar, die unter Windows einsetzbar sind, jedoch lediglich Authentisierung anbieten. Hier kann zwischen NTLM- und Kerberos-basierten Varianten gewählt werden.

SNC schützt beim Einsatz sowohl die Kommunikation des ABAP- als auch des Java-Stacks, ist jedoch jeweils separat zu konfigurieren.

SAP Informationsquellen

Quellen für SAP Dokumentationen zur SNC-Konfiguration finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Einsatz von SSL

Für alle HTTP-basierten Zugriffe ist SSL grundsätzlich zu empfehlen. Dies gilt auch für die interne Kommunikation zwischen Komponenten des SAP Systems und anderen Komponenten, die die Möglichkeit der SSL-Absicherung bieten (z. B. beim LDAP-Zugriff).

Da SSL Verschlüsselungsmechanismen nutzt, SAP jedoch aufgrund unterschiedlicher Export-/Import-Bestimmungen in den verschiedenen Ländern Verschlüsselungsmechanismen nicht standardmäßig ausliefert, muss die Verschlüsslungsbibliothek (SAP Cryptographic Library, SAP Cryptolib) zusätzlich installiert werden. Es ist zu beachten, dass die SSL-Unterstützung für den ABAP-Stack und den Java-Stack separat zu installieren ist.

SSL verhandelt das eingesetzte Schutzverfahren dynamisch zwischen den Kommunikationspartnern. Daher sollten schwache Verfahren aus der Liste der erlaubten Verfahren (der so genannten Cipher-Suite) gelöscht werden.

SAP Informationsquellen

Hinweise auf detaillierte Anleitung zur Installation und Konfiguration von SSL finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Ergänzende Kontrollfragen:

- Wird die Übertragung schützenswerter Daten von und zu SAP Systemen verschlüsselt?
- Wird SSL bei HTTP-basierter Kommunikation eingesetzt?

M 5.126 Absicherung der SAP RFC-Schnittstelle

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der Remote Function Call (RFC) Mechanismus ist für den ABAP-Stack die primäre Kommunikationsschnittstelle für die System-zu-System-Kommunikation. Auch der Java-Stack unterstützt die RFC-Kommunikation über den Java Connector (JCo).

SAP Informationsquellen

Hinweise auf SAP Dokumentationen zur RFC-Kommunikation finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

RFC-Berechtigungen restriktiv vergeben

Berechtigungen zum Aufruf von RFC-fähigen ABAP-Programmen (dann auch RFC-fähige Bausteine genannt) werden über das Berechtigungsobjekt S_RFC gesteuert. Jeder RFC-fähige Baustein erfordert je nach Funktionalität weitere Berechtigungen, die über zusätzliche Berechtigungsobjekte geprüft werden. Da der Aufruf meist über das Netz erfolgt, ist das SAP System über die RFC-Schnittstelle aus der Entfernung potentiell angreifbar.

Die RFC-Berechtigungen müssen daher geplant und restriktiv vergeben werden. Durch das S_RFC Berechtigungsobjekt kann gesteuert werden, auf welche RFC-Funktionsbausteine ein Benutzer zugreifen darf. Dabei unterliegt das Berechtigungsobjekt folgenden wichtigen Beschränkungen:

- Die Beschränkung kann nur auf Funktionsgruppen erfolgen, da nur der Wert RFC_TYPE = "FUGR" unterstützt wird.
- Die Prüfung des Parameters RFC_NAME, der die Liste der betroffenen Funktionsgruppen enthält, ist auf achtzehn Zeichen beschränkt. Die Liste kann zwar länger eingegeben werden, jedoch werden nur die ersten achtzehn Zeichen geprüft.

Der Zugriff kann also nur auf alle Funktionsbausteine einer Funktionsgruppe erteilt werden, und unter Umständen müssen mehrere Berechtigungen erstellt werden.

Generell sollte die S_RFC Berechtigung nicht den Zugriff auf alle RFC-Bausteine erlauben. Die Einstellung RFC_NAME="*" ist zu vermeiden. Es gibt in einem SAP System mehrere tausend RFC-fähige Funktionsbausteine, die damit zum Zugriff freigeschaltet würden. Auch auf RFC-fähige Bausteine von neu installierten Applikationen und Modulen könnte so automatisch zugegriffen werden. Ob die aufgerufene RFC-Funktion jedoch erfolgreich ausgeführt wird, hängt dann noch von Zugriffsprüfungen ab, die die RFC-Funktion selbst durchführt.

Werden die RFC-Berechtigungen geplant, ist zu bedenken, dass es unterschiedliche RFC-Typen (z. B. synchron, asynchron) gibt. Daher müssen alle Typen in die Planung einbezogen werden.

Die Berechtigung S_RFC ist nicht für den Java-Stack relevant.

Ausgehende RFC-Zugriffe können über das Berechtigungsobjekt S_ICF beschränkt werden, das den Zugriff auf Destinationen regelt (siehe M 4.263 *Absicherung von SAP Destinationen*).

Java-Stack RFC

Der Java Connector (JCo) bietet für den Java-Stack die Möglichkeit, über RFC zu kommunizieren. Dabei wird jedoch standardmäßig von den Systemkomponenten nur von ausgehenden RFC-Calls (Java-Stack als RFC-Client) Gebrauch gemacht. Zugriffe erfolgen auf den eigenen ABAP-Stack (z. B. um Benutzer und Rollen des ABAP-Stacks verfügbar zu machen) oder über Destinationen auf andere SAP Systeme oder externe RFC-Server.

Folgendes ist beim Einsatz des Java Connectors zu bedenken:

- Der Java-Stack nutzt den (ABAP-Stack-) Benutzer SAPJSF zum Zugriff auf den ABAP-Stack. Dieser muss während der Installation mit einem starken Passwort versehen werden.
- Die Destinationen (Destination-Service) im Java-Stack müssen vor unberechtigtem Zugriff geschützt werden.

Für Java-Stack RFC-Server-Programme ist Folgendes zu beachten:

- RFC-Server müssen durch eigene Programme implementiert werden. RFC-Server-Instanzen können über die JCo-Programmierschnittstelle erzeugt werden.
- Die JCo-RFC-Server-Implementierung bietet nur reine RFC-Kommunikationsfunktionen. Insbesondere Berechtigungen müssen zwingend durch die eigene Programmimplementierung geprüft und verwaltet werden.

Absicherung der RFC-Kommunikation mit SNC

Ergibt die Schutzbedarfsfeststellung, dass Kommunikationsstrecken geschützt werden müssen, auf denen RFC eingesetzt wird, so kann SNC empfohlen werden. M 5.125 *Absicherung der Kommunikation von und zu SAP Systemen* enthält weitere Informationen dazu.

Sichere Verwendung von "Trusted System"-Beziehungen

Zwischen SAP Systemen können Vertrauensbeziehungen eingerichtet werden, so dass Benutzer beim RFC-Zugriff kein Passwort angeben müssen. Beim Zugriff prüft das vertrauende SAP System (Trusting System), ob der Zugriff von einem vertrauten SAP System (Trusted System) aus erfolgt.

Über das Berechtigungsobjekt S_RFCACL kann im Zielsystem gesteuert werden, welche Benutzer Aufrufe ohne Passwortangabe durchführen dürfen. Dabei kann unter anderem nach SAP System-ID (SAPSID), Mandant und aufrufender Transaktion unterschieden werden.

Generell ist Folgendes zu beachten:

- Trusted System Beziehungen sollten nur nach reiflicher Überlegung und Risikobewertung eingesetzt werden.

- Für das Berechtigungsobjekt S_RCFACL sollten keine Blanko-Einstellungen mit "*" enthalten sein.
- Für RFC-Destinationen, die in vertrauenden SAP Systemen enden, sollten keine Benutzerinformation gespeichert werden, da sonst im vertrauenden System nicht mehr nach den aufrufenden Benutzern unterschieden werden kann.

Weitere Informationsquellen zum Thema finden sich in M 2.346 *Nutzung der SAP Dokumentation*. **SAP Informationsquellen**

RFC-Client-Programme: Konfiguration der sideinfo Datei

Für RFC-Clients kann über die Datei "sideinfo" eine globale Konfiguration für den RFC-Zugriff erfolgen. In der Datei können auch Authentisierungsinformationen angegeben werden, die dann für RFC-Zugriffe (genauer: beim Aufbau der unterliegenden CPIC-Kommunikation) genutzt werden. Alle Informationen sind in der Datei im Klartext gespeichert.

Folgendes sollte daher beachtet werden:

- Der Einsatz der sideinfo Datei sollte gut überlegt werden.
- Die Informationen der sideinfo Datei kann von allen lokalen RFC-Client-Programmen genutzt werden.
- Authentisierungsinformationen sollten nicht in der sideinfo Datei gespeichert werden. Die Anmeldeinformationen sollten durch das Client-Programm vom Benutzer erfragt werden.
- Die sideinfo Datei darf für Benutzer, die RFC-Client-Programme starten, nur lesend zugreifbar sein. Schreibzugriffe dürfen nur für den berechtigten Administrator möglich sein.

Die sideinfo Datei kann in einem SAP System an mehreren Stellen genutzt werden und kommt insbesondere auch auf dem SAP Gateway zum Einsatz.

Hinweise auf Detailinformationen finden sich in M 2.346 *Nutzung der SAP Dokumentation.* **SAP Informationsquellen**

Externe (non-SAP) RFC-Server sicher nutzen

Mit Hilfe des RFC Software Development Kits (RFC SDK) können RFC-Server-Programme erstellt werden, die ihre Funktionen über RFC anbieten. Werden externe RFC-Server-Programme eingesetzt ist Folgendes zu bedenken:

- Die Standard SAP Sicherheitsmechanismen und Verfahren (Authentisierung, Autorisierung, Verwaltung) sind für den externen RFC-Server nicht verfügbar.
- Die angebotenen Sicherheitsmechanismen hängen ausschließlich von der Implementierung des RFC-Server-Programms ab.
- Die Verwaltung von Benutzern und Berechtigungen kann durch das Server-Programm oder durch externe Komponenten erfolgen. Es sind auch Implementierungen möglich, die die RFC-Funktionen für jeden Zugreifenden ohne weitere Prüfungen verfügbar machen.

Bei Eigenentwicklungen oder bei der Beschaffung von Software sollte daher darauf geachtet werden, dass die gewünschten Sicherheitsanforderungen erfüllt werden.

Für die Installation von externen RFC-Servern ist darauf zu achten, dass ausschließlich die RFC-Bibliothek installiert wird. Insbesondere ist zu vermeiden, dass das gesamte RFC Software Development Kit (RFC SDK), das für die Entwicklung vom RFC-basierten Programmen genutzt wird, installiert und zugreifbar ist. Dies muss durch den Software-Verteilungsprozess sichergestellt werden.

Für Rechner, auf denen das RFC SDK installiert werden muss (z. B. Entwicklungsrechner), sollte der Zugriff auf die Programme im "bin"-Verzeichnis (Standardpfad: <Installationsverzeichnis>/Sap/rfcsdk/bin) der SDK-Installation beschränkt werden. Die Programme können unter anderem zum RFC-Zugriff auf SAP Systeme (startrfc) oder zum Starten von RFC-Servern (rfcexec) genutzt werden.

Die Zugriffsmöglichkeiten auf SAP Systeme (z. B. Produktion) sind für Rechner, auf denen das RFC SDK installiert ist, auf Netz-Ebene zu beschränken.

Angaben zu weiteren Informationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*. **SAP Informationsquellen**

secinfo Datei für SAP Gateway konfigurieren

Externe RFC-Server-Programme registrieren sich in der Regel bei der SAP Systemkomponente SAP Gateway, die die Client-Zugriffe auf die externen RFC-Server-Programme vermittelt. Diese können auf externe Anforderung auch explizit durch das SAP Gateway gestartet werden.

Die Zugriffs- und Startmöglichkeiten, die externen Zugreifern zur Verfügung stehen, werden über die Konfigurationsdatei "secinfo" gesteuert. Die Datei wird nicht automatisch erzeugt und muss daher unbedingt manuell erstellt werden. Existiert die Datei nicht, werden keine Beschränkungen umgesetzt, so dass jeder mit der technischen Zugriffsmöglichkeit beliebige Programme auf dem SAP Gateway-Rechner starten kann. Es genügt zunächst, eine leere Datei zu erzeugen, um zu erreichen, dass keine Berechtigungen bestehen. Danach können dann Berechtigungen und Zugriffseinschränkungen konfiguriert werden. Die Datei muss im "data"-Verzeichnis des SAP Gateways, also genauer der Gateway-Instanz, abgelegt sein (Standardpfad: /usr/sap/<Instanzname>/data).

Alternativ kann auch der Profilparameter "gw/rem_start" mit der Einstellung "DISABLED" genutzt werden, wenn generell keine externen RFC-Server-Programme zum Einsatz kommen.

Hinweise auf nähere Informationen dazu finden sich in M 2.346 *Nutzung der SAP Dokumentation*. **SAP Informationsquellen**

Ergänzende Kontrollfragen:

- Wurden die RFC-Berechtigungen geplant?
- Wurden minimale RFC-Berechtigungen vergeben?

- Wird SNC zur Absicherung von RFC-Verbindungen genutzt, über die schützenswerte Daten übertragen werden?
- Ist der Zugriff auf RFC SDK Installationen beschränkt?
- Existiert die Datei secinfo?

M 5.127 Absicherung des SAP Internet Connection Framework (ICF)

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Das Internet Connection Framework (ICF) eines SAP Systems erlaubt den HTTP-basierten Zugriff auf Funktionen des ABAP-Stacks. Daneben wird durch das ICF auch das Simple Mail Transport Protocol (SMTP) unterstützt. Es können verschiedene Dienste (Services) angesprochen werden. Die Dienste sind in einer dateisystemähnlichen Baumstruktur hierarchisch angeordnet. Der HTTP-Zugriffspfad (URL-Pfad-Anteil) wird durch den Pfad in der Baumstruktur bestimmt. Für die Administration des ICF wird die Transaktion SICF benutzt.

Die nachfolgend aufgeführten Empfehlungen sollten im Zusammenhang mit dem ICF beachtet werden.

SAP Informationsquellen

Hinweise auf SAP Dokumentationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Aktive ICF-Dienste

Es sollten nur die benötigten Dienste aktiviert werden. Für jeden aktivierten Dienst sollte dessen Funktion bekannt sein. Es ist empfehlenswert, zu jedem Dienst kurz zu notieren, welche Funktion er hat und ob er aktiviert werden darf.

Nach der Installation eines SAP Systems sind alle ICF-Dienste deaktiviert. Dennoch wird eine Prüfung dieses Sachverhaltes empfohlen. Auch nach der Installation von Updates und neuer ICF-Dienste sollte dies geprüft werden.

Die Möglichkeit, die komplette ICF-Baumhierarchie, die unter einem ICF-Objekt hängt, auf einmal zu aktivieren, sollte nicht genutzt werden. Dienste sollten immer einzeln aktiviert werden.

SSL-Schutz

Für den Zugriff auf ICF-Dienste kann einzeln konfiguriert werden, ob die Kommunikation beim Zugriff mit SSL geschützt sein muss. Es kann hier generell empfohlen werden (siehe M 5.125 *Absicherung der Kommunikation von und zu SAP Systemen*), SSL für alle Dienste zu aktivieren, um die übertragenen Daten vor unberechtigter Kenntnisnahme zu schützen. Da sich die auf einem ICF-Objekt eingestellten Eigenschaften in den Unterbaum vererben, genügt es, dazu die Konfiguration auf dem Wurzelknoten anzupassen.

Authentisierte Zugriffe

Für jeden ICF-Dienst muss definiert werden, mit welcher Authentisierungsvariante der Zugriff erlaubt werden soll. Dies gilt insbesondere für Eigenentwicklungen.

In der Regel empfiehlt sich folgende Konfiguration für die Benutzerauthentisierung:

- Anonyme Anmeldedaten: keine Werte eintragen.

- Sicherheitsanforderung: SSL
- Basic Authentication: Standard SAP-Benutzer

Soll auf Dienste anonym zugegriffen werden, müssen Anmeldeinformationen unter "Anonyme Anmeldedaten" angegeben werden. Alle anonymen Zugriffe erfolgen dann unter dem eingetragenen Benutzer. In diesem Fall sollten ausschließlich technische Benutzer verwendet werden, die vom Typ Service sind. Dialogbenutzer sollten nicht genutzt werden.

Es muss beachtet werden, dass die Anmeldedaten für anonyme Zugriffe, die für ein ICF-Objekt definiert sind, auch für alle Unterobjekte im Unterbaum gelten. Unterschiedliche Anmeldedaten (z. B. Client, Benutzer, Sprache) die auf verschiedenen Objekten definiert sind, die auf dem Baumpfad zu einem bestimmten Objekt liegen, können sich auch überlagern.

Generell findet nach dem Aufruf eines ICF-Dienstes (z. B. einer Business Server Pages Applikation, BSP) auch immer die normale Prüfung auf die von der Applikation genutzten Berechtigungsobjekte statt.

ICF-Administration

Die administrativen Transaktionen SICF (ICF Dienst-Verwaltung) und SMICM (ICF-Monitor) sind vor unberechtigten Zugriffen zu schützen (Berechtigungsobjekt: S_TCODE).

In produktiven Systemen sollten die Funktionen, die das detaillierte Protokollieren von Client-Anfragen erlauben (z. B. Debugging, Trace, Laufzeitanalyse, Recorder), nicht genutzt werden. Fehlersituationen sollten im Test- und Akzeptanzsystem untersucht werden.

ICF-Zugriffsberechtigungen

Personen, die auf ICF-Dienste zugreifen, sollten nicht gleichzeitig über die Dialogschnittstelle (SAPGui) Zugriff auf das SAP System besitzen, so dass den Personen ein Service-Benutzer zugeordnet werden kann.

Die Zugriffsberechtigung auf ICF-Dienste sollte restriktiv vergeben werden. Das Berechtigungsobjekt S_ICF wird für die Berechtigungsprüfung herangezogen. Für die Zugriffskontrolle auf ICF-Dienste muss folgende Konfiguration gewählt werden:

- Für das Feld ICF_FIELD muss der Wert "SERVICE" eingetragen werden.
- Für das Feld ICF_VALUE muss die Zeichenkette genutzt werden, die im betroffenen ICF-Dienst unter "Service-Daten/Service Optionen/SAP-Berechtigung" eingetragen ist. Ist für mehrere Dienste die gleiche Zeichenkette eingetragen, so kann der Zugriff auf all diese Dienste über eine Berechtigung gesteuert werden (siehe dazu auch M 4.263 *Absicherung von SAP Destinationen*).

Informationen auf Fehlerseiten

Die Fehlerseiten von ICF-Diensten sollten keine internen Informationen enthalten. Dies gilt insbesondere für selbst erstellte Dienste.

Ergänzende Kontrollfragen:

- Sind nur die benötigten ICF-Dienste aktiviert?
- Sind die Anforderungen an die Authentisierung für jeden Dienst bekannt?
- Ist der Zugriff auf die ICF-Administration eingeschränkt?
- Sind die ICF-Zugriffsberechtigungen restriktiv geplant und konfiguriert?

M 5.128 Absicherung der SAP ALE (IDoc/BAPI) Schnittstelle

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Application-Link-Enabling-Schnittstelle (ALE) wird als Kommunikationsmechanismus zur Integration von Geschäftsprozessen über mehrere SAP Systeme oder andere externe Systeme hinweg genutzt. Über die Schnittstelle werden Geschäftsdaten und Systemdaten (z. B. beim Einsatz der Zentralen Benutzerverwaltung) zwischen Sender- und Empfänger-System transportiert. Die Verarbeitung erfolgt in den Empfänger-Systemen automatisiert. Daher muss die ALE-Schnittstelle abgesichert werden. Dabei ist Folgendes zu beachten:

- ALE nutzt das RFC-Protokoll (genauer: transaktionaler RFC, tRFC) zur Datenübertragung. Daher sind alle RFC-spezifischen Sicherheitsmaßnahmen umzusetzen (siehe M 5.126 *Absicherung der SAP RFC-Schnittstelle*).
- ALE-Destinationen im Sender-System sind zu schützen, da hier Authentisierungsinformationen hinterlegt werden müssen (siehe M 4.263 *Absicherung von SAP Destinationen*).
- ALE-Berechtigungen im Empfänger-System sind restriktiv zu vergeben (siehe auch M 4.261 *Sicherer Umgang mit kritischen SAP Berechtigungen*).
- ALE-Administrationsberechtigungen dürfen nur den berechtigten Administratoren zugeordnet werden.
- Für die Benutzerkennungen, die in Sender-Systemen für ALE-Destinationen eingetragen sind, dürfen im Empfänger-System keinen ALE-Administrationsberechtigungen bestehen.
- Benutzerkennungen, die in Sender-Systemen für ALE-Destinationen eingetragen sind, müssen im Empfänger-System vom Typ "Kommunikation" sein.
- Normale Benutzer dürfen keine ALE-Berechtigungen besitzen.
- Für externe Nicht-SAP Systeme müssen die zum Zugriff auf die ALE-Schnittstelle genutzten Authentisierungsinformationen geschützt abgelegt sein. Die Informationen sollten nur für die Systemkomponenten oder ALE-Administratoren zugreifbar sein.

SAP Informationsquellen

Hinweise auf weitere Informationen zur Absicherung der ALE-Schnittstelle finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

Ergänzende Kontrollfragen:

- Wurde die ALE-Schnittstelle abgesichert?
- Sind die ALE-Authentisierungsdaten in externen Nicht-SAP Systemen vor unberechtigtem Zugriff geschützt abgelegt?

M 5.129 Sichere Konfiguration der HTTP-basierten Dienste von SAP Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Über die HTTP-Schnittstelle können unterschiedliche Dienste eines SAP-Systems angesprochen werden. Der Zugriff auf die Funktionen und Applikationen des Java-Stack erfolgt in der Regel über HTTP. Der ABAP-Stack ist über das Internet Connection Framework (ICF) mittels HTTP zugreifbar. Die HTTP-Schnittstelle muss generell sicher konfiguriert sein, so dass einerseits Zugriffe, die schützenswerte Daten übertragen, mit SSL geschützt sind und andererseits nur die benötigten Dienste aktiviert werden.

Die folgenden über HTTP zugreifbaren Schnittstellen sind mit besonderen Risiken verbunden:

- SOAP-Schnittstelle
- WebDAV-Schnittstelle
- Content-Server-Schnittstelle

Folgendes ist zu beachten:

SOAP-Schnittstelle

Das Simple Object Access Protocol (SOAP) ist ein Protokoll, über das Web-Dienste angesprochen werden können. Für die SOAP-Schnittstelle eines SAP Systems ist Folgendes zu berücksichtigen:

- Die SOAP-Schnittstelle (ABAP-Stack und Java-Stack) sollte nur authentisiert zugreifbar sein.
- Der SOAP-Zugriff ist über SSL zu schützen.
- Der ABAP-Stack stellt einen SOAP Dienst zum Aufruf von RFC-fähigen Bausteinen (ICF-Pfad: /sap/bc/soap/rfc) zur Verfügung. Ist dieser aktiv, können RFC-Bausteine über HTTP aufgerufen werden. Der Schutz des RFC-Ports eines SAP Systems durch Firewalls wird dadurch umgangen. Daher sollte der Dienst nur mit ausreichenden Sicherheitsvorkehrungen aktiviert werden. Gleiches gilt für den XML-basierten RFC-Dienst (ICF-Pfad: /sap/bc/xrfc).
- Der durch den Java-Stack angebotene Schutz durch WS-Security (Web Service Security, Standardsammlung der Organisationen W3C und OASIS) gilt nur für die in SOAP-Nachrichten übertragenen Daten. Damit ist auf Applikationsebene nicht prüfbar, ob die Daten über eine authentisierte Verbindung übertragen wurden. Authentisierungsdaten sollten daher im Rahmen der Applikation geprüft werden, wenn die Sender-Identität wichtig ist. Dazu müssen die Authentisierungsdaten in den SOAP-Nachrichten enthalten sein. Die Daten sind vor unberechtigter Kenntnisnahme zu schützen.

Generell muss auch die über SOAP angesprochene Applikation durch entsprechende Berechtigungsprüfungen die eigene Sicherheit sicherstellen.

SAP Informationsquellen

SAP Dokumentationen finden sich in M 2.346 *Nutzung der SAP Dokumentation*.

WebDAV-Schnittstelle

Das WebDAV-Protokoll (Web-based Distributed Authoring and Versioning) erlaubt einen dateisystemähnlichen Zugriff auf Informationen über das HTTP-Protokoll. Der WebDAV-Zugriff kann durch den ABAP- und den Java-Stack angeboten werden, wenn entsprechende Produkte oder Applikationen zum Einsatz kommen. Für den ABAP-Stack ist dies beispielsweise Knowledge Warehouse (KW, ICF-Pfad: /sap/bc/kw/fs), für den Java-Stack ist dies beispielsweise die Komponente Collaboration Management (CM, SAP Enterprise Portal Komponente).

Da der WebDAV-Zugriff unter Umständen auch auf das lokale Dateisystem erfolgen kann, muss dieses vor unberechtigten Zugriffen geschützt werden. Dabei steht der Schutz der über WebDAV angeboten Daten zwar im Vordergrund, kann ein Angreifer aber so auf das lokale Dateisystem zugreifen, können dadurch weitere Angriffe vorbereitet werden. Daher sollte der Zugriff nur authentisiert und über SSL geschützt erfolgen. Zusätzlich ist immer auf die Vergabe von Berechtigungen zu achten.

Content-Server-Schnittstelle

Über die Content-Server-Schnittstelle kann auf Dokument-Archive (Repositories) zugegriffen werden. Ist die Schnittstelle ungeschützt, so können Informationen und Dokumente über verfügbare Repositories abgerufen werden. Folgendes ist zu beachten:

- Die Content-Server-Schnittstelle (ICF-Pfad /sap/bc/contentserver) ist nur zu aktivieren, wenn sie benötigt wird.
- Der Zugriff sollte nur authentisiert und über SSL erfolgen.
- Beim Zugriff auf die Administrationsschnittstelle ist die Passwort-Abfrage zu erzwingen. Dazu ist der Parameter "AdminSecurity" in der Datei ContentServer.ini auf den Wert "1" zu setzen.
- Es ist zu beachten, dass die Administration innerhalb des SAP Systems über die Transaktion CSADMIN (und auch ICF-Einstellungen) und außerhalb des SAP Systems (z. B. ini-Datei) erfolgen muss.

SAP Informationsquellen

Hinweise auf weitere Dokumentationen finden sich in M 2.346 *Nutzung der SAP Dokumentation.*

Ergänzende Kontrollfragen:

- Wurde eine Grundsicherung des HTTP-Servers vorgenommen?
- Wurden nur benötigte Dienste aktiviert bzw. nicht benötigte deaktiviert?
- Wurde die SOAP-Schnittstelle abgesichert?
- Wurde eine verfügbare WebDAV-Schnittstelle abgesichert?
- Wurde die Content-Server-Schnittstelle abgesichert?

M 5.130 Absicherung des SANs durch Segmentierung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Ein Storage Area Network ist häufig als Fibre-Channel (FC-SAN) realisiert. Es besteht aus einem oder mehreren Switches, Speichersubsystemen wie Plattensubsystemen oder Sicherungsgeräten wie z. B. Bandlaufwerken. Ein oder mehrere Switches, die miteinander verbunden sind, bilden eine Fabric. An die Switches werden Server angeschlossen, denen Speicher aus den Ressourcen des SAN zugewiesen wird.

Speichersubsysteme, Server und deren Betriebssysteme können, unabhängig voneinander, auch mehrfach zugeordnet werden. So werden einerseits verschiedenen Servern unterschiedliche (logische) Speicherressourcen auf einem Speichersystem zugeordnet, andererseits können einem Server mehrere (räumliche getrennte) Speicherkomponenten zugeordnet werden, um Redundanz für den Server und damit dessen Anwendungen zu erreichen.

Demzufolge ist die Verwaltung und Rechte-Zuordnung der Speicherressourcen im SAN anzupassen. Es muss dabei sichergestellt werden, dass keine Daten aufgrund eines falschen Zugriffs zerstört werden und dass Server nur mit "ihrem" Ausschnitt der Speichereinheiten im SAN arbeiten. Dies wird erreicht, indem das SAN in Segmente oder Gruppen eingeteilt wird, so dass nur die Geräte innerhalb eines Segmentes miteinander kommunizieren können.

Die Segmentierung bringt außerdem weitere Vorteile mit sich:

- Speicherkomponenten, die Interoperabilitätsprobleme miteinander aufweisen, können so in getrennten Segmenten eingesetzt werden.
- Wichtige Anwendungen können einzelne Ports und damit eine bestimmte Bandbreite zugewiesen bekommen.
- Sensible Daten können damit besser isoliert werden.
- Verbesserung der Skalierbarkeit, da neue Endgeräte nicht auf Anhieb mit allen anderen kommunizieren können.

Um eine sinnvolle Segmentierung sicherzustellen sollte ein Konzept für die Zuordnung der SAN-Ressourcen erarbeitet werden. Die Informationen zur aktuellen Zuordnung der SAN-Ressourcen müssen stets dokumentiert und im Notfall verfügbar sein. Die aktuelle Ressourcenzuordnung sollte mit Hilfe der Verwaltungswerkzeuge einfach und übersichtlich erkennbar sein.

Segmentierung bei FC-SANs

Die interne Verwaltung und Zuordnung der Geräte in einem FC-SAN erfolgt über World Wide Names (WWN). Sie entsprechen in gewisser Weise den MAC-Adressen von Ethernet-Netzadaptern.

Die Segmentierung eines FC-SANs erfolgt durch Einteilung in Zonen (Zoning). Zoning-Funktion werden auf den Switches des SANs konfiguriert. Eine Zone kann Server, Speichersubsysteme und andere Switches als Mitglieder beinhalten.

Soft Zoning

SAN-Geräte haben einen eindeutigen WWN. Beim Soft Zoning werden Zonen durch die Gruppierung von WWNs gebildet. Die Zuordnung von Switch-Ports und SAN-Geräten zu Zonen erfolgt durch einen SAN internen Namensserver. Wenn sich ein SAN-Gerät an der Fabric anmeldet, teilt der Namensserver nur WWNs von Geräten der gleichen Zone mit.

Soft Zoning ist flexibel, da es unabhängig von der Verkabelung gehalten werden kann. Somit müssen Änderungen des Standortes von SAN-Geräten bei diesem Verfahren nicht eingepflegt werden.

Es gilt jedoch zu bedenken, dass Datenübertragungen zu gültigen WWNs nicht verhindert werden. Da manche Betriebssysteme WWNs intern speichern und in einem Cache vorhalten, kann es vorkommen, dass ein solches System auf Speichergeräte zugreift, die nach Willen des Administrators gar nicht mehr in der Zone enthalten ist. Damit sind Datenverluste zu befürchten.

Hard Zoning

Hard Zoning wird üblicherweise über Ports, gelegentlich auch über die WWN-Mechanik definiert. Der Begriff Hard Zoning kommt daher, dass es oft fest in Schaltungen (ASICs) im SAN-Switch, also in der Hardware, verankert ist. Soft-Zoning ist dagegen auf allen Ebenen durch Software realisiert.

Hard Zoning wird häufig auch als Port-Zoning bezeichnet. Die Segmentierung im SAN wird hergestellt, indem in Routing-Tabellen auf SAN-Switches Zonen ausschließlich über die Portnummern der Switche gebildet werden. Dadurch sind genau die Geräte, deren Portnummern als eine Zone zusammengestellt sind, Mitglied dieser Zone. Diese statische Zuordnung erzwingt, dass kein Datenverkehr zwischen Ports unterschiedlicher Zonen stattfindet. Die Einschränkung, dass Änderungen der Hardwarekonfiguration oder Standortwechsel von SAN-Geräten eine manuelle Anpassung der Tabellen erfordert, ist in der Praxis fast immer tragbar.

Da Speichernetze nur in seltenen Fällen häufigen Änderungen unterworfen sind, ist Hard Zoning oder ein adäquates herstellerspezifisches Verfahren als Schutz vor Datenverlust vorzuziehen.

Zudem sollte stets die kleinstmögliche Anzahl von Geräten in einer Zone zusammengefasst werden.

LUN Binding und Masking

Festplattensubsysteme in einem SAN stellen die eingebauten Platten als logical units zur Verfügung. Die Units können über ihre LUN (Logical Unit Number) adressiert werden. Um zu verhindern, dass jeder Rechner, der in einer Zone mit einem Festplattensubsystem stationiert ist, alle logischen oder physischen Platten dieses System sieht, können LUN Binding und LUN Masking eingesetzt werden.

LUN Binding ordnet Zugriffe auf die jeweiligen LUNs fest über bestimmte Fibre Channel Ports der Speichersysteme zu und erlaubt so die Adressierung der LUNs nur über bestimmte Netzzugänge.

Bei LUN Masking werden darüber hinaus Zugriffstabellen auf dem Plattensubsystem definiert, in denen die eindeutigen WWN Adressen der zugriffsberechtigten Server registriert sind. Alle anderen (maskierten) Platten sind für den Rechner unsichtbar.

Auf diese Weise kann auch eine fehlerhafte Konfiguration oder Bedienung eines Rechners mit SAN-Anschluss nur noch Auswirkung auf die für ihn sichtbar gemachten Platten haben.

Bei der Zuordnung von Servern und Speichersystemen im SAN sollte stets Zoning und LUN Masking kombiniert werden.

Virtuelle SANs (VSANs)

Analog zur Segmentierung von LANs in virtuelle Teilnetze (VLANs) ist auch eine Segmentierung eines SANs möglich. Dieses Konzept erweitert das Konzept des Zoning und bietet sowohl einen besseren Zugriffsschutz auf die Daten und Applikationen als auch Schutz vor einer breiteren Wirkung von Störungen, die so nur auf einen Teil des Netzes begrenzt werden können.

In einem VSAN werden mehrere Ports und damit mehrere Endgeräte einer Fibre Channel Fabric zu einer virtuellen Fabric zusammengefasst. Somit werden auf einer und derselben physikalischen Netzinfrastruktur mehrere virtuell getrennte Fabrics eingerichtet. Ein Switch kann dabei mehreren virtuellen SAN-Teilnetzen angehören. Für jedes VSAN werden separate Fabric Dienste wie Namensserver und Zoning realisiert. VSANs schränken also über das reine Zoning hinaus nicht nur die gegenseitige Sichtbarkeit von Endgeräten, sondern auch die gegenseitige Sichtbarkeit der Fabric-Konfigurationen ein.

Zoning findet unabhängig von einer Trennung in VSANs statt. Eine Zone kann sich nicht über mehrere VSANs erstrecken.

Durch Zoning wird der Zugriff und Datenfluss zwischen den Geräten reguliert. VSANs erlauben zusätzlich, alle in einem Teilnetz bereitgestellten Dienste zu isolieren und innerhalb des VSANs "abzukapseln".

Wenn ausschliesslich Zoning eingesetzt wird, bildet die gesamte Hardware des Speichernetzes eine "Sicherheitsdomäne". Wenn auf der Netzhardware des Speichernetzes VSANs konfiguriert werden, wird die Hardware logisch in verschiedene "Sicherheitsdomänen" aufgeteilt. Innerhalb dieser Domänen können dann "domänen-interne" Mechanismen wie Zoning und Port Binding eingesetzt werden.

Segmentierung bei iSCSI

Die Segmentierung im iSCSI Speichernetz erfolgt im Speichergerät analog zum Anschluss eines über FC-SAN angeschlossenen Gerätes. Der Unterschied liegt in der Verbindungszuweisung zwischen dem Server und dem Speichergerät.

Der iSCSI-HBA (Host Bus Adapter) wird als "Initiator" und der Port am Speichergerät als "Target" bezeichnet. Über mitgelieferte Management-Software werden beide über ihre IP-Adresse miteinander bekannt gemacht.

Um den Verbindungsaufbau abzusichern und die Authentizität von Initiator (=Server) und Target (=Festplatten) sicherzustellen, werden intern Sicherheitsprotokolle wie CHAP (Challenge Handshake Authentication Protocol)" oder iSNS (Internet Storage Naming Service) verwendet.

Die Zuordnung von Platten im Festplattensubsystem zu den angeschlossenen Rechnern kann wie bei FC-SANs über LUN Bindung und LUN Masking erfolgen.

Ergänzende Kontrollfragen:

- Gibt es ein schriftlich fixiertes Konzept für die Zuordnung von SAN-Ressourcen zu Servern?
- Ist die aktuelle Zoning-Konfiguration dokumentiert und auf in Notfällen verfügbar?
- Sind alle Zonen und LUN Masking Zuordnungen von einer einzigen Konsole schnell und übersichtlich zu erkennen?

M 5.131 Absicherung von IP-Protokollen unter Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Voreingestellte Sicherheitseinstellungen

Der TCP/IP-Stack ist nach einer Standardinstallation aktiviert. Die voreingestellten Sicherheitseinstellungen sind ein Kompromiss zwischen Sicherheit auf der einen und Abwärtskompatibilität und Offenheit gegenüber anderen Systemen auf der anderen Seite. Dies ist nur in Einzelfällen und dort auch nur bedingt ausreichend, daher ist zu überlegen, die Basiseinstellung auf ein höheres Sicherheitsniveau anzuheben. Erweitere Einstellungen zur Vorbeugung gegen Denial-of-Service-Attacken finden sich in der Maßnahme M 4.279 *Erweiterte Sicherheitsaspekte für Windows Server 2003*.

Hinweis: Ab Windows Server 2003 mit Service Pack 1 setzt der *Sicherheitskonfigurations-Assistent* (SCW) zur Vorbeugung gegen Denial-of-Service-Attacken (siehe G 4.22 *Software-Schwachstellen oder -Fehler*) einige weitere Einstellungen bei bestimmten Rollen automatisch (siehe M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003*).

Kommunikationsprotokolle der Internetprotokoll-Suite

Unsichere Protokolle im TCP/IP-Stack

Einige Protokolle des TCP/IP-Stacks können optional konfiguriert werden. Sie sind in unterschiedlicher Qualität in die Sicherheitsarchitektur des Betriebsystems integriert und bieten zudem häufig keine ausreichende Authentisierung und Integritätssicherung. Nach einer Standardinstallation ist auf einem Windows Server 2003 System kein unsicheres Protokoll konfiguriert. Wird ein optionales Protokoll installiert, müssen Mechanismen zum Schutz der ausgetauschten Informationen (z. B. kryptographische Funktionen, Authentisierungsfunktionen) entsprechend dem Anwendungsbereich und dem Sicherheitsbedarf konfiguriert werden.

In den Hilfsmitteln zum IT-Grundschutz (siehe *Hilfsmittel zum Windows Server 2003*) wird eine Übersicht von Protokollen der Internetprotokollsuite in verschiedenen Bereichen von Windows Server 2003 gegeben. Hier sind Hinweise zum geeigneten Umgang mit diesen Protokollen enthalten.

Besonders großen Einfluss auf die Sicherheit und Stabilität von Windows-Server-2003 Infrastrukturen haben die Protokolle zur IP-Adressenverteilung (DHCP) und zur Namenauflösung (DNS und WINS). Hierfür sind geeignete, nach den jeweiligen Einsatzbereichen differenzierte Konzepte für die gesamte Infrastruktur erforderlich. Eine Orientierung zum Erreichen des erforderlichen Sicherheitsniveaus findet sich in den Hilfsmitteln zum IT-Grundschutz (siehe *DHCP/DNS/WINS als Infrastrukturdienste unter Windows Server 2003* in *Hilfsmittel zum Windows Server 2003*).

Protokolle bei speziellen Rollen

Sonstige Protokollgruppen wie IP-Routing-, Multicast- und *Quality-of-Service*-Protokolle (QoS) kommen zum Einsatz, wenn der Server für spezielle Rollen konfiguriert ist. Ansonsten sollten sie deaktiviert sein. Für einen sicheren Betrieb gilt generell:

- Es ist das am besten geeignete Protokoll auszuwählen, alle anderen Protokolle müssen deaktiviert werden.

- Speziell für Protokolle der Anwendungsschicht ist immer für Integrität und verschlüsselte Authentisierung in einer Windows-Server-2003-Umgebung zu sorgen, möglichst mittels NTLMv2 oder Kerberos.
- Bei höherem Schutzbedarf müssen die Nutzdaten verschlüsselt werden.
- Der Einsatz des gewünschten Protokolls sollte in der Richtlinie für den IT-Verbund und die betroffenen IT-Systeme definiert und entsprechende Sicherheitsanforderungen formuliert werden.
- Der Einsatz von IPSec sollte überlegt werden, wenn ein gewünschtes Protokoll unter Windows Server 2003 den Sicherheitsanforderungen nicht entspricht (siehe M 5.90 *Einsatz von IPSec unter Windows 2000/XP*).

Dokumentation

Aktive Netz-Protokolle

Alle aktiven Netz-Protokolle des Servers sind zu erfassen. Wurde der Server mittels einer Vorlage des SCW konfiguriert, ist die Vorlage für eine Mindestdokumentation ausreichend (siehe M 2.366 *Nutzung von Sicherheitsvorlagen unter Windows Server 2003*). Die effektiven Authentisierungs- und Verschlüsselungsmethoden sowie der Einsatzzweck sind für jedes Protokoll zu dokumentieren.

Ergänzende Kontrollfragen:

- Ist der TCP/IP-Stack des Servers ausreichend gegen DoS-Attacken geschützt?
- Sind keine unsicheren Netz-Protokolle konfiguriert?
- Wurden alle nicht benötigten Netz-Protokolle deaktiviert?
- Wurde der Schutzbedarf für die Protokolle DHCP, DNS und WINS differenziert für die jeweiligen Einsatzbereiche eingeschätzt und ein geeignetes Infrastrukturkonzept für diese Protokolle entwickelt und umgesetzt?
- Sind alle optionalen IP-Protokolle ausreichend abgesichert, z. B. durch Authentisierung und kryptographische Verfahren?

M 5.132 Sicherer Einsatz von WebDAV unter Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Vorteil der geschützten Authentisierung von Windows-Benutzerkonten

Mit Hilfe von Web Distributed Authoring and Versioning (WebDAV) ist es möglich, Dateien eines Windows 2000 Servers/Windows Servers 2003 über eine HTTP-fähige Netzverbindung bereitzustellen. WebDAV ist unter Windows Server 2003 vor allem deshalb eine bessere Alternative zu FTP, weil sie eine geschützte Authentisierung von Windows-Benutzerkonten ermöglicht. Auch einige zusätzlich erhältliche Serverapplikationen bieten eine WebDAV-Schnittstelle, z. B. Microsoft Exchange Server und Windows Sharepoint Services. Geeignete WebDAV-Clients sind der Maßnahme M 4.282 *Sichere Konfiguration der IIS-Basis-Komponente unter Windows Server 2003* zu entnehmen. Die Planung des Einsatzes von WebDAV sollte wenigstens folgende Punkte berücksichtigen:

Planung des Einsatzes

1. Auf dem Server werden Internet Information Services (IIS) benötigt.
2. Über WebDAV-Freigaben können am Client zwar Dateien direkt auf dem Server bearbeitet werden (die Dateien werden dann automatisch gesperrt), ausführbare Programme können jedoch nicht direkt vom Server gestartet werden. Generell muss die geplante Client-Software erst auf Verträglichkeit mit WebDAV-Verbindungen hin getestet werden.

   Wie exponiert ist der WebDAV-Zugang (Intranet/Extranet/Internet)? Oder wird er nur sporadisch im LAN verwendet, z. B. für administrative Zwecke? Diese Fragen haben Einfluss auf die Sicherheitsanforderungen an den Authentisierungsprozess (z. B. anonym, Basis-Authentisierung über https, Kerberos usw.) und über die Art der Benutzerverwaltung. Auch die Anforderungen an die Absicherung des Servers an sich sind davon betroffen. Ergebnis der Frage kann sein, dass WebDAV mit anonymem Zugriff im Internet veröffentlicht werden soll und eine hohe Besucherzahl erwartet wird. Dann wäre der gesamte Server mit den Maßnahmen für öffentliche Webserver abzusichern (siehe Baustein B 5.10 *Internet Information Server*). Ein designbedingter Aspekt hierbei ist, dass bei Windows Server 2003 WebDAV auf demselben Server aktiviert werden muss, der die gewünschten Dateien bereithält. Im Hinblick auf Sicherheits-Gateways und DMZ-Szenarien ist keine Trennung zwischen Dateiserver und WebDAV-Server möglich.

   Ein anderes Ergebnis kann sein, dass gelegentlich ein Administrator auf kurzem Wege eine Softwareimage-Datei von einem Helpdesk-Server der Active-Directory-Domäne herunterladen muss. In diesem Fall könnte der Administrator bedarfsweise eine WebDAV-Freigabe erstellen und sich mittels seines Domänen-Benutzerkontos (Kerberos-Authentisierung) die WebDAV-Freigabe auf einen Laufwerksbuchstaben verbinden. Sofern M 4.282 *Sichere Konfiguration der IIS-Basis-Komponente unter Windows Server 2003* bereits umgesetzt worden ist, wäre der weitere Aufwand gering.

3. Sollen die Daten während der Übertragung verschlüsselt werden? Den einfachsten und zugleich einen sicheren Weg für eine Ende-zu-Ende-Verschlüsselung stellt ein sicherer Kanal mittels HTTPS dar, welcher im IIS konfiguriert wird. Nicht alle WebDAV-Clients unterstützen jedoch HTTPS optimal. Alternativ kann auch die Nutzung von VPN oder IPSec in Betracht gezogen werden, wobei der Aufwand verglichen zum Sicherheitsgewinn deutlich höher liegt. In jedem Fall ist ein Verfahren zu wählen, mit dem eine Ende-zu-Ende-Verschlüsselung sichergestellt werden kann.
4. Wenn kein sicherer Kanal (HTTPS) zur Verschlüsselung verwendet werden kann, dann müssen die geplanten WebDAV-Clients wenigstens Digest-Authentisierung oder die integrierte Windows-Authentisierung (NTLMv2 oder Kerberos) unterstützen. Das trifft auch zu, wenn VPN anstelle von HTTPS verwendet wird. Der Authentisierungsvorgang kann sonst nicht ausreichend geschützt werden.
5. Nach einer Standardinstallation von Windows Server 2003 ist der Webclient-Dienst aus Sicherheitsgründen deaktiviert. Es ist zu empfehlen, diese Standardeinstellung zu belassen und am Server darauf zu verzichten. Für den reinen Dateitransfer zu administrativen Zwecken genügt ein HTTP/HTTPS-Browser für den Zugriff auf WebDAV-Freigaben. Für die Authentisierungsmechanismen des HTTP/HTTPS-Browsers und die Verschlüsselung gelten die gleichen Anforderungen wie bei einem WebDAV-Client (die meisten Browser unterstützen die in Punkt 4. genannten Authentisierungsmechanismen).

Verwenden von Laufwerksbuchstaben und Verschlüsselung

HTTPS-Verschlüsselung

Windows XP enthält einen WebDAV-Redirector, der eine WebDAV-Freigabe einem Laufwerksbuchstaben zuordnen kann. Dies kann aus Gründen der Kompatibilität zu älteren Programmen nützlich sein. Jedoch funktioniert diese Zuordnung nicht über HTTPS-Verbindungen. Ist die Verwendung von Laufwerksbuchstaben und HTTPS notwendig, müssen hierfür Programme von Drittanbietern in Betracht gezogen werden. Eine unverschlüsselte Verbindung lediglich über HTTP ist nicht zu empfehlen.

EFS-Verschlüsselung

Alternativ zu HTTPS ist auch mit EFS eine Verschlüsselung der übertragenen Daten möglich. Die Daten werden auf dem Client verschlüsselt und dann in verschlüsselter Form zum Server übertragen, wo sie auch verschlüsselt abgelegt werden. Diese Möglichkeit beschränkt sich auf Windows 2000/XP und auf eine Dateigröße von bis zu 60 Megabyte. Das Verfahren mit EFS ist in normalen IT-Umgebungen nicht zu empfehlen, da hierbei zusätzliche Risiken entstehen (G 4.54 *Verlust des Schutzes durch das verschlüsselnde Dateisystem EFS*) und gegebenenfalls weitere Maßnahmen umzusetzen sind (M 4.278 *Sichere Nutzung von EFS unter Windows Server 2003*) umzusetzen sind.

Ergänzende Kontrollfragen:

- Ist der Webclient auf dem Server deaktiviert?
- Entspricht der WebDAV-Zugang den Authentisierungs- und Verschlüsselungsrichtlinien?
- Sind die Internet Information Services (IIS) auf dem WebDAV-Server der Einsatzumgebung entsprechend sicher konfiguriert?

M 5.133 Auswahl eines VoIP-Signalisierungsprotokolls

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Beim Einsatz von VoIP werden die Steuerinformationen und die eigentlichen Sprachdaten in der Regel getrennt voneinander, mittels unterschiedlicher Übertragungsprotokolle transportiert. Steuerinformationen, wie beispielsweise der Zustand "besetzt", werden über Signalisierungsprotokolle, zum Beispiel H.323 oder SIP (Session Initiation Protocol), übermittelt. Für die Übertragung der Sprachdaten ist hingegen ein Medientransportprotokoll, in der Regel RTP (Real-Time Transport Protocol), zuständig. Nur bei sehr wenigen Protokollen, wie IAX (InterAsterisk eXchange), erfolgt keine Trennung von Steuer- und Medieninformationen.

Es gibt verschiedene Signalisierungsprotokolle. Da diese Protokolle untereinander nicht kompatibel sind, spielt die Auswahl für den Aufbau eines VoIP-Netzes eine wichtige Rolle. VoIP-Komponenten, die kein gemeinsames Protokoll unterstützen, können ohne ein Gateway nicht miteinander kommunizieren. Der Einsatz eines Gateways, das die Anweisungen von einem Protokoll in ein anderes übersetzt, ist sehr aufwendig und umständlich. Daher ist darauf zu achten, dass möglichst nur ein Signalisierungsprotokoll eingesetzt wird.

Die Auswahl der eingesetzten VoIP-Komponenten beeinflusst stark die Auswahl des Signalisierungsprotokolls, da viele VoIP-Komponenten nur ein bestimmtes Signalisierungsprotokoll unterstützen. Bezüglich der Sicherheit spielen die Unterschiede zwischen den Protokollen nur eine geringe Rolle. Es sollte dokumentiert werden, welches Signalisierungsprotokoll ausgewählt wurde.

Im Folgenden werden die verbreiteten Signalisierungsprotokolle H.323 und SIP betrachtet. Neben diesen Protokollen werden auch jeweils alle Arten von VoIP-Komponenten, die für einen Gesprächsaufbau mindestens benötigt werden, vorgestellt.

H.323

Die Protokollgruppe um H.323 beschreibt die Übertragung von Echtzeitinformationen (Video, Audio, Daten) in paketorientierten Transportnetzen. H.323 wurde ursprünglich als Umsetzung des ISDN D-Kanal Protokolls Q.931 auf ein IP-basiertes Netz entwickelt. Innerhalb von dieser Protokollgruppe sind die Protokolle H.225.0, H.245 und H.450 und H.235 definiert. H.323 beschreibt den Rahmen der Signalisierungsprotokolle, H.225.0 die eigentliche Signalisierung, H.245 die Kontrolle der Übertragung der Sprachinformationen und H.450 die eigentliche Telefonie-Funktion. Die optionale Unterstützung von H.235 bietet Schutz der Integrität und Vertraulichkeit der Signalisierung. Vertiefende Informationen sind bei der International Telecommunications Union (ITU) zu finden, von der die Protokolle festgelegt wurden. Audio- und Videodaten werden per UDP, Faxdaten per UDP oder TCP übertragen. Vor der Übertragung dieser Echtzeitdaten werden so genannte logische RTP- und RTCP-Kanäle zwischen den Endpunkten (Terminals) aufgebaut.

An einer H.323-Kommunikation können folgende Komponenten beteiligt sein:

- Terminals stellen die Endpunkte einer H.323-Kommunikation beim Benutzer dar. Diese Endgeräte verfügen in der Regel über einen Lautsprecher und ein Mikrofon und bieten dem Benutzer die Möglichkeit, mit einem anderen Gesprächsteilnehmer eine Verbindung aufzubauen. Eine direkte Verbindung zwischen den Endgeräten ist nur bei bekannter IP-Adresse möglich.
- Gatekeeper werden zur Verwaltung eingesetzt. Da die direkte Verbindungsaufnahme zwischen Terminals nur bei bekannten IP-Adressen möglich ist, agiert ein Gatekeeper als zentrale Steuerkomponente in H.323-Netzen.
- Die Multipoint Control Unit (MCU) ermöglicht Konferenzen, also Gespräche zwischen mehr als zwei Anwendern. In der optionalen MCU laufen sämtliche Medienströme von den Teilnehmern zusammen.
- Gateways realisieren die Übergänge in andere Netze und nehmen dabei die Anpassung der Nutzdaten und der Signalisierungsinformation vor. Beispielsweise vermitteln Gateways zwischen IP- und leitungsvermittelnden Telefonnetzen.

Der größte Nachteil von H.323 ist die Komplexität des Protokolls. Die Vielzahl der verschiedenen Protokolle lässt H.323 sehr unübersichtlich und aufwendig wirken. Diese Komplexität erschwert die Fehlersuche und kann zu Mehrkosten führen. Erschwerend kommt hinzu, dass das im Folgenden vorstellte SIP von vielen Herstellern bei neueren Produkten priorisiert wird.

Session Initiation Protocol (SIP)

SIP ist ein textbasierendes Client-Server-Sitzungssignalisierungsprotokoll der IETF (Internet Engineering Task Force), das zur Steuerung des Verbindungsauf- und -abbaus von Multimediadiensten verwendet und in RFC 3261 beschrieben wird. Weitere Funktionalitäten, wie Videokonferenzen, Instant Messaging, verteilte Computerspiele und anderen Applikationen benötigen eine Erweiterung der SIP-Spezifikation. Diese sind in separaten RFCs zu finden. Der Multimedia-Nachrichtenstrom, wie die Sprachinformationen bei einem Telefonat, wird mit RTP gebildet. Die Signalisierung wird in der Praxis oft mit SSL bzw. TLS (Transport Layer Security) oder IPSec geschützt.

Das Adressierungsschema von SIP ähnelt stark dem einer E-Mail-Adresse (sip:benutzername@provider-name.org). Die Lokalisierung erfolg über DNS (Domain Name System). SIP unterstützt Punkt-zu-Punkt- und Punkt-zu-Mehrpunkt-IP-Verbindungen. Durch das einfache Klartextdesign der SIP-Pakete und der geringen Komplexität erfährt SIP eine immer größere Verbreitung.

Folgende VoIP-Komponenten können bei einer Kommunikation über SIP beteiligt sein:

- Die Endgeräte (Telefon, Softphone, Gateway) werden als User Agents (UA) bezeichnet. Ein User Agent kann die Rolle eines Clients bzw. eines Servers einnehmen. Der Initiator eines Gesprächs arbeitet als User Agent

Server (UAS), der Gerufene als User Agent Client (UAC). Ein SIP-Endsystem beinhaltet immer beide Funktionen.

- Der Location Server liefert bei einer entsprechende Nachfrage die IP-Adresse des gewünschten Gesprächspartners. Dieser kann über den Benutzernamen identifiziert werden.
- Ein Registrar ermöglicht den Benutzern die Anmeldung und Registrierung. Hierfür meldet sich das Endgerät mit einer Kennung (Benutzername, Kennwort) und seiner SIP-Adresse an den Registrar an. Der Registrar gibt die Adresse (IP-Adresse) des Endgeräts dem Location Server bekannt, unter der er öffentlich erreichbar ist. Aufgrund dieser Registrierung kann das Endgerät lokalisiert werden.
- Ein SIP-Proxy nimmt die Rolle eines Vermittlers ein, der die Signalisierungsnachrichten bearbeitet oder weiterleitet. Ein User Agent sendet eine Anfrage an den SIP-Proxy. Der SIP-Proxy interpretiert die Anfrage und adressiert sie, nach entsprechender Bearbeitung, an den User Agent. Wenn nötig, wird eine Nachricht durch den SIP-Proxy verändert.

Obwohl SIP standardisiert wurde, wird es oft von den Herstellern von VoIP-Komponenten unterschiedlich interpretiert. Diese fehlende Interoperabilität führt dazu, dass nicht alle VoIP-Funktionen bei VoIP-Netzen, an denen Komponenten von verschiedenen Herstellern beteiligt sind, vollständig zur Verfügung stehen. Hiervon ist meist die Authentisierung zwischen den Systemen, die Verschlüsselung und die Bereitstellung von Mehrwertdiensten betroffen. Bei der Beschaffung von VoIP-Komponenten sollte daher deren Interoperabilität mit vorhandenen Komponenten überprüft werden.

Beim Einsatz von SIP in Firewall- bzw. NAT-Umgebungen sind weiterhin einige Besonderheiten zu beachten. Endgeräte, die sich in NAT-Umgebungen befinden, können beispielsweise nur mit hohen Aufwand mit VoIP-Systemen außerhalb der NAT-Umgebung kommunizieren. Weitere Informationen hierzu sind in der Maßnahme M 5.137 *Einsatz von NAT für VoIP* zu finden.

Ergänzende Kontrollfragen:

- Ist dokumentiert, welches Signalisierungsprotokoll von den vorhandenen VoIP-Komponenten unterstützt wird?
- Wird bei der Beschaffung darauf geachtet, dass die neuen Komponenten das eingesetzte Signalisierungsprotokoll unterstützen?

M 5.134 Sichere Signalisierung bei VoIP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Weitaus wichtiger als der Schutz der Medienströme ist die Sicherstellung der Integrität und Vertraulichkeit der Signalisierungsinformationen beim Einsatz von VoIP. Eine Möglichkeit hierfür ist der Transport der Signalisierungsinformationen über verschlüsselte VPN-Kanäle. Eine weitere Möglichkeit besteht im Einsatz von Signalisierungsprotokollen, die eigene Schutzmechanismen bereitstellen. Die beiden wichtigsten Protokolle zur VoIP-Signalisierung sind SIP und H.225 (Setup-Signalisierung) sowie H.245 (Aufbau der logischen Kanäle) innerhalb des H.323 Frameworks. Die Sicherheitsmechanismen dieser Signalisierungsprotokolle werden im Folgenden beschrieben.

Neben diesen Protokollen gibt es weitere Signalisierungsprotokolle wie IAX2, das über keine eigenen Sicherheitsmechanismen verfügt. Darüber hinaus existieren spezielle Signalisierungsprotokolle, wie beispielsweise MGCP, zur Steuerung von Media Gateways, die ebenfalls keine eigenen Sicherheitsmechanismen bieten. Die Absicherung dieser Protokolle muss daher im Allgemeinen durch geeignete Sicherheitsmaßnahmen auf der Vermittlungsschicht erfolgen.

H.235

Grundsätzlich kann die Signalisierung über das Framework H.323 durch Sicherheitsmechanismen auf der Transport- oder Vermittlungsschicht (beispielsweise SSL bzw. TLS oder IPSEC) geschützt werden. Diese vom Signalisierungsprotokoll unabhängigen Mechanismen können für Umgebungen mit erhöhten Sicherheitsanforderungen eingesetzt werden. Im Weiterem kann zusätzlich, auch als einziger Schutz der Signalisierung bei normalem Schutzbedarf, das Protokoll H.235 zum Schutz der Integrität und Vertraulichkeit genutzt werden. Es muss entschieden werden, ob und wie die Signalisierung mit H.323 geschützt werden soll. Die Entscheidung ist zu dokumentieren.

H.235 definiert umfangreiche Sicherheitsmechanismen zum Schutz von H.323-basierter Telefonie. Die spezifizierten Mechanismen umfassen insbesondere den Schutz der Anrufsignalisierung (H.225/Q.931) und des Steuerungskanals (H.245) sowie die Sicherheit des Medienstroms.

H.235 betrachtet alle Systemkomponenten, die Endpunkte eines verschlüsselten H.245 Kontrollkanals oder eines verschlüsselten logischen Kanals sind, als vertrauenswürdige Komponenten, die entsprechend authentisiert werden müssen. Beispiele für vertrauenswürdige und zu authentisierende Systemkomponenten sind Gateways.

Eine der folgenden Arten der Authentisierung sollte ausgewählt werden:

a) Authentisierung mittels symmetrischer Kryptographie und eines gemeinsamen, zuvor ausgetauschten Geheimnisses (beispielsweise eines Passwortes). Als kryptographische Verfahren können entweder symmetrische Verschlüsselungsverfahren oder Keyed-Hash-Funktionen dienen, wobei das gemeinsame Geheimnis jeweils als symmetrischer kryptographischer Schlüssel verwendet oder kryptographisch sicher daraus abgeleitet wird.

b) Authentisierung basierend auf zertifizierten öffentlichen Schlüsseln und signierten Nachrichten.

Jedes dieser Verfahren kann jeweils mit zwei Nachrichten unter Verwendung von Zeitstempeln oder mit drei Nachrichten mit zufälligen Challenges als Challenge-Response-Protokoll implementiert werden.

c) Diffie-Hellman-Schlüsselvereinbarungsprotokoll mit optionaler Authentisierung: In einer ersten Phase führen beide Kommunikationsparteien ein Diffie-Hellman-Schlüsselvereinbarungsprotokoll basierend auf zertifizierten öffentlichen Schlüsseln durch. Der dabei erzeugte gemeinsame symmetrische Schlüssel wird in der optionalen zweiten Authentisierungsphase zur eigentlichen Authentisierung, basierend auf symmetrischer Verschlüsselung, verwendet.

H.235 spezifiziert im Weiterem einen Mechanismus (Media Anti-Spam), über den ein Empfänger von RTP-Paketen effizient überprüfen kann, ob ein RTP-Paket authentisch ist und von einem autorisierten Sender stammt. Dazu wird ein kurzer MAC (Message Authentication Code) über ausgewählte Felder des RTP-Paketes berechnet, den der Empfänger prüft, bevor er mit der eigentlichen Verarbeitung des RTP-Paketes beginnt. Der MAC kann entweder durch einen Verschlüsselungsalgorithmus oder durch eine Keyed-Hash-Funktion berechnet werden. Dieser Mechanismus ist zur Abwehr von DoS-Angriffen durch RTP-Flooding und SPIT auf bekannt gewordenen RTP-Ports gedacht und sollte, wenn möglich, aktiviert werden.

Wird die Kommunikation über H.235 von den VoIP-Gateways nicht unterstützt, so ist dringend zu empfehlen, den Zugriff auf das Gateway auf Basis von IP-Adressen und H.323-Identitäten so weit wie möglich einzuschränken. Dafür empfiehlt sich der Einsatz eines Gatekeepers und die Einschränkung des Zugriffs auf das VoIP-Gateway nur im "Routed Mode". Im Gegensatz zum "Bridged Mode", bei dem der Gatekeeper nur an der Authentisierung und die Registrierung beteiligt ist, findet beim "Routed Mode" die gesamte Signalisierung über den Gatekeeper statt.

SIP

Ein grundlegendes Problem in der Absicherung von Signalisierungsprotokollen, wie beispielsweise SIP, besteht darin, dass bei der Signalisierung häufig mehrere Komponenten (Endgeräte und Server) involviert sind, die jeweils Teile der Signalisierungsnachrichten lesen oder sogar verändern müssen. Aus diesem Grund ist eine einfache Anwendung von Ende-zu-Ende Sicherheitsmechanismen nicht möglich, anwendungsspezifische Anpassungen müssen vorgenommen werden.

Der SIP-Standard befürwortet deshalb die Verwendung von Sicherheitsmechanismen auf Schichten unterhalb der Anwendungsschicht. Dabei wird nur jeweils die Kommunikation zwischen den einzelnen SIP-Komponenten (UA, Proxy-, Registrar-, Redirect- und Location-Server) abgesichert, was häufig als "Hop-by-Hop"-Sicherheit bezeichnet wird.

Als weiteres Argument für "Hop-by-Hop"-Sicherheitsmechanismen wird im Standard SIP 2.0 darauf hingewiesen, dass den Servern ohnehin in gewissem Umfang vertraut werden muss. Hier sollte jedoch deutlich zwischen Vertrauen

bezüglich Signalisierung und Vertrauen bezüglich des Medientransports, d. h. der Sprachdaten, unterschieden werden. Bei erhöhten Sicherheitsanforderungen sollte deshalb geprüft werden, ob zusätzlich geeignete Ende-zu-Ende-Sicherheitsmechanismen zum Schutz des Medientransports erforderlich sind. Dies betrifft beispielsweise auch den Schlüsselaustausch für SRTP.

Besonders bei erhöhten Sicherheitsanforderungen sollte die Signalisierung mit SIP mit SSL bzw. TLS (Transport Layer Security) geschützt werden. Die SIP-Spezifikation RFC 3261 schreibt vor, dass alle konformen SIP-Server (Proxy-Server, Redirect-Server, Location-Server und Registrar-Server) das TLS-Protokoll mit gegenseitiger Authentisierung sowie Einweg-Authentisierung unterstützen müssen. Die Endgeräte sollten TLS verwenden, um ihre Kommunikation mit Proxy-, Redirect- sowie Registrar-Servern zu schützen.

Ergänzende Kontrollfragen:

- Werden die Signalisierungsinformationen verschlüsselt übertragen?

M 5.135 Sicherer Medientransport mit SRTP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Das Real-Time Transport Protocol (RTP) wird zur Übertragung von Mediendaten der IP-Telefonie und das Real-Time Streaming Protocol (RTSP) zu deren Kontrolle eingesetzt. Beide Protokolle bieten keine eigenen Schutzmechanismen gegen das Abhören und gegen Manipulationen von IP-Telefonaten an. Erweiterungen von RTP/RTCP sind SRTP/SRTCP, die Schutzmechanismen für die Übertragung zur Verfügung stellen. Beim Einsatz von VoIP sollte überlegt werden, die Nutzdaten durch den Einsatz von SRTP/SRTCP zu schützen. Die Entscheidung ist zu dokumentieren.

Überblick

SRTP kann in VoIP eingesetzt werden, um Vertraulichkeit, Authentizität und Schutz gegen Replay-Angriffe (Wiedereinspielen von Nachrichten) für die Medienübertragung auf Basis von RTP zu erreichen. Es ermöglicht eine sichere Unicast- und Broadcast-Übertragung. Zum Transport werden die RTP/RTCP-Pakete in SRTP/SRTCP-Pakete eingebettet.

Schlüsselmanagement

Das Protokoll SRTP definiert einen Masterschlüssel und jeweils einen Sitzungsschlüssel für Verschlüsselung und Authentisierung. SRTP enthält keinen eigenen Mechanismus zur Erzeugung und Verwaltung der mindestens 128 Bit langen Masterschlüssel. Dies muss mit anderen Standards, wie z. B. Multimedia Internet Keying (MIKEY) realisiert werden.

Falls SRTP eingesetzt wird, ist festzulegen, in welchen zeitlichen Abständen der Masterschlüssel einerseits und die Sitzungsschlüssel andererseits gewechselt werden.

Verschlüsselung

Bei der Verwendung von SRTP im Rahmen von VoIP sollte in der Regel das symmetrische Verschlüsselungsverfahren AES-CTR (Advanced Encryption Standard - Counter Mode) aktiviert werden. Es eignet sich sowohl für Ende-zu-Ende- als auch für abschnittsweise ("Hop-by-Hop") Verschlüsselung.

Authentizität und Integrität

Authentizität und Integrität von RTP-Nachrichten können in SRTP mittels der Funktion HMAC-SHA1 in Kombination mit einem entsprechenden Sitzungsschlüssel gesichert werden. Dabei beträgt die empfohlene Länge der übertragenen Prüfsumme 80 Bit. Demnach muss die 160 Bit lange Prüfsumme aus HMAC-SHA1 auf 80 Bit reduziert werden. Diese Anpassung verringert zwar die Übertragungsgröße von SRTP-Paketen, schwächt aber den Integritätsschutz der Nachrichten. Daher sollte diese Anpassung nur in Ausnahmefällen aktiviert werden. Alternativ können auch Funktionen verwendet werden, die auf anderen anerkannten Hash-Algorithmen basieren. Für die Auswahl ist zu beachten, dass für die verbreitesten Hash-Algorithmen SHA-1 und MD5 kryptographische Schwächen entdeckt wurden, die zu einer Verringerung der

Komplexität führen (siehe auch M 2.164 *Auswahl eines geeigneten kryptographischen Verfahrens*). Die Auswahl der Hash-Funktion ist zu begründen und dokumentieren.

Der gleiche Sicherheitsmechanismus ist auch für SRTCP vorgesehen.

SRTP erlaubt eine schwächere Authentisierung (z. B. 32 Bit) beziehungsweise gar keine Authentisierung von Nachrichten für solche Anwendungen, bei denen es unwahrscheinlich ist, dass der Angreifer eine verschlüsselte Nachricht so manipulieren kann, dass eine spätere Entschlüsselung eine sinnvolle Nachricht liefern wird. Wenn möglich, sollte die schwächere Authentisierung für RTP-Pakete nicht verwendet werden. Für RTCP sollte bei erhöhten Sicherheitsanforderungen der oben beschriebene Schutz mittels HMAC-SHA1-Prüfsumme aktiviert werden.

Schutz gegen Replay-Angriffe (Wiedereinspielen von Nachrichten)

SRTP bietet Schutz gegen Replay-Angriffe, bei denen ein Angreifer abgefangene RTP- oder RTCP-Pakete speichert und diese später erneut verschickt, um unter anderem Denial of Service Angriffe durchzuführen. Um das Wiedereinspielen von Nachrichten verhindern zu können, muss ein Integritätsschutz und Nachrichten-Authentisierung vorhanden sein. Der Empfänger von SRTP-Paketen führt dann eine so genannte Replay-Liste, die Kennzahlen von vorher empfangenen authentischen Paketen enthält.

Die maximal mögliche Anzahl der gespeicherten Kennzahlen muss vorher festgelegt werden. Beim Empfang eines neuen Pakets wird diese Liste auf Übereinstimmungen untersucht, und die wiederholten Pakete werden verworfen. Bei IP-Telefonen, die einen geringeren Speicher besitzen, ist die Länge der Replay-Liste ein Sicherheitsparameter, der im Fall von erhöhten Sicherheitsanforderungen berücksichtigt werden sollte. Der Umfang der Replay-Liste ist größtmöglich auszuwählen und die Entscheidung ist zu dokumentieren.

Schlüsselmanagement mit MIKEY

MIKEY (Multimedia Internet KEYing) beschreibt das Schlüsselmanagement für die Echtzeit-Multimedia-Kommunikation und ermöglicht den Austausch von Schlüsseln sowie weiteren Sicherheitsparametern zwischen den Teilnehmern. In VoIP kann MIKEY für den Austausch des Masterschlüssels und weiterer Sicherheitsparameter benutzt werden, um eine sichere SRTP-Übertragung zwischen den Endgeräten zu ermöglichen.

MIKEY ist unabhängig vom darunterliegenden Signalisierungsprotokoll, wie H.323 oder SIP. Zudem unterstützt MIKEY einen parallelen Austausch von Schlüsseln und Sicherheitsparametern für unterschiedliche Kommunikationssitzungen und Kommunikationsprotokolle. Demnach ist es möglich, RTP- und RTCP-Verbindungen getrennt voneinander abzusichern. Mit dem Bündelungskonzept von Kommunikationssitzungen erlaubt es MIKEY, einen gemeinsamen Masterschlüssel für mehrere parallele Sitzungen zu benutzen. Somit können z. B. VoIP-Konferenzen effizienter abgesichert werden.

Falls der Einsatz von VoIP mit Hilfe kryptographischer Mechanismen abgesichert werden soll, müssen die von den VoIP-Systemen unterstützten Verfahren für den Schlüsselaustausch in Erfahrung gebracht werden. Von diesen

Verfahren ist ein geeignetes Verfahren festzulegen und die getroffene Wahl ist zu dokumentieren.

Ergänzende Kontrollfragen:

- In welchen zeitlichen Abständen werden die Schlüssel beim Einsatz von SRTP gewechselt?
- Welche Hash-Algorithmen werden eingesetzt und welche Länge hat die Prüfsumme?
- Wie werden die Schlüssel zwischen den Gesprächspartnern ausgetauscht?

M 5.136 Dienstgüte und Netzmanagement bei VoIP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Das Netzmanagement bildet ein wichtiges Glied in der Kette der Sicherung eines VoIP-Dienstes. Neben dem Schutz vor Angriffen dient das Netzmanagement im Wesentlichen der Verfügbarkeit und der Güte des Dienstes. Risiken, wie beispielsweise ein Ausfall durch Überlastung, können damit verringert werden.

DiffServ und Class-of-Service nach IEEE 802.1p

Ein wichtiger Ansatz für die Sicherstellung der Dienstgüte in IP-Netzen sind die so genannten Differentiated Services (DiffServ). Beim DiffServ-Ansatz werden einzelne Datenströme nach ihren Anforderungen an die Dienstgüte klassifiziert. Die technische Umsetzung erfolgt über das Feld TOS (Type Of Service) im IP-Header der Datenpakete. Einzelnen Klassen werden bestimmte Werte des TOS-Feldes im IP-Header zugeordnet. Entsprechend dem Wert des TOS-Feldes wird das Datenpaket in den Netzknoten priorisiert behandelt.

Damit die benötigte Dienstgüte in der Sicherungsschicht gewährleistet werden kann, wird die Markierung gemäß DiffServ auf das Feld Class of Service (CoS) im Ethernet-Rahmen abgebildet. Die Verwendung der CoS-Bits ist im IEEE-Standard 802.1p festgelegt. Diese zusätzliche Markierung im Ethernet-Rahmen soll die Weiterleitung der Pakete in Layer-2-Geräten, wie Switches, die den IP-Header (Layer 3) nicht auswerten, beeinflussen.

Beim Einsatz von DiffServ muss sichergestellt werden, dass die Datenpakete mit genau der DiffServ-Klasse markiert werden, die für die jeweilige Kommunikationsart vorgesehen ist. Hierzu gehört auch, dass überprüft wird, ob eine Kommunikationsart zur Reservierung von bevorzugten Ressourcen berechtigt ist und ob die tatsächliche Kennzeichnung der Datenpakete mit der jeweils vorgesehenen Klasse übereinstimmt (Policing).

Unterstützen die VoIP-Netze das Modell der Differentiated Services, so muss dies lückenlos implementiert werden. Fehlt beispielsweise das Policing im DiffServ-Netz, können Anwendungen ihre Datenpakete mit unzulässig hoher Priorität markieren, wodurch eventuell die Sprachströme massive Paketverluste erfahren und Sprachverbindungen nicht mehr möglich sind.

VoIP-Dienste sind in einem DiffServ-Netz aber nicht nur durch mutwillige Eingriffe gefährdet. Eine falsche Dimensionierung der Netzkomponenten kann zur punktuellen Überlastung von Verbindungen oder Netzressourcen (Prozessoren der Router, Firewalls) führen und damit ebenfalls den Dienst zum Erliegen bringen.

Overprovisioning

Häufig werden beim Einsatz von IP-Telefonie die Markierungen der Datenströme nicht berücksichtigt. Es wird davon ausgegangen, dass moderne lokale Netze sowie WANs ausreichend überdimensioniert sind, um Stauungen in Warteschlangen zu vermeiden. Dieser Ansatz wird als Overprovisioning bezeichnet. Im Fall von Overprovisioning ist ein permanentes Monitoring potentieller Engpässe im Netz notwendig. Dabei bildet nicht zwangsläufig die

Datenrate einer Strecke den Flaschenhals einer Verbindung. Es kann genauso die CPU-Performance eines Routers, die Backplane eines Switches oder die Durchsatzrate einer Firewall sein. Entscheidend ist deshalb ein lückenloses Monitoring der CPU-Last und der Auslastung einzelner Verbindungen in den Netzen sowie periodische Analysen, beispielsweise mit Hilfe von aktiven Messungen der Einweg-Verzögerungen.

Bei der Verwendung des Overprovisioning muss beachtet werden, dass keine festen Garantien der Qualität von Sprachanwendungen gegeben werden können. Vielmehr bauen die Aussagen und Abschätzungen auf Erfahrungswerte aus der Vergangenheit. Das Verhalten der Netze kann sich durch die Einführung neuer Anwendungen, wie beispielsweise Videokonferenzen oder Grid-Computing, gänzlich ändern. Speziell beim Einsatz von Overprovisioning können VoIP-Anwendungen durch das Auftreten großer Datenströme stark beeinträchtigt werden.

MPLS

MPLS (MultiProtocol Label Switching) kann in Weitverkehrsnetzen verwendet werden, um Kanäle mit garantierter Bandbreite für Sprachverbindungen vom restlichen Verkehr zu isolieren. Damit kann das Prinzip des Overprovisioning auf einzelne MPLS-Kanäle angewendet werden. Da VoIP-Verkehr weniger Schwankungen der Datenrate als sonstiger IP-Verkehr hat, ist davon auszugehen, dass VoIP-Kanäle stärker gefüllt werden können als Strecken, auf denen VoIP-Verkehr zusammen mit dem restlichen Datenverkehr übertragen wird.

Es ist zu beachten, dass MPLS hauptsächlich Vorteile hinsichtlich der Dienstgüte, jedoch nur einen geringen Schutz von Vertraulichkeit und Integrität der Datenübertragung bieten kann. Die Datenpakete der MPLS-Kanäle werden, ähnlich einem VLAN-Tagging, mit einem zusätzlichen Header versehen und unverschlüsselt mit dem restlichen Verkehr übertragen. Somit können solche Kanäle, ähnlich wie Ethernet-Verkehr, mit einem geeigneten Sniffer an bestimmten Komponenten des Netzes eventuell abgehört und manipuliert werden.

Traffic Shaping

Traffic Shaping wird in Gateways zwischen lokalen und Weitverkehrsnetzen eingesetzt, um die Datenrate bestimmter, in der Regel nachrangiger, Verkehrsarten zu drosseln. Beispiele hierfür sind Datenübertragungen, wie FTP-Verbindungen, bei denen zeitliche Verzögerungen toleriert werden können. Die Erfahrung zeigt jedoch, dass diese Maßnahmen relativ leicht umgangen werden können, wenn beim Traffic Shaping ausschließlich die Portnummern der Datenpakete als Kriterium herangezogen werden.

Resource Reservation Protocol (RSVP)

Das Resource Reservation Protocol (RSVP) dient einer Ende-zu-Ende-Signalisierung der Dienstgüte für einzelne Datenströme. Ursprünglich wurde RSVP für die Realisierung von so genannten Integrated Services (IntServ) in IP-Netzen konzipiert, das im Gegensatz zu DiffServ eine durchgängige Dienstgüte garantieren kann. Für den Einsatz von RSVP in der ursprünglichen Form müssen alle Vermittlungsknoten, Betriebssysteme sowie Anwendungen

das Protokoll beherrschen. Zurzeit ist sowohl die Unterstützung in den Betriebssystemen als auch in den Anwendungen unzureichend oder gar nicht gegeben. Somit kommen RSVP und IntServ für VoIP derzeit nicht in Betracht.

Ergänzende Kotrollfragen:

- Welche Maßnahmen werden ergriffen, um eine Überlastung zu verhindern?

M 5.137 Einsatz von NAT für VoIP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

NAT (Network Address Translation) ermöglicht das Übersetzen von privaten/internen IP-Adressen in öffentliche/externe IP-Adressen. Bei dieser Adressumwandlung werden durch ein entsprechendes NAT-Gateway private Quell-IP-Adressen und die dazugehörigen privaten Quell-Ports in öffentliche Quell-IP-Adressen mit öffentlichen Quell-Ports übersetzt. Damit das NAT-Gateway Rückpakete bzw. eingehende Pakete, die an die öffentliche IP-Adresse gerichtet sind, an den richtigen internen Host weiterleiten kann, unterhält es eine entsprechende Zuordnungstabelle zwischen öffentlichen IP-Adressen/Ports und privaten IP-Adressen/Ports.

Durch NAT werden im UDP- bzw. TCP-Header des Medienstroms die Quell-IP-Adresse und die Quell-Portnummer modifiziert. Die Angaben über die Quell-IP-Adresse und den Quell-Port im Nachrichtenteil der Signalisierungsnachricht bleiben dagegen unverändert. Als Folge können keine Medienströme an ein VoIP-Telefon, das sich hinter einem NAT-Gateway befindet, gesendet werden. VoIP-Geräte, die sich im Internet befinden, können keinen Medienstrom zu einem VoIP-Telefon senden, das sich hinter einem NAT-Gateway befindet, da die private IP-Adresse nicht ins Internet geroutet wird.

In den folgenden Abschnitten werden Möglichkeiten aufgezeigt, die einen VoIP-Betrieb in einer NAT-Umgebung ermöglichen.

MIDCOM

MIDCOM steht für Middlebox Commmunications und ist ein Entwurf der IETF, der eine Lösung für die NAT- und Firewall-Problematik im Zusammenhang mit VoIP bietet. Ein MIDCOM-System besteht aus einer Middlebox und einem Server, der die Middlebox steuert bzw. konfiguriert. Der Steuerungsserver ist ein VoIP-Server (H.323-Gatekeeper, SIP-Proxy, etc.), der sich im Signalisierungspfad befindet und den Austausch der SDP-Daten (Session Description Protocol) verfolgt. Anhand dieser Daten steuert der Server über das MIDCOM-Protokoll die Middlebox (NAT-Gateway, Firewall), die die Zuordnungen in die NAT-Tabelle einträgt und die entsprechenden Ports öffnet. In der folgenden Abbildung ist die MIDCOM-Architektur skizziert.

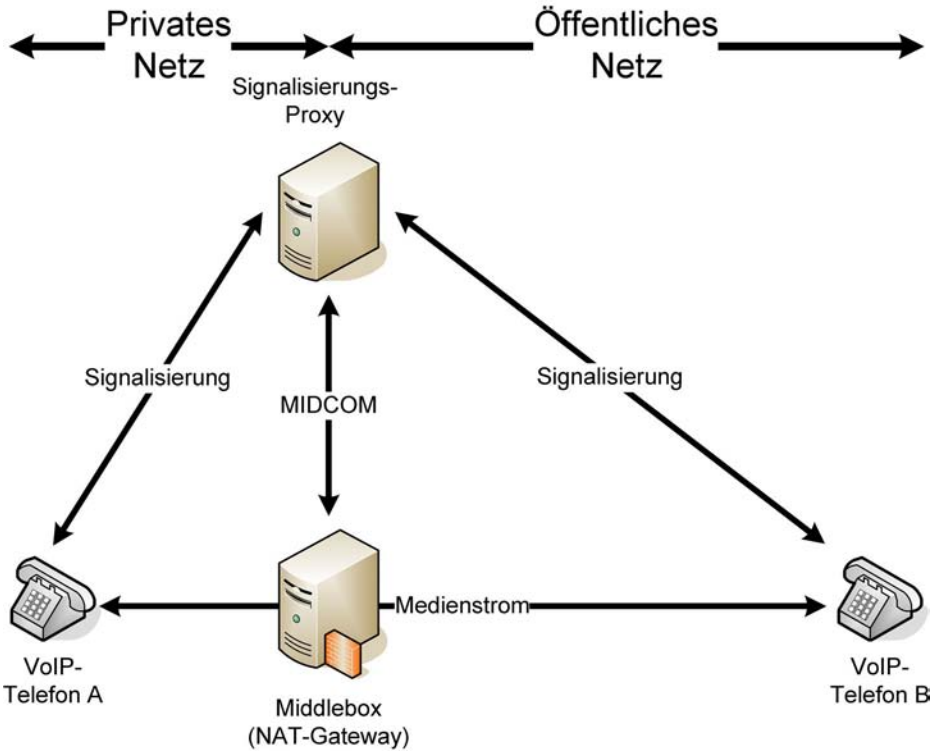


Abbildung: Darstellung der MIDCOM-Architektur

Da der Steuerungsserver selbst mit dem Internet kommunizieren muss, ist dieser Server ebenfalls durch eine Firewall zu schützen. Ein erfolgreicher Angriff auf den Steuerungsserver ermöglicht unter Umständen weitere Angriffe, insbesondere auf die von ihm kontrollierte Middlebox (NAT-Gateway, Firewall). Dies kann weitere erhebliche Gefährdungen nach sich ziehen.

Session Border Controller

Da sich MIDCOM noch im Entwurfsstadium befindet, haben Hersteller begonnen, proprietäre Lösungen auf den Markt zu bringen, die die NAT- und Firewall-Problematik lösen. Diese Session Border Controller bieten häufig Zusatzfunktionen, wie beispielsweise die Überwachung von Service Level Agreements (SLA), Rufannahmesteuerung (Call Admission Control) und Gebührenermittlung (Billing). Die Systeme werden als Appliances oder Server angeboten. Die folgende Abbildung zeigt ein Beispiel des Einsatzes eines Session Border Controllers, der aus einem Signalisierungs- und einem RTP-Proxy besteht.

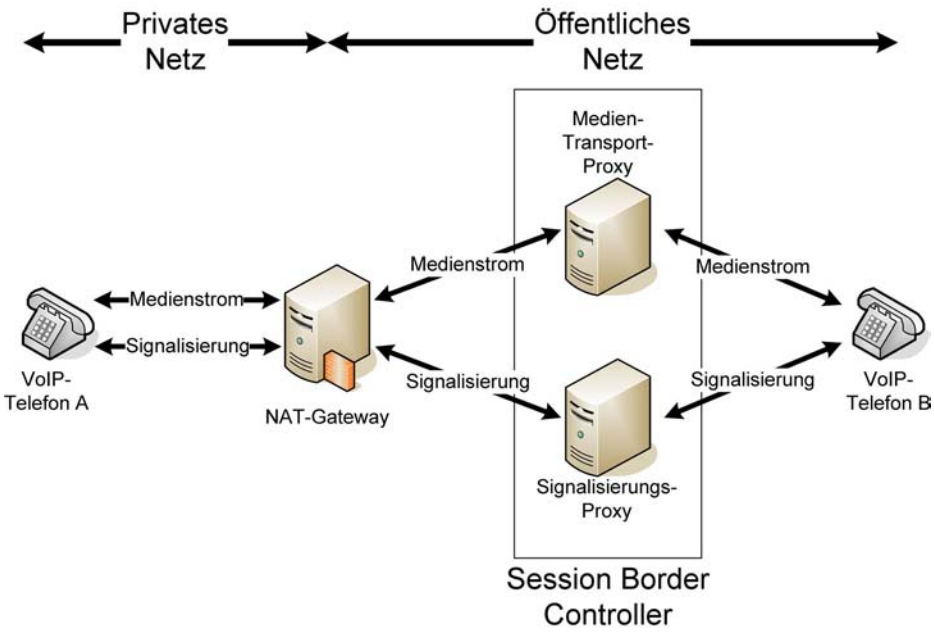


Abbildung: Beispiel für den Einsatz eines Session Border Controllers

Sämtlicher Verkehr (Signalisierung und Medienstrom) läuft in diesem Beispiel über den Session Border Controller. Dem VoIP-Telefon B ist die tatsächliche IP-Adresse des VoIP-Telefons A nicht bekannt.

UPnP

UPnP (Universal Plug and Play) ist ein Industriestandard, der vor allem im Heimbereich immer größere Verbreitung findet. Mit der UPnP-Architektur soll die Vernetzung von PCs und Endgeräten (beispielsweise Drucker, Scanner, WLAN Access Points) vereinfacht werden. Durch UPnP können Applikationen die öffentliche IP-Adresse des NAT-Gateways lernen, die zu verwendenden NAT-Zuordnungen vorgeben und nach der Beendigung einer Sitzung wieder entfernen. Es kann auch eine so genannte Lease Time vorgegeben werden, die die Dauer der Gültigkeit einer NAT-Zuordnung festlegt. Werden mehrere NAT-Gateways hintereinander geschaltet, kann mit UPnP kein NAT-Durchgang erzielt werden.

STUN

Mit Hilfe von STUN (Simple Traversal of User Datagram Protocol (UDP) Through NATs) wird Endsystemen, die sich hinter einem NAT-Gateway befinden, ermöglicht, ihre öffentliche IP-Adresse zu ermitteln und die NAT-Zuordnung des Gateways zu lernen. Symmetric NAT wird von STUN jedoch nicht unterstützt. Die NAT-Zuordnungen werden bei VoIP im Signalisierungsprotokoll übertragen, so dass eingehende RTP-Ströme an die entsprechende NAT-Zuordnung adressiert werden, um so das VoIP-Telefon zu erreichen, das sich hinter dem NAT-Gateway befindet. Die STUN-Technologie wird bereits von vielen VoIP-Telefonen unterstützt und von den meisten VoIP-Providern angeboten.

TURN

TURN (Traversal Using Relay NAT) erlaubt Systemen hinter einem NAT-Gateway bzw. einer Firewall, eingehende TCP- und UDP-Verbindungen zu empfangen. Gleichzeitig wird verhindert, dass diese Möglichkeit für den Betrieb von öffentlich erreichbaren Servern, wie Webserver oder E-Mail-Server, genutzt werden kann, indem je Kombination aus IP-Adresse und Port nur eine Sitzung zu einem Peer erlaubt wird. Im Gegensatz zu STUN können mit TURN auch Systeme hinter symmetrischen NAT-Gateways eingehende Verbindungen empfangen. TURN ist ein einfaches Client/Server-Protokoll, wobei die Authentisierung auf der Basis von Passwörtern erfolgt.

ICE

Da bei TURN sämtliche Medienströme über den TURN-Server geführt werden, ist es sinnvoll, einen TURN-Server nur dann einzusetzen, wenn mit STUN der Empfang eingehender Verbindungen nicht möglich ist. ICE (Interactive Connectivity Establishment) stellt eine Methode für SIP dar, um einen NAT-Durchgang auf Grundlage mehrerer über SDP bekannt gegebener Adressen zu ermöglichen, wobei auf die Protokolle STUN, TURN, RSIP und MIDCOM zurückgegriffen wird. Es wird davon ausgegangen, dass einem Client mehrere Adressen (beispielsweise von STUN oder TURN gelernte Adressen) zur Verfügung stehen, über die er Medienströme empfangen kann. Da die Endsysteme nicht wissen, welche Adresse funktioniert, werden die Adressen nacheinander nach ihrer Priorität geprüft, wobei die Adresse mit der höchsten Priorität als erstes getestet wird. Die Prioritäten werden anhand der geringsten Kosten und dem Maximum an QoS (Quality of Service) festgelegt und dann nacheinander innerhalb des SDP aufgeführt. ICE ist für SIP konzipiert, funktioniert jedoch auch mit RTSP und H.323 und ermöglicht, dass ein Endgerät unabhängig von der NAT-Umgebung betrieben werden kann.

Wird das LAN über einen NAT-Gateway an das Internet angeschlossen, ist zu empfehlen, eine der vorgestellten Mechanismen auszuwählen. Die Entscheidung ist zu dokumentieren.

M 5.138 Einsatz von RADIUS-Servern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

In großen Netzen sollten möglichst Authentisierungsserver eingesetzt werden, wie z. B. RADIUS-Server. RADIUS (Remote Authentication Dial-In User Service) ist ein Client-Server-Protokoll, das zur Authentisierung, Autorisierung und zum Accounting (AAA-System) von Benutzern für die zentralen Absicherung von Verbindungen dient. Das Protokoll ist in mehreren RFCs beschrieben, der wesentliche ist RFC 2865.

Ein Authentisierungsserver soll gewährleisten, dass ausschließlich berechtigte Nutzer auf das interne Netz zugreifen können, der Zugriff kann zusätzlich auf bestimmte Endgeräten eingeschränkt werden. Hierbei findet zunächst eine Identifikation, z. B. anhand einer Kennung, und anschließend die Authentikation, z. B. über ein Passwort, statt. Die Übertragung dieser Daten sollte verschlüsselt erfolgen. Hierbei wird häufig das Protokoll EAP (Extensible Authentication Protocol) genutzt. Die Authentisierung erfolgt bei EAP Port-basiert und beruht auf dem Standard IEEE 802.1X. Dies bedeutet, dass der Zugang zum Netz erst dann erlaubt wird, wenn sich der Client eindeutig am RADIUS-Server identifiziert hat.

Die zum Einsatz kommenden Authentisierungsserver sind geeignet abzusichern (siehe M 4.250 *Auswahl eines zentralen, netzbasierten Authentisierungsdienstes*).

Für die Shared Secrets zwischen RADIUS-Server und RADIUS-Client sind ausreichend lange, komplexe kryptographische Schlüssel zu verwenden. Dabei kann, wenn die administrativen Möglichkeiten gegeben sind, für jede RADIUS-Client-Server-Beziehung ein anderes Shared Secret verwendet werden.

Für RADIUS sollten Komponenten eingesetzt werden, die den Anforderungen aus den RFCs zu RADIUS entsprechen, um eine größtmögliche Interoperabilität zwischen den verschiedenen Komponenten sicherzustellen. Die Authentisierungs- und Abrechnungsprotokolle sollten in einem gesonderten Datenbanksystem gespeichert werden können.

Die RADIUS-Kommunikation sollte auf Port 1812 bzw. 1813 beschränkt werden. Die Ports 1645 bzw. 1646 sollten nach Möglichkeit nicht verwendet werden. Andere Ports sind zu schließen, soweit technisch möglich. Die RADIUS-Kommunikation des Servers ist auf die dem Server bekannten und authentischen RADIUS-Clients zu beschränken.

Bei hohem Schutzbedarf hinsichtlich der Vertraulichkeit der Authentisierungsinformationen ist IPSec zur Sicherung der RADIUS-Kommunikation empfehlenswert, wobei jedoch nicht auf die RADIUS-eigenen Verfahren zur Absicherung der Kommunikation verzichtet werden sollte. Ebenso ist hierbei über einen Einsatz eines redundanten RADIUS-Servers nachzudenken.

Die Richtlinien, nach denen ein RADIUS-Server eine Authentisierungsanfrage beantwortet, sollten so restriktiv wie möglich gewählt werden. Hierbei sollten die zulässigen Einwahlzeiten, die MAC-Adresse und der Port-Typ des sich

verbindenden RADIUS-Clients, sowie die IP-Adresse des RADIUS-Clients und die EAP-Methode zur Authentikation festgelegt werden.

Ergänzende Kontrollfragen:

- Wie werden die Authentisierungsinformationen bei der Übertragung geschützt?
- Wie werden Angriffe auf den RADIUS-Server verhindert?

M 5.139 Sichere Anbindung eines WLANs an ein LAN

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Ein Ziel bei der Nutzung von WLAN-Komponenten ist häufig die bequeme und mobile Anbindung an andere Netze. Dies können andere WLANs, aber auch existierende LANs in der eigenen Institution sein. Hierbei sollten zwei Sicherheitsaspekte unterschieden werden:

- der Schutz der benutzten WLAN-Komponenten vor Missbrauch bei der Nutzung fremder Netze und
- der Schutz der internen LANs gegen Missbrauch von außen.

Bei der Anbindung eines WLANs an ein LAN muss der Übergang zwischen WLAN und LAN entsprechend des höheren Schutzbedarfs abgesichert werden. Diesen hat im Allgemeinen das LAN. Bei der WLAN-Kopplung mit einem LAN sind grundsätzlich zwei Ansätze möglich:

- Es kann versucht werden, im WLAN ein Sicherheitsniveau zu erreichen, dass dem innerhalb des vorhandenen drahtgebundenen LANs entspricht. Dazu müssen aber im Allgemeinen die bei Standard-WLAN-Komponenten integrierten Sicherheitsmechanismen erweitert, beispielsweise durch stärkere Kryptoalgorithmen, sowie ein hoher Aufwand für zusätzliche Absicherungen betrieben werden.
- Auf der anderen Seite kann ein pragmatischer Ansatz gewählt werden, bei dem davon ausgegangen wird, dass sowohl die auf der Funkstrecke übertragenen Daten als auch die WLAN-Komponenten nicht dem Sicherheitsniveau des LAN entsprechen. Daher sind Zugriffe aus dem WLAN hierbei wie solche aus dem Internet zu behandeln und somit nur über ein Sicherheitsgateway zuzulassen. Diese Vorgehensweise ist zu empfehlen.

Je höherwertiger die Absicherung auf der Luftschnittstelle und der aktiven Komponenten des Distribution System ist, desto weniger umfangreich müssen die am Übergabepunkt zum LAN zu realisierenden Maßnahmen ausfallen. In jedem Fall muss aber am Übergabepunkt eine vollständige Sperrung der WLAN-Kommunikation ins interne LAN möglich sein, sobald ein Angriff auf das WLAN erkannt wird.

Das Koppelelement zwischen dem Distribution System des WLANs und LAN muss mindestens ein Layer-3-Router sein, um eine effektive Trennung der Broadcast-Domänen zu erreichen. Der Einsatz weitergehender Mechanismen, etwa eines dynamischen Paketfilters anstelle eines Routers, muss je nach Einsatzumgebung und entsprechend des Schutzbedarfs entschieden werden.

Bei höherem Schutzbedarf sollte außerdem die Sicherheit der Authentisierung verbessert werden, beispielsweise durch den Einsatz von EAP-TLS, so dass eine gegenseitige starke Authentikation zwischen den WLAN-Clients und einem Authentikationsserver innerhalb des LANs möglich ist.

Ergänzende Kontrollfragen:

- Wurde das LAN durch ein zusätzliches Sicherheitsgateway gegenüber dem WLAN abgesichert?
- Ist der Zugriff aus dem WLAN auf das LAN notwendig und erwünscht? Ist diese Entscheidung dokumentiert?

M 5.140 Aufbau eines Distribution Systems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Ein Distribution System ist ein Netz, das Access Points untereinander und mit der weiteren Infrastruktur, wie z. B. einem kabelgebundenen Netz, verbindet. Generell werden zwei Arten von Distribution Systemen unterschieden:

- kabelgebundenes Distribution System

  Alle Access Points werden untereinander und mit der weiteren Infrastruktur verkabelt.

- Wireless Distribution System

  Eine direkte Verkabelung zwischen den Access Points ist hierbei nicht mehr notwendig. Allein die Stromversorgung muss für jeden Access Point gewährleistet sein.

In beiden Fällen sollte die Kommunikation zwischen den Access Points stets verschlüsselt statt finden, um die Vertraulichkeit der übermittelten Daten zu gewährleisten. Bei einem kabelgebundenen Distribution System können hierfür beispielsweise IPSec-VPN-Tunnel eingesetzt werden, bei einem Wireless Distribution System nach IEEE 802.11i kann zusätzlich CCMP verwendet werden. Bei einem Wireless Distribution System ist neben dem Schutz der Vertraulichkeit und Integrität aber auch die Verfügbarkeit wesentlich und es sollten Maßnahmen ergriffen werden, um eventuelle Denial-of-Service-Angriffe usw. zu unterbinden. Durch den Einsatz von Wireless Intrusion Detection Systemen und regelmäßige Sicherheitschecks können Schwachstellen schnell gefunden und entsprechende Gegenmaßnahmen eingeleitet werden.

Beim Aufbau eines Distribution Systems muss darüber hinaus die prinzipielle Entscheidung getroffen werden, ob aus Sicherheitsgründen eine eigene Infrastruktur aufgebaut bzw. geschaltet wird, also eine physikalische Segmentierung zur Infrastruktur des internen LANs erfolgt. Als Alternative kann geprüft werden, ob eine logische Segmentierung durch VLANs ausreichend ist.

physikalisches Distribution System

Wird eine eigene physikalische Infrastruktur für das Distrubtion System eingerichtet, so spielt vor allem die räumliche Ausdehnung des Versorgungsgebietes eine wesentliche Rolle. In der Regel werden mehrere Access Points durch Layer-2- bzw. Layer-3-Switches zusammengefasst, wobei eine Skalierung bei 12, 24 oder 48 Ports je Switch üblich ist. Sollen beispielsweise 100 Access Points miteinander zu einem Distribution System verbunden werden, so sind somit drei bis zehn Switches erforderlich. Eine direkte Verbindung der Access Points an Switches im zentralen Serverraum ist in der Regel nicht möglich, somit müssen die Switches über das gesamte Areal, das mit WLAN ausgestattet werden soll, verteilt werden. Dabei ist zu gewährleisten, dass die Switches ausreichend vor einem externen Zugriff geschützt sind und dass je nach Verfügbarkeit des Distribution Systems für eine Redundanz bei den Switches gesorgt ist. Für den Aufbau einer eigenen physikalischen Infrastruktur sind allerdings größere Investitionen und zusätzliche Sicherheitsmaßnahmen notwendig.

logisches Distribution System

Bei einer logischen Segmentierung werden zur Kontrolle des Datenflusses über die Access Switches des kabelbasierten LANs virtuelle LANs (VLANs) gebildet. Soll eine Segmentierung von WLAN-Clients innerhalb des Distribution Systems erfolgen, muss beim Access Point zusätzlich eine Zuordnung eines WLAN-Clients zu einem VLAN erfolgen. Die Konfiguration eines logischen Distribution Systems innerhalb einer bestehenden LAN-Infrastruktur ist unter betriebstechnischen und damit unter Verfügbarkeitsaspekten nicht ganz unproblematisch und setzt extrem gut geschulte Administratoren voraus. Solange die gesamte LAN- und WLAN-Infrastruktur nur normal verfügbar sein soll, ist die Konfiguration von VLANs ein gangbarer Weg. Sobald allerdings eine höhere Verfügbarkeit angestrebt wird, sind VLANs für ein Distribution System nicht zu empfehlen.

Ergänzende Kontrollfragen:

- Soll ein kabelgebundenes oder Wireless Distribution System aufgebaut werden? Wurde die Entscheidung dokumentiert und hinterlegt?
- Wurde eine physikalische oder logische Segmentierung vorgenommen? Wurde das auch dokumentiert und hinterlegt?

M 5.141 Regelmäßige Sicherheitschecks in WLANs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Es sollte regelmäßig, mindestens monatlich, ein WLAN-Sicherheitscheck durchgeführt werden.

WLANs sollten regelmäßig mit WLAN-Analysatoren und Netz-Sniffern überprüft werden, ob es eventuell Sicherheitslücken wie schwache Passwörtern, mangelhafte Verschlüsselung oder einen aktiven SSID-Broadcast gibt. Aber auch nach unbefugt installierten WLANs sollte gesucht werden.

Netz-Analyse-Programme

Zur Überwachung und Analyse von Dienstequalität und Sicherheit sind in WLANs ebenso wie auch in anderen Netzen spezifische Werkzeuge hilfreich. Für einen sicheren Betrieb von WLANs ist die Überprüfung, in wie weit die vorgegebenen Sicherheitsrichtlinien eingehalten werden und wie es um die Verfügbarkeit des WLANs bestellt ist, besonders wichtig. Zu letzterem gehören auch Messungen der Performance und Fehleranalysen. Nützlich sind aber auch Tools, die einen Überblick über alle aktiven WLAN-Teilnehmer, sowie über bisher erkannte Netzteilnehmer geben.

Netz-Analyse- oder Sniffer-Programme lesen Datenströme mit und untersuchen die übermittelten Datenpakete nach verschiedenen, einstellbaren Kriterien. Sie können beispielsweise nach bestimmten Mustern in den Datenpaketen suchen oder Routing-Information auswerten.

Netz-Analyse-Tools sollten regelmäßig eingesetzt werden, um

- nach unautorisierten WLANs innerhalb der Institutionsgrenzen zu suchen,
- regelmäßig zu überprüfen, ob alle notwendigen Sicherheitsmechanismen aktiviert wurden,
- um Funklöcher aufzuspüren und die Signalqualität von Funknetzen auszuwerten.

Überwachung der WLAN-Infrastruktur

Zur Überwachung der WLAN-Infrastruktur kann im einfachsten Fall eine Standortaufnahme über einen mit Spezial-Software ausgestatten WLAN-Client als Stichprobe durchgeführt werden, mit dem das Versorgungsgebiet abgelaufen wird. Hierdurch kann der Betrieb von unerlaubt aufgestellten Access Points ermittelt werden.

Eine bessere Kontrolle ist aber bei Einsatz eines WLAN-Management-Systems gegeben, mit dessen Hilfe regelmäßig folgende Aktion durchgeführt werden sollten:

- Erkennung von Fremdgeräten, insbesondere fremder Access Points
- Durchführung von Wireless Site Surveys, also Untersuchungen, um Informationen zu Abdeckung, Datenraten, Bandbreite, QoS usw. über ein WLAN zu erhalten

- Protokollierung von Anmeldezeiten
- Überwachung der Konfiguration von WLAN-Netzelementen

Einsatz eines Wireless Intrusion Detection Systems

Bei der Planung eines Access Point-basierten Wireless Intrusion Detection Systems (IDS) sollte zunächst festgelegt werden, ob eine eigene Messinfrastruktur aufgebaut wird oder die im Produktivnetz verwendeten Access Points und WLAN-Clients in bestimmten Intervallen in einen Messmodus geschaltet werden. Wird hierbei keine vollständige Erfassung des zu überwachenden Bereichs realisiert, können Angriffe im WLAN auf Funkebene nicht erkannt werden. Darüber hinaus ist zu berücksichtigen, dass ein Access Point bzw. WLAN-Client im Messbetrieb keine Daten übertragen kann und damit eine Reduktion der Performance und gegebenenfalls der Verfügbarkeit der WLAN-Datenübertragung in Kauf genommen wird. Ebenso bleibt bei der Nutzung der zum Produktivnetz gehörenden Access Points im Scan-Modus immer ein Zeitfenster bestehen, in dem keine Überwachung auf der Luftschnittstelle möglich ist.

In jedem Fall muss beim Einsatz eines Intrusion Detection Systems oder gar eines Intrusion Prevention System (IPS) das normale Kommunikationsverhalten im WLAN ermittelt bzw. auf Basis von Messungen definiert werden (siehe auch M 5.71 *Intrusion Detection und Intrusion Response Systeme*).

Alarm- und Fehlerbehandlung

Die WLAN-Administration sollte über eine Alarm- und Fehlerbehandlung verfügen. Hierbei sind folgende Aufgaben durch die Administratoren wahrzunehmen:

- Auswertung und Bewertung von Alarmen, z. B. bei einer Häufung von fehlgeschlagenen Authentisierungsversuchen an einem Access Point
- Auswertung von Statistiken zur Fehlersuche
- Auslösung von Maßnahmen bei einem vermuteten Sicherheitsvorfall
- Anpassung von Schwellwerten zur Alarmauslösung an eine geänderte WLAN-Nutzung

Penetrationstest

Im Zuge eines Sicherheitschecks kann ein WLAN auch mit Hilfe von Penetrationstests auf Schwachstellen untersucht werden. Dabei sind alle getroffenen Sicherheitsmaßnahmen genau zu prüfen, ob diese den Angriffen gewachsen sind, gegen die sie wirken sollen. Ein Penetrationstest sollte mindestens halbjährlich, spätestens jedoch jährlich, erfolgen.

Dokumentation

Bei der Durchführung des Sicherheitschecks sollten die Administratoren alle Schritte so dokumentieren, dass sie (beispielsweise bei einem Verdacht auf ein kompromittiertes System) nachvollzogen werden können. Die Ergebnisse des Sicherheitschecks müssen dokumentiert werden, Abweichungen vom Soll zustand muss nachgegangen werden.

Ergänzende Kontrollfragen:

- Sind die Administratoren in die Alarm- und Fehlerbehandlung bei Angriffen auf das WLAN eingewiesen?
- Werden die Durchführung und die Ergebnisse des WLAN-Sicherheitschecks dokumentiert?

M 6 Maßnahmenkatalog Notfallvorsorge

M 6.1	Erstellung einer Übersicht über Verfügbarkeitsanforderungen	
M 6.2	Notfall-Definition, Notfall-Verantwortlicher	
M 6.3	Erstellung eines Notfall-Handbuches	
M 6.4	Dokumentation der Kapazitätsanforderungen der IT-Anwendungen	
M 6.5	Definition des eingeschränkten IT-Betriebs	
M 6.6	Untersuchung interner und externer Ausweichmöglichkeiten	
M 6.7	Regelung der Verantwortung im Notfall	
M 6.8	Alarmierungsplan	
M 6.9	Notfall-Pläne für ausgewählte Schadensereignisse	
M 6.10	Notfall-Plan für DFÜ-Ausfall	
M 6.11	Erstellung eines Wiederanlaufplans	
M 6.12	Durchführung von Notfallübungen	
M 6.13	Erstellung eines Datensicherungsplans	
M 6.14	Ersatzbeschaffungsplan	
M 6.15	Lieferantenvereinbarungen	
M 6.16	Abschließen von Versicherungen	
M 6.17	Alarmierungsplan und Brandschutzübungen	
M 6.18	Redundante Leitungsführung	
M 6.19	Datensicherung am PC	**entfallen**
M 6.20	Geeignete Aufbewahrung der Backup-Datenträger	
M 6.21	Sicherungskopie der eingesetzten Software	
M 6.22	Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen	
M 6.23	Verhaltensregeln bei Auftreten eines Computer-Virus	
M 6.24	Erstellen eines Notfall-Bootmediums	
M 6.25	Regelmäßige Datensicherung der Server-Festplatte	**entfallen**
M 6.26	Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten	
M 6.27	Sicheres Update des BIOS	
M 6.28	Vereinbarung über Lieferzeiten "lebensnotwendiger" TK-Baugruppen	
M 6.29	TK-Basisanschluss für Notrufe	

M 6.30	Katastrophenschaltung
M 6.31	Verhaltensregeln nach Verlust der Systemintegrität
M 6.32	Regelmäßige Datensicherung
M 6.33	Entwicklung eines Datensicherungskonzepts
M 6.34	Erhebung der Einflussfaktoren der Datensicherung
M 6.35	Festlegung der Verfahrensweise für die Datensicherung
M 6.36	Festlegung des Minimaldatensicherungskonzeptes
M 6.37	Dokumentation der Datensicherung
M 6.38	Sicherungskopie der übermittelten Daten
M 6.39	Auflistung von Händleradressen zur Fax-Wiederbeschaffung
M 6.40	Regelmäßige Batterieprüfung/-wechsel
M 6.41	Übungen zur Datenrekonstruktion
M 6.42	Erstellung von Rettungsdisketten für Windows NT
M 6.43	Einsatz redundanter Windows NT/2000 Server
M 6.44	Datensicherung unter Windows NT
M 6.45	Datensicherung unter Windows 95
M 6.46	Erstellung von Rettungsdisketten für Windows 95
M 6.47	Aufbewahrung der Backup-Datenträger für Telearbeit
M 6.48	Verhaltensregeln nach Verlust der Datenbankintegrität
M 6.49	Datensicherung einer Datenbank
M 6.50	Archivierung von Datenbeständen
M 6.51	Wiederherstellung einer Datenbank
M 6.52	Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten
M 6.53	Redundante Auslegung der Netzkomponenten
M 6.54	Verhaltensregeln nach Verlust der Netzintegrität
M 6.55	Reduzierung der Wiederanlaufzeit für Novell Netware Server
M 6.56	Datensicherung bei Einsatz kryptographischer Verfahren
M 6.57	Erstellen eines Notfallplans für den Ausfall des Managementsystems
M 6.58	Etablierung eines Managementsystems zur Behandlung von Sicherheitsvorfällen
M 6.59	Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen

M 6.1 Erstellung einer Übersicht über Verfügbarkeitsanforderungen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Verantwortliche der einzelnen IT-Anwendungen

Für die in einem IT-System betriebenen IT-Anwendungen und deren Daten sind die Verfügbarkeitsanforderungen festzustellen. Da eine IT-Anwendung nicht zwingend jeden Bestandteil des IT-Systems benötigt, sind die Verfügbarkeitsanforderungen der IT-Anwendungen auf die wesentlichen Komponenten des IT-Systems abzubilden. Das Ergebnis dieser Arbeit kann in Form einer Übersicht mit folgenden Inhalten dargestellt werden:

IT-System	IT-Komponente	IT-Anwendung	tolerierbare Ausfallzeit
Zentralsystem	Host	Reisekosten	5 Arbeitstage
		Buchhaltung	**3 Stunden**
	DFÜ	E-Mail	3 Arbeitstage
		Buchhaltung	**1 Arbeitstag**
	Drucker	Reisekosten	10 Arbeitstage
		Buchhaltung	2 Arbeitstage
		Einsatzplanung	**1 Arbeitstag**
LAN	Server	Datenerfassung	1 Arbeitstag
		Leitstelle	**4 Stunden**
	PC	Datenerfassung	10 Arbeitstage
	PC	Leitstelle	**4 Stunden**

(Lesart: Die IT-Komponente Host im IT-System "Zentralsystem" hat aufgrund der IT-Anwendung Buchhaltung eine maximal tolerierbare Ausfallzeit von 3 Stunden.)

Eine praktikable Vorgehensweise ist es, zu den einzelnen IT-Anwendungen den Verfahrensverantwortlichen nach den tolerierbaren Ausfallzeiten der benutzten IT-Komponenten zu befragen, um danach die Ergebnisse nach IT-System und Komponenten geordnet in der Tabelle aufzuführen.

Die Übersicht erleichtert es, die besonders zeitkritischen Komponenten des IT-Systems zu extrahieren, für die die Notfallvorsorge unumgänglich ist. Bei Ausfall einer Komponente gibt diese Übersicht darüber hinaus Auskunft über die betroffenen IT-Anwendungen und deren Verfügbarkeitsanforderungen.

Die Anforderungen an die Verfügbarkeit sind von den Anwendern bzw. Fachabteilungen zu begründen, sofern dies nicht schon an anderer Stelle ge-

schehen ist. Die Verfügbarkeitsanforderungen sind von der Behörden- bzw. Unternehmensleitung zu bestätigen.

Bei Ausfall einer Komponente des IT-Systems ermöglicht diese Übersicht eine schnelle Aussage, ab wann ein Notfall vorliegt. Dass ein Notfall auch bei Ausfall einer besonders zeitkritischen Komponente nicht zwingend eintreten muss, lässt sich anhand des Ersatzbeschaffungsplans (siehe M 6.14 *Ersatzbeschaffungsplan*) und der Untersuchung über interne und externe Ausweichmöglichkeiten (siehe M 6.6 *Untersuchung interner und externer Ausweichmöglichkeiten*) ermitteln.

Ergänzende Kontrollfragen:

- Liegen begründete Verfügbarkeitsanforderungen für jede IT-Anwendung vor?
- Entsprechen die Verfügbarkeitsanforderungen dem aktuellen Verfahrensstand? Wann wurde die Tabelle letztmalig aktualisiert?

M 6.2 Notfall-Definition, Notfall-Verantwortlicher

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Nicht jeder Teil- oder Gesamtausfall des Systems stellt jedoch einen Notfall dar. Oftmals lassen sich Ausfälle des IT-Systems durch geplante Maßnahmen, z. B. Ersatzbeschaffung, auch in kurzer Zeit beheben. Der Notfall tritt erst dann ein, wenn ein Zustand erreicht wird, bei dem innerhalb der geforderten Zeit eine Wiederherstellung der Verfügbarkeit (siehe M 6.1 *Erstellung einer Übersicht über Verfügbarkeitsanforderungen*) nicht möglich ist und sich daraus ein sehr hoher Schaden ergibt. Schon bei Eintritt eines Ereignisses, in dessen Folge der Notfall entstehen könnte, sind die erforderlichen Maßnahmen zu ergreifen, die zu einer Schadensreduzierung führen.

Für die autorisierte und rechtzeitige Einleitung von Notfallmaßnahmen bedarf es der Benennung eines Notfall-Verantwortlichen. Die Behörden- bzw. Unternehmensleitung muss den Notfall-Verantwortlichen sowohl für die Entscheidung autorisieren, ob ein Notfall eingetreten ist, als auch für die Einleitung erforderlicher Notfallmaßnahmen.

Ergänzende Kontrollfrage:

- Wer ist autorisiert, über einen Notfall zu entscheiden?

M 6.3 Erstellung eines Notfall-Handbuches

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Verantwortliche der einzelnen IT-Anwendungen

In einem Notfall-Handbuch sind alle Maßnahmen, die nach Eintritt eines Notfall-auslösenden Ereignisses zu ergreifen sind, und alle dazu erforderlichen Informationen zu dokumentieren. Das Notfall-Handbuch ist so zu gestalten, dass ein sachverständiger Dritter in der Lage ist, die im Handbuch spezifizierten Notfallmaßnahmen durchzuführen.

Nachfolgend wird beispielhaft ein umfassendes Inhaltsverzeichnis eines Notfallhandbuchs zur Orientierung aufgeführt. Welche Teile dieses Vorschlags übernommen werden können, ist abhängig von der vorhandenen System- und Anwendungsdokumentation und kann daher nur individuell entschieden werden.

Inhaltsverzeichnis Notfall-Handbuch

Teil A: Sofortmaßnahmen

1	Alarmierung im Notfall
1.1	Alarmierungsplan und Meldewege
1.2	Adresslisten betroffener Mitarbeiter
1.3	Festlegung konkreter Aufgaben für einzelne Personen/Funktionen im Notfall
1.4	Notrufnummern (z. B. Feuerwehr, Polizei, Notarzt, Wasser- und Stromversorger, Ausweichrechenzentrum, externes Datenträgerarchiv, externe Telekommunikationsanbieter)
...	
2	Handlungsanweisung für spezielle Ereignisse
2.1	Brand
2.2	Wassereinbruch
2.3	Stromausfall
2.4	Ausfall der Klimaanlage
2.5	Explosion
2.6	Sabotage
2.7	Ausfall der Datenfernübertragungseinrichtung
2.8	Einbruch
2.9	Vandalismus
2.10	Bombendrohung
2.11	Streik / Demonstrationen
2.12	...

Teil B: Regelungen für den Notfall

3	Allgemeine Regelungen
3.1	Notfall-Verantwortliche
3.2	Benennung der an der Durchführung der Notfallpläne beteiligten Organisationseinheiten, Kompetenzverteilung
3.3	Organisationsrichtlinien, Verhaltensregeln
...	
4	Tabelle der Verfügbarkeitsanforderungen

Teil C: Wiederanlaufpläne für kritische Komponenten

5	Wiederanlauf-Planung
5.1	Wiederanlauf-Plan für Komponente 1 (z. B. Host)
5.1.1	Wiederbeschaffungsmöglichkeiten
5.1.2	Interne / externe Ausweichmöglichkeiten
5.1.3	DFÜ-Versorgung
5.1.4	Eingeschränkter IT-Betrieb
5.1.5	Wiederanlaufreihenfolge
5.2	Wiederanlauf-Plan für Komponente 2 (z. B. Drucker)
...	

Teil D: Dokumentation

6	Beschreibung der IT-Systeme
6.1	Beschreibung des IT-Systems A (im Überblick)
6.1.1	Beschreibung der Hardware-Komponenten
6.1.2	Beschreibung der Software-Komponenten
6.1.2.1	Bestandsverzeichnis der Systemsoftware
6.1.2.2	Bestandsverzeichnis der zu dem IT-System gehörenden Systemdaten
6.1.3	Beschreibung der Netzanbindungen des IT-Systems
6.1.4	Beschreibung der IT-Anwendungen
6.1.4.1	Bestandsverzeichnis der Anwendungssoftware
6.1.4.2	Bestandsverzeichnis der zu einer IT-Anwendung gehörenden Daten
6.1.4.3	Kapazitätsanforderungen einzelner IT-Anwendungen im Normalfall
6.1.4.4	Minimale Kapazitätsanforderungen der IT-Anwendungen für den Notfall
6.1.4.5	Wiederanlaufverfahren der IT-Anwendungen
6.1.5	Datensicherungsplan
6.1.6	Beschreibung der notwendigen Infrastruktureinrichtungen
6.1.7	Sonstige Unterlagen (Handbücher etc.)
...	
7	Wichtige Informationen
7.1	Ersatzbeschaffungsplan
7.2	Hersteller- und Lieferantenverzeichnis
7.3	Verzeichnis der Dienstleistungsunternehmen des Fachgebiets "Sanierung"

Letztes Änderungsdatum: _____

Das Notfall-Handbuch ist durch die Behörden- bzw. Unternehmensleitung in Kraft zu setzen und muss nach Bedarf aktualisiert werden. Die Verfügbarkeit des Notfallhandbuchs ist von zentraler Bedeutung. Deshalb ist ein aktuelles Exemplar extern auszulagern. Zusätzlich ist das Notfall-Handbuch allen im Handbuch genannten Personen oder Organisationseinheiten zur Kenntnis zu geben.

Ergänzende Kontrollfragen:

- Ist das Notfall-Handbuch aktuell?
- Werden alle möglichen Notfälle betrachtet?

M 6.4 Dokumentation der Kapazitätsanforderungen der IT-Anwendungen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Verantwortliche der einzelnen IT-Anwendungen

Im Hinblick auf interne und externe Ausweichmöglichkeiten für den Betrieb der IT-Anwendungen sind für diese Kapazitätsanforderungen zu dokumentieren. Hierunter fallen u. a.:

- CPU-Leistung,
- Plattenkapazitäten,
- DFÜ-Leistung und
- Leistungen weiterer Hardware-Komponenten (Drucker, Belegleser etc.).

Die Kapazitätsanforderungen einer IT-Anwendung sind dahingehend zu untersuchen, ob sie für den Zeitraum eines Notfalls reduziert werden können, um auf diese Weise einen eingeschränkten IT-Betrieb zu ermöglichen (z. B. Reduzierung der Anzahl der angeschlossenen Terminals). Diese eingeschränkten Kapazitätsanforderungen für den Notfall sind ebenfalls zu dokumentieren und zu aktualisieren.

Ergänzende Kontrollfragen:

- Liegen Kapazitätsanforderungen für jede IT-Anwendung vor?
- Entsprechen die Kapazitätsanforderungen dem aktuellen Verfahrensstand?
- Wurden die IT-Anwendungen dahingehend untersucht, ob eine Senkung der Kapazitätsanforderungen möglich ist?

M 6.5 Definition des eingeschränkten IT-Betriebs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Verantwortliche der einzelnen IT-Anwendungen

Für den Fall, dass Teile des IT-Systems ausfallen, ist zu untersuchen, ob ein eingeschränkter IT-Betrieb notwendig und möglich ist. Um bei einem eingeschränkten IT-Betrieb möglichst viele IT-Anwendungen betreiben zu können, ist die für jede einzelne IT-Anwendung die zur Verfügung gestellte Kapazität auf das notwendige Maß zu reduzieren (siehe M 6.4 *Dokumentation der Kapazitätsanforderungen der IT-Anwendungen*).

Für den eingeschränkten IT-Betrieb muss festgelegt werden, welche IT-Anwendungen mit welcher Priorität betrieben werden. Dies ist schriftlich zu fixieren.

Auch manuelle Ersatzverfahren können geeignet sein, um die Verfügbarkeitsanforderungen einer IT-Anwendung zu senken. Die für den Einsatz eines manuellen Ersatzverfahrens erforderlichen Hilfsmittel (Formulare, Papierlisten, Mikrofiche) müssen dazu allerdings bereitgehalten werden.

Ergänzende Kontrollfragen:

- Wurde festgelegt, welche IT-Anwendung mit welcher Priorität im eingeschränkten IT-Betrieb durchzuführen ist?
- Sind die qualitativen und quantitative Vorgaben für den eingeschränkten IT-Betrieb mit den Fachbereichen abgesprochen?

M 6.6 Untersuchung interner und externer Ausweichmöglichkeiten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Verantwortliche der einzelnen IT-Anwendungen

Um Kapazitätsengpässe im eingeschränkten IT-Betrieb zu vermeiden, sind interne und externe Ausweichmöglichkeiten zu untersuchen.

Bei der Untersuchung von Ausweichmöglichkeiten ist insbesondere auf die technischen Anforderungen an das Ausweich-IT-System zu achten. Kompatibilität und ausreichende Kapazitätsreserven (siehe M 6.4 *Dokumentation der Kapazitätsanforderungen der IT-Anwendungen*) des Ausweich-IT-Systems sind Grundvoraussetzung für dessen Benutzung.

Zunächst steht die interne Verlagerung von IT-Anwendungen von einem IT-System auf ein anderes IT-System im Vordergrund (z. B. Ausweichen auf den Entwicklungsrechner, wenn der Produktionsrechner ausfällt). Externe Ausweichmöglichkeiten sind dann heranzuziehen, wenn mit internen Ausweichmöglichkeiten die Verfügbarkeitsanforderungen nicht mehr oder nicht wirtschaftlich erfüllt werden können.

Ausweichmöglichkeiten für nicht IT-spezifische Komponenten sind auch zu berücksichtigen. Beispielsweise im Bereich der Infrastruktur sind Ausweichmöglichkeiten für IT-Räume in Betracht zu ziehen.

Ergänzende Kontrollfragen:

- Wurden interne und externe Ausweichmöglichkeiten auf ihre Wirksamkeit hin untersucht?
- Wird die Konfiguration, Kapazität und Kompatibilität von internen und externen Ausweichmöglichkeiten dem aktuellen Verfahrensstand angepasst?
- Sind bei externen Ausweichmöglichkeiten Integrität und Vertraulichkeit der ausgelagerten IT-Anwendungen und Daten gewährleistet?

M 6.7 Regelung der Verantwortung im Notfall

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Leiter IT, Leiter Organisation, IT-Sicherheitsmanagement, Verantwortliche der einzelnen IT-Anwendungen

Für den Zeitraum nach Eintritt des schädigenden Ereignisses bis hin zur vollständigen Wiederherstellung der Verfügbarkeit kann eine zeitlich befristete **Notfall-Organisation** erforderlich sein.

Es müssen Verantwortliche bestimmt sein, die befugt sind zu entscheiden, ob ein Notfall eingetreten ist, und die die entsprechenden Maßnahmen des Notfallhandbuchs einleiten (siehe M 6.2 *Notfall-Definition, Notfall-Verantwortlicher*). Die an der Durchführung der Maßnahmen im Bereich der Notfallvorsorge beteiligten Organisationseinheiten müssen befugt sein, die ihnen übertragenen Aufgaben eigenverantwortlich durchzuführen. Die hierzu erforderlichen Regelungen sind schriftlich festzuhalten. Dieses "Notfall-Organigramm" muss von der Behörden- bzw. Unternehmensleitung autorisiert werden.

Ergänzende Kontrollfragen:

- Existiert eine Beschreibung der Notfall-Organisation?
- Ist die Notfall-Organisation allen im Notfallhandbuch genannten Personen und Organisationseinheiten bekannt?
- Wann wurde sie zuletzt aktualisiert?
- Wer koordiniert welche Maßnahmen?

M 6.8 Alarmierungsplan

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Leiter IT, Leiter Organisation, IT-Sicherheitsmanagement, Verantwortliche der einzelnen IT-Anwendungen

Ein Alarmierungsplan enthält eine Beschreibung des Meldewegs, über den bei Eintritt eines Notfalls die zuständigen Personen oder Organisationseinheiten zu informieren sind. Die Alarmierung kann z. B. über Telefon, Fax, Funkrufdienste oder Kurier erfolgen. Beschrieben werden muss, wer wen benachrichtigt, wer ersatzweise zu benachrichtigen ist bzw. wie bei Nichterreichen zu verfahren ist. Zu diesem Zweck sind evtl. Adress- und Telefonlisten zu führen.

Der Alarmierungsplan muss sämtlichen Notfall-Verantwortlichen zur Verfügung stehen, darüber hinaus an zentraler Stelle redundant vorgehalten werden (z. B. Pforte, Bewachungspersonal). Die im Alarmierungsplan genannten Personen müssen den sie betreffenden Teil kennen. Allen Mitarbeitern müssen die Ansprechpartner bekannt sein, denen das Eintreten eines evtl. Notfall-auslösenden Ereignisses gemeldet werden kann.

Es kann verschiedene Alarmierungspläne für unterschiedliche Schadensfälle geben (Feuer, Wasser, DFÜ-Ausfall). Dann muss darauf geachtet werden, dass alle Schadensfälle abgedeckt sind.

Mit der Erstellung eines Alamierungsplans sollte auch die Festlegung eines Ruf- oder Bereitschaftsdienstes erwogen werden.

Kontrollfragen:

- Wird der Alarmweg sporadisch getestet?
- Wann wurde der Alarmierungsplan letztmalig überarbeitet?
- Sind noch alle im Alarmierungsplan genannten Personen Mitarbeiter der Behörde bzw. des Unternehmens?

M 6.9 Notfall-Pläne für ausgewählte Schadensereignisse

Verantwortlich für Initiierung: Leiter IT, Leiter Organisation, IT-Sicherheitsmanagement, Verantwortliche der einzelnen IT-Anwendungen

Verantwortlich für Umsetzung: Notfall-Verantwortliche

Notfall-Pläne beinhalten Handlungsanweisungen und Verhaltensregeln für bestimmte Schadensereignisse. Hierbei handelt es sich um Ereignisse, die diejenigen Teile des IT-Systems gefährden, die von existentieller Bedeutung sind. Ein Notfall-Plan ist auf die möglichst schnelle Wiederherstellung der Verfügbarkeit gerichtet.

Ein Notfall-Plan muss auch das Zusammenwirken eines schädigenden Ereignisses und der getroffenen Notfall-Maßnahme berücksichtigen. Beispielsweise kann durch den Einsatz einer Sprinkleranlage ein Brand bekämpft werden. Jedoch können durch den Wassereinsatz wiederum auch neue Gefährdungen entstehen, z. B. für die Stromversorgung oder für Datenträgerarchive.

Notfall-Pläne sind je nach Umfeldgegebenheiten für folgende Ereignisse aufzustellen:

- Brand,
- Wassereinbruch,
- Stromausfall,
- Ausfall der Klimaanlage,
- Explosion,
- Ausfall der Datenfernübertragungseinrichtung (siehe M 6.10 *Notfall-Plan für DFÜ-Ausfall*),
- Sabotage.

Die Wirksamkeit von Notfallplänen ist durch Notfallübungen (siehe M 6.12 *Durchführung von Notfallübungen*) zu überprüfen.

Ergänzende Kontrollfragen:

- Liegen Notfall-Pläne vor?
- Wurde die Wirksamkeit der Notfall-Pläne überprüft?

M 6.10 Notfall-Plan für DFÜ-Ausfall

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Verantwortliche der einzelnen IT-Anwendungen

Verantwortlich für Umsetzung: Notfall-Verantwortliche, Administrator

Der Notfall-Plan für den DFÜ-Ausfall beinhaltet die Handlungsanweisungen, die bei Ausfall von DFÜ-Einrichtungen durchzuführen sind. Insbesondere müssen die bestehenden internen und externen Ausweichmöglichkeiten bekannt sein, bevor die Entscheidung fixiert wird, wie ein Ausfall kompensiert werden soll.

Alternative Ausweichmöglichkeiten sind zum Beispiel:

- Ersatz der Datenübertragung durch Austausch von Datenträgern oder Druckerzeugnissen per Kurier (siehe hierzu Baustein B 5.2 *Datenträgeraustausch*),
- Datenübertragung über andere DFÜ-Einrichtungen oder
- Einsatz mobiler Kommunikationseinrichtungen (z. B. Bündelfunk, Mobiltelefonie, Satellitenkommunikation).

Ergänzende Kontrollfragen:

- Sind die für die Nutzung von Ausweichmöglichkeiten erforderlichen DFÜ-Kapazitäten hinreichend bemessen?

M 6.11 Erstellung eines Wiederanlaufplans

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Verantwortliche der einzelnen IT-Anwendungen

Verantwortlich für Umsetzung: Leiter IT, Notfall-Verantwortliche, Administrator

Für einen geregelten Wiederanlauf nach Ausfall einer IT-Komponente sind folgende Informationen zu dokumentieren (siehe Beispiel in M 6.3 *Erstellung eines Notfall-Handbuches*, Teil C):

- Wiederbeschaffungsmöglichkeiten, zum Beispiel die Nutzung eines Testrechners für den Dialogbetrieb oder die Ersatzbeschaffung (siehe M 6.14 *Ersatzbeschaffungsplan*),
- interne/externe Ausweichmöglichkeiten für IT-Anwendungen (siehe M 6.6 *Untersuchung interner und externer Ausweichmöglichkeiten*) sind aufzuzählen,
- DFÜ-Versorgung (siehe M 6.10 *Notfall-Plan für DFÜ-Ausfall*) für den Notbetrieb, um die minimal notwendigen Datenübertragungen zu gewährleisten,
- die im eingeschränkten IT-Betrieb (siehe M 6.5 *Definition des eingeschränkten IT-Betriebs*) laufenden IT-Anwendungen,
- Systemstart der IT-Komponente und Einbindung in das IT-System und
- um den Anforderungen an die Verfügbarkeit (siehe M 6.1 *Erstellung einer Übersicht über Verfügbarkeitsanforderungen*) der einzelnen IT-Anwendungen gerecht zu werden, ist eine Reihenfolge für den Wiederanlauf der IT-Anwendungen festzulegen.

Die für den Wiederanlauf einer IT-Anwendungen erforderlichen Schritte sind im Notfall-Handbuch aufzuzeigen (siehe Beispiel in M 6.3 *Erstellung eines Notfall-Handbuches,* Teil D). Beispiele für solche Schritte sind:

- Aufbau und Installation der notwendigen Hardware-Komponenten,
- Einspielen der Systemsoftware,
- Einspielen der Anwendungssoftware,
- Bereitstellen der notwendigen Daten einschließlich Konfigurationsdateien,
- Wiederanlauf.

Eine revisionsfähige Protokollierung des Wiederanlaufs ist zu gewährleisten.

Der Wiederanlaufplan ist durch Notfallübungen (sowohl bei internen als auch bei externen Ausweichmöglichkeiten) auf seine Durchführbarkeit zu testen. Insbesondere ist bei der Durchführung solcher Übungen der ausschließliche Einsatz der Software und Daten zu testen, die in internen oder externen Sicherungsarchiven aufbewahrt werden.

Der Wiederanlauf kann, je nach Umfang der betriebenen IT-Anwendungen, mit erheblichen Zeitaufwand verbunden sein. Der Zeitaufwand für die mit

dem Wiederanlauf verbundenen Maßnahmen kann durch solche Übungen ermittelt werden und ist bei der Überarbeitung des Wiederanlaufplans zu berücksichtigen.

Ergänzende Kontrollfragen:

- Entspricht der Wiederanlaufplan den Anforderungen der derzeitigen IT-Anwendungen?
- Wurde der Wiederanlaufplan erprobt?
- Sind die zeitlichen Vorgaben des Wiederanlaufs mit den Fachbereichen abgesprochen?

M 6.12 Durchführung von Notfallübungen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Notfall-Verantwortliche, Administrator

Notfallübungen dienen der Prüfung der Wirksamkeit von Maßnahmen im Bereich der Notfallvorsorge. Einerseits wird durch eine Notfallübung der effektive und reibungslose Ablauf eines Notfall-Plans erprobt und andererseits werden bisher unerkannte Mängel aufgedeckt. Typische Übungen sind:

- die Durchführung einer Alarmierung,
- Durchführung von Brandschutzübungen (siehe M 6.17 *Alarmierungsplan und Brandschutzübungen*),
- Funktionstests von Stromaggregaten,
- Wiederanlauf nach Ausfall einer ausgewählten IT-Komponente und
- Wiedereinspielen von Datensicherungen.

Die Ergebnisse einer Notfallübung sind zu dokumentieren.

Notfallübungen sind regelmäßig zu wiederholen. Da diese Übungen den normalen Betriebsablauf stören können, sollte die Häufigkeit an der Gefährdungslage orientiert sein, jedoch sollten die entsprechenden Notfallübungen zumindest einmal jährlich stattfinden. Soweit erforderlich sind Schulungsmaßnahmen der Mitarbeiter durchzuführen (Erste Hilfe, Brandbekämpfung etc.)

Vor Durchführung einer Notfallübung ist das Einverständnis der Behörden- bzw. Unternehmensleitung einzuholen.

Ergänzende Kontrollfragen:

- Werden die Notfallübungen regelmäßig wiederholt?
- Führen aufgedeckte Mängel zu einer Überarbeitung der Notfall-Pläne?

M 6.13 Erstellung eines Datensicherungsplans

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Verantwortliche der einzelnen IT-Anwendungen

Mit Hilfe des Datensicherungsplans muss ein sachverständiger Dritter in der Lage sein, sämtliche für den Wiederanlauf einer IT-Anwendung erforderliche Software (Betriebssystemsoftware, Anwendungssoftware) und deren Daten in angemessener Zeit beschaffen und installieren zu können.

Ein Datensicherungsplan muss Auskunft geben können über:

- Speicherungsort der Daten im Normalbetrieb (Plattenspeicher-Belegungsplan),
- den Bestand der gesicherten Daten (Bestandsverzeichnis),
- die Zeitpunkte der Datensicherungen,
- Art und Umfang der Datensicherung (logische/physikalische, Teil-/Vollsicherung),
- das Verfahren zur Datensicherung und zur Rekonstruktion der gesicherten Daten und
- den Ort der Aufbewahrung (Hinweis auf ggf. erforderliche Zutrittsmittel).

Die systematische Erarbeitung eines Datensicherungskonzeptes, aus dem sich ein Datensicherungsplan ableitet, wird im Baustein B 1.4 *Datensicherungskonzept* beschrieben.

Ergänzende Kontrollfragen:

- Werden Datensicherungsmaßnahmen entsprechend dem Datensicherungskonzept durchgeführt?
- Wurde im Rahmen von Notfallübungen überprüft, ob aus externen Datensicherungsbeständen die Datenträger ohne Verzögerung beschafft werden konnten?
- Wie aktuell ist das bestehende Datensicherungskonzept?

M 6.14 Ersatzbeschaffungsplan

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Verantwortliche der einzelnen IT-Anwendungen

Erhöht Verfügbarkeit

Bei Ausfall einzelner Teile des IT-Systems ist neben der Reparatur die Ersatzbeschaffung zunächst die Maßnahme, die am zielgerichtetsten die Wiederherstellung der Verfügbarkeit verfolgt. Um den Vorgang der Ersatzbeschaffung zu beschleunigen, ist die Erstellung eines Ersatzbeschaffungsplans sinnvoll. Dieser muss für jede wichtige IT-Komponente Angaben machen über:

- Bezeichnung der IT-Komponente (Name, Geräte-Nr., Beschaffungsdatum),
- Hersteller,
- Lieferant,
- Lieferzeit und
- Dauer der Reinstallation.

Lassen sich für eine IT-Komponente mehrere Hersteller oder Lieferanten benennen, so sind sie alternativ aufzuführen. Gegebenenfalls lassen sich auch anderweitige Produkte benennen. Bei einer Ersatzbeschaffungsmaßnahme sind solche Angaben für eine sparsame Mittelbewirtschaftung erforderlich.

Regelmäßig aktualisieren

Ersatzbeschaffungsmaßnahmen müssen neben der Wiederherstellung der Verfügbarkeit des IT-Systems auch der Fortentwicklung der Informationstechnik berücksichtigen. Entsprechen eingesetzte Teile des IT-Systems nicht mehr dem Stand der Technik, so darf eine Ersatzbeschaffung nicht ausschließlich darauf gerichtet sein, den alten Zustand wiederherzustellen. Dies erfordert eine regelmäßige Überarbeitung des Ersatzbeschaffungsplans (siehe auch M 2.2 *Betriebsmittelverwaltung*).

In einem Ersatzbeschaffungsplan sollte auch festgehalten werden, für welche Arten von IT-Systemen eine schnellstmögliche Ersatzbeschaffung unerlässlich ist, eine mittelfristige ausreicht oder evtl. gar keine erforderlich ist. Nicht bei jedem Ausfall eines IT-Systems oder einer IT-Komponente ist eine kostenträchtige Neubeschaffung notwendig. Wenn beispielweise ein PC in einem LAN mit einer Vielzahl gleichartiger Clients ausfällt, kann im allgemeinen kurzfristig auf andere, ähnliche Endgeräte zurückgegriffen werden. Mittelfristig können evtl. vorhandene Ersatzteile eingebaut werden. Fällt hingegen ein zentraler Router aus, muss so schnell wie möglich für Ersatz gesorgt werden, da hier meistens die gesamte Organisation betroffen ist.

Bei Bedarf: Ersatzsysteme vor Ort

Es kann Geschäftsprozesse geben, die als so kritisch für die Organisation angesehen werden, dass für alle hierfür eingesetzten IT-Systeme Ersatzsysteme vor Ort vorrätig gehalten werden. Dann sollten diese nicht in denselben Gebäudeteilen, also z. B. Serverraum oder Rechenzentrum, aufbewahrt werden, sondern zumindest in einem anderen Brandabschnitt.

Ergänzende Kontrollfragen:

- In welchem Turnus wird der Ersatzbeschaffungsplan überarbeitet?
- Wird der Ersatzbeschaffungsplan bei Änderungen überarbeitet?

M 6.15 Lieferantenvereinbarungen

Verantwortlich für Initiierung: Leiter IT, Leiter Beschaffung

Verantwortlich für Umsetzung: Leiter Beschaffung

Bei Kauf von Informationstechnik ergibt sich für den IT-Betreiber die Notwendigkeit, Ersatzbeschaffungsmaßnahmen zu planen. Von besonderer Bedeutung beim Kauf ist eine vom Hersteller oder Lieferanten zugesicherte Nachkaufgarantie, Ersatzteillieferung, garantierte Lieferzeiten, die Garantiezeit bei auftretenden Mängeln sowie der angebotene Support.

Miet- bzw. Leasingverträge müssen Regelungen über schadensvorbeugende Wartungsarbeiten und die Anforderungen an die Beseitigung von Störungen oder Schäden beinhalten.

Im Gegensatz zum Kauf von Informationstechnik ist bei deren Miete oder Leasing eine Vielzahl von Risiken über den Vermieter bereits abgesichert. In der Regel schließt ein Vermieter eine Feuerversicherung für die vermietete Informationstechnik ab, die vom Mieter durch den Mietvertrag mitbezahlt wird. Somit ist bei Miete oder Leasing von Informationstechnik auf die nicht vom Vertrag abgedeckten Versicherungslücken zu achten.

Ergänzende Kontrollfrage:

- Gibt es für zentrale IT-Komponenten Lieferantenvereinbarungen?

M 6.16 Abschließen von Versicherungen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Behörden-/Unternehmensleitung

Für Bundesbehörden ist der Abschluss von Versicherungen unüblich.

Die auch bei hinreichender Notfallplanung nicht auszuschließenden Restrisiken lassen sich teilweise durch Versicherungen abdecken. Die Versicherungsarten lassen sich gliedern in:

- Sachversicherungen
  - Feuerversicherung
  - Leitungswasserversicherung
  - Einbruchdiebstahlversicherung
  - Montage-/Demontage-Versicherung
  - Transportversicherung
  - Datenträgerversicherung
  - Elektronik-Versicherung
- Folgekostenversicherungen
  - Feuer-Betriebsunterbrechungs-Versicherung
  - Maschinen-Betriebsunterbrechungs-Versicherung
  - Mehrkostenversicherung
  - Elektronik-Betriebsunterbrechungs-Versicherung
- Personenbezogene Versicherungen
  - Vertrauensschadenversicherung
  - Computer-Missbrauch-Versicherung
  - Datenschutzversicherung

Ergänzende Kontrollfrage:

Wurden für die Restrisiken ausreichende Versicherungen abgeschlossen?

M 6.17 Alarmierungsplan und Brandschutzübungen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Brandschutzbeauftragter

Verantwortlich für Umsetzung: Brandschutzbeauftragter

Es ist erforderlich, Pläne für die im Brandfall zu ergreifenden Maßnahmen zu erstellen. In einem solchen Plan ist z. B. niederzulegen,

- welche Maßnahmen bei welchen Ereignissen zu treffen sind,
- ob und wie Gebäudeteile evtl. zu räumen sind (Personen und Geräte),
- wer zu informieren ist und
- welche hilfeleistenden Kräfte zu informieren sind.

Ergänzt werden kann der Alarmierungsplan um Verhaltensregeln für den Brandfall, die allen Mitarbeitern bekannt zu geben sind. Dazu siehe auch Baustein B 1.3 *Notfallvorsorge-Konzept*.

Der beste Alarmierungsplan nützt allerdings wenig, wenn nicht sichergestellt ist, dass die darin aufgelisteten Maßnahmen richtig und praktikabel sind. Es ist also erforderlich, den Alarmplan regelmäßig zu prüfen und zu aktualisieren. Eine dieser Prüfungsmaßnahmen ist die Durchführung von Brandschutzübungen.

Beispiel:

Eine im Herbst 1993 in einem 21-geschossigen Bonner Bürogebäude durchgeführte Brandschutzübung hat gezeigt, dass viele Mitarbeiter nicht wussten, wo ein Feuerlöscher oder wo das Treppenhaus ist. Im Ernstfall kann diese Unkenntnis zu einer Katastrophe führen. Teilweise wurde die Übung ignoriert, man verließ aus Bequemlichkeit den Raum nicht.

Gerade in Brandschutzübungen soll das richtige Verhalten im Brandfall geschult und geübt werden, um Menschenleben zu schützen und Schäden u. a. für die IT zu vermeiden. Die Durchführung solcher Übungen ist vorher mit der Behörden- bzw. Unternehmensleitung abzustimmen.

Ergänzende Kontrollfrage:

- Welche Resultate ergab die letzte Brandschutzübung?

M 6.18 Redundante Leitungsführung

Verantwortlich für Initiierung: Leiter IT, Verantwortliche der einzelnen IT-Anwendungen

Verantwortlich für Umsetzung: Haustechnik, Administrator

Bei der redundanten Leitungsführung werden zwischen geeigneten Punkten im Netz neben den im normalen Betrieb genutzten Leitungen zusätzliche Verbindungen eingerichtet. Diese sollten über eine andere Trasse geführt werden. Dadurch besteht die Möglichkeit, bei Störungen auf die redundante Verbindung umzuschalten. Diese Umschaltung kann automatisch oder von Hand erfolgen. Die automatische Umschaltung ist an einer Stelle anzuzeigen, die die Störungsbeseitigung auf der normalen Leitung veranlasst.

Die Funktionsfähigkeit von redundanten Leitungen ist in sinnvollen Zeitabständen durch tatsächliche Nutzung auf ihre Funktionsfähigkeit hin zu überprüfen. Die Dimensionierung, die Prüfintervalle und die grundsätzliche Notwendigkeit von redundanten Leitungen ist direkt von der Verfügbarkeitsanforderung an das Netz abhängig. Ebenso muss man das Verhältnis der Bereitstellungszeit der redundanten Leitung zur Wiederherstellungszeit der normalen Leitung berücksichtigen. Es ist allerdings von entscheidender Bedeutung, ob es sich um Leitungen im öffentlichen Bereich (z. B. Telekom) oder im privaten Bereich handelt.

- Bei Leitungen im öffentlichen Bereich hat der Benutzer keinen Einfluss auf deren Schutz. Das öffentliche Netz stellt grundsätzlich eine ausreichende Zahl von redundanten Leitungen zur Verfügung. Meistens reicht es aus, bei Ausfall einer Verbindung (gleichgültig ob Festverbindung oder Wählleitung) durch Aufbau einer Wählleitung die Verbindung wiederherzustellen. Die Schaltung von redundanten Festverbindungen ist in der Regel zu teuer und meistens verzichtbar.
- In einem privaten Netz kann der Betreiber die Sicherheit von Leitungen wesentlich beeinflussen. Kostenüberlegungen führen meist dazu, dass es keine redundanten Leitungen gibt. In privaten Netzen verursachen redundante Leitungen jedoch außer den Herstellungskosten keine laufenden Ausgaben.

M 6.19 Datensicherung am PC

ist mit der Version 2006 entfallen

M 6.19 Datensicherung am PC

Diese Maßnahme ist mit Version 2005 entfallen.

M 6.20 Geeignete Aufbewahrung der Backup-Datenträger

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Backup-Datenträger unterliegen besonderen Anforderungen hinsichtlich ihrer Aufbewahrung:

- Der Zugriff auf diese Datenträger darf nur befugten Personen möglich sein, so dass eine Entwendung ausgeschlossen werden kann.
- Ein ausreichend schneller Zugriff muss im Bedarfsfall gewährleistet sein.
- Der Aufbewahrungsort muss auch die klimatischen Bedingungen für eine längerfristige Aufbewahrung von Datenträgern gewährleisten.
- Für den Katastrophenfall müssen die Backup-Datenträger räumlich getrennt vom Rechner aufbewahrt werden, wenn möglich in einem anderen Brandabschnitt.

Zu beachten sind auch die Anforderungen aus M 2.3 *Datenträgerverwaltung*.

Ergänzende Kontrollfrage:

- Wo werden die Datenträger der Datensicherung eines jeden Rechners aufbewahrt?
- Erfüllt der Aufbewahrungsort neben den geforderten Zugriffsmöglichkeiten auch die klimatischen Bedingungen für eine längerfristige Aufbewahrung von Datenträgern?

M 6.21 Sicherungskopie der eingesetzten Software

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Von den Originaldatenträgern erworbener Software bzw. von der Originalsoftware bei Eigenentwicklungen ist eine Sicherungskopie zu erstellen, von der bei Bedarf die Software wieder eingespielt werden kann. Die Originaldatenträger und die Sicherungskopien sind getrennt voneinander aufzubewahren. Es ist darauf zu achten, dass der physikalische Schreibschutz des Datenträgers ein versehentliches Löschen oder Überschreiben der Daten verhindert.

Wird die Software auf CD-ROM zur Verfügung gestellt, sollte alternativ nach der Installation von der CD-ROM eine Sicherungskopie der installierten Software erstellt werden, da der Datenumfang auf der CD-ROM i. allg. zu umfangreich ist.

Ein unerlaubter Zugriff, z. B. zur Erstellung einer Raubkopie, muss ausgeschlossen sein.

Ergänzende Kontrollfragen:

- Sind Sicherungskopien der eingesetzten Software angefertigt worden?
- Ist die Aufbewahrung der Datenträger ausreichend sicher?

M 6.22 Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Für die Rekonstruktion eines Datenbestandes muss geprüft werden, ob mit den vorhandenen Sicherungskopien der Daten ein solches Vorhaben durchgeführt werden kann. Durch technische Defekte, falsche Parametrisierung, einer schlichten Überalterung der Medien, einer unzureichenden Datenträgerverwaltung oder der Nichteinhaltung von Regeln, die in einem Datensicherungskonzept gefordert werden, ist es möglich, dass eine Rekonstruktion eines Datenbestandes nicht möglich ist. Daher ist es notwendig, dass sporadisch überprüft wird, ob die erzeugten Datensicherungen zur Wiederherstellung verlorener Daten genutzt werden können.

Ergänzende Kontrollfrage:

- Wann wurde zuletzt überprüft, ob die gesicherten Daten rekonstruiert werden können?

M 6.23 Verhaltensregeln bei Auftreten eines Computer-Virus

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Wenn ein Rechner von einem Computer-Virus befallen ist, sollte das Anti-Viren-Programm dies anzeigen. Dafür muss es natürlich auf dem aktuellsten Stand sein. Anzeichen für einen Virenbefall können außerdem unerklärliches Systemverhalten, unerklärlicher Ressourcenverbrauch oder unerwartete Netz-Zugriffe sein.

Anti-Viren-Programme können erkannte Infektionen automatisch entfernen. Dabei werden infizierte Dateien (Wirtsdateien) bereinigt, d. h. der originale Dateizustand wird wieder hergestellt. Eigenständige Schadprogramme können vom Anti-Viren-Programm gelöscht werden. Alternativ werden die infizierten Dateien in Quarantäne gestellt.

Benutzer sollten vor allem folgende Punkte beachten:

1. Ruhe bewahren!
2. Falls möglich, holen Sie einen fachkundigen PC-Betreuer zur Hilfe.
3. Beenden Sie die laufenden Programme.

Die weiteren Schritte sollte möglichst ein Administrator durchführen.

- Booten Sie den Rechner von einem virenfreien, schreibgeschützten Datenträger. Hierzu können Sie eine System- bzw. Boot-Diskette benutzen (die Notfalldiskette, siehe M 6.24 *Erstellen eines Notfall-Bootmediums*). Alternativ kann auch von einer aktuell erstellten, virenfreien, bootfähigen CD-ROM oder einem USB-Stick gebootet werden. Hierzu kann beispielsweise Knoppix verwendet werden, eine komplett von CD-ROM lauffähige Zusammenstellung von GNU/Linux-Software (siehe www.knoppix.org).

  Eventuell muss vorher noch die Boot-Reihenfolge im CMOS-Setup geändert werden (siehe M 4.84 *Nutzung der BIOS-Sicherheitsmechanismen*).
- Überprüfen Sie den Rechner mit einem aktuellen Anti-Viren-Programm um festzustellen, ob tatsächlich ein Computer-Virus aufgetreten ist und um welchen Computer-Virus es sich handelt. Dabei sollte ein Protokoll erstellt werden.
- Führen Sie eine Datensicherung durch, aber überschreiben Sie keine aktuelle Datensicherung.
- Entfernen Sie den Virus und überprüfen Sie mit dem Anti-Viren-Programm die Festplatte erneut.
- Untersuchen Sie alle anderen Datenträger (Disketten, Wechselplatten) auf Virenbefall und entfernen Sie die Computer-Viren.
- Warnen Sie andere IT-Benutzer, wenn ein Datenaustausch mit dem infizierten Rechner erfolgte.

Windows-Betriebssysteme haben Schutzmechanismen, die eine Desinfektion des Systems verhindern können. Zur Entfernung der Infektion müssen diese Schutzmechanismen zunächst deaktiviert werden. Daher sollten folgende Schritte durchlaufen werden:

- Deaktivieren Sie die Windows Systemwiederherstellung.
- Starten Sie den. Computer im abgesicherten Modus neu (mit Administratorberechtigung), damit das zuvor aktualisierte Anti-Viren-Programm Zugriff auf normalerweise geschützte Dateien und Systembereiche hat.
- Entfernen Sie die Infektion mit dem Anti-Viren-Programm.
- Starten Sie das System wieder mit voller Funktionalität.
- Überprüfen Sie den Rechner zur Kontrolle erneut auf Virenbefall.
- Aktivieren Sie die Systemwiederherstellung wieder.

Hinweis: Nachdem alle Schadprogramme entfernt worden sind, sollten alle von diesem Rechner aus genutzten Zugangskennungen und Passwörter geändert werden, um Missbrauch vorzubeugen.

Sollte der Computer-Virus Daten gelöscht oder verändert haben, versuchen Sie, die Daten aus den Datensicherungen (siehe M 6.32 *Regelmäßige Datensicherung*) und die Programme aus den Sicherungskopien der Programme (siehe M 6.21 *Sicherungskopie der eingesetzten Software*) zu rekonstruieren.

Ergänzende Kontrollfragen:

- Sind diese Verhaltensregeln allen Mitarbeitern bekanntgegeben worden?
- Gibt es fachkundige Personen, die im Bedarfsfall die oben genannten Schritte durchführen können?

M 6.24 Erstellen eines Notfall-Bootmediums

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Bei der Einrichtung eines Rechners sollte ein Bootmedium erstellt werden, das bei Ausfall einer Festplatte zum Starten des Systems oder bei Auftreten eines Computer-Virus zum Erzeugen eines kontrollierten Systemzustands genutzt werden kann. Solche Medien können beispielsweise "Notfalldisketten" oder CDs sein, deren Erstellung das jeweilige Betriebssystem eventuell anbietet, es können aber auch eigens eingerichtete CDs oder portable Laufwerke (beispielsweise USB-Sticks oder externe Festplatten mit USB- oder Firewire-Schnittstelle) erstellt werden. Art und Umfang des Notfall-Bootmediums richten sich nach dem Einsatzzweck des Rechners und den vorhandenen Schnittstellen.

Das Notfall-Bootmedium sollte idealerweise alle notwendigen Programme und Daten enthalten, die im Falle von Problemen wie

- Datenverlust durch Fehlbedienung,
- Bedienungs- und Administrationsfehlern, die die Benutzung und einen Neustart verhindern,
- Infektion des Systems mit Schadsoftware (beispielsweise Computerviren),
- Kompromittierung des Systems durch einen Angreifer, oder auch
- Hardwareproblemen

zu einer Untersuchung und falls möglich der Behebung der Probleme benötigt werden. Gegebenenfalls können unterschiedliche Medien für verschiedene Problemszenarien erstellt werden, die jeweils nur einen Teil dieser Szenarien abdecken.

Grundausstattung für ein Notfall-Bootmedium

Als "Grundausstattung" werden folgende Programme empfohlen:

- Virenscanner mit aktuellen Signaturen,
- Programme zur Bearbeitung von Systemkonfigurationsdateien oder -datenbanken (Dateieditor, Registryeditor oder ähnliche)
- Programm zur Wiederherstellung des Bootsektors der Systemplatte
- Backup- / Recoveryprogramme,
- Diagnoseprogramme zur Analyse von Hardwaredefekten,

sowie eventuell Programme zur weitergehenden Analyse, etwa zur Entdeckung von Rootkits oder zur forensischen Analyse eines kompromittierten Systems.

Dabei ist es wichtig, dass alle Programme und Bibliotheken ausschließlich vom Bootmedium geladen werden. Es dürfen keine Komponenten des installierten Systems verwendet werden.

Auch alle Treiber berücksichtigen!

Bei der Erstellung des Bootmediums ist außerdem darauf zu achten, dass neben den notwendigen Programmen auch alle Treiber vorhanden sind, die für den Zugriff auf die eingebauten Platten des Rechners benötigt werden. Dazu zählen beispielsweise Treiber für Festplattencontroller (insbesondere RAID-Controller) und Treiber für eine Festplattenverschlüsselung oder Festplattenkomprimierung.

Falls das Bootmedium genügend Speicherplatz bietet, so können weitere Programme oder Dokumentation auf dem Medium gespeichert werden. Beispielsweise kann es die Effizienz der Fehlersuche erhöhen, wenn auf dem Bootmedium stets eine aktuelle Dokumentation der Systemkonfiguration enthalten ist.

Das Notfall-Bootmedium muss selbst frei von Viren und anderen Schadprogrammen sein. Die eingesetzten Programmversionen sollten daher nur aus vertrauenswürdigen Quellen (etwa direkt von der CD des Herstellers) oder nach Überprüfung vorhandener digitaler Signaturen verwendet werden.

Es ist nicht unbedingt notwendig, für jedes System ein eigenes Bootmedium zu erstellen. Ein entsprechend flexibel angelegtes Bootmedium kann für eine große Anzahl verschiedener Systeme ausreichend sein. Auf dem Bootmedium braucht nicht einmal notwendigerweise das selbe Betriebssystem eingesetzt zu werden, wie auf dem Zielsystem selbst. Aus Gründen der Kompatibilität ist dies jedoch oft vorteilhaft. Es muss jedoch unbedingt durch entsprechende Tests sichergestellt werden, dass das Medium auch wirklich bei allen Rechnern funktioniert, für die es eingesetzt werden soll. Je nach Betriebssystem müssen außerdem noch systemspezifische Aspekte beachtet werden, die in den jeweiligen Bausteinen beschrieben werden.

Bootmedium aktualisieren

Nach Veränderungen am Zielsystem, etwa einem Update des Betriebssystems oder Konfigurationsänderungen muss gegebenenfalls das Notfall-Bootmedium und die darauf gespeicherte Dokumentation aktualisiert werden. Änderungen am Bootmedium müssen dokumentiert werden.

Das Notfall-Bootmedium muss für die Systembetreuer schnell greifbar sein, damit im Falle einer Störung nicht wertvolle Zeit verloren geht. Andererseits muss es auch so sicher aufbewahrt werden, dass Unbefugte keinen Zugriff darauf haben.

Notfall-Bootmedium testen!

Die Funktion des Notfall-Bootmediums sollte regelmäßig getestet und die Bedienung der darauf gespeicherten Programme geübt werden, damit sichergestellt ist, dass das Medium im Fall von Problemen funktioniert und die Administratoren mit der Bedienung vertraut sind. Es ist empfehlenswert, mit dem Medium eine Art "Kurzanleitung" in gedruckter Form aufzubewahren, die für typische Einsatzszenarien die wichtigsten Schritte zusammenfasst.

Ergänzende Kontrollfragen:

- Wurde für jeden eingesetzten Rechnertyp bzw. jede Betriebssystem-Version ein Notfall-Bootmedium erstellt?
- Wo wird dieses Medium aufbewahrt? Ist der schnelle Zugriff für die Administratoren sichergestellt?
- Wird die Funktion des Notfall-Bootmediums regelmäßig getestet?

M 6.25 Regelmäßige Datensicherung der Server-Festplatte

Diese Maßnahme ist mit Version 2005 entfallen.

M 6.26 Regelmäßige Datensicherung der TK-Anlagen-Konfigurationsdaten

Verantwortlich für Initiierung: TK-Anlagen-Verantwortlicher

Verantwortlich für Umsetzung: Administrator

Die in der TK-Anlage gespeicherten Daten sind in regelmäßigen Abständen zu sichern. Dies kann mit Hilfe eines anlageninternen oder -externen Bandlaufwerkes geschehen. Der Sicherungszyklus hängt dabei stark von der Anzahl der durchgeführten Administrationsvorgänge ab. Als ein Beispiel für einen sinnvollen Wert kann eine Datensicherung nach ca. 50 Administrationsvorgängen angenommen werden. Legt man den durchaus üblichen Wert von einer Veränderung pro Teilnehmer und Jahr zugrunde, so ergibt sich hieraus bei 600 Teilnehmern ein Datensicherungszyklus von einem Monat. Neben diesen regelmäßigen Datensicherungen sollte nach grundlegenden Änderungen ebenfalls eine Datensicherung erfolgen.

Ergänzende Kontrollfragen:

- Wird eine regelmäßige Datensicherung durchgeführt?
- Kann die TK-Anlage mit den Datensicherungsbeständen ordnungsgemäß hochgefahren werden?
- Wurden entsprechende Tests schon einmal durchgeführt?
- Werden die Sicherungsbänder sicher aufbewahrt?

M 6.27 Sicheres Update des BIOS

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator, Benutzer

Basic Input Output System

Viele IT-Systeme, beispielsweise PCs, benötigen für den Start bzw. für den Betrieb ein *Basic Input Output System* (BIOS). Dieses BIOS setzt sich aus Programmcode und Daten zusammen und dient dazu, wichtige Konfigurationseinstellungen am IT-System vorzunehmen und elementare Ein-/Ausgabe-Funktionen bereitzustellen. In vielen Fällen wird mit diesen Funktionen das eigentliche Betriebssystem geladen, das dann entweder selbst die Kontrolle über die Hardware übernimmt oder weiterhin auf BIOS-Funktionen zurückgreift. Gespeichert wird das BIOS meist in speziellen Speicherbausteinen (z. B. EEPROM oder Flash-EPROM), deren Inhalt auch beim Abschalten der Stromversorgung erhalten bleibt.

BIOS kann Fehler enthalten

Insbesondere bei PCs hat die Vielfalt der Konfigurationsmöglichkeiten dazu geführt, dass das BIOS sehr komplex und damit auch fehleranfälliger geworden ist. Viele Hersteller sind daher dazu übergegangen, einen Update-Mechanismus für das BIOS zu implementieren und regelmäßig fehlerbereinigte Versionen des BIOS zur Verfügung zu stellen. Zur Durchführung des BIOS-Updates bietet der Hersteller meist auch ein spezielles Programm an, mit dem der Inhalt der entsprechenden Speicherbausteine überschrieben werden kann.

Grundsätzlich sollte der Update-Mechanismus für das BIOS genutzt werden, um IT-Systeme mit möglichst fehlerfreien BIOS-Versionen auszustatten. Dabei sind jedoch folgende Hinweise zu beachten:

altes BIOS sichern

- Als erstes sollte vom derzeit installierten BIOS eine Datensicherung durchgeführt werden. Hierzu bietet die vom Hersteller angebotene Software in der Regel die Möglichkeit, das installierte BIOS auszulesen und als Datei abzuspeichern. Falls sich nach dem BIOS-Update Probleme ergeben, kann diese BIOS-Version wiederhergestellt werden.

bei zentralen Systemen BIOS archivieren

- Bei zentralen IT-Systemen, beispielsweise Servern, Netzkoppelelementen und TK-Anlagen, sollten die jeweils aktuell verwendete und die davor letzte funktionsfähige BIOS-Version archiviert werden. Dabei ist darauf zu achten, dass die Datei eindeutig dem jeweiligen IT-System zugeordnet werden kann.

wichtige Einstellungen dokumentieren

- In vielen Fällen hat ein BIOS-Update Einfluss auf die gespeicherten Konfigurationsdaten. Unter Umständen werden dabei alle vorgenommenen Einstellungen auf Standardwerte zurückgesetzt und gehen somit verloren. Ein modernes BIOS für PCs ist zwar in der Lage, viele Konfigurationsdaten selbst zu ermitteln ("Auto Detect"), insbesondere bei spezielleren Geräten kann es jedoch erforderlich sein, die vorgenommenen Einstellungen vor dem BIOS-Update zu dokumentieren. Hierzu sollten die Empfehlungen des Herstellers beachtet werden.

- BIOS-Updates und Software zum Einspielen von BIOS-Updates werden vom Hersteller oft im Internet zur Verfügung gestellt. Es ist darauf zu achten, dass beides nur vom Hersteller selbst oder von offiziellen Spiegelservern bezogen wird. Im Zweifelsfall sollte beim Hersteller nachgefragt werden, ob eine bestimmte im Internet bereitgestellte Version tatsächlich vom Hersteller freigegeben wurde.

BIOS-Update aus vertrauenswürdiger Quelle beziehen

- Inkompatibilitäten oder beschädigten Dateien können dazu führen, dass ein IT-System nach einem BIOS-Update nicht mehr funktioniert. Oft ist es nicht einmal mehr möglich, die vorhergehende, funktionsfähige BIOS-Version wiederherzustellen. In der Regel kann dann nur noch der Händler oder der Hersteller das Gerät wieder betriebsbereit machen, und das IT-System steht u. U. längere Zeit nicht zur Verfügung. Daher muss vor dem BIOS-Update sichergestellt werden, dass eine geeignete Ausweichlösung (z. B. ein Ersatzgerät) zur Verfügung steht, falls ein solcher Ausfall nicht toleriert werden kann.

ggf. Ausweichlösung bereithalten

- Neue BIOS-Versionen sollten vor dem Einsatz möglichst getestet werden. Möglich ist dies jedoch nur, wenn mehrere IT-Systeme vorhanden sind, die alle mit dem gleichen BIOS arbeiten. In diesem Fall sollte die neue BIOS-Version zunächst nur auf einem dieser IT-Systeme installiert und dieses Gerät einige Zeit im Betrieb beobachtet werden. Wenn sich dabei keine Probleme zeigen, können die übrigen IT-Systeme nachgezogen werden.

neue BIOS-Version möglichst testen

- Einige Hersteller empfehlen für ihre Geräte nicht einfach die neueste BIOS-Version. Stattdessen gibt es Tabellen, in denen abhängig von Einsatzszenario oder Modellnummer des IT-Systems eine bestimmte BIOS-Version empfohlen wird. Dies betrifft hauptsächlich Netzkoppelelemente. Die Empfehlungen des Herstellers sollten beachtet werden.

Ergänzende Kontrollfragen:

- Wird die vorhandene BIOS-Version vor dem Update gesichert?
- Werden BIOS-Updates ausschließlich aus vertrauenswürdigen Quellen bezogen?
- Werden die Empfehlungen des Herstellers für das BIOS-Update beachtet?

Titel und Inhalt dieser Maßnahme wurden geändert. Das "Sichern des CMOS-RAM", insbesondere der Festplattengeometrie, ist in der Regel nicht mehr erforderlich, weil nahezu alle modernen Festplatten einen entsprechenden Auto-Konfigurationsmechanismus unterstützen.

M 6.28 Vereinbarung über Lieferzeiten "lebensnotwendiger" TK-Baugruppen

Verantwortlich für Initiierung: TK-Anlagen-Verantwortlicher

Verantwortlich für Umsetzung: TK-Anlagen-Verantwortlicher

Lebensnotwendige Baugruppen, wie zentrale Steuereinheiten, digitale Koppelfelder etc. sollten auch bei redundanter Auslegung in hinreichend kurzer Zeit lieferbar sein oder bevorratet werden. Redundante Baugruppen sollten ab und zu mit den aktiven ausgetauscht werden.

Ergänzende Kontrollfragen:

- Welche Ihrer Baugruppen sind "lebensnotwendig"?
- Sind diese redundant ausgelegt?
- Wird die Funktionsfähigkeit der Reservebaugruppen regelmäßig überprüft?
- Wie lang sind die Lieferzeiten für die lebensnotwendigen Baugruppen?

M 6.29 TK-Basisanschluss für Notrufe

Verantwortlich für Initiierung: TK-Anlagen-Verantwortlicher

Verantwortlich für Umsetzung: Administrator

Bei einem Total- oder Teilausfall der TK-Anlage kann es geschehen, dass über die an diese Anlage angeschlossenen Amtsleitungen keine Verbindungen mehr möglich sind. Um dennoch Hilfe heranholen zu können, ist es sinnvoll, einen völlig separaten Basis-Anschluss bzw. analogen Fernsprechanschluss einzurichten.

Ergänzende Kontrollfragen:

- Wie können Notrufe weitergegeben werden, wenn die TK-Anlage ausgefallen ist?

M 6.30 Katastrophenschaltung

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Notfall-Verantwortliche, TK-Anlagen-Verantwortlicher

Verantwortlich für Umsetzung: Administrator

Um in Ausnahmesituationen zur Einleitung von Maßnahmen Telefonleitungen verfügbar zu haben, bieten einige TK-Anlagen die Möglichkeit, in einer sog. Katastrophenschaltung die vorhandenen kommenden und gehenden Leitungen vorher festgelegten Anschlüssen zuzuweisen. Dies gewährleistet, dass in einem Katastrophenfall wichtige Einrichtungen handlungsfähig bleiben. Steht diese Möglichkeit zur Verfügung, sollte sie genutzt werden.

Ergänzende Kontrollfragen:

- Wird die Zuordnung der Leitungen für die Katastrophenschaltung aktualisiert?
- Wird im Notfall-Handbuch festgelegt, wann die Katastrophenschaltung auszulösen ist?
- Wird die Nutzung der Leitungen im Notfall-Handbuch benannt?

M 6.31 Verhaltensregeln nach Verlust der Systemintegrität

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator, Benutzer

missbräuchliche Nutzung

Falls sich das Unix-System in nicht vorgesehener Weise verhält (zum Beispiel undefiniertes Systemverhalten, nicht auffindbare Daten, veränderte Dateiinhalte, ständige Verringerung des freien Speicherplatzes, ohne dass etwas abgespeichert wurde), kann ein Verlust der Systemintegrität vorliegen. Dieser kann durch missbräuchliche Nutzung des Systems verursacht worden sein, zum Beispiel durch Veränderungen der Systemeinstellungen, Einspielen eines Trojanisches Pferdes oder eines Computer-Virus.

Dann sollten die Benutzer folgende Punkte beachten:

Keine Panik!

- Ruhe bewahren!
- Benachrichtigen Sie den Administrator.
- Beenden Sie laufende Programme.

Der Administrator sollte folgende Schritte durchführen:

- Herunterfahren des Systems,
- Hochfahren des Systems, so dass nur Zugriff von der Konsole aus möglich ist (z. B. Single-User-Modus),
- **vollständige Datensicherung**

  Anfertigung einer Komplettdatensicherung (Dies ist beispielsweise hilfreich, wenn bei der nachfolgenden Untersuchung Daten oder Spuren zerstört werden.),
- **ausführbare Dateien prüfen**

  Überprüfung der ausführbaren Dateien auf sichtbare Veränderungen, z. B. Erstellungsdatum und Dateigröße (Da diese von einem Angreifer auch wieder auf ihre Ursprungswerte zurückgesetzt werden können, sollte die Integrität der Dateien mit Prüfsummenverfahren wie *tripwire* überprüft werden.),
- **Originaldateien wieder einspielen**

  Löschen der ausführbaren Dateien und Wiedereinspielen der Original-Dateien von schreibgeschützten Datenträgern (siehe M 6.21 *Sicherungskopie der eingesetzten Software*) (keine Programme aus der Datensicherung wiedereinspielen),
- Überprüfen und ggf. Wiedereinspielen der Systemverzeichnisse und -dateien und ihrer Attribute (z. B. */etc/inetd.conf*, */etc/hosts.equiv*, *cron*- und *at*-jobs, etc.),
- **Attribute prüfen**

  Überprüfung der Attribute aller Benutzerverzeichnisse und -dateien z. B. mit Prüfsummenverfahren wie *tripwire* und gegebenenfalls Zurücksetzen auf Minimal-Einstellungen (nur Rechte für den Eigentümer, keine *root*-Dateien in Benutzerbereichen, *.rhost*- und *.forward*-Dateien, auch gesperrte Accounts),
- Änderung aller Passwörter,
- Benachrichtigung der Benutzer mit der Bitte, ihre Bereiche auf Unregelmäßigkeiten zu prüfen.

neue Passwörter zufällig erzeugen

Nach der Änderung aller Passwörter müssen diese den betroffenen Benutzern mitgeteilt werden. Hierbei sollte **kein** allen Benutzern bekanntes Passwort oder Ableitungsschema benutzt werden. Besser ist es, die Passwörter zufällig zu erzeugen und den Benutzern auf zuverlässigem Weg mitzuteilen, z. B. in versiegelten Umschlägen. Diese Passwörter sollten unmittelbar nach der Erstanmeldung geändert werden.

Alarmplan heranziehen

Wenn Anzeichen auf einen vorsätzlichen Angriff gegen ein Unix-System vorliegen, ist für die Schadensminimierung und weitere Schadensabwehr sofortiges Handeln notwendig. Hierzu ist ein Alarmplan erforderlich, in dem die einzuleitenden Schritte aufgeführt werden und festgelegt wird, welche Personen über den Vorfall zu unterrichten sind (siehe auch M 6.60 *Verhaltensregeln und Meldewege bei Sicherheitsvorfällen*). Der Alarmplan enthält gegebenenfalls auch Informationen darüber, ob und wie der Datenschutzbeauftragte und die Rechtsabteilung zu beteiligen sind.

Falls sich Probleme ergeben, können Sie sich an die Hotline des BSI wenden unter Telefon 0228-9582-5222 oder E-Mail *certbund@bsi.bund.de*.

Falls Daten gelöscht oder unerwünscht geändert wurden, können diese aus den Datensicherungen wiedereingespielt werden.

Ergänzende Kontrollfragen:

- Werden die Benutzer regelmäßig darüber informiert, dass bei Auftreten von Unregelmäßigkeiten sofort der Administrator benachrichtigt werden muss?
- Wird diese Regelung auch angewendet?
- Gibt es Administratoren mit entsprechenden Kenntnissen?
- Ist ein Verfahren zur schnellen Vergabe von Passwörtern etabliert und getestet?

M 6.32 Regelmäßige Datensicherung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Zur Vermeidung von Datenverlusten müssen regelmäßige Datensicherungen durchgeführt werden. In den meisten Rechnersystemen können diese weitgehend automatisiert erfolgen. Es sind Regelungen zu treffen, welche Daten von wem wann gesichert werden.

Es müssen mindestens die Daten regelmäßig gesichert werden, die nicht aus anderen Informationen abgeleitet werden können. Dokumentationen, Programm- und Programmablaufbeschreibungen sind gemäß M 2.111 *Bereithalten von Handbüchern* vorzuhalten.

Empfehlenswert ist die Erstellung eines Datensicherungskonzepts.

Abhängig von der Menge und Wichtigkeit der laufend neu gespeicherten Daten und vom möglichen Schaden bei Verlust dieser Daten ist folgendes festzulegen:

- Zeitintervall

  Beispiele: täglich, wöchentlich, monatlich

- Zeitpunkt

  Beispiele: nachts, freitags abends

- Anzahl der aufzubewahrenden Generationen

  Beispiel: Bei täglicher Komplettsicherung werden die letzten sieben Sicherungen aufbewahrt, außerdem die Freitagabend-Sicherungen der letzten zwei Monate.

- Umfang der zu sichernden Daten

  Am einfachsten ist es, Partitionen bzw. Verzeichnisse festzulegen, die bei der regelmäßigen Datensicherung berücksichtigt werden. Eine geeignete Differenzierung kann die Übersichtlichkeit vergrößern sowie Aufwand und Kosten sparen helfen.

  Beispiel: selbsterstellte Dateien und individuelle Konfigurationsdateien

- Speichermedien (abhängig von der Datenmenge)

  Beispiele: Bänder, Kassetten, CDs oder DVDs, Festplatten

- Vorherige Löschung der Datenträger vor Wiederverwendung (z. B. bei Bändern oder Kassetten)

- Zuständigkeit für die Durchführung (Administrator, Benutzer)

- Zuständigkeit für die Überwachung der Sicherung, insbesondere bei automatischer Durchführung (Fehlermeldungen, verbleibender Platz auf den Speichermedien)

- Dokumentation der erstellten Sicherungen (Datum, Art der Durchführung der Sicherung sowie gewählte Parameter, Beschriftung der Datenträger)

inkrementelle Sicherung

Wegen des großen Aufwands können Komplettsicherungen in der Regel höchstens einmal täglich durchgeführt werden. Die seit der letzten Sicherung erstellten Daten können nicht wiedereingespielt werden. Daher und zur Senkung der Kosten sollten zwischen den Komplettsicherungen regelmäßig inkrementelle Sicherungen durchgeführt werden, das heißt, nur die seit der letzten Komplettsicherung neu erstellten Daten werden gesichert. (Werden zwischen zwei Komplettsicherungen mehrere inkrementelle Sicherungen durchgeführt, können auch jeweils nur die seit der letzten inkrementellen Sicherung neu erstellten Daten gesichert werden.)

Eine inkrementelle Sicherung kann häufiger erfolgen, zum Beispiel sofort nach Erstellung wichtiger Dateien oder mehrmals täglich. Die Vereinbarkeit mit dem laufenden Betrieb ist sicherzustellen.

Für eingesetzte Software ist separat zu entscheiden, ob sie von der regelmäßigen Datensicherung erfasst werden muss. Dies hängt beispielsweise davon ab, wie aufwendig eine Neuinstallation von den Originaldatenträgern und das Einspielen von Patches und Updates ist. Unter Umständen ist es ausreichend, Sicherungskopien von den Originaldatenträgern anzufertigen.

Es muss regelmäßig getestet werden, ob die Datensicherung auch wie gewünscht funktioniert, vor allem, ob gesicherte Daten problemlos zurückgespielt werden können.

Benutzer informieren

Alle Benutzer sollten über die Regelungen zur Datensicherung informiert sein, um gegebenenfalls auf Unzulänglichkeiten (zum Beispiel zu geringes Zeitintervall für ihren Bedarf) hinweisen oder individuelle Ergänzungen vornehmen zu können (zum Beispiel zwischenzeitliche Spiegelung wichtiger Daten auf der eigenen Platte). Auch die Information der Benutzer darüber, wie lange die Daten wiedereinspielbar sind, ist wichtig. Werden zum Beispiel bei wöchentlicher Komplettsicherung nur zwei Generationen aufbewahrt, bleiben in Abhängigkeit vom Zeitpunkt des Verlustes nur zwei bis drei Wochen Zeit, um die Wiedereinspielung vorzunehmen.

Falls bei vernetzten Rechnern nur die Server-Platten gesichert werden, ist sicherzustellen, dass die zu sichernden Daten regelmäßig von den Benutzern oder automatisch dorthin überspielt werden. Bei größeren Änderungen an IT-Systemen oder im IT-Verbund muss der Datensicherungsprozess entsprechend angepasst werden.

Verschlüsselung vertraulicher Daten

Vertrauliche Daten sollten vor der Sicherung möglichst verschlüsselt werden, wobei darauf zu achten ist, dass eine Entschlüsselung auch nach einem längeren Zeitraum möglich sein muss (siehe M 6.56 *Datensicherung bei Einsatz kryptographischer Verfahren*).

Der Ausdruck von Daten auf Papier ist keine angemessene Art der Datensicherung.

Ergänzende Kontrollfragen:

- Sind alle Daten eines Rechners gesichert?
- Wurde die Datensicherung getestet?
- Wird der Datensicherungsvorgang dokumentiert?

- Ist der Datensicherungsvorgang konform zu einem vorhandenen Datensicherungskonzept?
- Wird der Datensicherungsprozess bei größeren Änderungen des IT-Verbundes überprüft und falls notwendig auch angepasst?

M 6.33 Entwicklung eines Datensicherungskonzepts

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Leiter IT, Verantwortliche der einzelnen IT-Anwendungen

Die Verfahrensweise der Datensicherung wird von einer großen Zahl von Einflussfaktoren bestimmt. Das IT-System, das Datenvolumen, die Änderungsfrequenz der Daten und die Verfügbarkeitsanforderungen sind einige dieser Faktoren. Im Datensicherungskonzept gilt es, eine Lösung zu finden, die diese Faktoren berücksichtigt und gleichzeitig unter Kostengesichtspunkten wirtschaftlich vertretbar ist.

Die technischen Möglichkeiten, Datensicherungen durchzuführen, sind vielfältig. Jedoch wird die Auswahl immer von den genannten Faktoren bestimmt. Daher gilt es zunächst, die Einflussgrößen der IT-Systeme und der damit realisierten IT-Anwendungen zu bestimmen und nachvollziehbar zu dokumentieren. Anschließend muss die geeignete Verfahrensweise entwickelt und dokumentiert werden. Zum Abschluss muss durch die Behörden-/Unternehmensleitung die Durchführung angeordnet werden.

Das Datensicherungskonzept muss für die Gewährleistung einer funktionierenden Datensicherung die Datenrestaurierbarkeit mittels praktischer Übungen als Verpflichtung vorsehen (siehe M 6.41 *Übungen zur Datenrekonstruktion)*.

Die Ergebnisse sollten aktualisierbar und erweiterbar in einem Datensicherungskonzept niedergelegt werden. Ein möglicher Aufbau eines Datensicherungskonzepts ist im nachfolgenden Inhaltsverzeichnis beispielhaft aufgezeigt:

Inhaltsverzeichnis Datensicherungskonzept

1. Definitionen

- Anwendungsdaten, Systemdaten, Software, Protokolldaten
- Vollsicherung, inkrementelle Datensicherung

2. Gefährdungslage zur Motivation

- Abhängigkeit der Institution vom Datenbestand
- Typische Gefährdungen wie ungeschulte Benutzer, gemeinsam genutzte Datenbestände, Computer-Viren, Hacker, Stromausfall, Festplattenfehler
- Institutionsrelevante Schadensursachen
- Schadensfälle im eigenen Haus

3. Einflussfaktoren je IT-System

- Spezifikation der zu sichernden Daten
- Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten
- Rekonstruktionsaufwand der Daten ohne Datensicherung
- Datenvolumen

- Änderungsvolumen
- Änderungszeitpunkte der Daten
- Fristen
- Vertraulichkeitsbedarf der Daten
- Integritätsbedarf der Daten
- Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer

4. Datensicherungsplan je IT-System

4.1 Festlegungen je Datenart

- Art der Datensicherung
- Häufigkeit und Zeitpunkt der Datensicherung
- Anzahl der Generationen
- Datensicherungsmedium
- Verantwortlichkeit für die Datensicherung
- Aufbewahrungsort der Backup-Datenträger
- Anforderungen an das Datensicherungsarchiv
- Transportmodalitäten
- Rekonstruktionszeiten bei vorhandener Datensicherung

4.2 Festlegung der Vorgehensweise bei der Datenrestaurierung

4.3 Randbedingungen für das Datensicherungsarchiv

- Vertragsgestaltung (bei externen Archiven)
- Refresh-Zyklen der Datensicherung
- Bestandsverzeichnis
- Löschen von Datensicherungen
- Vernichtung von unbrauchbaren Datenträgern

4.4 Vorhalten von arbeitsfähigen Lesegeräten

5. Minimaldatensicherungskonzept

6. Verpflichtung der Mitarbeiter zur Datensicherung

7. Sporadische Restaurierungsübungen

Einzelne Punkte dieses Datensicherungskonzepts werden in den Maßnahmen M 6.34 *Erhebung der Einflussfaktoren der Datensicherung*, M 6.35 *Festlegung der Verfahrensweise für die Datensicherung*, M 6.37 *Dokumentation der Datensicherung*, M 6.41 *Übungen zur Datenrekonstruktion* und M 2.41 *Verpflichtung der Mitarbeiter zur Datensicherung* näher ausgeführt, so dass nach Bearbeitung dieser Maßnahmen für jedes relevante IT-System die

wesentlichen Teile eines anwenderspezifischen Datensicherungskonzepts erstellt sind.

Ergänzende Kontrollfragen:

- Ist für die Institution ein aktuelles Datensicherungskonzept dokumentiert?
- Sind sämtliche betroffenen IT-Systeme in diesem Konzept aufgeführt?
- Wie werden Mitarbeiter über den sie betreffenden Teil des Konzepts unterrichtet?
- Wird die Einhaltung dieses Konzepts kontrolliert?
- Wie werden Änderungen der Einflussfaktoren berücksichtigt?

M 6.34 Erhebung der Einflussfaktoren der Datensicherung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Verantwortliche der einzelnen IT-Anwendungen

Für jedes IT-System, eventuell sogar für einzelne IT-Anwendungen mit besonderer Bedeutung, müssen die nachfolgenden Einflussfaktoren ermittelt werden. Dazu können die Systemadministratoren und die Verantwortlichen der einzelnen IT-Anwendungen befragt werden. Die Ergebnisse sind nachvollziehbar zu dokumentieren.

Nachfolgend soll an einem fiktiven Beispiel aufgezeigt werden, wie die Ermittlung der Einflussfaktoren in der Praxis vollzogen werden kann. Das Beispiel geht von einem servergestützten LAN mit 10 angeschlossenen PCs als Workstations aus. Das IT-System dient der Auftragsbearbeitung mittels einer Kundendatenbank. Die Anwendungsdaten werden zentral auf dem Netzserver gespeichert.

Im einzelnen muss ermittelt werden:

Spezifikation der zu sichernden Daten

Ermittelt werden sollte der Datenbestand des IT-Systems (der IT-Anwendung), der für die Erledigung der Fachaufgaben erforderlich ist. Dazu gehören die Anwendungs- und Betriebssoftware, die Systemdaten (z. B. Initialisierungsdateien, Makrodefinitionen, Konfigurationsdaten, Textbausteine, Passwortdateien, Zugriffsrechtedateien), die Anwendungsdaten selbst und Protokolldaten (Login-Protokollierung, Protokolle über Sicherheitsverletzungen, Datenübertragungsprotokolle, ...).

Beispielergebnis 1: Spezifikation der zu sichernden Daten

IT-System: Servergestütztes LAN mit 10 angeschlossenen PCs

Zu sichernde Daten:

- Software:

  Netzbetriebssystem, Betriebssysteme der PCs, Textverarbeitungssoftware, Datenbank-Software etc. in Form von Standardsoftware

- Systemdaten:

  am Netz-Server: Systeminterne Einstellungen (z. B. Rechtestruktur, Passworte)

  an den PCs: Initialisierungsdateien der Textverarbeitungssoftware und der Datenbank-Software, Makrodefinitionen und Textbausteine

- Anwendungsdaten auf dem Netz-Server:

  Dateien mit Schriftverkehr, Kundendatenbank

- Protokolldaten auf dem Netz-Server:

  Protokollierung der Netzaktivitäten

Verfügbarkeitsanforderungen der IT-Anwendungen an die Daten

Für die im ersten Schritt spezifizierten Daten müssen nun die Verfügbarkeitsanforderungen festgelegt werden. Ein erprobtes Maß dazu ist die Angabe der maximal tolerierbaren Ausfallzeit (mtA). Sie gibt an, über welchen Zeitraum die Fachaufgabe ohne diese Daten weitergeführt werden kann, ohne dass auf Datensicherungsbestände zurückgegriffen werden muss. Betrachtet werden sollte dabei auch, ob aufgrund der Papierlage ohne IT-Unterstützung kurzfristig weitergearbeitet werden kann.

Beispielergebnis 2: Verfügbarkeitsanforderungen

- Software:

  mtA 1 Tag

- Systemdaten:

  am Netz-Server: mtA 1 Tag

  am PC: mtA 1 Woche (auf einen PC kann bis zu einer Woche verzichtet werden)

- Anwendungsdaten:

  Dateien mit Schriftverkehr: mtA 1 Woche

  Kundendatenbank: mtA 1 Tag

- Protokolldaten: mtA 3 Tage

Rekonstruktionsaufwand der Daten ohne Datensicherung

Um ein unter wirtschaftlichen Gesichtspunkten angemessenes Datensicherungskonzept zu entwickeln, ist es notwendig zu wissen, ob und mit welchem Aufwand zerstörte Datenbestände rekonstruiert werden können, wenn eine Datensicherung nicht zur Verfügung steht. Untersucht werden sollte, aus welchen Quellen die Daten rekonstruiert werden können. Beispiele hierfür sind die Aktenlage, Ausdrucke, Mikrofiche, Befragungen und Erhebungen.

Gemessen werden sollte der pekuniäre Aufwand oder der Arbeitsaufwand von Datenerfassungskräften in Arbeitstagen (AT).

Beispielergebnis 3: Rekonstruktionsaufwand

- Software:

  Wiederbeschaffung durch Kauf und anschließender Installation innerhalb eines Tages (sofern keine Originalsoftware mehr vorliegt)

- Systemdaten:

  am Netz-Server: manuelle Rekonstruktion: 1 AT

  am PC: 1 AT

- Anwendungsdaten:

Dateien mit Schriftverkehr: zielorientierte Erfassung aus aktueller Papierlage: 10 AT (eine vollständige Nacherfassung des Schriftverkehrs ist nicht erforderlich)

Kundendatenbank: Kompletterfassung aus Papierlage: 10 AT

- Protokolldaten:

  nicht rekonstruierbar, da kein Ausdruck auf Papier erfolgt

Datenvolumen

Für die Auswahl des Speichermediums ist ein entscheidender Faktor das gespeicherte und zu sichernde Datenvolumen. Die erforderliche Angabe richtet sich ausschließlich auf die zu sichernden Daten und sollte als Maßeinheit Megabyte (MB) benutzen.

Beispielergebnis 4: Datenvolumen

- Software:

  100 MB

- Systemdaten:

  am Netz-Server: 2 MB

  am PC: 0,3 MB

- Anwendungsdaten:

  Dateien mit Schriftverkehr: 100 MB

  Kundendatenbank: 10 MB

- Protokolldaten:

  10 MB (wöchentliche Kontrolle nebst Löschung)

Änderungsvolumen

Um die Häufigkeit der Datensicherung und das adäquate Sicherungsverfahren bestimmen zu können, muss bekannt sein, wieviele Daten/Dateien sich in einem bestimmten Zeitabschnitt ändern. Als Arbeitsgröße wäre hier eine Einheit MB/Woche denkbar. Notwendig sind Angaben, ob bestehende Dateien inhaltlich geändert oder ob neue Dateien erzeugt werden.

Beispielergebnis 5: Änderungsvolumen

- Software:

  durchschnittlich 50 MB bei einem Versionswechsel, höchstens einmal jährlich

- Systemdaten:

  am Netz-Server: 0,1 MB/Woche

  am PC: 0,1 MB/Woche

- Anwendungsdaten:

Dateien mit Schriftverkehr: 1 MB/Woche durch neue Dateien

Kundendatenbank: 10 MB/Woche durch Änderungen in der Datenbank (die Datenbank kann nur vollständig gesichert werden).

- Protokolldaten:

  10 MB/Woche

Änderungszeitpunkte der Daten

Es gibt IT-Anwendungen, bei denen sich Datenänderungen nur zu bestimmten Terminen ergeben, wie zum Beispiel der Abrechnungslauf zur Lohnbuchhaltung zum Monatsende. In solchen Fällen ist eine Datensicherung unverzüglich nach einem solchen Termin sinnvoll. Daher sollte für die zu sichernden Daten angegeben werden, ob sie sich täglich, wöchentlich oder zu bestimmten Terminen ändern.

Beispielergebnis 6: Änderungszeitpunkte

- Software:

  Änderungen nur bei einem Versionswechsel

- Systemdaten:

  häufige Änderungen

- Anwendungsdaten:

  Dateien mit Schriftverkehr: tägliche Änderungen

  Kundendatenbank: tägliche Änderungen

- Protokolldaten:

  ständige Änderung

Fristen

Für die Daten ist zu klären, ob bestimmte Fristen einzuhalten sind. Hierbei kann es sich um Aufbewahrungsfristen oder auch um Löschfristen im Zusammenhang mit personenbezogenen Daten handeln. Diese Fristen sind bei der Festlegung der Datensicherung zu berücksichtigen.

Beispielergebnis 7: Fristen

- Software:

  Aufbewahrung der Datensicherungsbestände ist nicht erforderlich

- Systemdaten:

  Aufbewahrung der Datensicherungsbestände ist nicht erforderlich

- Anwendungsdaten:

  Dateien mit Schriftverkehr: Aufbewahrungsfrist für Buchungsbelege beträgt sechs Jahre (§257 HGB); ein (Jahres-) Datensicherungsbestand ist für diese Zeit aufzuheben

Kundendatenbank: Aufbewahrung der Daten ist nicht erforderlich, Löschfristen sind gemäß BDSG (§20 bzw. § 35) zu beachten

- Protokolldaten:

  nach der wöchentlichen Auswertung der Protokolldaten müssen regelmäßig 2 MB der Daten für ein Jahr bzw. bis zur Prüfung durch den Datenschutzbeauftragten aufbewahrt werden

Vertraulichkeitsbedarf der Daten

Der Vertraulichkeitsbedarf einer Datei überträgt sich bei einer Datensicherung auf die Sicherungskopie. Bei der Zusammenführung von Sicherungskopien mit gleichem Vertraulichkeitsbedarf auf einem Datenträger, kann sich durch die Kumulation ein höherer Vertraulichkeitsbedarf der gespeicherten Daten ergeben. Anzugeben ist also, wie hoch der Vertraulichkeitsbedarf der einzelnen zu sichernden Daten ist und zusätzlich, welche Kombinationen von Daten einen höheren Vertraulichkeitsbedarf haben als die Daten selbst.

Beispielergebnis 8: Vertraulichkeitsbedarf

- Software:

  geringer Vertraulichkeitsbedarf, da es sich um öffentlich zugängliche Daten handelt, lediglich Copyright-Vereinbarungen sind zu beachten

- Systemdaten:

  am Netz-Server: mittel vertraulich (Passworte sind verschlüsselt gespeichert)

  am PC: nicht vertraulich

- Anwendungsdaten:

  Dateien mit Schriftverkehr: Einzeldateien besitzen mittleren Vertraulichkeitsbedarf, sämtliche Dateien zusammen einen hohen Vertraulichkeitsbedarf

  Kundendatenbank: hoher Vertraulichkeitsbedarf

- Protokolldaten:

  hoher Vertraulichkeitsbedarf (personenbezogene Daten, die ein Nutzungsprofil ermöglichen)

Integritätsbedarf der Daten

Für Datensicherungen muss sichergestellt sein, dass die Daten integer gespeichert wurden und während der Aufbewahrungszeit nicht verändert werden. Dies ist um so wichtiger, je höher der Integritätsbedarf der Nutzdaten ist. Daher ist für die Datensicherungen anzugeben, wie hoch der Integritätsbedarf ist.

Beispielergebnis 9: Integritätsbedarf

- Software:

  Die Software muss hohe Integritätsansprüche erfüllen.

- Systemdaten:

  am Netz-Server: hoher Integritätsbedarf (wegen Rechteverwaltung)

  am PC: hoher Integritätsanspruch

- Anwendungsdaten:

  Dateien mit Schriftverkehr: Einzeldateien besitzen einen mittleren Integritätsbedarf

  Kundendatenbank: hoher Integritätsbedarf

- Protokolldaten:

  Die Daten besitzen bis zur Auswertung einen hohen Integritätsbedarf, nach der Auswertung besitzen nur noch die aufzubewahrenden Daten einen mittleren Integritätsbedarf.

Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer

Um entscheiden zu können, wer die Datensicherung durchführt, der IT-Benutzer selbst oder speziell beauftragte Mitarbeiter bzw. die Systemadministratoren, ist ausschlaggebend, über welche Kenntnisse und datenverarbeitungsspezifischen Fähigkeiten der IT-Benutzer verfügt und welche Werkzeuge ihm zur Verfügung gestellt werden können. Falls die zeitliche Belastung bei der Durchführung einer Datensicherung für IT-Benutzer zu hoch ist, sollte dies angegeben werden.

Beispielergebnis 10: Kenntnisse

- Der Netzadministrator verfügt über ausreichende Kenntnisse, die Datensicherung am Netz-Server durchzuführen. Die IT-Benutzer des PCs verfügen über ausreichende Kenntnisse und Fähigkeiten, die Datensicherung der PC-Systemdaten selbständig durchzuführen.

Ergänzende Kontrollfragen:

- Wurden bei der Erhebung der Einflussfaktoren sowohl die Systemadministratoren als auch die IT-Anwender eingebunden?
- Wie werden diese Angaben aktualisiert?
- Werden neue Anforderungen rechtzeitig in einem aktualisierten Datensicherungskonzept berücksichtigt?

M 6.35 Festlegung der Verfahrensweise für die Datensicherung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, IT-Verfahrensverantwortlicher

Die Verfahrensweise, wie die Datensicherung durchzuführen ist, wird von den in M 6.34 *Erhebung der Einflussfaktoren der Datensicherung* erhobenen Einflussfaktoren bestimmt. Für jedes IT-System und für jede Datenart muss die Verfahrensweise der Datensicherung festgelegt werden. Bei Bedarf ist sogar noch eine Unterscheidung für einzelne IT-Anwendungen des IT-Systems vorzunehmen, wenn sich hier differente Datensicherungsstrategien ergeben, was insbesondere im Großrechnerbereich sinnvoll sein kann.

Folgende Modalitäten einer Datensicherung sind für die Festlegung einer Verfahrensweise für die Datensicherung zu betrachten:

- Art der Datensicherung,
- Häufigkeit und Zeitpunkt der Datensicherung,
- Anzahl der Generationen,
- Vorgehensweise und Speichermedium,
- Verantwortlichkeit für die Datensicherung,
- Aufbewahrungsort,
- Anforderungen an das Datensicherungsarchiv,
- Transportmodalitäten und
- Aufbewahrungsmodalität.

In der nachfolgenden Tabelle werden die Abhängigkeiten zwischen den Modalitäten einer Datensicherung und den Einflussfaktoren dargestellt und anschließend erläutert:

	Art der Datensicherung	Häufigkeit und Zeitpunkte der Datens.	Anzahl der Generationen	Vorgehensweise und Speichermedium	Verantwortlichkeit für Datens.	Aufbewahrungsort	Anforderungen an DS-Archiv	Transportmodalitäten	Aufbewahrungsmodalität
Verfügbarkeitsanforderungen	X	(X)	X	X	X	X	X	X	
Rekonstruktionsaufwand ohne Datens.		(X)	X						
Datenvolumen	X		X	X		X	X	X	
Änderungsvolumen	X	X	X	X					
Änderungszeitpunkte der Daten	(X)	X						(X)	
Fristen				X			X		X
Vertraulichkeitsbedarf der Daten				(X)	X		X	X	X
Integritätsbedarf der Daten			(X)	(X)	X		X	X	X
Kenntnisse der IT-Benutzer	X			X	X				

X bedeutet direkter Einfluss, (X) bedeutet indirekter Einfluss

Tabelle: Datensicherung

Erläuterungen:

Art der Datensicherung

Folgende Datensicherungsarten lassen sich aufzeigen:

- **Datenspiegelung**: bei der Datenspiegelung werden die Daten redundant und zeitgleich auf verschiedenen Datenträgern gespeichert. Da es sich meist um schnelle Datenträger handelt, entstehen durch die doppelte Auslegung der Datenträger und durch die notwendige Steuerungssoftware entsprechend hohe Kosten. Der wesentliche Vorteil der Datenspiegelung ist, dass der Ausfall eines dieser Speicher ohne Zeitverlust überbrückt werden kann.
- **Volldatensicherung**: bei der Volldatensicherung werden sämtliche zu sichernden Dateien zu einem bestimmten Zeitpunkt auf einen zusätzlichen Datenträger gespeichert. Es wird dabei nicht berücksichtigt, ob die Dateien sich seit der letzten Datensicherung geändert haben oder nicht. Daher benötigt eine Volldatensicherung einen hohen Speicherbedarf. Der Vorteil ist, dass die Daten vollständig für den Sicherungszeitpunkt vorliegen und die Restaurierung von Dateien einfach und schnell möglich ist, da nur die betroffenen Dateien aus der letzten Volldatensicherung extrahiert werden müssen. Werden Volldatensicherungen selten durchgeführt, so kann sich durch umfangreiche nachträgliche Änderungen innerhalb einer Datei ein hoher Nacherfassungsaufwand ergeben.
- **Inkrementelle Datensicherung**: bei der inkrementellen Datensicherung werden im Gegensatz zur Volldatensicherung nur die Dateien gesichert, die sich gegenüber der letzten Datensicherung (Volldatensicherung oder inkrementelle Sicherung) geändert haben. Dies spart Speicherplatz und verkürzt die erforderliche Zeit für die Datensicherung. Für die Restaurierung der Daten ergibt sich i. allg. ein höherer Zeitbedarf, da die Dateien aus Datensicherungen verschiedener Zeitpunkte extrahiert werden müssen. Die inkrementelle Datensicherung basiert immer auf einer Volldatensicherung. In periodischen Zeitabständen werden Volldatensicherungen erzeugt, in der Zeit dazwischen werden eine oder mehrere inkrementelle Datensicherungen vollzogen. Bei der Restaurierung wird die letzte Volldatensicherung als Grundlage genommen, die um die in der Zwischenzeit geänderten Dateien aus den inkrementellen Sicherungen ergänzt wird.
- **Differentielle Datensicherung**: bei der differentiellen Datensicherung werden nur die Dateien gesichert, die sich gegenüber der letzten Volldatensicherung geändert haben. Eine differentielle Datensicherung benötigt mehr Speicherplatz als eine inkrementelle, Dateien lassen sich aber einfacher und schneller restaurieren. Für die Restaurierung der Daten reicht die letzte Volldatensicherung sowie die aktuellste differentielle, nicht wie bei der inkrementellen, wo u. U. mehrere Datensicherungen nacheinander eingelesen werden müssen.

Eine spezielle Form dieser genannten Datensicherungsstrategien ist die Image-Datensicherung. Bei der Image-Datensicherung werden nicht die einzelnen Dateien eines Festplattenstapels gesichert, sondern die physikalischen

Sektoren der Festplatte. Es handelt sich dabei um eine Vollsicherung, die sehr schnell auf eine gleichartige Festplatte restauriert werden kann.

Eine weitere Form ist das Hierarchische Speicher-Management (HSM). Hierbei geht es in erster Linie um die wirtschaftliche Ausnutzung teurer Speicher. Dateien werden abhängig von der Häufigkeit, mit der auf sie zugegriffen wird, auf schnellen Online-Speichern (Festplatten) gehalten, auf Nearline-Speicher (automatische Datenträger-Wechselsysteme) ausgelagert oder auf Offline-Speichern (Magnetbänder) archiviert. Gleichzeitig bieten diese HSM-Systeme i. A. auch automatische Datensicherungsroutinen kombiniert aus inkrementeller Datensicherung und Volldatensicherung.

Eine redundante Datenspeicherung bieten RAID-Systeme an (Redundant Array of Inexpensive Disks). Das RAID-Konzept beschreibt die Verbindung von mehreren Festplatten unter dem Kommando eines sogenannten Array-Controllers. Man unterscheidet verschiedene RAID-Level, wovon RAID-Level 1 die Datenspiegelung beschreibt.

RAID-Systeme ersetzen keine Datensicherung! RAID-Systeme helfen nicht bei Diebstahl oder Brand, daher müssen auch die auf RAID-Systemen gespeicherten Daten auf zusätzliche Medien gesichert werden und diese Medien auch in anderen Brandabschnitten untergebracht werden.

Für die Entscheidung, welche Datensicherungsstrategie angewendet werden soll, sind die folgenden Einflussfaktoren zu berücksichtigen, um eine für die Anforderungen geeignete und gleichzeitig wirtschaftliche Form zu finden:

Verfügbarkeitsanforderungen:

Sind die Verfügbarkeitsanforderungen sehr hoch, so ist eine Datenspiegelung in Erwägung zu ziehen, sind die Verfügbarkeitsanforderungen hoch, so sollte einer Volldatensicherung gegenüber der inkrementellen Datensicherung der Vorzug gegeben werden.

Datenvolumen und Änderungsvolumen:

Entspricht das Änderungsvolumen annähernd dem Datenvolumen (z. B. bei der Nutzung einer Datenbank), so verringert sich die Speicherplatzersparnis der inkrementellen Datensicherung so stark, dass eine Vollsicherung in Erwägung gezogen werden kann. Ist jedoch das Änderungsvolumen erheblich kleiner als das Datenvolumen, so spart die inkrementelle Datensicherung Speicherplatz und damit Kosten im großen Umfang.

Änderungszeitpunkte der Daten:

Einen geringen Einfluss auf die Datensicherungsstrategie können die Änderungszeitpunkte der Daten haben. Gibt es Zeitpunkte, an denen anwendungsbezogen der Komplettdatenbestand gesichert werden muss (z. B. nach buchhalterischen Wochen-, Monats- oder Jahresabschlüsse), so kommt zu diesen Zeitpunkten nur eine Vollsicherung in Frage.

Kenntnisse der IT-Benutzer:

Die Implementierung einer Datenspiegelung setzt entsprechende Kenntnisse des Systemadministrators voraus, erfordert jedoch auf Seiten der IT-Benutzer keinerlei Kenntnisse. Eine Volldatensicherung lässt sich auch von

einem IT-Benutzer mit geringen Systemkenntnissen durchführen. Demgegenüber erfordert eine inkrementelle Datensicherung schon mehr Systemkenntnisse und Erfahrungen im Umgang mit Datensicherungen.

Häufigkeit und Zeitpunkte der Datensicherung

Tritt ein Datenverlust ein (z. B. durch Headcrash auf der Festplatte), so müssen zur Restaurierung der Daten sämtliche Datenänderungen seit der letzten Datensicherung nochmals vollzogen werden. Je kürzer der zeitliche Abstand der Datensicherungen ist, um so geringer ist i. allg. auch der für eine Restaurierung und Nacherfassung erforderliche Zeitaufwand. Gleichzeitig muss beachtet werden, dass der Zeitpunkt der Datensicherung nicht nur periodisch (täglich, wöchentlich, werktags, ...) gewählt werden kann, sondern dass auch ereignisabhängige Datensicherungen (z. B. nach x Transaktionen, nach Ausführung eines bestimmten Programms, nach Systemänderungen) notwendig sein können.

Zur Auswahl der Häufigkeit und Zeitpunkte der Datensicherung sind folgende Einflussfaktoren zu beachten.

Verfügbarkeitsanforderungen, Rekonstruktionsaufwand ohne Datensicherung und Änderungsvolumen:

Der zeitliche Abstand der Datensicherungen ist so zu wählen, dass die Restaurierungs- und Nacherfassungszeit (Rekonstruktionsaufwand der geänderten Daten, für die keine Datensicherung vorhanden ist) der in diesem Zeitraum geänderten Daten (Änderungsvolumen) kleiner als die maximal tolerierbare Ausfallzeit ist.

Änderungszeitpunkte der Daten:

Gibt es Zeitpunkte, an denen sich die Daten in großem Umfang ändern (z. B. Programmlauf für Gehaltszahlung oder Versionswechsel der Software) oder an denen der Komplettdatenbestand vorliegen muss, so bietet es sich an, unmittelbar danach eine Volldatensicherung durchzuführen. Dazu sind neben den periodischen die ereignisabhängigen Datensicherungszeitpunkte festzulegen.

Anzahl der Generationen

Einerseits werden Datensicherungen in kurzen Zeitabständen wiederholt, um eine Kopie eines möglichst aktuellen Datenbestandes verfügbar zu haben, andererseits muss die Datensicherung gewährleisten, dass gesicherte Daten möglichst lange aufbewahrt werden. Bezeichnet man eine Volldatensicherung als Generation, so bedarf es einer Festlegung der Anzahl der aufzubewahrenden Generationen und des zeitlichen Abstandes, der zwischen den Generationen liegen muss. Diese Anforderungen lassen sich an folgenden Beispielen erläutern:

- Wird eine Datei absichtlich oder unabsichtlich gelöscht, so ist diese Datei in allen späteren Datensicherungen nicht mehr verfügbar. Stellt sich heraus, dass diese gelöschte Datei dennoch benötigt wird, so muss zur Restaurierung auf eine ältere Datensicherung zurückgegriffen werden, die zeitlich vor dem Löschen erstellt wurde. Ist eine solche Generation nicht mehr vorhanden, so muss die Datei neu erfasst werden.

- Tritt ein Integritätsverlust in einer Datei auf (z. B. durch einen technischen Defekt, durch unbeabsichtigtes Ändern einer Datei oder durch einen Computer-Virus), so ist es wahrscheinlich, dass dies nicht direkt, sondern erst zeitlich versetzt bemerkt wird. Um die Integrität der Datei wiederherstellen zu können, muss dann auf eine Generation zurückgegriffen werden, die vor dem Integritätsverlust erstellt wurde.
- Es kann nicht ausgeschlossen werden, dass die Erstellung einer Datensicherung fehlerhaft oder unvollständig durchgeführt wurde. In diesem Fall ist es oftmals hilfreich, wenn auf eine weitere Generation zurückgegriffen werden kann.

Um diese Vorteile des Generationenprinzips aufrechterhalten zu können, muss jedoch eine Randbedingung eingehalten werden: der zeitliche Abstand der Generationen darf ein Mindestmaß nicht unterschreiten. Beispiel: In einem automatisierten Datensicherungsverfahren kommt es zu wiederholten Abbrüchen des Datensicherungslaufs. Hierdurch würden nacheinander sämtliche Generationen überschrieben werden. Verhindert werden kann dies, indem vor Überschreiben einer Generation das Mindestalter überprüft und nur dann überschrieben wird, wenn dieses Alter überschritten ist.

Charakterisieren lässt sich ein Generationsprinzip durch zwei Größen: das Mindestalter der ältesten Generation und die Anzahl der verfügbaren Generationen. Dabei gilt:

- je höher das Mindestalter der ältesten Generation ist, je größer ist die Wahrscheinlichkeit, dass zu einer Datei mit Integritätsverlust (eine gelöschte Datei, die im Nachhinein als notwendig erkannt wird, ist ebenfalls darunter zu fassen) noch eine Vorläuferversion vorhanden ist,
- je größer die Anzahl der verfügbaren Generationen ist, um so aktueller ist die angeforderte Vorläuferversion.

Die Anzahl der Generationen steht aber im direkten Zusammenhang mit den Kosten der Datensicherung, da Datenträger in ausreichender Zahl zur Verfügung stehen müssen. Dies folgt aus der Notwendigkeit, dass für jede Generation eigene Datenträger benutzt werden sollten. Aus Wirtschaftlichkeitsgründen muss daher die Anzahl der Generationen auf ein sinnvolles Maß beschränkt werden.

Für die Wahl der Parameter des Generationsprinzips ergeben sich folgende Einflüsse:

Verfügbarkeitsanforderungen und Integritätsbedarf der Daten:

Je höher die Verfügbarkeitsanforderungen oder der Integritätsbedarf der Daten sind, umso mehr Generationen müssen vorhanden sein, um im Fall des Integritätsverlustes die Restaurierungszeit zu minimieren. Wenn der Verlust einer Datei oder eine Integritätsverletzung möglicherweise erst sehr spät bemerkt werden kann, sind zusätzliche Quartals- oder Jahressicherungsdatenbestände empfehlenswert.

Rekonstruktionsaufwand ohne Datensicherung:

Sind die Daten zwar umfangreich, aber auch ohne Datensicherung rekonstruierbar, so kann dies als eine weitere "Pseudo-Generation" ins Kalkül gezogen werden.

Datenvolumen:

Je höher das Datenvolumen ist, desto höher sind auch die Kosten einer Generation aufgrund des benötigten Speicherplatzes. Ein hohes Datenvolumen kann deshalb die Anzahl der Generationen aus wirtschaftlichen Gründen beschränken.

Änderungsvolumen:

Je höher das Änderungsvolumen ist, um so kürzer sollten die Zeitabstände zwischen den Generationen sein, um eine möglichst zeitnahe Version der betreffenden Datei zu haben, um den Restaurierungsaufwand durch Nachbearbeitung gering zu halten.

Vorgehensweise und Speichermedium

Nach der Festlegung der Art der Datensicherung, der Häufigkeit und des Generationenprinzips gilt es nun, die Vorgehensweise einschließlich des erforderlichen und wirtschaftlich angemessenen Datenträgers auszuwählen. Zunächst sollen einige gängige Datensicherungsverfahren beispielhaft aufgezeigt werden:

Beispiel 1: Manuelle dezentrale Datensicherung am PC

Bei nichtvernetzten PCs wird die Datensicherung vom IT-Anwender meist manuell als Vollsicherung der Anwendungsdaten durchgeführt. Als Speichermedium werden Disketten verwendet.

Beispiel 2: Manuelle zentrale Datensicherung im Unix-System

Für Unix-Systeme mit angeschlossenen Terminals oder PCs mit Terminalemulation bietet sich aufgrund des zentralen Datenbestandes die zentrale Datensicherung an. Sie wird oft als Kombination von wöchentlichen Vollsicherungen und täglichen inkrementellen Datensicherungen mittels Streamer-Tapes vom Unix-Administrator manuell durchgeführt.

Beispiel 3: Manuelle zentrale Datensicherung im lokalen Netz

Im Bereich eines lokalen Netzes mit angeschlossenen PCs wird vielfach die Datensicherung dergestalt durchgeführt, dass der angeschlossene PC-Benutzer seine zu sichernden Anwendungsdaten auf einem zentralen Server im Netz ablegt und dass dann der Netzadministrator die Daten dieses Servers zentral sichert, wozu eine wöchentliche Vollsicherung und eine tägliche inkrementelle Sicherung durchgeführt werden.

Beispiel 4: Automatische zentrale Datensicherung im Großrechnerbereich

Vergleichbar dem Beispiel 2 werden im Großrechnerbereich zentrale Datensicherungen als Kombination von wöchentlichen Vollsicherungen und täglichen inkrementellen Datensicherungen durchgeführt. Vielfach wird dies automatisch mit Hilfe eines Tools (HSM) initiiert. Für einzelne

IT-Anwendungen werden vielfach noch zusätzliche ereignisorientierte Volldatensicherungen vollzogen.

Beispiel 5: Automatische zentrale Datensicherung im verteilten System

Eine weitere Variante besteht aus der Kombination der Beispiele 3 und 4. Die lokalen Daten der verteilten Systeme werden auf einen zentralen Großrechner bzw. auf einen zentralen Server übertragen, auf dem die Datensicherung als Kombination von Vollsicherungen und inkrementellen Datensicherungen durchgeführt wird.

Beispiel 6: Voll-automatische zentrale Datensicherung dezentral gespeicherter Daten im verteilten System

Im Gegensatz zum vorangegangenen Beispiel erfolgt hier der Transfer vom dezentralen zum zentralen System automatisch. Mittlerweile werden Tools angeboten, die einen Zugriff von einem zentralen Datensicherungsserver auf die dezentralen Datenbestände erlauben. Eine Datensicherung kann somit transparent für den dezentralen Anwender zentral erfolgen.

Um das Datenvolumen auf dem Speichermedium zu minimieren, können zusätzlich Datenkompressionsalgorithmen angewandt werden. Teilweise kann das Datenvolumen damit um bis zu 80 % reduziert werden. Es ist bei Anwendung der Kompression sicherzustellen, dass die gewählten Parameter und Algorithmen im Rahmen der Datensicherung dokumentiert und für die Datenrestaurierung (Dekompression) vorgehalten werden.

Für die **Vorgehensweise** gibt es zwei Parameter, die festgelegt werden müssen: den Automatisierungsgrad und die Zentralisierung (Speicherort).

Beim Automatisierungsgrad ist zwischen manuell und automatisch zu unterscheiden:

- Manuelle Datensicherung bedeutet, dass der Anstoß zur Datensicherung manuell gegeben wird. Vorteilhaft kann sein, dass der Ausführende individuell den Termin der Datensicherung dem Arbeitsablauf anpassen kann. Nachteilig ist, dass die Wirksamkeit und Güte der Datensicherung dann von der Motivation und Disziplin des Ausführenden abhängt. Durch Krankheit oder sonstige Abwesenheitsgründe können Datensicherungen ausfallen.
- Automatische Datensicherungen werden programmgesteuert zu bestimmten Terminen angestoßen. Vorteilhaft ist, dass die Disziplin und Zuverlässigkeit der Ausführenden nachrangig ist, wenn der Terminplan vollständig und aktuell ist. Nachteilig kann sein, dass die Steuerungsprogramme Kosten verursachen, der Terminplan aktuellen Änderungen angepasst werden muss oder wichtige Änderungen nicht unmittelbar gesichert werden.

Bezüglich der Zentralisierung sind zentral und dezentral durchgeführte Datensicherungen zu unterscheiden:

- Zentrale Datensicherungen zeichnen sich dadurch aus, dass der Speicherort und die Durchführung der Datensicherung am zentralen IT-System von einem Ausführenden durchgeführt werden. Diese Verfahrensweise hat den Vorteil, dass nur ein Mitarbeiter intensiv geschult werden muss und die IT-

Anwender des IT-Systems von dieser Arbeit entlastet werden. Vorteilhaft ist weiterhin, dass durch das höhere zentrale Datenaufkommen kostengünstigere Speichermedien verwendet werden können. Nachteilig ist, dass evtl. vertrauliche Daten übertragen und von nicht Befugten eingesehen werden könnten.

- Dezentrale Datensicherungen werden von den IT-Anwendern selbst durchgeführt, ohne dass die Daten auf ein zentrales IT-System übertragen werden müssen. Vorteilhaft ist, dass der IT-Anwender die Kontrolle über die Daten und die Backup-Datenträger behält, insbesondere wenn es sich um vertrauliche Daten handelt. Nachteilig ist, dass die konsequente Datensicherung damit von der Zuverlässigkeit der IT-Anwender abhängt und dass dezentrale Lösungen den IT-Anwendern Zeitaufwand abfordern.

Nach der Entscheidung, ob die Datensicherung manuell oder automatisch, zentral oder dezentral durchgeführt wird, muss nun der geeignete Datenträger für die Datensicherung gefunden werden. Dazu können folgende Parameter betrachtet werden:

- **Datenträger-Anforderungszeit:** der Zeitaufwand für die Vorbereitung der Daten-Restaurierung ist bestimmt durch die Zeit, die benötigt wird, den erforderlichen Datensicherungs-Datenträger zu identifizieren und im System verfügbar zu machen. Kassetten in einem Roboter-System können innerhalb von Minuten zur Restaurierung bereit stehen, ausgelagerte Bänder müssen unter Umständen erst aufwendig transportiert und aufgelegt werden.
- **Zugriffszeit, Transferrate:** der Zeitaufwand für die Erstellung und Restaurierung der Daten selbst hängt von der mittleren Zugriffszeit auf die Daten des Datenträgers und von der Datentransferrate ab. Festplatten erlauben einen Zugriff auf bestimmte Dateien im Millisekunden-Bereich, ein Magnetband muss erst zur entsprechenden Stelle gespult werden. Bei der Auswahl des Datenträgers ist zu berücksichtigen, dass bei entsprechend hohen Transferraten es nicht zu einer Überlastung der Übertragungskanäle kommen darf.
- **Praktikabilität/Speicherkapazität:** je umständlicher die Datensicherung ist, um so größer ist die Gefahr, dass sie fehlerhaft vollzogen oder von den Verantwortlichen überhaupt nicht durchgeführt wird. Datenträger mit zu kleiner Speicherkapazität verhindern eine effektive Datensicherung, da der ständige Wechsel zeitaufwendig und fehleranfällig ist.
- **Kosten:** die Kosten für die Datensicherung, also Beschaffungskosten für Lese-/ Schreibgeräte und Datenträger, erforderliche Rechen- und Arbeitszeit müssen in einem angemessenen Verhältnis zum Sicherungszweck stehen. Hierbei ist auch die Lebensdauer der Datenträger und der Zuverlässigkeit zu berücksichtigen. Auf keinen Fall dürfen die laufenden Datensicherungskosten die Summe der Restaurierungskosten ohne Datensicherung und der Folgeschäden übersteigen.

Die folgenden Einflussgrößen müssen dabei beachtet werden:

Verfügbarkeitsanforderungen:

Je höher die Verfügbarkeitsanforderungen sind, desto schneller muss auf die Datenträger als Speichermedium der Datensicherung zugegriffen werden können und desto schneller müssen die benötigten Daten vom Datenträger wieder einspielbar sein.

Aus Verfügbarkeitsgründen muss sichergestellt sein, dass die Speichermedien auch bei Ausfall eines Lesegerätes zur Restaurierung genutzt werden können. Die Kompatibilität und Funktion eines Ersatzgerätes ist zu gewährleisten.

Daten- und Änderungsvolumen:

Mit zunehmenden Datenvolumen werden i. allg. preisgünstige Bandspeichermedien wie Magnetbänder oder Bandkassetten (Data Cartridge) benutzt.

Fristen:

Müssen Löschfristen eingehalten werden (z. B. bei personenbezogenen Daten), so muss das ausgewählte Speichermedium die Löschung ermöglichen. Speichermedien, die nicht oder nur mit großem Aufwand löschbar sind (z. B. WORM), sollten in diesem Fall vermieden werden.

Vertraulichkeitsbedarf und Integritätsbedarf der Daten:

Ist der Vertraulichkeits- oder Integritätsbedarf der zu sichernden Daten hoch, so überträgt sich dieser Schutzbedarf auch auf die zur Datensicherung eingesetzten Datenträger. Ist eine Verschlüsselung der Datensicherung nicht möglich, kann über die Auswahl von Datenträgern nachgedacht werden, die aufgrund ihrer kompakten Bauart und Transportabilität in Datensicherungsschränken oder Tresoren untergebracht werden können.

Kenntnisse der IT-Benutzer:

Die Kenntnisse und datenverarbeitungsspezifische Fähigkeiten der IT-Benutzer entscheiden darüber, ob eine Verfahrensweise gewählt werden kann, in der der IT-Benutzer selbst manuell für die Datensicherung tätig wird, ob andere ausgebildete Personen die Datensicherung dezentral durchführen oder ob eine automatisierte Datensicherung praktikabler ist.

Verantwortlichkeit für die Datensicherung

Für die Entscheidung, wer für die Durchführung der Datensicherung verantwortlich ist, kommen drei Personengruppen in Frage. Zunächst kann es der IT-Benutzer selbst sein (typischerweise bei dezentralen und nichtvernetzen IT-Systemen), der Systemverwalter oder ein für die Datensicherung speziell ausgebildeter Administrator. Wird die Datensicherung nicht vom Benutzer selbst durchgeführt, sind die Verantwortlichen auf Verschwiegenheit bezüglich der Dateninhalte zu verpflichten und ggf. eine Verschlüsselung in Betracht zu ziehen.

Darüber hinaus sind die Entscheidungsträger zu benennen, die eine Daten-Restaurierung veranlassen können. Zu klären ist weiterhin, wer berechtigt ist, auf Datensicherungsträger zuzugreifen, insbesondere wenn sie in Datensicherungsarchiven ausgelagert sind. Es muss sichergestellt sein, dass nur Berechtigte Zutritt erhalten. Abschließend ist zu definieren, wer berechtigt ist, eine Daten-Restaurierung des Gesamtdatenbestandes oder ausgewählter, einzelner Dateien operativ durchzuführen.

Bei der Festlegung der Verantwortlichkeit ist insbesondere der Vertraulichkeits-, Integritätsbedarf der Daten und die Vertrauenswürdigkeit der zuständigen Mitarbeiter zu betrachten. Es muss sichergestellt werden, dass der Verantwortliche erreichbar ist und ein Vertreter benannt und eingearbeitet wird.

Als Einflussfaktor ist zu beachten:

Kenntnisse der IT-Anwender:

Die Kenntnisse und datenverarbeitungsspezifischen Fähigkeiten der IT-Benutzer entscheiden darüber, ob die Datensicherung eigenverantwortlich je IT-Benutzer durchgeführt werden sollte. Sind die Kenntnisse der IT-Benutzer nicht ausreichend, ist die Verantwortung dem Systemadministrator oder einer speziell ausgebildeten Person zu übertragen.

Aufbewahrungsort

Grundsätzlich sollten Datensicherungsmedien und Originaldatenträger in unterschiedlichen Brandabschnitten aufbewahrt werden. Werden Datensicherungsmedien in einem anderen Gebäude oder außerhalb des Betriebsgeländes aufbewahrt, so sinkt die Wahrscheinlichkeit, dass in einem Katastrophenfall die Datensicherungen in Mitleidenschaft gezogen werden. Je weiter jedoch die Datenträger von der zur Restaurierung notwendigen IT-Peripherie (z. B. Bandstation) entfernt ist, desto länger können die Transportwege und Transportzeiten sein, und desto länger ist die Gesamtrestaurierungszeit. Als Einflussfaktor ist daher zu betrachten:

Verfügbarkeitsanforderungen:

Je höher die Verfügbarkeitsanforderungen sind, um so schneller müssen die Datenträger der Datensicherung verfügbar sein. Werden aus Sicherheitsgründen die Datenträger extern ausgelagert, so ist bei sehr hohen Verfügbarkeitsanforderungen zu erwägen, Kopien der Datensicherung zusätzlich in unmittelbarer Nähe des IT-Systems vorzuhalten.

Vertraulichkeitsbedarf und Integritätsbedarf der Daten:

Je höher dieser Bedarf ist, um so besser muss verhindert werden, dass an den Datenträgern manipuliert werden kann. Die notwendige Zutrittskontrolle lässt sich i. allg. nur durch entsprechende infrastrukturelle und organisatorische Maßnahmen erreichen, siehe Baustein B 2.5 *Datenträgerarchiv*.

Datenvolumen:

Mit steigendem Datenenvolumen gewinnt die Sicherheit des Aufbewahrungsortes an Bedeutung.

Anforderungen an das Datensicherungsarchiv

Aufgrund der Konzentration von Daten auf Datensicherungsmedien besitzen diese einen mindestens ebenso hohen Schutzbedarf bezüglich Vertraulichkeit und Integrität wie die gesicherten Daten selbst. Bei der Aufbewahrung in einem zentralen Datensicherungsarchiv sind daher entsprechend wirksame IT-Sicherheitsmaßnahmen wie z. B. Zutrittskontrolle notwendig.

Zusätzlich muss durch organisatorische und personelle Maßnahmen (Datenträgerverwaltung) sichergestellt werden, dass der schnelle und gezielte Zugriff auf benötigte Datenträger möglich ist. Hierzu sind die Maßnahme M 2.3 *Datenträgerverwaltung* und Baustein B 2.5 *Datenträgerarchiv* zu beachten.

Folgende Einflussfaktoren müssen beachtet werden:

Verfügbarkeitsanforderungen:

Je höher die Verfügbarkeitsanforderungen sind, um so schneller muss der gezielte Zugriff auf benötigte Datenträger möglich sein. Wenn eine manuelle Bestandsführung den Verfügbarkeitsanforderungen nicht genügt, können automatisierte Zugriffsverfahren (z. B. Roboter-Kassettenarchiv) zum Einsatz kommen.

Datenvolumen:

Das Datenvolumen bestimmt letztendlich die Anzahl der aufzubewahrenden Datenträger. Für entsprechend große Datenvolumen ist eine ausreichende Aufbewahrungskapazität im Datenträgerarchiv vorzusehen.

Fristen:

Sind Löschungsfristen einzuhalten, muss die Organisation des Datensicherungsarchivs dem angepasst sein und ggf. müssen auch die erforderlichen Löscheinrichtungen vorhanden sein. Zu den vorgegebenen Löschungszeitpunkten ist im Datensicherungsarchiv die Löschung zu initiieren bzw. durchzuführen und zu dokumentieren. Ist eine Löschung technisch nicht möglich, so ist durch organisatorische Maßnahmen eine Wiederverwendung zu löschender Daten zu verhindern.

Vertraulichkeits- und Integritätsbedarf der Daten:

Je höher dieser Bedarf ist, um so besser muss verhindert werden, dass an den Datenträgern manipuliert werden kann. Die notwendige Zutrittskontrolle lässt sich i. allg. nur durch entsprechende infrastrukturelle und organisatorische Maßnahmen erreichen vergleichbar dem Baustein B 2.5 *Datenträgerarchiv*.

Transportmodalitäten

Bei der Durchführung einer Datensicherung werden Daten transportiert. Sei es, dass sie über ein Netz oder eine Leitung übertragen werden, sei es, dass Datenträger zum Datenträgerarchiv transportiert werden. Dabei gilt es folgendes zu beachten:

Verfügbarkeitsanforderungen:

Je höher die Verfügbarkeitsanforderungen sind, desto schneller müssen die Daten zur Restaurierung bereitstellbar sein. Dies ist bei der Auswahl des Datenübertragungsmediums bzw. bei Auswahl des Datenträger-Transportweges zu berücksichtigen.

Datenvolumen:

Wenn zur Datenrestaurierung die Daten über ein Netz übertragen werden, so muss bei der Auswahl der Übertragungskapazität des Netzes das Datenvolumen beachtet werden. Es muss gewährleistet sein, dass das Datenvolumen innerhalb der erforderlichen Zeit (Verfügbarkeitsanforderung) übertragen werden kann.

Änderungszeitpunkte der Daten:

Werden Datensicherungen über ein Netz durchgeführt (insbesondere zu ausgewählten Terminen), kann aufgrund des zu übertragenen Datenvolumens ein Kapazitätsengpass entstehen. Daher ist zum Zeitpunkt der Datensicherung eine ausreichende Datenübertragungskapazität sicherzustellen.

Vertraulichkeits- und Integritätsbedarf der Daten:

Je höher dieser Bedarf ist, um so besser muss verhindert werden, dass die Daten auf dem Transport abgehört, unbefugt kopiert oder manipuliert werden. Bei Datenübertragungen ist schließlich eine Verschlüsselung oder ein kryptographischer Manipulationsschutz zu überdenken, beim physikalischen Transport sind sichere Behältnisse und Wege zu benutzen und ggf. auch der Nutzen und Aufwand einer Verschlüsselung abzuwägen.

Aufbewahrungsmodalität

Im Rahmen des Datensicherungskonzeptes sollte mitbetrachtet werden, ob für bestimmte Daten Aufbewahrungs- oder Löschfristen einzuhalten sind.

Fristen:

Falls Aufbewahrungsfristen einzuhalten sind, kann dem durch die Archivierung einer Datensicherungsgeneration nachgekommen werden. Sind die Aufbewahrungsfristen lang, so ist zusätzlich sicherzustellen, dass die erforderlichen Lesegeräte bevorratet werden und dass unter Umständen ein Refresh (erneutes Aufspielen der magnetisch gespeicherten Daten) bei magnetischen Datenträgern erforderlich werden kann, da diese mit der Zeit ihre Magnetisierung und damit den Dateninhalt verlieren.

Falls Löschfristen einzuhalten sind, muss der organisatorische Ablauf festgelegt werden und ggf. müssen auch die erforderlichen Löscheinrichtungen vorhanden sein. Zu den vorgegebenen Löschungszeitpunkten ist die Löschung zu initiieren bzw. durchzuführen.

Ergänzende Kontrollfragen:

- Wird die Vorgehensweise zur Datensicherung bei veränderter IT-Ausstattung aktualisiert?
- Werden sporadisch Übungen zur Daten-Restaurierung durchgeführt?
- Werden Kontrollen durchgeführt, ob die im Datensicherungskonzept festgelegten Modalitäten eingehalten werden?
- Werden die Verantwortlichen für ihre Aufgaben bei der Datensicherung ausreichend geschult?

M 6.36 Festlegung des Minimaldatensicherungskonzeptes

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Für ein Unternehmen/eine Behörde ist festzulegen, welche Minimalforderungen zur Datensicherung eingehalten werden müssen. Damit können viele Fälle, in denen eingehende Untersuchungen und die Erstellung eines Datensicherungskonzeptes zu aufwendig sind, pauschal behandelt werden. Weiterhin ist damit eine Grundlage gegeben, die generell für alle IT-Systeme gültig ist und auch für neue IT-Systeme, für die noch kein Datensicherungskonzept erarbeitet wurde.

Ein Beispiel soll dies erläutern:

Minimaldatensicherungskonzept

Software:

Sämtliche Software, erworben oder selbst erstellt, ist einmalig mittels einer Vollsicherung zu sichern.

Systemdaten:

Systemdaten sind mindestens einmal monatlich mit einer Generation zu sichern.

Anwendungsdaten:

Alle Anwendungsdaten sind mindestens einmal monatlich mittels einer Vollsicherung im Drei-Generationen-Prinzip zu sichern.

Protokolldaten:

Sämtliche Protokolldaten sind mindestens einmal monatlich mittels einer Vollsicherung im Drei-Generationen-Prinzip zu sichern.

Ergänzende Kontrollfragen:

- Werden sämtliche Mitarbeiter, auch neu eingestellte, auf ein Datensicherungskonzept oder ersatzweise auf das Minimaldatensicherungskonzept hingewiesen und verpflichtet?
- Wird das Minimaldatensicherungskonzept aktualisiert?
- Werden die notwendigen Betriebsmittel für die Minimaldatensicherung bereitgestellt?

M 6.37 Dokumentation der Datensicherung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Verantwortliche für die Datensicherung

In einem Datensicherungskonzept muss festgelegt werden, wie die Dokumentation der Datensicherung zu erfolgen hat. Für eine ordnungsgemäße und funktionierende Datensicherung ist eine Dokumentation erforderlich. So ist bei der Erstellung der Datensicherung für jedes IT-System zu dokumentieren:

- das Datum der Datensicherung,
- der Datensicherungsumfang (welche Dateien/Verzeichnisse wurden gesichert),
- der Datenträger, auf dem die Daten im operativen Betrieb gespeichert sind,
- der Datenträger, auf dem die Daten gesichert wurden,
- die für die Datensicherung eingesetzte Hard- und Software (mit Versionsnummer) und
- die bei der Datensicherung gewählten Parameter (Art der Datensicherung usw.).

Darüber hinaus bedarf es einer Beschreibung der Vorgehensweise für die Wiederherstellung eines Datensicherungsbestandes. Auch hier muss eine Beschreibung der erforderlichen Hard- und Software, der benötigten Parameter und der Vorgehensweise, nach der die Datenrekonstruktion zu erfolgen hat, erstellt werden.

Ergänzende Kontrollfragen:

- Werden die Datensicherungen im genannten Umfang dokumentiert?
- Kann eine Datenrestaurierung aufgrund der Dokumentation vorgenommen werden, selbst wenn derjenige, der die Datensicherung vorgenommen hat, verhindert ist?

M 6.38 Sicherungskopie der übermittelten Daten

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Sind die zu übertragenden Daten nur zum Zweck der Datenübertragung erstellt bzw. zusammengestellt worden und nicht auf einem weiteren Medium gespeichert, sollte eine Sicherungskopie dieser Daten vorgehalten werden. Bei Verlust oder Beschädigung des Datenträgers kann der Versand mit geringfügigem Aufwand erneut erfolgen.

Ergänzende Kontrollfrage:

- Ist die Erstellung einer Sicherungskopie für auszutauschende Datenträger vorzusehen?

M 6.39 Auflistung von Händleradressen zur Fax-Wiederbeschaffung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Fax-Verantwortlicher, Beschaffer

Es sollte in den Not- und Katastrophenplan eine Liste von Fachhändlern für Faxgeräte aufgenommen werden, bei denen im Notfall unverzüglich neue Geräte beschafft werden können, wenn eine Reparatur aus Zeitgründen nicht möglich ist.

Ergänzende Kontrollfrage:

- Existiert eine Liste der Fachhändler für Faxgeräte im Notfallplan?

M 6.40 Regelmäßige Batterieprüfung/-wechsel

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Batterien und Akkumulatoren verlieren mit der Zeit ihre Kapazität. Daher sollten bei Anrufbeantwortern mit digitaler Ansagetext- oder Anrufspeicherung diese Energiequellen für die Notstromversorgung regelmäßig ausgewechselt werden. In der Regel sollte ein Batteriewechsel im Jahresrhythmus erfolgen.

Ergäzende Kontrollfrage:

- Wird der Batteriewechsel jährlich vorgenommen?

M 6.41 Übungen zur Datenrekonstruktion

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Verantwortliche für die Datensicherung

Die Rekonstruktion von Daten mit Hilfe von Datensicherungsbeständen muss sporadisch, zumindestens aber nach jeder Änderung des Datensicherungsverfahrens, getestet werden. Hierbei muss zumindest einmal nachgewiesen werden, dass eine vollständige Datenrekonstruktion (z. B. der Gesamtdatenbestand eines Servers) möglich ist. Auf diese Weise kann zuverlässig ermittelt werden, ob

- die Datenrekonstruktion überhaupt möglich ist,
- die Verfahrensweise der Datensicherung praktikabel ist,
- eine ausreichende Dokumentation der Datensicherung vorliegt, damit ggf. auch ein Vertreter die Datenrekonstruktion vornehmen kann und
- die erforderliche Zeit zur Datenrekonstruktion den Anforderungen an die Verfügbarkeit entspricht (siehe M 6.1 *Erstellung einer Übersicht über Verfügbarkeitsanforderungen*).

Bei Übungen zur Datenrekonstruktion sollte auch berücksichtigt werden, dass

- die Daten gegebenenfalls auf einem Ausweich-IT-System installiert werden müssen und
- für die Datensicherung und Datenrekonstruktion unterschiedliche Schreib-/Lesegeräte benutzt werden.

Ergänzende Kontrollfrage:

- Kann ein sachverständiger Dritter die Datenrestaurierung anhand der vorhandenen Dokumentation durchführen?

M 6.42 Erstellung von Rettungsdisketten für Windows NT

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator

Für jedes unter Windows NT betriebene System, das über ein Diskettenlaufwerk verfügt, sollte ein Satz von Reparaturdisketten bereitgehalten werden. Dieser besteht für Rechner mit Intel-Prozessoren aus den drei Setup-Disketten, die mit Windows NT geliefert werden, sowie einer Notfalldiskette, mit der sich der anfängliche Setup-Status wiederherstellen lässt, wenn Dateien beschädigt werden. Für jeden Rechner muss eine eigene Notfalldiskette erstellt werden, da diese Disketten nicht zwischen verschiedenen Rechnern ausgetauscht werden können.

Während des Windows NT Setup wird der Benutzer gefragt, ob er eine Notfalldiskette erstellen will. Zur Erstellung der Notfalldiskette muss eine leere Diskette auf Anforderung in Laufwerk A: eingelegt werden, auf der dann die zur Reparatur des Systems benötigten Informationen gespeichert werden.

Sofern bei der Installation keine Notfalldiskette erstellt wurde, kann diese auch nachträglich mit dem Dienstprogramm *RDISK* (im Windows-Systemverzeichnis *%SystemRoot%\SYSTEM32*, z. B. *\WINNT\SYSTEM32*) erzeugt werden. Das Programm ist mit dem Parameter */s* zu starten, wenn die Benutzerkonten und die Zugriffsberechtigungen mit gesichert werden sollen. Die Wahl dieses Parameters kann jedoch dazu führen, dass die Sicherung nicht mehr auf eine Diskette paßt, wenn auf dem betreffenden System eine größere Anzahl von Benutzerprofilen definiert ist. Daher sollte zunächst die Option "*Notfall-Informationen aktualisieren*" gewählt werden, um den aktuellen Systemzustand zu retten, und dann sollte mit der Option "*Erstellen einer Notfalldiskette*" die eigentliche Notfalldiskette generiert werden.

Hinweis: Dieser Prozess sollte nach jeder Veränderung der Systemkonfiguration wiederholt werden, damit die Notfalldiskette stets den aktuellen Systemzustand widerspiegelt. Nur so wird sichergestellt, dass in den Reparaturinformationen neue Angaben zur Konfiguration, wie Zuweisung von Laufwerkbuchstaben, Stripe Sets, Datenträgersätzen, Spiegelungen usw. berücksichtigt werden. Im anderen Fall kann der Zugriff auf bestimmte Laufwerke nach Systemfehlern unmöglich sein. Die Erstellung der Notfalldiskette sollte nach dem nächsten erfolgreichen Systemstart durchgeführt werden, um sicher zu sein, dass eine lauffähige Systemversion gesichert wird.

Falls keine Setup-Disketten verfügbar sind, können diese mit dem Windows NT Setup-Programm (*WINNT* für das Setup von MS-DOS oder Windows 95, *WINNT32* für das Setup von Windows NT aus) der Windows NT Installations-CD erzeugt werden, indem dieses Programm mit dem Parameter */ox* aufgerufen wird. Das Programm fordert dann drei leere Disketten in Laufwerk A: an und kopiert die zum Starten von Windows NT benötigten Dateien auf diese Disketten.

Falls Systemdateien, Boot-Variablen oder der Boot-Sektor beschädigt werden, und sich die vorherige Startkonfiguration mit der Methode der letzten als

funktionierend bekannten Konfiguration nicht wiederherstellen lässt, muss der Reparaturprozess im Windows NT Setup verwendet werden, um den ursprünglichen Systemzustand wiederherzustellen.

Zum Reparieren einer Windows NT Installation benötigt das Setup-Programm entweder die Konfigurationsinformationen, die im Unterverzeichnis *REPAIR* des Windows-Verzeichnisses *%SystemRoot%*, z. B. in *\WINNT\REPAIR,* gespeichert sind, oder die Notfalldiskette.

Zum Wiederherstellen einer beschädigten Windows NT Installation ist die erste der drei Setup-Disketten in Laufwerk A: einzulegen und der Rechner dann von diesem Laufwerk aus zu booten. Im Textbildschirm des Setup-Programms, in dem gefragt wird, ob Windows NT installiert oder Dateien repariert werden sollen, ist der Parameter **r** einzugeben. Das Setup-Programm fragt dann nach der Notfalldiskette. Falls keine Notfalldiskette vorhanden ist, zeigt das Setup-Programm eine Liste der vorhandenen Windows NT Installationen an, die auf dem Computer gefunden wurden, und fragt, welche Installation repariert werden soll. Nach Erscheinen der abschließenden Meldung ist die Notfalldiskette aus Laufwerk A: zu entfernen und der Rechner neu zu starten.

Der Reparaturprozess im Setup-Programm ermöglicht es, verschiedene Elemente zur Reparatur auszuwählen:

- **Systemdateien** - Das Setup-Programm überprüft die Übereinstimmung des Verzeichnisbaumes von Windows NT mit der Protokolldatei auf der Notfalldiskette, um sicherzustellen, dass alle Systemdateien vorhanden und unbeschädigt sind. Fehlen Dateien oder werden beschädigte Dateien gefunden, so werden diese von der jeweiligen Windows NT Setup-Quelle (z. B. CD-ROM) wiederhergestellt. Das Setup-Programm überprüft auch die Windows NT Dateien auf der System-Partition, um sicherzustellen, dass alle Boot-Dateien vorhanden und unbeschädigt sind.
- **Standard-Systemkonfiguration** - Das Setup-Programm bietet die Möglichkeit, fehlerhafte Dateien der Registrierung aus denjenigen wiederherzustellen, die bei der Installation von Windows NT angelegt wurden. Dabei ist zu beachten, dass Benutzerkonten und Berechtigungen, die seit der ersten Installation bzw. der letzten Aktualisierung der Notfalldiskette eingerichtet wurden, verloren gehen.
- **Boot-Variablen** - Bei Wahl dieser Option stellt das Setup-Programm die Boot-Variablen für die spezielle Installation von Windows NT auf der Festplatte von der Notfalldiskette wieder her.
- **Boot-Sektor** (nur bei Computern mit x86-Prozessor) - Bei Wahl dieser Option legt das Setup-Programm auf der System-Partition einen neuen Boot-Sektor an.

Falls andere Dateien fehlen oder beschädigt sind, so stellt das Setup-Programm diese von der entsprechenden Windows NT Setup-Diskette oder von CD-ROM wieder her. Falls die System-Partition auf einem Computer mit x86-Prozessor irrtümlich formatiert oder geändert wurde, so dass Windows NT nicht mehr startet, stellt das Reparaturprogramm die ursprüngliche Boot-Konfiguration wieder her.

Hinweis: Wenn die Systemdateien repariert werden, entfernt Setup die Sicherheitseinstellungen von diesen Dateien, falls diese sich auf einer NTFS-Partition befinden. Dies ist sinnvoll, um falsch vergebene Berechtigungen für Systemdateien zurücksetzen zu können, die sonst verhindern würden, dass Windows NT auf die Systemdateien zugreifen kann, die zum Starten des Systems erforderlich sind. Es ist aus diesem Grund unbedingt erforderlich, die Notfalldiskette und die Setup-Disketten so zu verwahren, dass sie gegen Missbrauch geschützt sind.

Ergänzende Kontrollfragen:

- Sind die Informationen auf der Notfalldiskette aktuell?
- Werden die Reparaturdisketten unter Verschluss gehalten, um eventuellen Missbrauch zu vermeiden?
- Ist für jedes Windows NT System eine Notfalldiskette erstellt worden?

M 6.43 Einsatz redundanter Windows NT/2000 Server

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

In Abhängigkeit von den Verfügbarkeitsanforderungen der Daten und Anwendungen ist eine Redundanz zu schaffen, die einem Totalverlust der Daten mit akzeptablem Aufwand vorbeugt. Je nach diesen Anforderungen sind Teile des Datenbestandes oder auch der gesamte Datenbestand parallel auf mehreren Plattenspeichern zu führen, so dass auch bei Ausfall eines Plattenlaufwerks dessen Daten nicht verloren sind und die Benutzer weiterarbeiten können, ohne auf das Wiedereinspielen einer Datensicherung warten zu müssen.

Die Systeme können je nach den definierten Verfügbarkeitsanforderungen so ausgelegt werden, dass bei Ausfall eines Servers dessen Aufgaben von einem oder mehreren anderen Servern übernommen werden können. Dabei muss jedoch dafür gesorgt werden, dass diese verteilten Datenbestände konsistent bleiben, und dies muss auch bei Ausfall einzelner Geräte gewährleistet bleiben. In dieser Beziehung bestehen gravierende Unterschiede hinsichtlich der Leistungsfähigkeit verschiedener Redundanzkonzepte:

RAID-Plattensysteme

- Eine direkte physikalische Redundanz lässt sich mit RAID-Plattensystemen (RAID: Redundant Array of Independent Disks) erreichen. Zu beachten ist bei der Entscheidung für dieses Verfahren, dass der räumliche Abstand zwischen den einzelnen Platten eines RAID-Systems starken Einschränkungen unterworfen ist, so dass im Falle eines Brandes oder eines ähnlichen Schadens alle Parallelkopien gleichermaßen zerstört werden. RAID-Systeme sind daher kein Ersatz für Datensicherungen.

Windows NT/2000 Cluster

- Durch Einsatz von Windows NT/2000 Clustern können parallele Kopien des Datenbestandes verteilt auf verschiedene Platten und unter Kontrolle verschiedener Rechner geführt werden. Durch die Verwendung leistungsstarker Cluster mit bis zu vier Servern lässt sich die Zahl der Serversysteme reduzieren, was wiederum zu einer Reduktion des Administrationsaufwandes und damit zu einer Verbesserung der Sicherheit führt.
- Die Replikation einzelner Verzeichnisse erlaubt eine ähnlich weite Verteilung der Daten, doch stehen hier keine Synchronisationsmechanismen zur Verfügung, die es erlauben, auch die aktuell in Bearbeitung befindlichen Dateien konsistent parallel zu führen. Ein Ausfall des primären Plattenlaufwerks führt hier somit immer zu mehr oder weniger großen Datenverlusten. Der Einsatz der Replikatordienste unter Windows NT oder Windows 2000 sollte daher auf die Fälle beschränkt bleiben, in denen nur an einer Stelle geändert wird, und er darf keinesfalls als Ersatz für die regelmäßige Durchführung von Datensicherungen angesehen werden.

Um einem Ausfall der Server vorzubeugen, sind diese bei Bedarf redundant auszulegen. Hier stehen mehrere Möglichkeiten zur Verfügung, unter denen, ausgehend von der tolerierbaren Ausfallzeit, eine geeignete Alternative auszuwählen ist:

separate Rechner

- Wenn Ausfälle in der Größenordnung einer halben Stunde tolerierbar sind, ist ein separater Rechner zur Verfügung zu stellen, der bei Ausfall eines Servers dessen Aufgaben übernimmt. Um Zugriff auf die Daten des ausge-

fallenen Servers zu erhalten, müssen dessen Plattenlaufwerke auf den Ausweichrechner umgeschaltet werden.

Cluster-Systeme

- Wenn Ausfälle von maximal einigen Minuten tolerierbar sind, ist ein Cluster-System mit Zugriff aller Rechner auf alle Platten einzusetzen. Das System ist so zu konfigurieren, dass bei Ausfall eines Servers automatisch auf einen Ersatzrechner innerhalb des Systems umgeschaltet wird.

voll redundantes, ausfallsicheres System

- Wenn äußerstenfalls Ausfälle im Sekundenbereich toleriert werden können, ist der Einsatz eines voll redundanten, ausfallsicheren Systems mit parallel arbeitenden mehrfachen CPUs erforderlich. In diesem Fall bleibt ein Ausfall einer CPU oder eines Hauptspeichermoduls für den Benutzer unbemerkbar. Diese Lösung bietet somit die größte Ausfallsicherheit, doch ist sie gleichzeitig auch erheblich aufwendiger und teurer als die beiden anderen Lösungen, so dass man nur bei extremen Anforderungen an die Verfügbarkeit auf sie zurückgreifen wird. Windows NT kann derzeit so hohe Anforderungen nicht erfüllen, so dass in diesem Fall Spezialsysteme einzusetzen sind, die unter anderen Betriebssystemen laufen.

Es muss in jedem Fall anhand einer sorgfältigen Analyse festgestellt werden, welche konkreten Verfügbarkeitsanforderungen gegeben sind, und im Rahmen einer detaillierten Planung der System- und Netzarchitektur muss dann eine geeignete Kombination redundanter Rechner und/oder Plattenlaufwerke gefunden werden, die diesen Anforderungen genügt.

Ergänzende Kontrollfrage:

- Sind die aktuellen Verfügbarkeitsanforderungen der Anwendungen und deren Abhängigkeiten untereinander bekannt?

M 6.44 Datensicherung unter Windows NT

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Unter Windows NT kann die Datensicherung mit dem zum System gehörigen Dienstprogramm *NTBACKUP.EXE* durchgeführt werden, wobei zu beachten ist, dass dieses Programm nur Sicherungen auf Band unterstützt und auch nicht in der Lage ist, die Sicherungsbänder zu verschlüsseln, so dass diese gesichert aufbewahrt werden müssen.

Bei der Durchführung der Datensicherung sind die folgenden Punkte zu beachten:

- Für die Datensicherung sind Zugriffsrechte auf das Windows-Systemverzeichnis *%SysRoot%\SYSTEM32* (in der Regel *\WINNT\SYSTEM32*) notwendig, da *NTBACKUP* dort temporäre Dateien und Log-Dateien anlegt.

Registry sichern

- Die Sicherungssoftware ist in der Lage, die Registrierung des lokalen Rechners zu sichern. Dies sollte in regelmäßigen Abständen und nach größeren Änderungen der Konfiguration durchgeführt werden.
- In regelmäßigen Abständen (nach jeweils etwa 20 Nutzungen) sollten zur Datensicherung verwendete Viertelzoll-Bänder durch Wahl der Option "*Band spannen*" sauber aufgewickelt werden, um lockere Stellen und dadurch mögliche Beschädigung des Bandes durch Abrieb zu vermeiden. 4 mm (DAT-) und 8 mm (Video 8-) Bänder erfordern diese Maßnahme nicht; die entsprechende Operation steht für diese Bänder nicht zur Verfügung.
- Bei Angabe der Option "*Band löschen"* sollte "*Sicheres Löschen"* gewählt werden, wenn schutzwürdige Daten auf dem Band waren, da hiermit die alten Daten überschrieben werden. Sofern diese Option nicht gewählt wird, bleibt der größte Teil der ursprünglich auf diesem Band gespeicherten Daten erhalten und kann ohne großen Aufwand wieder rekonstruiert werden.

Protokolldatei anlegen

- Bei der Durchführung der Sicherungsoperation ist unbedingt die Möglichkeit zu nutzen, eine Protokolldatei anzulegen. Nach Abschluss der Operation ist die Protokolldatei daraufhin zu überprüfen, ob alle zu sichernden Daten auch tatsächlich gesichert werden konnten oder ob während der Sicherung Fehler aufgetreten sind. Dabei ist die Option "*Alle Angaben protokollieren*" empfehlenswert, da man damit auch feststellen kann, ob alle zu sichernden Daten gesichert wurden und ob überhaupt die Verzeichnisse in die Datensicherung einbezogen wurden, die gesichert werden sollen.
- Bei der Wiederherstellung gesicherter Dateien wird deren Zugriffsschutz ebenfalls wiederhergestellt, sofern diese Dateien in einem Verzeichnis wiederhergestellt werden, das keine explizite Zugriffskontrolle für die darin gespeicherten Dateien vorgibt. Ist jedoch eine solche Vorgabe im Verzeichnis spezifiziert, so wird diese übernommen, und die ursprüngliche Zugriffskontrollinformation wird ignoriert.

- Die Auswahl der zu sichernden Dateien und Verzeichnisse kann unter der graphischen Bedienoberfläche nicht gespeichert werden. Um regelmäßig dieselben Verzeichnisse zu sichern, können Skripten angelegt werden; diese sind jedoch nicht für Dateiauswahl geeignet.

Wegen der durch das Dienstprogramm *NTBACKUP.EXE* gegebenen Einschränkungen sollte für umfangreichere Installationen bzw. bei hohen Verfügbarkeitsanforderungen zusätzliche Software zur Durchführung von Datensicherungen eingesetzt werden. Bei der Auswahl derartiger Sicherungssoftware sollte darauf geachtet werden, dass sie die folgenden Anforderungen erfüllt:

- Die eingesetzten Dateisysteme, also FAT, NTFS und ggf. auch HPFS sollten bei der Sicherung und Wiederherstellung unterstützt werden.
- Es sollte möglich sein, Sicherungen automatisch zu vorwählbaren Zeiten bzw. in einstellbaren Intervallen durchführen zu lassen, ohne dass hierzu manuelle Eingriffe (außer dem eventuell notwendigen Bereitstellen von Sicherungsdatenträgern) erforderlich wären.
- Es sollte möglich sein, einen oder mehrere ausgewählte Benutzer automatisch über das Sicherungsergebnis und eventuelle Fehlermeldungen per E-Mail oder ähnliche Mechanismen zu informieren.
- Die Sicherungssoftware sollte die Sicherung des Backup-Mediums durch ein Passwort, oder noch besser durch Verschlüsselung unterstützen. Weiterhin sollte sie in der Lage sein, die gesicherten Daten in komprimierter Form abzuspeichern.
- Durch Vorgabe geeigneter Include- und Exclude-Listen bei der Datei- und Verzeichnisauswahl sollte genau spezifiziert werden können, welche Daten zu sichern sind und welche nicht. Es sollte möglich sein, diese Listen zu Sicherungsprofilen zusammenzufassen, abzuspeichern und für spätere Sicherungsläufe wieder zu benutzen.
- Es sollte möglich sein, die zu sichernden Daten in Abhängigkeit vom Datum ihrer Erstellung bzw. ihrer letzten Modifikation auszuwählen.
- Die Sicherungssoftware sollte die Erzeugung logischer und physischer Vollkopien sowie inkrementeller Kopien (Änderungssicherungen) unterstützen.
- Die Sicherung sollte auch auf Festplatten und Netzlaufwerken erfolgen können.
- Die Sicherungssoftware sollte in der Lage sein, nach der Sicherung einen automatischen Vergleich der gesicherten Daten mit dem Original durchzuführen und nach der Wiederherstellung von Daten einen entsprechenden Vergleich zwischen den rekonstruierten Daten und dem Inhalt des Sicherungsdatenträgers durchzuführen.
- Bei der Wiederherstellung von Dateien sollte es möglich sein auszuwählen, ob die Dateien am ursprünglichen Ort oder auf einer anderen Platte bzw. in einem anderen Verzeichnis wiederhergestellt werden. Ebenso sollte es möglich sein, das Verhalten der Software für den Fall zu steuern, dass am Zielort schon eine Datei gleichen Namens vorhanden ist. Dabei sollte man

wählen können, ob diese Datei immer, nie oder nur in dem Fall, dass sie älter als die zu rekonstruierende Datei ist, überschrieben wird, oder dass in diesem Fall eine explizite Anfrage erfolgt.

Zusätzlich zur Durchführung der normalen Datensicherungen ist es empfehlenswert, die aktuelle Systemkonfiguration nach jeder größeren Änderung mit dem Dienstprogramm *RDISK* in den Rettungsverzeichnis *%SystemRoot%\REPAIR* (z. B. *\WINNT\REPAIR)* sowie auf eine Notfalldiskette zu sichern, um sie bei eventuellen Inkonsistenzen wiederherstellen zu können (siehe auch M 6.42 *Erstellung von Rettungsdisketten für Windows NT*). Dabei ist zu beachten, dass die aktuellen Sicherheitseinträge der Registrierung (in den Bereichen *SECURITY* und *SAM*) nur dann gesichert werden, wenn *RDISK* mit dem Parameter **/s** aufgerufen wird. Dies kann jedoch dazu führen, dass die Sicherung nicht mehr auf eine Diskette paßt, wenn auf dem betreffenden System eine größere Anzahl von Benutzerprofilen definiert ist.

Eine Sicherung der Registrierung ist auch mit dem Dienstprogramm *REGBACK.EXE* des Windows NT Resource Kits möglich; die Wiederherstellung erfolgt in diesem Fall mit dem Dienstprogramm *REGREST.EXE* des Windows NT Resource Kits.

Ergänzende Kontrollfragen:

- Sind alle Daten eines Rechners gesichert?
- Wird der Datensicherungsvorgang dokumentiert?
- Ist der Datensicherungsvorgang konform zu einem vorhandenen Datensicherungskonzept?

M 6.45 Datensicherung unter Windows 95

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Generell zu beachten sind die Anforderungen aus M 6.32 *Regelmäßige Datensicherung*. Nachfolgend soll aufgezeigt werden, welche besonderen Aspekte unter Windows 95 zu berücksichtigen sind.

Unter Windows 95 sollten nach Möglichkeit nur Programme zur Datensicherung eingesetzt werden, die lange Dateinamen unterstützen (zum Beispiel das Windows 95 Programm *BACKUP.EXE*). Zur Konvertierung langer Dateinamen in die 8.3-Dateinamen-Konvention steht das zum Lieferumfang gehörenden Programm *LFNBK.EXE* zur Verfügung. Allerdings ist beim Einsatz dieses Programmes besondere Vorsicht geboten, da möglicherweise Dateinamen oder sogar einzelne Dateien nicht rekonstruiert werden können, falls nach der Sicherung Veränderungen an der Verzeichnisstruktur auf dem PC, von dem gesichert wurde, vorgenommen worden sind.

Ergänzende Kontrollfrage:

- Werden Programme zur Datensicherung eingesetzt, die lange Dateinamen nicht verarbeiten können?

M 6.46 Erstellung von Rettungsdisketten für Windows 95

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Für jeden Windows 95-Rechner sollten Rettungsdisketten erstellt werden, um bei Systemproblemen den Rechner wieder starten und ggf. benutzerspezifischen Profile wieder herstellen zu können.

Dazu benötigt man zum einen eine startfähige Systemdiskette, die für alle Rechner gemeinsam genutzt werden kann, zum anderen eine rechner- und benutzerspezifische Diskette, die die individuellen Einstellungen des Benutzers und des jeweiligen Rechners enthält.

Erzeugen der startfähigen Systemdiskette

Eine für alle Rechner nutzbare Systemdiskette kann mit der Registerkarte *STARTDISKETTE* unter der Systemsteuerungsoption *SOFTWARE* erzeugt werden. Allerdings benötigt man dazu eine Windows 95 CD. Stattdessen kann der erfahrene Benutzer alle relevante Dateien auch manuell auf die Diskette kopieren. Dazu gehören beispielsweise *COMMAND.COM*, *IO.SYS*, *DRVSPACE.BIN* und *MSDOS.SYS*. In diesem Fall sollten außerdem der deutsche Tastaturtreiber *KEYB.COM* sowie *KEYBOARD.SYS*, *COUNTRY.SYS* und ggf. weitere Systemdateien (z. B. einen CD-ROM-Treiber) kopiert werden. Die deutsche Tastatur stellt man dann mit dem Befehl *KEYB GR,,KEYBOARD.SYS* ein. Für andere notwendige Dateien, z. B. einen Editor, Programme zur Festplattendekomprimierung oder Backup-Programme, kann ggf. eine zusätzliche Diskette verwendet werden.

Erzeugen von rechner- und benutzerspezifischen Disketten

Hierzu wird für jeden Rechner eine vorformatierte Diskette und das Programm *EMERGENCY RECOVERY UTILITY (ERU)* benötigt, welches zum Systemumfang gehört. Dieses wird zwar nicht standardmäßig installiert, befindet sich aber auf der mitgelieferten Windows 95 CD-ROM. Mit diesem Programm lassen sich in einfacher Weise die relevanten und aktuellen Systemdateien, insbesondere die Datei mit den Benutzereinstellungen *USER.DAT* bzw. die Datei mit den Systemeinstellungen *SYSTEM.DAT*, auf Diskette kopieren. Die Dateien *USER.DAT* und *SYSTEM.DAT* beinhalten die entsprechenden Informationen, die unter Windows 3.x in den *ini*-Dateien gespeichert sind. Diese Diskette sollte bei umfangreichen oder wichtigen Änderungen an der Rechnerkonfiguration oder an den Benutzereinstellungen aktualisiert werden.

Nach dem Erstellen der Rettungsdisketten sollten diese auf Computer-Viren überprüft und danach schreibgeschützt werden.

Nutzung der Start-Diskette

Um von der Systemdiskette zu starten, wird diese in das Diskettenlaufwerk eingelegt, die Start-Reihenfolge im BIOS zugunsten des Diskettenlaufwerkes

priorisiert und der Rechner neu gestartet. Der Rechner fährt dann im Zeilenmodus hoch.

Nutzung der rechner- und benutzerspezifischen Diskette

Falls der Rechner ordnungsgemäß startet (mit oder ohne Start-Diskette), die rechner- und benutzerspezifischen Dateien jedoch zerstört sind, können diese mit dem Programm *ERD.EXE*, das sich auf der rechner- und benutzerspezifischen Diskette befindet, zurückgespielt werden. Die korrespondierende Dateien auf der Festplatte werden zuvor in das Verzeichnis *C:\WINDOWS\ERUNDO* verschoben und können mit den Befehl *ERD /UNDO* ggf. rekonstruiert werden.

Hinweis: Für die Nutzung des Programmes *ERD.EXE* ist es notwendig, den Rechner im Zeilenmodus zu starten. Dies erreicht man zum Beispiel, indem man von der Startdiskette startet, beim Beenden von Windows 95 *COMPUTER IM MS-DOS MODUS STARTEN* wählt oder beim Starten des Rechners während der Nachricht "Windows 95 wird gestartet" die F8-Taste betätigt und anschließend"*5. Nur Eingabeaufforderung*" wählt. Letzteres ist allerdings nur dann möglich, wenn in der Datei *MSDOS.SYS* die Zeile **BootKeys=1** eingetragen ist.

Ergänzende Kontrollfragen:

- Wurde für Windows 95 Rechner eine startfähige Systemdiskette erstellt?
- Wurde für **jeden** Windows 95 Rechner eine rechner- und benutzerspezifische Rettungsdiskette erstellt?

M 6.47 Datensicherung bei der Telearbeit

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Telearbeiter

Bei Telearbeit können Daten auf verschiedenen IT-Systemen und an verschiedenen Orten verarbeitet werden, also beispielsweise auf Servern und Clients in der Institution, aber auch auf Clients am Telearbeitsplatz. Die Datensicherung aller relevanten Daten am Telearbeitsplatz muss sichergestellt sein. Das Datensicherungskonzept der Institution darf sich nicht auf die Server beschränken, sondern auch die am Telearbeitsplätze müssen in dieses einbezogen werden.

Generell bieten sich folgende Verfahren am Telearbeitsplatz zur Datensicherung an:

1. Datensicherung auf externen Datenträgern

   Hierfür müssen die Telearbeiter die erforderliche technische Ausstattung haben und entsprechend geschult sein.

2. Datensicherung über Netz

   Die Sicherung der lokalen Daten kann auch über die Netzanbindung an das Netz der Institution erfolgen. Vorteilhaft ist hier, dass die Datensicherung nicht von den Benutzern selbstständig durchgeführt werden muss und diese auch keine Datenträger verwalten müssen.

   Entscheidend bei der Datensicherung über eine Netzverbindung ist, dass deren Bandbreite für das Volumen der zu sichernden Daten ausreichen muss. Die Datenübertragung darf nicht zu lange dauern und nicht zu übermäßigen Verzögerungen führen, wenn der Benutzer gleichzeitig auf entfernte Ressourcen zugreifen muss. Bei gängigen Zugangstechnologien (z. B. ISDN, Modem) bedeutet dies, dass nur geringe Datenmengen pro Sicherungsvorgang transportiert werden können. Einige Datensicherungsprogramme bieten daher die Möglichkeit an, lediglich Informationen über die Änderungen des Datenbestands seit der letzten Datensicherung über die Netzverbindung zu übertragen. In vielen Fällen kann hierdurch das zu transportierende Datenvolumen stark reduziert werden.

   Eine wichtige Anforderung an die zur Datensicherung verwendete Software ist, dass unerwartete Verbindungsabbrüche erkannt und ordnungsgemäß behandelt werden. Die Konsistenz der gesicherten Daten darf durch Verbindungsabbrüche nicht beeinträchtigt werden.

Bei beiden Verfahren zur Datensicherung ist es wünschenswert, das Volumen der zu sichernden Daten zu minimieren. Neben dem Einsatz verlustfreier Kompressionsverfahren, die in viele Datensicherungsprogrammen integriert sind, können auch inkrementelle oder differentielle Sicherungsverfahren zum Einsatz kommen (siehe auch M 6.35 *Festlegung der Verfahrensweise für die Datensicherung*). Hierdurch erhöht sich jedoch unter Umständen der Aufwand für die Wiederherstellung einer Datensicherung.

Die Datensicherung sollte möglichst weitgehend automatisiert werden, so dass die Benutzer möglichst wenig Aktionen selbst durchführen müssen. Wenn die

Mitarbeit der Benutzer erforderlich ist, sollten sie zur regelmäßigen Durchführung der Datensicherung verpflichtet werden (siehe M 2.41 *Verpflichtung der Mitarbeiter zur Datensicherung*). Schließlich sollte sporadisch geprüft werden, ob angelegte Datensicherungen wiederhergestellt werden können (siehe M 6.22 *Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen*).

Aufbewahrung der Backup-Datenträger

Falls Datensicherungen im häuslichen Bereich durchgeführt werden, müssen Backup-Datenträger dort verschlossen aufbewahrt werden. Es ist sicherzustellen, dass nur der Telearbeiter selber bzw. sein Vertreter darauf Zugriff hat.

Jeweils eine Generation der Backup-Datenträger sollte jedoch in der Institution aufbewahrt werden, damit im Katastrophenfall der Vertreter auf die Backup-Datenträger zugreifen kann.

Ergänzende Kontrollfragen:

- Werden alle Daten, die bei der Telearbeit bearbeitet werden, regelmäßig gesichert?
- Ist das gewählte Verfahren zur Datensicherung für das Volumen des Datenbestands geeignet?
- Sind bei der Datensicherung möglichst wenig Aktionen des Benutzers erforderlich?
- Wo werden die Datenträger der Datensicherungen des Telearbeiters aufbewahrt?

M 6.48 Verhaltensregeln nach Verlust der Datenbankintegrität

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Falls sich das Datenbanksystem in nicht vorgesehener Weise verhält (zum Beispiel undefiniertes Systemverhalten, nicht auffindbare Tabellen oder Datensätze, veränderte Tabelleninhalte, unerklärlich langes Antwortzeitverhalten oder ähnliches), kann ein Verlust der Datenbankintegrität vorliegen. Dieser kann auch durch missbräuchliche Nutzung des Systems verursacht worden sein, zum Beispiel durch Veränderungen der Systemeinstellungen.

Für solche Problemfälle sollte ein Konzept (Wiederherstellungskonzept) erstellt werden, das Prüfungen, Entscheidungen und Aktionen beschreibt, um die Datenbank auf schnellem und sicherem Wege wieder zur Verfügung stellen zu können (siehe M 6.51 *Wiederherstellung einer Datenbank*).

Ein weiterer wichtiger Aspekt ist die Benachrichtigung der Benutzer der Datenbank. Dies sollte unverzüglich nach Auftreten von Anzeichen für einen Integritätsverlust erfolgen, bevor die Arbeiten zur Wiederherstellung beginnen. Für diesen Fall und für die Situation, dass einem Benutzer Unregelmäßigkeiten bei der Nutzung der Datenbank auffallen, sollten den Benutzern Verhaltensregeln in Form eines Merkblattes an die Hand gegeben werden, das mindestens folgende Punkte enthalten sollte:

- Ruhe bewahren!
- Benachrichtigen Sie den Datenbankadministrator
- Greifen Sie nicht mehr auf die Datenbank zu
- Befolgen Sie die Anweisungen des Datenbankadministrators

Der Datenbankadministrator sollte genau nach dem Wiederherstellungskonzept vorgehen, das unter anderem folgende Schritte vorsehen sollte, die je nach Fehlerursache durchzuführen sind:

Information

- Umgehende Benachrichtigung aller betroffenen Benutzer mit der Bitte, keine weiteren Datenbankzugriffe durchzuführen und auf neue Anweisungen zu warten.
- Turnusmäßige Information der betroffenen Benutzer über den aktuellen Stand der Fehlerbehebung.

Sicherung des aktuellen Zustands

- Herunterfahren des Datenbanksystems.
- Hochfahren des Datenbanksystems im Exklusiv-Modus (falls dies vom Datenbanksystem unterstützt wird).
- Sichern aller Dateien, die Aufschluss über die Art und Ursache des aufgetretenen Problems geben könnten (z. B. ob tatsächlich ein Angriff erfolgt ist und auf welche Weise der Angreifer eindringen konnte), d. h. insbesondere Sichern aller relevanten Protokolldateien.

Analyse und Interpretation

- Überprüfung und Interpretation der Protokolldateien nach Auffälligkeiten (in Zusammenarbeit mit dem Revisor und/oder dem IT-Sicherheitsbeauftragten).
- Überprüfung der Zugriffsrechte auf Systemtabellen.
- Überprüfung der Datenbank-Software auf sichtbare Veränderungen, z. B. Erstellungsdatum und Größe der entsprechenden Dateien. (Da diese von einem Angreifer auch wieder auf ihre Ursprungswerte zurückgesetzt werden können, sollte ein Prüfsummenverfahren eingesetzt werden.)

Situationsabhängige Reaktion

- Löschen der Datenbank-Software und Wiedereinspielen der Original-Dateien von schreibgeschützten Datenträgern (siehe M 6.21 *Sicherungskopie der eingesetzten Software*). Programme aus existierenden Datensicherungen sollten nur dann wiedereingespielt werden, wenn hinreichend sicher ist, dass die wiedereingespielte Software den Fehler nicht bereits enthält.
- Zurücksetzen der Passwörter.
- Zurücksetzen der Zugriffsrechte auf Systemtabellen.
- Benachrichtigung der Benutzer mit der Bitte, ihre Bereiche auf Unregelmäßigkeiten zu prüfen.

Nach dem Zurücksetzen der Passwörter auf ein Default-Passwort müssen die Benutzer unverzüglich aufgefordert werden, bei der nächsten Anmeldung neue Passwörter zu vergeben und hierbei die Vorgaben der Passwortrichtlinie zu beachten. Ist das Zurücksetzen auf ein Default-Passwort nicht möglich oder durch die Passwortrichtlinie untersagt, sollten die Passwörter zufällig erzeugt und den Benutzern auf zuverlässigem Weg mitgeteilt werden, z. B. in versiegelten Umschlägen. Diese Passwörter sollten direkt nach der Erstanmeldung geändert werden. Der Administrator sollte kontrollieren, dass die Default-Passwörter unmittelbar abgeändert wurden.

Falls Daten gelöscht oder unerwünscht geändert wurden, können diese aus den Datensicherungen wiedereingespielt werden (siehe M 6.51 *Wiederherstellung einer Datenbank*).

Wenn Anzeichen auf einen vorsätzlichen Angriff gegen eine Datenbank vorliegen, ist für die Schadensminimierung und weitere Schadensabwehr sofortiges Handeln notwendig. Hierzu ist ein Alarmplan erforderlich, in dem die einzuleitenden Schritte aufgeführt werden und festgelegt wird, welche Personen über den Vorfall zu unterrichten sind (siehe auch M 6.60 *Verhaltensregeln und Meldewege bei Sicherheitsvorfällen*). Der Alarmplan enthält gegebenenfalls auch Informationen darüber, ob und wie der Datenschutzbeauftragte und die Rechtsabteilung zu beteiligen sind.

Ergänzende Kontrollfragen:

- Werden die Benutzer regelmäßig darüber informiert, dass bei Auftreten von Unregelmäßigkeiten sofort der Datenbankadministrator benachrichtigt werden muss?
- Wird diese Regelung auch angewendet?
- Gibt es Datenbankadministratoren mit entsprechenden Kenntnissen?
- Existiert ein Wiederherstellungskonzept bzw. ein Alarmplan?
- Ist ein Verfahren zur schnellen und sicheren Vergabe von Passwörtern etabliert und getestet?

M 6.49 Datensicherung einer Datenbank

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Sicherung der Daten eines Datenbanksystems kann in aller Regel nicht mit den Datensicherungsprogrammen auf Betriebssystemebene vollständig abgedeckt werden. Letztere bilden in den meisten Fällen lediglich das Bindeglied, um die zu sichernden Daten auf ein Sicherungsmedium zu schreiben. Zur Sicherung des DBMS und der Daten müssen dagegen für die meisten Datenbankprodukte zusätzlich die jeweiligen Dienstprogramme des DBMS eingesetzt werden.

Die einfachste Möglichkeit einer Datenbanksicherung, die zugleich die sicherste darstellt, ist eine Komplettsicherung der Datenbank in heruntergefahrenem Zustand. Dabei werden alle zur Datenbank gehörenden Dateien auf dem Sicherungsmedium gesichert. Meist ist dieses Vorgehen allerdings aus Gründen der Verfügbarkeitsanforderungen an die Datenbank oder aufgrund des zu sichernden Datenvolumens nicht durchführbar.

Eine Alternative zur oben beschriebenen Komplettsicherung ist eine Online-Sicherung der Datenbank. Die Sicherung erfolgt dann während des laufenden Betriebs, d. h. die Datenbank muss nicht heruntergefahren werden. Die Nachteile dieser Sicherungsart sind, dass Inkonsistenzen nicht explizit ausgeschlossen werden können, und dass auch in diesem Fall bei einer Zerstörung der Datenbank eine (Offline-) Komplettsicherung existieren muss, auf der aufbauend die Online-Sicherungen zurückgespielt werden können. Online-Sicherungen sollten aus diesem Grund nur dann durchgeführt werden, wenn eine permanente Verfügbarkeit der Datenbank gefordert ist. Auf eine Offline-Komplettsicherung, die in vertretbar großen Zeitabständen durchgeführt werden kann, sollte trotzdem nicht verzichtet werden.

Partielle Datenbanksicherungen stellen eine weitere Möglichkeit dar. Sie sollten immer dann verwendet werden, wenn das zu sichernde Datenvolumen zu groß ist, um eine vollständige Sicherung durchführen zu können. Dies kann daraus resultieren, dass die Kapazitäten der Sicherungsmedien nicht ausreichen oder dass der zur Verfügung stehende Zeitrahmen je Sicherung nicht genügt, um eine vollständige Sicherung durchführen zu können.

Falls möglich, so sollten in jedem Fall alle Transaktionen zwischen zwei Offline-Komplettsicherungen archiviert werden. Oracle bietet dazu beispielsweise die Möglichkeit an, indem der sogenannte ARCHIVE-Mode für die Datenbank aktiviert wird. Transaktionen werden bei Oracle in sogenannten Log-Dateien protokolliert, von denen es mehrere gibt. Diese werden nacheinander beschrieben und sobald alle Log-Dateien voll sind, so wird wieder die erste Log-Datei überschrieben. Der ARCHIVE-Mode erstellt von diesen Log-Dateien eine Sicherungskopie, bevor sie wieder überschrieben werden. Auf diese Art und Weise können bei einer Zerstörung der Datenbank alle Transaktionen komplett rekonstruiert werden. Auch hierfür ist allerdings die Existenz einer Komplettsicherung der Datenbank die Voraussetzung. Die Dauer eines solchen Recovery wächst mit der Anzahl der zurückzuspielenden Archiv-Log-Dateien an.

Für die Datensicherung eines Datenbanksystems muss ein eigenes Datensicherungskonzept erstellt werden. Einflussfaktoren für ein solches Konzept sind:

- **Verfügbarkeitsanforderungen an die Datenbank**

  Wenn beispielsweise eine Datenbank werktags rund um die Uhr zur Verfügung stehen muss, so kann eine Komplettsicherung nur am Wochenende durchgeführt werden, da dies im allgemeinen ein Herunterfahren der Datenbank erfordert.

- **Datenvolumen**

  Das gesamte zu sichernde Datenvolumen muss mit den zur Verfügung stehenden Sicherungskapazitäten verglichen werden. Dabei muss festgestellt werden, ob die Sicherungskapazitäten (z. B. ein DAT-Tape pro Sicherungslauf) für das entsprechende Datenvolumen der Datenbank ausreichend dimensioniert sind.

  Falls dies nicht der Fall ist, muss ein Konzept zur Teilsicherung des Datenvolumens erstellt werden. Dies kann z. B. bedeuten, dass die Daten einzelner Anwendungen oder einzelner Bereiche der Datenbank immer im Wechsel gesichert werden bzw. nur die aktuellen Änderungen. Die Möglichkeiten einer Teilsicherung hängen von der verwendeten Datenbank-Software ab.

- **Maximal verkraftbarer Datenverlust**

  Hier muss festgelegt werden, ob bei einer Zerstörung der Datenbank der Datenverlust eines Tages verkraftbar ist, oder ob die Datenbank bis zur letzten Transaktion wiederherstellbar sein muss. Dies ist im allgemeinen bei einer hohen Anforderung an die Verfügbarkeit bzw. Integrität der Daten der Fall.

- **Wiederanlaufzeit**

  Auch die maximal zulässige Zeitdauer des Wiederherstellens der Datenbank nach einem Absturz muss festgelegt werden, um den Verfügbarkeitsanforderungen zu genügen.

- **Datensicherungsmöglichkeiten der Datenbank-Software**

  Im allgemeinen werden von einer Datenbank-Standardsoftware nicht alle denkbaren Datensicherungsmöglichkeiten unterstützt, wie z. B. eine partielle Datenbanksicherung. Im konkreten Fall gilt es also zu prüfen, ob das erstellte Datensicherungskonzept mit den zur Verfügung stehenden Mechanismen auch umgesetzt werden kann.

Anhand dieser Informationen kann ein Konzept für die Datensicherung der Datenbank erstellt werden. In diesem Sicherungskonzept wird unter anderem festgelegt (siehe hierzu auch Baustein B 1.4 *Datensicherungskonzept*)

- wer für die ordnungsgemäße Durchführung von Datensicherungen zuständig ist,
- in welchen Zeitabständen eine Datenbanksicherung durchgeführt wird,
- in welcher Art und Weise die Datenbanksicherung zu erfolgen hat,
- zu welchem Zeitpunkt die Datenbanksicherung durchgeführt wird,
- die Spezifikation des zu sichernden Datenvolumens je Sicherung.
- wie die Erstellung von Datensicherungen zu dokumentieren ist, und
- wo die Datensicherungsmedien aufbewahrt werden.

Beispiel:

Sicherung von Montag bis Samstag:

- Startzeit: morgens um 3.00h
- Es erfolgt eine vollständige Sicherung der Daten, wobei die Datenbank nicht heruntergefahren, sondern die Möglichkeit der Online-Sicherung des DBMS genutzt wird.

Sicherung am Sonntag

- Startzeit: morgens um 3.00h
- Die Datenbank wird heruntergefahren und es erfolgt eine Komplettsicherung der Datenbank.

Ergänzende Kontrollfragen:

- Existiert eine Dokumentation, wie im Falle eines Absturzes der Datenbank diese wiederherzustellen ist?
- Ist für die Institution ein aktuelles Datensicherungskonzept für den Bereich Datenbanken dokumentiert?
- Wie werden Mitarbeiter über den sie betreffenden Teil des Konzepts unterrichtet?
- Wird die Einhaltung dieses Konzepts kontrolliert?
- Wie werden Änderungen der Einflussfaktoren berücksichtigt?

M 6.50 Archivierung von Datenbeständen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator

Ist eine Archivierung von Daten eines Datenbanksystems erforderlich, so muss dazu ein entsprechendes Konzept erstellt werden, durch das sichergestellt wird, dass die Datenbestände zu einem späteren Zeitpunkt wieder vollständig und konsistent zur Verfügung gestellt werden zu können. Hierbei sind folgende Punkte zu berücksichtigen:

Archivierung

- Die zur Verfügung stehenden Archivierungsmöglichkeiten müssen identifiziert werden.
- Es muss dokumentiert werden, welches Datenmodell den zu archivierenden Daten zugrunde liegt.
- Der Zeitpunkt der Archivierung ist zu dokumentieren.
- Die Version des Datenbankmanagementsystems und der benutzten Dienstprogramme sind zu dokumentieren.
- Aufbau, Systematik und Ordnungskriterien des Archivs müssen spezifiziert werden.
- Für alle Archivierungsmedien ist anhand von Herstellerangaben und Erfahrungswerten eine maximale physikalische Lebensdauer zu bestimmen. Entsprechend müssen Zeitpunkte für die Auffrischung des archivierten Datenbestandes festgelegt werden.
- Die geforderte Verfügbarkeit der archivierten Datenbestände ist regelmäßig zu überprüfen und gegebenenfalls an die konkreten Anforderungen anzupassen. Notwendige Anpassungen haben unter anderem Auswirkungen auf die Wahl des Archivierungsmediums sowie auf die Art und Weise der Archivierung. Bei hohen Verfügbarkeitsanforderungen müssen eventuell mehrere historische Versionen der gleichen Datenbanken parallel zugreifbar gehalten werden.
- Es muss sichergestellt sein, dass vorgegebene Aufbewahrungsfristen eingehalten werden.

Wiedereinspielen

- Der aktuelle Datenbestand darf von dem archivierten Datenbestand nicht beeinflusst werden.
- Für die Wiedereinspielung von archivierten Datenbeständen muss genügend Speicherplatz zur Verfügung gestellt werden.
- Der archivierte Datenbestand muss wiederherstellbar sein, auch wenn sich zwischenzeitlich das Datenmodell oder die Datenbankversion geändert hat. In diesem Fall müssen das Datenmodell und die entsprechenden Dienstprogramme zum Archivierungszeitpunkt bekannt sein, um den alten Stand wiederherstellen zu können.

- Wenn die wiedereingespielten Daten von einer Anwendung verarbeitet werden sollen, muss auch von dieser Anwendung eine Version vorhanden sein, die das "alte" Datenmodell unterstützt.
- Es muss regelmäßig überprüft werden, ob sich der archivierte Datenbestand wiedereinspielen lässt.

Bei der Archivierung von Datenbeständen, die personenbezogene Daten enthalten, müssen darüber hinaus die Vorschriften der Datenschutzgesetze und die daraus folgenden Regelungen berücksichtigt werden. Dies bedeutet beispielsweise, dass die Betroffenen ein Recht auf Berichtigung, Sperrung bzw. Löschung der über sie gespeicherten Daten haben. Unter Umständen müssen Daten nach einer gewissen Zeit vollständig, d. h. auch auf den existierenden Sicherungen und Archiven, gelöscht werden. Um dies zu gewährleisten, sind entsprechende technisch-organisatorische Verfahren zu entwickeln. Insbesondere müssen auch nach dem Wiedereinspielen alter Datenbestände alle Korrekturen, Änderungen, Sperrungen bzw. Löschungen erhalten bleiben, die zwischen dem Datum der Sicherung des wiedereingespielten Datenbestands und dem Wiedereinspielen erfolgt sind.

Ergänzende Kontrollfragen:

- Existiert eine Dokumentation, wie beim Wiedereinspielen von archivierten Datenbeständen zu verfahren ist?
- Ist für die Institution ein aktuelles Archivierungskonzept dokumentiert?
- Wie werden Änderungen der Einflussfaktoren berücksichtigt?

M 6.51 Wiederherstellung einer Datenbank

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Für die Wiederherstellung von Datenbanken ist ein Konzept zu erstellen, das die Abläufe des Wiedereinspielens von Datenbanksicherungen regelt. Grundlagen dieses Konzepts sind:

- das Datensicherungskonzept (siehe M 6.49 *Datensicherung einer Datenbank*) und
- die möglichen Fehlersituationen, die ein Wiedereinspielen von Datenbanksicherungen erforderlich machen können (siehe unter anderem auch M 6.48 *Verhaltensregeln nach Verlust der Datenbankintegrität*).

Anhand dieser Punkte ist abzuleiten, welche Datenbanksicherungen in welcher Form wiedereingespielt werden müssen.

Die Wiederherstellung einer Datenbank kann eine komplexe Aufgabe sein, die ein äußerst sorgfältiges Vorgehen erfordert und deren Schritte durch regelmäßige Testläufe geprobt werden sollten. Trotzdem kann es passieren, dass eine Wiederherstellung nicht reibungslos und fehlerfrei funktioniert.

Bei der Wiederherstellung sind zwei Aspekte aufeinander abzustimmen. Einerseits sollte die betroffene Datenbank so schnell wie möglich den Benutzern wieder zur Verfügung stehen, auf der anderen Seite sollte ein möglichst aktueller Stand der Datenbank hergestellt sowie die Schadensursache analysiert werden. Sollte der Ausfall der Datenbank nicht eindeutig auf einen Hardware-Schaden zurückzuführen sein, ist der Umfang der Inkonsistenz oft nur schwer festzustellen. Auch kann die Datenbank nicht immer ohne Probleme bis zur letzten Transaktion vor Entdeckung des Fehlers wiederhergestellt werden.

In solchen Fällen ist zu entscheiden, ob ein begrenzter Aktualitätsverlust oder eher eine längere Betriebsunterbrechung zu vertreten ist. Dies hängt wesentlich vom Einsatzgebiet der Datenbank, von der Art des Fehlers und von der Zeit zwischen dem ersten Auftreten des Fehlers und seiner Entdeckung bzw. der ersten Reaktion darauf ab. Insbesondere bei Schäden durch falsche Administration oder unzulässige Manipulation ist das genaue Ausmaß des Schadens oft schwer festzustellen.

Hierzu sollten Entscheidungsrichtlinien sowie entsprechende Handlungsanweisungen Bestandteil des Wiederherstellungskonzepts sein. Um die Datenbank so schnell wie möglich wieder zur Verfügung zu stellen, sollte die betroffene Datenbank in einem getrennten System oder Speicherbereich wiederhergestellt und für den Benutzer freigegeben werden. Wenn Zugriffsfunktionalitäten von den Daten getrennt sind (siehe M 2.134 *Richtlinien für Datenbank-Anfragen*) kann dies meist für die Benutzer transparent durchgeführt werden.

Auf keinen Fall sollte die zerstörte Datenbank ohne weitere Prüfung (siehe M 6.48 *Verhaltensregeln nach Verlust der Datenbankintegrität*) durch ein einfaches Zurückspielen der Datenbanksicherung überschrieben werden. Häufig lässt sich die für inkonsistent gehaltene Datenbank wieder bereinigen,

ohne dass eine vollständige Restaurierung der Datenbank notwendig ist, sondern indem lediglich einzelne Datenbestände wiedergestellt werden. Auch im Fall einer partiellen Wiederherstellung ist abzuwägen, ob zuerst die Datenbank an anderer Stelle auf einem Test-System wiederhergestellt wird und nach der Sicherstellung der ordnungsgemäßen Wiederherstellbarkeit die Originaldatenbank bereinigt wird.

Auch wenn sich die beschädigte Datenbank nicht mehr reparieren lässt, sollte sie dennoch zur Analyse und Feststellung der Fehlerursache erhalten bleiben.

Im Wiederherstellungskonzept sollte festgelegt sein, welche Ressourcen in welchem Umfang für den Notfall bereitgehalten werden müssen. Eckpunkte, die hierbei beachtet werden müssen, sind insbesondere Speicherkapazitäten und Festplattenbereiche. Diese Größen sind regelmäßig anhand der aktuellen Datenbankgrößen zu überprüfen, um sicherzustellen, dass im Notfall die Auswirkungen auf andere Datenbanken minimiert werden können.

Ergänzende Kontrollfragen:

- Wurde ein Konzept zum Wiedereinspielen von Datenbanksicherungen erstellt?
- Wann wurde das Wiedereinspielen von Datenbanksicherungen das letzte Mal geübt?
- Werden für den Notfall genügend Speichermedien bereitgehalten?

M 6.52 Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

An die Verfügbarkeit der zentralen aktiven Netzkomponenten müssen hohe Anforderungen gestellt werden, da in der Regel viele Benutzer vom reibungslosen Funktionieren eines lokalen Netzes abhängig sind. Damit in einem Fehlerfall der Betrieb so schnell wie möglich wieder aufgenommen werden kann, müssen alle Konfigurationsdaten der aktiven Netzkomponenten in elektronischer Form gesichert werden (siehe auch M 6.32 *Regelmäßige Datensicherung*). Diese Sicherung kann prinzipiell lokal an den einzelnen Komponenten erfolgen oder über das Netz, z. B. mit Hilfe eines Netzmanagement-Tools. Wurden die Daten elektronisch gesichert, kann in diesem Fall das Wiederherstellen einer Konfiguration schneller und sicherer durchgeführt werden und eine zeitaufwendige manuelle Eingabe entfallen. Das Wiedereinspielen der Daten kann hierbei automatisch, z. B. durch ein zentrales Netzmanagement-Tool oder manuell durch den Eingriff eines Administrators erfolgen.

TFTP vermeiden

Bei einer Sicherung der Konfigurationsdaten über das Netz ist jedoch, im Gegensatz zu einer lokalen Sicherung, zu beachten, dass die übertragenen Daten eventuell mitgelesen werden können und potentielle Angreifer möglicherweise sicherheitskritische Informationen über die Konfiguration der aktiven Netzkomponenten, wie z. B. Passwörter, und damit möglicherweise über die gesamte Netzkonfiguration erhalten. Dabei werden im allgemeinen die Protokolle *Trivial File Transfer Protocol* (TFTP) oder *Remote Copy Protocol* (RCP) eingesetzt, wobei nach Möglichkeit RCP mit Authentisierung verwendet werden sollte (siehe M 5.20 *Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp*). TFTP bietet dagegen keine Schutzmechanismen vor einem unbefugten Zugriff auf die Konfigurationsdaten (siehe auch M 5.21 *Sicherer Einsatz von telnet, ftp, tftp und rexec*), so dass von dessen Einsatz abgeraten wird.

Wiederherstellbarkeit prüfen

Bei allen Sicherungsmethoden muss ein Test durchgeführt werden, ob die Sicherung ordnungsgemäß durchgeführt wurde und die Wiederherstellung der Konfigurationsdaten möglich ist. Dies gilt insbesondere bei der Sicherung über das Netz, da hier nach einem Fehlerfall das Netz u. U. in einem Zustand ist, der keine Wiederherstellung über das Netz ermöglicht.

Ergänzende Kontrollfragen:

- Sind alle Konfigurationsdaten aktiver Netzkomponenten gesichert?
- Wird der Datensicherungsvorgang dokumentiert?
- Ist der Datensicherungsvorgang konform zu einem vorhandenen Datensicherungskonzept (siehe M 6.13 *Erstellung eines Datensicherungsplans*)?

M 6.53 Redundante Auslegung der Netzkomponenten

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Beschaffungsstelle

An die Verfügbarkeit der zentralen Netzkomponenten müssen hohe Anforderungen gestellt werden, da in der Regel viele Benutzer vom reibungslosen Funktionieren eines lokalen Netzes abhängig sind. Damit in einem Fehlerfall der Betrieb so schnell wie möglich wieder aufgenommen werden kann, ist in Abhängigkeit von den entsprechenden Verfügbarkeitsanforderungen im jeweiligen Bereich Redundanz zu schaffen, die einem Teil- oder Totalausfall der relevanten Netzkomponenten mit akzeptablem Aufwand vorbeugt.

Dabei gibt es zwei verschiedene Möglichkeiten, Redundanz zu erreichen:

- Die Netzkomponenten können redundant im Lager vorgehalten werden, um in einem Notfall kurzfristig einen Austausch durchführen zu können. Wird dies nicht beachtet, sind oft langwierige Beschaffungsvorgänge nötig, bevor die Störung behoben werden kann. Alternativ sind Wartungs- bzw. Lieferverträge mit den entsprechenden Herstellern abzuschließen, die einen schnellen Ersatz defekter Komponenten garantieren (siehe auch M 6.14 *Ersatzbeschaffungsplan*). Danach können die gesicherten Konfigurationsdaten wieder eingespielt werden, um die Ausfallzeit der betroffenen Netzsegmente so gering wie möglich zu halten (siehe M 6.52 *Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten*).
- Es ist weiterhin sinnvoll, bereits bei der Konzeption des Netzes eine redundante Auslegung der Netzkomponenten einzuplanen. So sollten alle zentralen Switches und je nach den verwendeten Protokollen alle Router zumindest doppelt in das Netz eingebunden sein, um die Anbindung der Server und die Verbindung zwischen den einzelnen Netzkomponenten redundant zu halten (siehe Abbildung 1). Die korrekte Funktionsweise ist durch eine geeignete logische Netzkonfiguration zu gewährleisten.

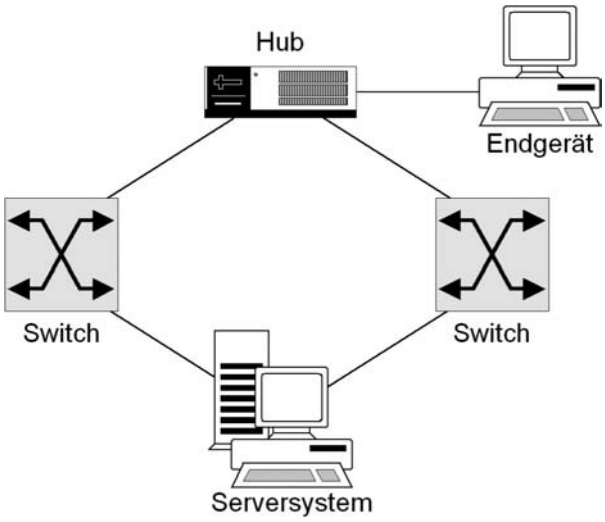


Abbildung 1: Redundante Verbindungen der Netzkomponenten

Ist je nach Verfügbarkeitsanforderungen auch eine Redundanz im Endgeräte-Bereich nötig, so müssen zusätzlich alle Endgeräte mit zwei Netzadaptern ausgerüstet werden (siehe Abbildung 2).

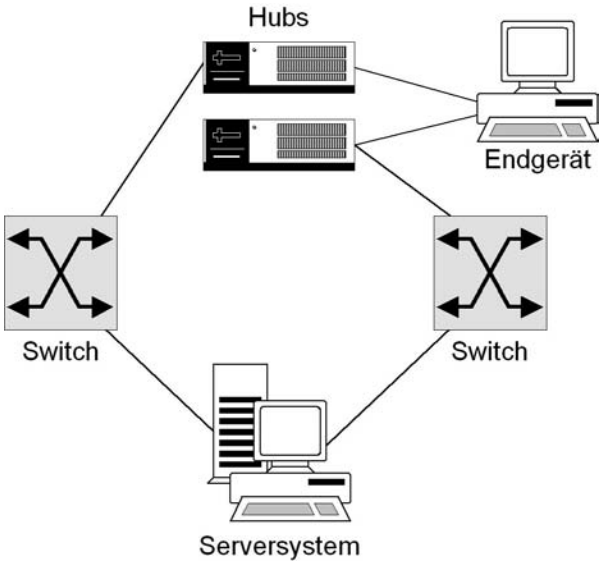


Abbildung 2: Redundanz bis in den Endgeräte-Bereich

Dabei gilt es im konkreten Fall zu prüfen, ob diese Technik von den eingesetzten aktiven Netzkomponenten und Betriebssystemen unterstützt wird.

Weiterhin stellt das Netzteil von aktiven Netzkomponenten eine häufige Störungsursache dar, da diese auf eine stabile Stromversorgung angewiesen sind. Viele Komponenten lassen sich deshalb mit redundanten Netzteilen ausrüsten oder sind hiermit bereits ausgestattet. So lässt sich die Ausfallsicherheit einzelner Netzkomponenten erhöhen, ohne dass zwei Netzkomponenten eingesetzt werden müssen. Durch solch eine Maßnahme wird aber nicht die Ausfallsicherheit der eigentlichen Funktionalität der Netzkomponenten erhöht.

Es muss in jedem Fall anhand einer sorgfältigen Analyse festgestellt werden, welche konkreten Verfügbarkeitsanforderungen gegeben sind. Im Rahmen einer detaillierten Planung der System- und Netzarchitektur muss dann ein geeignetes Redundanzkonzept entwickelt werden, welches diesen Anforderungen genügt. In diesem Zusammenhang ist auch die Maßnahme M 6.18 *Redundante Leitungsführung* zu beachten.

Ergänzende Kontrollfragen:

- Wurden die Verfügbarkeitsanforderungen an das Netz ermittelt und dokumentiert?
- Werden alle wichtigen Netzkomponenten im Lager vorgehalten bzw. existieren dazu Lieferverträge?
- Wurde bei der Planung des Netzes die Redundanz der Komponenten berücksichtigt?

M 6.54 Verhaltensregeln nach Verlust der Netzintegrität

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

missbräuchliche Nutzung

Falls sich das Netz in nicht vorgesehener Weise verhält (z. B. Server sind nicht verfügbar, Zugriff auf Netzressourcen ist nicht möglich, Netzperformance bricht dauerhaft ein), kann ein Verlust der Netzintegrität vorliegen. Dieser kann durch missbräuchliche Nutzung des Netzes verursacht worden sein, z. B. durch Veränderungen der Konfigurationen der aktiven Netzkomponenten oder deren Beschädigung.

Dann sollten die Benutzer folgende Punkte beachten:

- Sicherung der Arbeitsergebnisse und ggf. Beendigung aktiver Programme.
- **Administrator benachrichtigen**
  Der Administrator muss über eine geeignete Eskalationsstufe (z. B. User Help Desk) von den Benutzern benachrichtigt werden. Dabei ist sicherzustellen, dass der Administrator durch den Benachrichtigungsprozess in seiner Arbeit nicht wesentlich behindert wird.

Der Netzadministrator sollte folgende Schritte durchführen:

- Eingrenzen des fehlerhaften Verhaltens auf ein Netzsegment bzw. eine Netzkomponente,
- Überprüfen der Konfigurationen der dort vorhandenen aktiven Netzkomponenten (darunter fällt auch die Kontrolle der Passwörter),
- **Protokolldateien sichern**
  Sichern aller Dateien, die Aufschluss über die Art und Ursache des aufgetretenen Problems geben könnten (z. B. ob tatsächlich ein Angriff erfolgt ist und auf welche Weise der Angreifer eindringen konnte), d. h. insbesondere Sichern aller relevanten Protokolldateien,
- ggf. Wiedereinspielen der Original-Konfigurationsdaten (siehe M 6.52 *Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten*),
- ggf. Überprüfung der eingesetzten Hardware (Verkabelung, Steckverbindungen, aktive Netzkomponenten usw.) auf Defekte und
- Benachrichtigung der Benutzer mit der Bitte, ihre Arbeitsbereiche auf Unregelmäßigkeiten zu prüfen.

Alarmplan heranziehen

Wenn Anzeichen auf einen vorsätzlichen Angriff gegen das Netz vorliegen, ist für die Schadensminimierung und weitere Schadensabwehr sofortiges Handeln notwendig. Hierzu ist ein Alarmplan erforderlich, in dem die einzuleitenden Schritte aufgeführt werden und festgelegt wird, welche Personen über den Vorfall zu unterrichten sind (siehe auch M 6.60 *Verhaltensregeln und Meldewege bei Sicherheitsvorfällen*). Der Alarmplan enthält ggf. auch Informationen darüber, ob und wie der Datenschutzbeauftragte und die Rechtsabteilung zu beteiligen sind.

Ergänzende Kontrollfragen:

- Wie ist sichergestellt, dass der Administrator effektiv benachrichtigt wird?
- Wird diese Regelung auch angewendet?
- Ist ein Verfahren zur schnellen Vergabe von Passwörtern etabliert und getestet?

M 6.55 Reduzierung der Wiederanlaufzeit für Novell Netware Server

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um die Wiederanlaufzeit eines Novell Netware Servers nach einem Ausfall zu reduzieren, sollten die erforderliche Software und die notwendigen Starttreiber (für Festplatte, Netzadapterkarte usw.) für den Fall einer Neuinstallation gesondert abgespeichert und auf externen Datenträgern ausgelagert werden. Es empfiehlt sich eine Aufbewahrung zusammen mit den Backup-Medien der sonstigen Datensicherungen. Die benötigten Konfigurationsparameter können der zugehörigen Dokumentation des Servers entnommen werden (siehe M 2.153 *Dokumentation von Novell Netware 4.x Netzen*).

Weiterhin sollte eine Vorgehensweise für den Wiederanlauf eines Netware Servers mit den dafür verantwortlichen Personen entwickelt werden. Diese Prozedur sollte regelmäßig im Rahmen von Notfallübungen simuliert und durchgeführt werden, um das Verfahren zu verifizieren und auf seine Durchführbarkeit zu testen. Insbesondere ist bei der Durchführung solcher Übungen zu testen, ob der ausschließliche Einsatz der Software und Daten, die in internen oder externen Sicherungsarchiven aufbewahrt werden reicht, um eine vollständige Rekonstruktion durchzuführen.

Die für einen Wiederanlauf der Novell Netware Server erforderlichen Schritte müssen in einem Notfall-Handbuch erläutert werden (siehe M 6.3 *Erstellung eines Notfall-Handbuches*, Teil D). Beispiele für solche Schritte sind:

- Aufbau und Installation der eventuell notwendigen Hardware-Komponenten,
- Einspielen der Systemsoftware,
- Einspielen der Starttreiber,
- Bereitstellen der notwendigen Daten einschließlich Konfigurationsdateien und
- Wiederanlauf.

Der Wiederanlauf kann, je nach Umfang und Komplexität der NDS, mit einem erheblichen Zeitaufwand verbunden sein. Der Zeitaufwand für die mit dem Wiederanlauf verbundenen Maßnahmen kann durch solche Übungen ermittelt werden und ist bei der Überarbeitung des Wiederanlaufplans zu berücksichtigen.

Ergänzende Kontrollfragen:

- Wurde der Wiederanlaufplan erprobt?
- Wann wurde zuletzt überprüft, ob die gesicherten Daten rekonstruiert werden können?

M 6.56 Datensicherung bei Einsatz kryptographischer Verfahren

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragter

Beim Einsatz kryptographischer Verfahren darf die Frage der Datensicherung nicht vernachlässigt werden. Neben der Frage, wie sinnvollerweise eine Datensicherung der verschlüsselten Daten erfolgen sollte, muss auch überlegt werden, ob und wie die benutzten kryptographischen Schlüssel gespeichert werden sollen. Daneben ist es noch zweckmäßig, die Konfigurationsdaten der eingesetzten Kryptoprodukte zu sichern.

Datensicherung der Schlüssel

Es muss sehr genau überlegt werden, ob und wie die benutzten kryptographischen Schlüssel gespeichert werden sollen, da jede Schlüsselkopie eine potentielle Schwachstelle ist.

Trotzdem kann es aus verschiedenen Gründen notwendig sein, kryptographische Schlüssel zu speichern. Es gibt unterschiedliche Methoden der Schlüsselspeicherung:

- die Speicherung zu Transportzwecken auf einem transportablen Datenträger, z. B. Diskette, Chipkarte (dient vor allem zur Schlüsselverteilung bzw. zum Schlüsselaustausch, siehe M 2.46 *Geeignetes Schlüsselmanagement*),
- die Speicherung in IT-Komponenten, die dauerhaft auf kryptographische Schlüssel zugreifen müssen, also z. B. zur Kommunikationsverschlüsselung und
- die Schlüsselhinterlegung als Vorbeugung gegen Schlüsselverlust oder im Rahmen von Vertretungsregelungen.

Hierbei ist grundsätzlich zu beachten:

- Kryptographische Schlüssel sollten so gespeichert bzw. aufbewahrt werden, dass Unbefugte sie nicht unbemerkt auslesen können. Beispielsweise könnten Schlüssel in spezieller Sicherheitshardware gespeichert werden, die die Schlüssel bei Angriffen automatisch löscht. Falls sie in Software gespeichert werden, sollten sie auf jeden Fall überschlüsselt werden. Hierbei ist zu bedenken, dass die meisten Standard-Anwendungen, bei denen Schlüssel oder Passwörter in der Anwendung gespeichert werden, dies im allgemeinen mit leicht zu brechenden Verfahren geschieht. Als weitere Variante kann auch das Vier-Augen-Prinzip bei der Schlüsselspeicherung benutzt werden, also die Speicherung eines Schlüssels in Schlüsselhälften oder Schlüsselteilen.
- Von Kommunikationsschlüsseln und anderen kurzlebigen Schlüsseln sollten keine Kopien erstellt werden. Damit eine unautorisierte Nutzung ausgeschlossen ist, sollten auch von privaten Signaturschlüsseln i. allg. keine Kopien existieren. Falls jedoch für die Schlüsselspeicherung eine reine Softwarelösung gewählt wurde, d. h. wenn keine Chipkarte o. Ä.

verwendet wird, ist das Risiko des Schlüsselverlustes erhöht, z. B. durch Bitfehler oder Festplattendefekt. In diesem Fall ist es unter Umständen weniger aufwendig, eine ausreichend gesicherte Möglichkeit der Schlüsselhinterlegung zu schaffen, als bei jedem Schlüsselverlust alle Kommunikationspartner zu informieren.

- Von langlebigen Schlüsseln, die z. B. zur Archivierung von Daten oder zur Generierung von Kommunikationsschlüsseln eingesetzt werden, sollten auf jeden Fall Sicherungskopien angefertigt werden.

Datensicherung der verschlüsselten Daten

Besondere Sorgfalt ist bei der Datensicherung von verschlüsselten Daten bzw. beim Einsatz von Verschlüsselung während der Datenspeicherung notwendig. Treten hierbei Fehler auf, sind nicht nur einige Datensätze, sondern meist alle Daten unbrauchbar.

Die Langzeitspeicherung von verschlüsselten oder signierten Daten bringt viele zusätzliche Probleme mit sich. Hierbei muss nicht nur sichergestellt werden, dass die Datenträger regelmäßig aufgefrischt werden und jederzeit noch die technischen Komponenten zum Verarbeiten dieser zur Verfügung stehen, sondern dass die verwendeten kryptographischen Algorithmen und die Schlüssellänge noch dem Stand der Technik entsprechen. Bei der langfristigen Archivierung von Daten kann es daher sinnvoller sein, diese unverschlüsselt zu speichern und dafür entsprechend sicher zu lagern, also z. B. in Tresoren.

Die verwendeten Kryptomodule sollten vorsichtshalber immer archiviert werden, da die Erfahrung zeigt, dass auch noch nach Jahren Daten auftauchen, die nicht im Archiv gelagert waren.

Datensicherung der Konfigurationsdaten der eingesetzten Produkte

Bei komplexeren Kryptoprodukten sollte nicht vergessen werden, deren Konfigurationsdaten zu sichern (siehe auch M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen*). Die gewählte Konfiguration sollte dokumentiert sein, damit sie nach einem Systemversagen oder einer Neuinstallation schnell wieder eingerichtet werden kann.

Ergänzende Kontrollfragen:

- Gibt es eine Vorgabe innerhalb des Unternehmens bzw. der Behörde zur Hinterlegung von Schlüsselkopien?
- Wie wird sichergestellt, dass auf verschlüsselt gespeicherte Daten auch nach längeren Zeiträumen noch zugegriffen werden kann?

M 6.57 Erstellen eines Notfallplans für den Ausfall des Managementsystems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Auch ein Managementsystem kann aus verschiedenen Gründen ausfallen, etwa durch einen Rechnerabsturz durch Software- oder Hardwarefehler, durch einen Stromausfall oder Sabotage. Da Managementsysteme vor allem bei größeren Systemen eingesetzt werden, sollten für diese Systeme sowohl ein Notfallvorsorge-Konzept wie in Baustein B 1.3 *Notfallvorsorge-Konzept* beschrieben als auch ein Datensicherungskonzept (siehe Baustein B 1.4 *Datensicherungskonzept*) vorhanden sein.

Im Rahmen eines solchen Notfallvorsorgekonzeptes müssen dann auch für den Ausfall des Managementsystems Regelungen festgelegt und dokumentiert werden. Insbesondere sind Regelungen zu treffen, die Verhaltensrichtlinien für den Ausfall der verschiedenen Managementsystemkomponenten (Manager, Management Server, Managementkonsole) enthalten.

Desweiteren ist die Erstellung eines Wiederanlaufplanes für das Managementsystem insgesamt oder dessen Einzelkomponenten zwingend erforderlich. Im Idealfall sollte ein automatisches Wiederanlaufen des Managementsystems erfolgen. Im Rahmen der Datensicherung sollten für den Fall des Datentotalverlustes (Plattencrash) Sicherungskopien der Managementsystemsoftware vorhanden sein. Der Aufbewahrungsort ist im Notfallhandbuch zu vermerken. Ebenso sind dort die Kenntnisse zu vermerken, die benötigt werden, um Zutritt oder Zugriff zum Aufbewahrungsort zu erhalten, z. B. Namen und Telefonnummern der Mitarbeiter, die erforderliche Tresorkombinationen oder Passwörter kennen (siehe auch M 2.22 *Hinterlegen des Passwortes*).

M 6.58 Etablierung eines Managementsystems zur Behandlung von Sicherheitsvorfällen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Mit der zunehmenden Einbindung der IT in alle Abläufe einer Behörde oder eines Unternehmens nimmt auch die Abhängigkeit von deren korrekten Funktionieren immer weiter zu. Eine wichtige Aufgabe des IT-Sicherheitsmanagements ist daher die Vorbereitung auf den angemessenen Umgang mit Sicherheitsvorfällen aller Art. Sicherheitsvorfälle können durch eine Vielzahl von Ereignissen ausgelöst werden und z. B. zum Verlust der Verfügbarkeit, Integrität und/oder Vertraulichkeit von Daten, einzelnen IT-Systemen oder des gesamten Netzes führen.

Sicherheitsvorfälle, die im Rahmen des IT-Sicherheitsmanagements einer besonderen Behandlung bedürfen, sind solche, die das Potential für große Schäden besitzen. Sicherheitsprobleme, die nur lokal begrenzte und geringfügige Schäden verursachen oder verursachen können, sollten auch in der lokalen Verantwortlichkeit gelöst werden, um das IT-Sicherheitsmanagement nicht zu überlasten.

Ziele bei der Behandlung von Sicherheitsvorfällen

Die Behandlung von Sicherheitsvorfällen verfolgt als Teil des IT-Sicherheitsmanagements dabei folgende Ziele:

- Reaktionsfähigkeit, damit Sicherheitsvorfälle und Sicherheitsprobleme rechtzeitig bemerkt und an eine zuständige Stelle gemeldet werden,
- Entscheidungsfähigkeit, ob es sich um ein lokales Sicherheitsproblem oder um einen Sicherheitsvorfall handelt,
- Handlungsfähigkeit, damit bei einem Sicherheitsvorfall die notwendigen Maßnahmen kurzfristig ergriffen und umgesetzt werden,
- Schadensminimierung, in dem weitere potentiell betroffene Bereiche rechtzeitig benachrichtigt werden und
- Effektivität, in dem die Fähigkeit zur Behandlung von Sicherheitsvorfällen geübt und überwacht wird.

Beteiligung der Leitungsebene

Um diese Ziele erreichen zu können, ist ein Managementsystem zur Behandlung von Sicherheitsvorfällen zu etablieren. Unbedingte Voraussetzung dafür ist, dass die Behörden- oder Unternehmensleitung beteiligt wird und letztlich das Managementsystem in Kraft setzt, um die notwendige Sensibilisierung für IT-Sicherheit, die Vergabe von Entscheidungskompetenzen und die Unterstützung der Sicherheitsziele zu gewährleisten.

Zur Etablierung eines Managementsystems zur Behandlung von Sicherheitsvorfällen kann man sich an folgenden Schritten orientieren:

Schritt 1: Berücksichtigung in der Sicherheitsleitlinie

Als Teil des IT-Sicherheitsmanagements sollte die Behandlung von Sicherheitsvorfällen in der Sicherheitsleitlinie bzw. im IT-Sicherheitskonzept der Behörde bzw. des Unternehmens geregelt werden. Hier ist festzulegen, dass Sicherheitsvorfälle und Sicherheitsprobleme von den Benutzern und Betroffenen dem zuständigen Sicherheitsverantwortlichen gemeldet werden.

Darüber hinaus sind die Entscheidungsfindungswege zu beschreiben und die Notwendigkeit zu motivieren. Mit der Aufnahme in die Sicherheitsleitlinie wird gleichzeitig die Unterstützung der IT-Sicherheit durch die Behörden- bzw. Unternehmensleitung manifestiert.

Schritt 2: Festlegung von Verantwortlichkeiten

In diesem Schritt wird festgelegt, wer welche Verantwortung beim Auftreten von Sicherheitsvorfällen hat. Verantwortung tragen dabei unter anderem folgende Gruppen für die exemplarisch beschriebenen Aufgaben:

- IT-Benutzer: Meldung von Sicherheitsproblemen und -vorfällen
- IT-Administratoren: Entgegennahme von Meldungen und erste Entscheidungsvorbereitung zwischen Sicherheitsproblem und -vorfall sowie Einleitung der Eskalation
- Verantwortliche für IT-Anwendung: Beteiligung als Träger des Schutzbedarfs der betroffenen IT-Anwendung bei Entscheidungsfindung und Maßnahmenauswahl
- IT-Sicherheitsbeauftragte bzw. IT-Sicherheitsmanagement: Entgegennahme von Meldungen und Entscheidungsfindung zwischen Sicherheitsproblem und -vorfall, Einschaltung des Eskalationswegs und Einleitung notwendiger Maßnahmen
- Sicherheitsvorfall-Team: ein aus betroffenen IT-Administratoren, IT-Anwendern, IT-Sicherheitsbeauftragten, Öffentlichkeitsarbeit und ggf. Leitungsebene zusammengesetztes Team zur Abwicklung eines Sicherheitsvorfalls
- Öffentlichkeitsarbeit bzw. Pressestelle: bei Bedarf Vorbereitung der Informationspolitik bezüglich des Sicherheitsvorfalls
- IT-Sicherheitsrevision: Überprüfung des Managementsystems und Nachbereitung eines Sicherheitsvorfalls
- Behörden-/Unternehmensleitung: Abschließende Entscheidungsfindung

Die Verantwortlichkeiten sind zu regeln und in Kraft zu setzen. Näheres ist in Maßnahme M 6.59 *Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen* beschrieben.

Schritt 3: Verhaltensregeln und Meldeweg bei Auftreten eines Sicherheitsvorfalls

Für die effektive Behandlung von Sicherheitsvorfällen ist entscheidend, dass sich Betroffene richtig und besonnen verhalten und den Vorfall unverzüglich weitermelden. Dazu sind die Verhaltensregeln (Ruhe bewahren, Meldepflicht, Auskunftspflicht über Begleitumstände, etc.) zu fixieren und die IT-Benutzer entsprechend zu schulen. Insbesondere ist dabei festzulegen, an wen ein IT-Sicherheitsproblem oder -vorfall gemeldet werden muss.

typische Sicherheitsvorfälle im Vorfeld berücksichtigen

Für eine Reihe von typischerweise zu erwartenden Sicherheitsvorfällen (z. B. Auftreten eines Computer-Virus, Datenmanipulation durch Innentäter, Hackingversuche durch Außentäter, ...) können vorab Handlungsanweisungen ausgearbeitet werden, was in einem solchen Fall zu tun ist. Dies beschleunigt

im Ernstfall die Reaktionen und trägt damit zur Schadensbegrenzung bei. Da der Aufwand zur Erstellung dieser Handlungsoptionen nicht unerheblich ist, sollte er auf die relevanten planbaren Bereiche beschränkt werden.

Ausführlich wird dieses Thema in der Maßnahme M 6.60 *Verhaltensregeln und Meldewege bei Sicherheitsvorfällen* beschrieben.

Schritt 4: Eskalationsstrategie bei Sicherheitsvorfällen

Je kritischer ein Sicherheitsvorfall ist, desto mehr Kompetenzen werden bei der Behandlung des Sicherheitsvorfalls in der Regel benötigt. Dies kann so weit führen, dass die Behörden- bzw. Unternehmensleitung informiert und eingeschaltet werden muss, um notwendige Maßnahmen wie Verbot der Informationsweitergabe, Einschaltung der Polizei, kostenträchtige Ersatzmaßnahmen etc. einleiten zu dürfen. Dazu bedarf es jedoch einer im Vorfeld erarbeiteten Eskalationsstrategie, wer in welchen Fällen hinzuzuziehen ist. Näheres dazu ist in Maßnahme M 6.61 *Eskalationsstrategie für Sicherheitsvorfälle* beschrieben.

Schritt 5: Prioritätensetzung

Da ein Sicherheitsvorfall meist aus einer Verkettung verschiedener Ursachen entsteht und auch Auswirkungen auf verschiedene betroffene IT-Anwendungsbereiche besitzt, sollten die zu treffenden Maßnahmen anhand einer Prioritätenliste umgesetzt werden. Diese Prioritätensetzung hängt vom Schutzbedarf, von den IT-Einsatzbereichen und -Anwendungen sowie von den individuellen Abhängigkeiten der Behörde bzw. des Unternehmens ab. Analog zur Schutzbedarfsfeststellung ist vorab eine Prioritätensetzung durchzuführen, um festzulegen, in welcher Reihenfolge die aus einem Sicherheitsvorfall resultierenden Schäden bearbeitet werden sollen (siehe M 6.62 *Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen*).

Schritt 6: Methodik zur Untersuchung und Bewertung von Sicherheitsvorfällen

Nach Eingang einer Meldung über eine sicherheitsrelevante Unregelmäßigkeit muss zunächst entschieden werden, ob es sich um ein lokales Sicherheitsproblem oder um einen Sicherheitsvorfall mit ggf. zu erwartenden größeren Schäden handelt. Für diese Entscheidung sind eine Reihe von Einflussfaktoren (potentielle Schadenshöhe und Folgeschäden, Ursache, betroffene IT-Systeme, notwendige Sofortmaßnahmen) zu erheben und zu bewerten. Bei Bedarf sind gemäß einer Eskalationsstrategie die nächsten Managementebenen einzubeziehen. Einzelheiten dazu finden sich in Maßnahme M 6.63 *Untersuchung und Bewertung eines Sicherheitsvorfalls*.

Schritt 7: Umsetzung von Maßnahmen zur Behebung von Sicherheitsvorfällen

Bei der Umsetzung der notwendigen Maßnahmen zur Behebung von Sicherheitsvorfällen ist zu beachten, dass diese Maßnahmen meist unter Zeitdruck vollzogen werden. Daher kann nicht ausgeschlossen werden, dass durch diese Maßnahmen neue Probleme entstehen. Als Folge dessen ist es sinnvoll, die Umsetzung der Maßnahmen ausreichend zu dokumentieren. Darüber hinaus sollte, vorsätzliches Handeln bei Sicherheitsvorfällen vorausgesetzt, auch die Behandlung des "Täters" mitbedacht werden.

Unter Umständen sind personelle Konsequenzen zu überdenken. Näheres dazu findet man in M 6.64 *Behebung von Sicherheitsvorfällen*.

Schritt 8: Benachrichtigung betroffener Stellen

Sollte sich herausstellen, dass ein Sicherheitsvorfall in den Auswirkungen nicht nur auf die Behörde bzw. das Unternehmen oder einzelne Organisationsbereiche beschränkt ist, muss zur Schadensminimierung eine Benachrichtigung der evtl. betroffenen Stellen erfolgen. Dazu sollten vorab die Kommunikationswege erhoben werden und eine Abhängigkeitsanalyse durchgeführt worden sein, um die Benachrichtigung zu beschleunigen (siehe M 6.65 *Benachrichtigung betroffener Stellen*).

Schritt 9: Nachbereitung eines Sicherheitsvorfalls

Um den Lerneffekt eines eingetretenen Sicherheitsvorfalls nicht zu vernachlässigen, sollte für die Behandlung von Sicherheitsvorfälle die Nachbereitung festgelegt werden. Oftmals lassen sich daraus Verbesserungen für den Umgang mit Sicherheitsvorfällen herausarbeiten oder Rückschlüsse auf die Wirksamkeit der IT-Sicherheitskonzeption ziehen. Dabei sind unter anderem folgende Aspekte zu beachten:

- Reaktionszeit,
- Bekanntheitsgrad des Meldewegs,
- Wirksamkeit der Eskalationsstrategie,
- Effektivität der Untersuchung und
- Möglichkeiten der Benachrichtigung betroffener Stellen.

Ausführlich behandelt wird dieses Thema in Maßnahme M 6.66 *Nachbereitung von Sicherheitsvorfällen*.

Schritt 10: Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle

Je schneller ein Sicherheitsvorfall entdeckt und gemeldet wird, umso effektiver können Gegenmaßnahmen ergriffen werden. Hierbei kann es sinnvoll sein, die technisch möglichen Detektionsmaßnahmen zu nutzen, um Verzögerungen durch menschliches Handeln zu reduzieren. Hier sind insbesondere Viren-Suchprogramme, Auswertungen von Protokolldaten und Intrusion Detection Systeme zu nennen. Die Identifikation und Aktivierung dieser Maßnahmen sowie deren Meldewege werden in Maßnahme M 6.67 *Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle* beschrieben.

Schritt 11: Effizienzprüfung

Um die Effektivität eines Managementsystems zur Behandlung von Sicherheitsvorfällen messen zu können und um die notwendige Praxis dieser Managementaufgaben zu fördern, sind Übungen bzw. Planspiele durchzuführen. Da dies eines erheblichen Personaleinsatzes bedarf und sich auf den normalen Geschäftsablauf störend auswirken kann, sollte dies auf wichtige Bereiche beschränkt werden. Weitere Anregungen finden sich in Maßnahme M 6.68 *Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen*.

Konzept erstellen und regelmäßig aktualisieren

Die Ergebnisse dieser Schritte sollten sinnvollerweise in einem "Konzept zur Behandlung von Sicherheitsvorfällen" dokumentiert werden. Dieses Konzept ist in regelmäßigen Abständen zu aktualisieren und in geeigneter Weise den Betroffenen bekannt zu geben.

Ergänzende Kontrollfragen:

- Gibt es klar definierte Abläufe und Regeln für die verschiedenen Arten von Sicherheitsvorfällen?
- Sind die Verhaltensregeln und Meldewege bei Sicherheitsvorfällen schriftlich fixiert?
- Sind diese allen Mitarbeitern bekannt?

M 6.59 Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Aufgaben und Kompetenzen festlegen

Um die Verantwortlichkeiten zur Behandlung von Sicherheitsvorfällen festzulegen, bietet es sich an, sich am imaginären zeitlichen Ablauf eines Sicherheitsvorfalls zu orientieren. Für die handelnden Personengruppen ist dabei festzulegen, welche Aufgaben und Kompetenzen sie haben und auf welche Art sie verpflichtet bzw. unterrichtet werden. Beispielhaft soll dies für einige der typischerweise betroffenen Gruppen beschrieben werden.

IT-Benutzer

Aufgabe:

Sobald IT-Benutzer eine sicherheitsrelevante Unregelmäßigkeit bemerken, müssen sie die entsprechenden Verhaltensregeln einhalten und die Unregelmäßigkeit melden.

Kompetenz:

IT-Benutzer müssen entscheiden, welcher Meldeweg in dem vorliegenden Fall einzuschlagen ist (siehe M 6.60 *Verhaltensregeln und Meldewege bei Sicherheitsvorfällen*).

Verpflichtung / Unterrichtung:

Jeder IT-Benutzer sollte über die Sicherheitsleitlinie des Hauses verpflichtet werden, sicherheitsrelevante Unregelmäßigkeiten zu melden. Darüber hinaus sollten alle Benutzer schriftliche Handlungsanweisungen ausgehändigt bekommen, wie sie sich zu verhalten haben und an wen welche Vorfälle zu melden sind.

IT-Administrator

Aufgabe:

Der IT-Administrator erhält in diesem Zusammenhang die Aufgabe, Meldungen über sicherheitsrelevante Unregelmäßigkeiten, die mit den von ihm betreuten IT-Systemen verbunden sind, entgegenzunehmen. Anschließend hat er zu entscheiden, ob er selbst diese Unregelmäßigkeit behebt oder ob er die nächst höhere Eskalationsebene zu unterrichten hat.

Kompetenz:

Ein Administrator muss entscheiden können, ob ein Sicherheitsproblem vorliegt, ob er dieses eigenverantwortlich beheben kann, ob er sofort andere Personen hinzuzieht (entsprechend dem Eskalationsplan) und wen er informiert.

Verpflichtung / Unterrichtung:

Dies sollte in der Stellenbeschreibung und im Konzept zur Behandlung von Sicherheitsvorfällen festgelegt werden.

IT-Sicherheitsbeauftragter / IT-Sicherheitsmanagement

Aufgabe:

Der IT-Sicherheitsbeauftragte nimmt Meldungen über Sicherheitsvorfälle entgegen. Er führt die Untersuchung und Bewertung des Vorfalls durch. Er wählt notwendige Maßnahmen aus und veranlasst deren Umsetzung, soweit dies nicht seinen Kompetenzbereich überschreitet. Bei Bedarf ruft er ein Sicherheitsvorfall-Team zusammen bzw. unterrichtet zur Eskalation die Leitungsebene.

Kompetenz:

Er ist befugt, die Bewertung eines Sicherheitsvorfalls durchzuführen, einen Vorfall weiter zu eskalieren. Darüber hinaus sind ihm finanzielle und personelle Ressourcen (z. B. 100.000 EURO und 2 Personenmonate) zugebilligt, die er zur Behebung von Vorfällen selbständig einsetzen darf.

Verpflichtung / Unterrichtung:

Das IT-Sicherheitsmanagement erarbeitet das Konzept zur Behandlung von Sicherheitsvorfällen. Daher sollten alle IT-Sicherheitsbeauftragten über ihre Aufgaben und Kompetenzen bei der Behandlung von Sicherheitsvorfällen informiert sein.

IT-Sicherheitsrevision

Aufgabe:

Der IT-Sicherheitsrevision kann die Aufgabe übertragen werden, in Abständen die Wirksamkeit des Managementsystems für Sicherheitsvorfälle zu prüfen. Darüber hinaus kann sie beauftragt werden, bei der Nachbereitung von Sicherheitsvorfällen mitzuwirken.

Kompetenz:

In Absprache mit der Leitungsebene können genannte Prüfungen initiiert und durchgeführt werden.

Verpflichtung / Unterrichtung:

Dies sollte in der Stellenbeschreibung und im Konzept zur Behandlung von Sicherheitsvorfällen festgelegt werden.

Öffentlichkeitsarbeit / Pressestelle

Aufgabe:

Die Information der Öffentlichkeit sollte bei schwerwiegenden Sicherheitsvorfällen ausschließlich durch die Pressestelle erfolgen. Dabei sollte der Vorfall nicht beschönigt oder verharmlost, sondern sachlich dargestellt werden, um keinen Imageverlust bei gegenteiligen Informationen zu erleiden.

Kompetenz:

Die Pressestelle muss Informationen über den Sicherheitsvorfall zusammen mit den technischen Experten aufbereiten und mit der Leitungsebene vor der Weitergabe abstimmen.

Verpflichtung / Unterrichtung:

Dies sollte in der Stellenbeschreibung und im Konzept zur Behandlung von Sicherheitsvorfällen festgelegt werden.

Behörden-/Unternehmensleitung

Aufgabe:

Sie wird bei schwerwiegenden Sicherheitsvorfällen unterrichtet und ggf. mit der Entscheidungsfindung konfrontiert.

Kompetenz:

Als die die Gesamtverantwortung tragende Stelle kann sie die Verantwortung an oben genannte Gruppen delegieren. Darüber hinaus kann sie Polizei und Strafverfolgungsbehörden einschalten, wenn der Verdacht auf kriminelle Handlungen besteht.

Verpflichtung / Unterrichtung:

Die Behörden- bzw. Unternehmensleitung muss dem Konzept zur Behandlung von Sicherheitsvorfällen und den darauf aufbauenden Eskalationsplänen zustimmen. Dabei wird die Leitungsebene auch über ihre Rolle bei der Behandlung von Sicherheitsvorfällen unterrichtet.

Sicherheitsvorfall-Team

Neben diesen Gruppen kann es bei einem schwierigen oder schwerwiegenden Sicherheitsvorfall notwendig sein, zu dessen Behandlung ein Sicherheitsvorfall-Team zeitlich befristet einzuberufen. Dies wird üblicherweise vom IT-Sicherheitsbeauftragten initiiert, der ggf. die Leitungsebene vorab beteiligt.

Mitglieder benennen und Aufgaben festlegen

Auch wenn das Sicherheitsvorfall-Team nur für einen konkreten Sicherheitsvorfall zusammentritt, müssen bereits im Vorfeld dessen Mitglieder benannt und in ihre Aufgaben eingewiesen sein, damit die Reaktion auf den Sicherheitsvorfall schnellstmöglich erfolgen kann. Die Mitglieder des Sicherheitsvorfall-Teams sollten befugt sein, die ihnen übertragenen Aufgaben eigenverantwortlich durchzuführen. Die hierzu erforderlichen Regelungen sind schriftlich festzuhalten und von der Behörden- bzw. Unternehmensleitung zu autorisieren. Insbesondere ist festzulegen, wer die Leitung dieses Teams übernimmt.

Zu einem Sicherheitsvorfall-Team können (je nach Art des Sicherheitsvorfalls) beispielsweise gehören:

- Behörden-/Unternehmensleitung,
- IT-Sicherheitsmanagement / IT-Sicherheitsbeauftragter,
- Leiter IT,
- Pressestelle,
- Datenschutzbeauftragter,
- Justitiar und
- Personalrat/Betriebsrat.

Falls es erforderlich ist, müssen weitere Bereiche hinzugezogen werden, wie z. B.

- die betroffenen Fachabteilungen (Leiter, IT-Verfahrensverantwortlicher),
- IT-Administratoren,
- die Bereiche Beschaffung, Haustechnik, Innerer Dienst, Organisation, Personal und
- Brandschutzbeauftragter.

Regelungen für Mehrarbeit

Es sollte im Vorfeld abgeklärt sein, wie mit der im Rahmen von Sicherheitsvorfällen anfallenden Mehrarbeit umzugehen ist, also ob die Arbeitszeitregelungen der Behörde bzw. des Unternehmens um Ausnahmeregelungen für Mehrarbeit, Wochenendarbeit, etc. bei Sicherheitsvorfällen erweitert werden muss. Darüber hinaus ist auch sicherzustellen, dass dieses Team bei Bedarf auch die Diensträume außerhalb der regulären Arbeitszeit nutzen kann.

Ergänzende Kontrollfragen:

- Ist ein Sicherheitsvorfall-Team benannt worden?
- Sind die betroffenen Mitglieder des Teams in ihre Aufgaben eingewiesen worden?
- Wer koordiniert welche Maßnahmen?
- Wann wurde der Aufbau des Katastrophen-Management-Teams zuletzt aktualisiert?

M 6.60 Verhaltensregeln und Meldewege bei Sicherheitsvorfällen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Viele Sicherheitsvorfälle werden erst durch falsche Reaktionen zu einem größeren Problem, wenn überhastet Entscheidungen getroffen werden, beispielsweise wenn spontan Daten gelöscht werden, die zum Nachvollziehen des Ereignisses notwendig gewesen wären.

Zu unterscheiden ist hierbei zwischen allgemein gültigen Verhaltensregeln, die für sämtliche vorstellbaren Sicherheitsvorfälle gelten, und den IT-spezifischen Verhaltensregeln. Folgende allgemein gültige Verhaltensregeln können für alle Arten von sicherheitsrelevanten Unregelmäßigkeiten festgehalten werden:

Keine Panik!

- Alle Beteiligten sollten Ruhe bewahren und keine übereilten Maßnahmen ergreifen.

Geordnet vorgehen!

- Unregelmäßigkeiten sollten gemäß eines Meldeplans unverzüglich gemeldet werden.
- Gegenmaßnahmen dürfen erst nach Aufforderung durch Berechtigte ergriffen werden.

Nichts verschleiern!

- Alle Begleitumstände sind ungeschönt, offen und transparent zu erläutern, um damit zur Schadensminderung beizutragen.

Einschätzung des Schadens

- Es sollte eine erste auf den persönlichen Erfahrungen beruhende Einschätzung der möglichen Schadenshöhe, der Folgeschäden, der potentiell intern und extern Betroffenen und möglicher Konsequenzen abgegeben werden.
- Informationen über den Sicherheitsvorfall dürfen nicht unautorisiert an Dritte weitergegeben werden.

Diese allgemeinen Verhaltensregeln müssen in geeigneter Weise allen potentiell betroffenen Angehörigen einer Behörde bzw. eines Unternehmens bekanntgegeben werden.

Verhaltensregeln bekannt geben

Darüber hinaus können spezifische Verhaltensregeln an die Betroffenen weitergegeben werden, insbesondere an diejenigen, die als Meldestellen für Sicherheitsvorfälle fungieren und die ersten Entscheidungen fällen bzw. die ersten Maßnahmen ergreifen sollen. Dazu gehören die IT-Administratoren, die IT-Anwendungsverantwortlichen und das IT-Sicherheitsmanagement. Zu diesen Verhaltensregeln zählen die in den folgenden Maßnahmen beschriebenen:

- M 6.23 *Verhaltensregeln bei Auftreten eines Computer-Virus*,
- M 6.31 *Verhaltensregeln nach Verlust der Systemintegrität*
- M 6.48 *Verhaltensregeln nach Verlust der Datenbankintegrität*
- M 6.54 *Verhaltensregeln nach Verlust der Netzintegrität*

Neben der Festlegung der Verhaltensregeln sind auch die Meldewege zu definieren. Hier bietet sich folgendes Muster an:

- Bei Gefährdungen höherer Gewalt wie Feuer, Wasser, Stromausfall, Einbruch und Diebstahl sind die örtlich verfügbaren Einsatzkräfte zu unterrichten (Feuerwehr, Haustechnik, Pforte, Wachdienst, ...).
- Bei hardware-technischen Problemen oder bei Unregelmäßigkeiten bei Betrieb der IT-Systeme ist der zuständige IT-Administrator zu benachrichtigen.
- Bei vermuteten vorsätzlichen Handlungen und bei ansonsten nicht zuzuordnenden Ereignissen (z. B. Datenmanipulationen, unerlaubter Ausübung von Rechten, Spionage- und Sabotageverdacht) ist der IT-Sicherheitsbeauftragte bzw. das IT-Sicherheitsmanagement zu benachrichtigen.

Meldewege bekannt geben

Wichtig ist hier insbesondere, dass allen Mitarbeitern die Ansprechpartner und die Meldewege für alle Arten von Sicherheitsvorfällen bekannt sind. Hierzu könnte z. B. im internen Telefonverzeichnis oder im Intranet eine Liste mit Namen, Telefonnummern und E-Mailadressen der jeweiligen Ansprechpartner enthalten sein. Es darf jedoch weder schwierig noch zeitaufwendig sein, Verdachtsfälle weiterzumelden. Dafür müssen schnelle und sichere Kommunikationsverbindungen bereitstehen. Die Authentizität des Kommunikationspartners und die Vertraulichkeit der über den Verdachtsfall gemeldeten Informationen ist sicherzustellen.

Es sollten auch alle Mitarbeiter darüber informiert sein, dass Auskünfte über den Sicherheitsvorfall gegenüber Dritten nur über das IT-Sicherheitsmanagement erfolgen dürfen (siehe M 6.65 *Benachrichtigung betroffener Stellen*).

Übungen durchführen

Durch Übungen sollte auch sporadisch überprüft werden, ob die Verhaltensregeln für Sicherheitsvorfälle angemessen und durchführbar sind und ob sie allen Mitarbeitern bekannt sind (siehe auch M 6.68 *Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen*).

Besonders bei Sicherheitsvorfällen zeigt es sich immer wieder, wie wichtig ein gutes Betriebsklima und eine gesunde Kommunikationskultur sind, damit Sicherheitsvorfälle auch umgehend weitergemeldet und offen angegangen werden (siehe auch M 3.8 *Vermeidung von Störungen des Betriebsklimas*).

Merkblatt mit Meldeplan und den wichtigsten Verhaltensregeln

Ein Beispiel, wie die Verhaltensregeln und der Meldeplan jedem betroffenen Mitarbeiter bekanntgegeben werden können, ist ein von der Behörden- bzw. Unternehmensleitung unterzeichnetes Informationsblatt, auf dem die wichtigsten Informationen zusammengefasst sind und das am Arbeitsplatz und **ergänzend** im Intranet vorgehalten werden kann. Ein Beispiel für ein solches Informationsblatt findet sich unter den Hilfsmitteln zum IT-Grundschutz. Damit die Information im Ernstfall auch tatsächlich verfügbar ist, ist es nicht sinnvoll, diese nur in elektronischer Form zu verbreiten, da dann auch genau diese Information vom Sicherheitsvorfall betroffen sein könnte.

Alle Informationsblätter zu potentiellen Sicherheitsvorfällen müssen bei jeder relevanten Änderung in der Organisation sofort aktualisiert werden, damit die dort beschriebenen Verhaltensregeln noch greifen und die Meldewege korrekt sind.

Ergänzende Kontrollfragen:

- Gibt es klar definierte Verhaltensregeln für die verschiedenen Arten von Sicherheitsvorfällen?
- Sind diese allen Mitarbeitern bekannt?
- Wann wurde diese Information letztmalig aktualisiert?

M 6.61 Eskalationsstrategie für Sicherheitsvorfälle

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement, Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, IT-Sicherheitsmanagement

Nachdem die Verantwortlichkeiten für Sicherheitsvorfälle geregelt sind (siehe M 6.59 *Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen*) und die Verhaltensregeln und Meldewege allen Betroffenen bekanntgegeben worden sind (siehe M 6.60 *Verhaltensregeln und Meldewege bei Sicherheitsvorfällen*), ist als Nächstes zu regeln, wie mit eingegangenen Meldungen weiter verfahren wird.

Derjenige, der eine Meldung über einen Sicherheitsvorfall erhalten hat, muss diesen zunächst untersuchen und bewerten (siehe auch M 6.63 *Untersuchung und Bewertung eines Sicherheitsvorfalls*). Falls es sich tatsächlich um einen Sicherheitsvorfall handelt, müssen weitere Maßnahmen ergriffen werden. Dabei stellen sich folgende Fragen:

- Wer ist im Fall einer Eskalation, also der Ausweitung der Aktionskette, zu unterrichten?
- In welchen Fällen ist eine sofortige Eskalation vorzunehmen?
- Unter welchen Umständen ist ansonsten eine Eskalation durchzuführen?
- Wann wird diese Eskalation vorgenommen (sofort, am nächsten Tag, am nächsten Werktag)?
- Über welche Medien wird die Meldung weitergegeben?

Die Antworten zu diesen Fragen sind in einer Eskalationsstrategie festzulegen und bekannt zu geben. Die Eskalationsstrategie kann in drei Schritten erstellt werden:

Schritt 1: Festlegung der Eskalationswege

Wer informiert wen?

Wer für die Behandlung von Sicherheitsvorfällen verantwortlich ist, wurde in Maßnahme M 6.59 *Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen* festgelegt. In der Festlegung des Eskalationsweges ist zu definieren, wer an wen eine Meldung weitergibt. Dies lässt sich in einfacher Weise durch einen gerichteten Graphen veranschaulichen. Dabei sollten sowohl die regulären Eskalationswege als auch der Vertretungsfall berücksichtigt werden.

Beispiel:

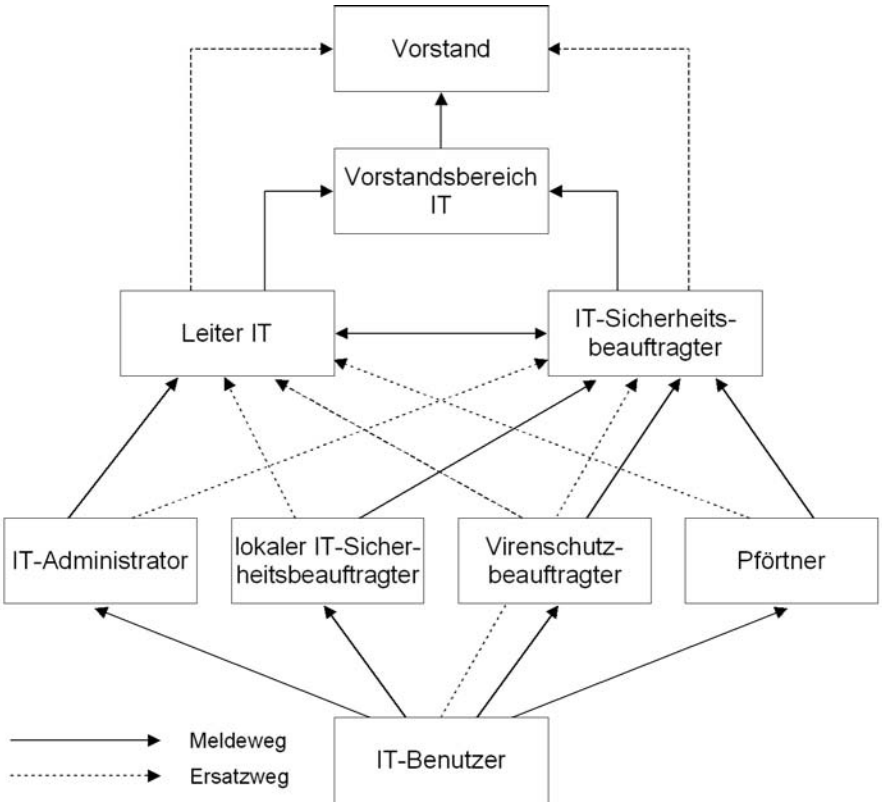


Abbildung: Meldewege

Schritt 2: Entscheidungshilfe für Eskalation

Wer muss wie schnell informiert werden?

In diesem Schritt ist zunächst festzulegen, in welchen Fällen eine sofortige Eskalation ohne weitere Untersuchungen und Bewertungen durchgeführt werden sollte. Ein Beispiel für eine tabellarische Aufstellung ist:

Ereignis	**sofortige Unterrichtung von**
Infektion mit einem Computer-Virus	Virenschutzbeauftragter, Administrator
Brand	Pförtner, Feuerwehr
Vorsätzliche Handlungen und vermutete kriminelle Handlungen	IT-Sicherheitsbeauftragter
Verdacht auf Werksspionage	IT-Sicherheitsbeauftragter, Vorstand
Notwendigkeit, Polizeien und Strafverfolgungsbehörden einzuschalten	Vorstand
Existenzbedrohende Schäden	Vorstand

Tabelle: Wann muss wer informiert werden

Anschließend ist für die restlichen Fälle vorzugeben, wann eine Eskalation stattzufinden hat. Gründe dafür können sein:

- Die zu erwartende Schadenshöhe übertrifft den Verantwortungsbereich der Stelle, die die Meldung entgegengenommen hat.
- Die Kosten und Ressourcen für die Schadensregulierung übertreffen deren Kompetenzbereich.
- Die Komplexität des Sicherheitsvorfalls übersteigt deren Kompetenz- bzw. Zuständigkeitsbereich.

Schritt 3: Art und Weise der Eskalation

Wie wird alarmiert?

Hierbei ist festzulegen, auf welche Weise die jeweils nächste Stelle in der Eskalationskette unterrichtet werden soll. Möglichkeiten dazu sind:

- persönliche Vorsprache
- schriftlicher Bericht
- E-Mail
- Telefon, Handy
- Bote mit verschlossenem Umschlag

Ebenso ist festzulegen, wann diese Meldung weitergegeben wird. Beispiele sind:

- bei Ereignissen, die eine sofortige Weitergabe erfordern: sofort innerhalb einer Stunde.
- bei Ereignissen, die Sofortmaßnahmen erforden: sofort innerhalb einer Stunde.
- bei Ereignissen, die zwar beherrscht werden, aber einer Unterrichtung der nächsten Eskalationsstufe erfordern: am nächsten Werktag.

Diese Eskalationsstrategie sollten alle möglichen Empfänger von Meldungen über Sicherheitsvorfälle erhalten, um zügige Reaktionen zu ermöglichen.

Regelungen für Mehrarbeit

Zur Eindämmung eines Sicherheitsvorfalls ist im Allgemeinen kurzfristiges Handeln erforderlich. Eventuell müssen Mitarbeiter aus anderen Projekten abgerufen oder auch außerhalb der Arbeitszeit herangezogen werden. Daher muss auch geregelt sein, wie mit der anfallenden Mehrarbeit umzugehen und wie eine Rufbereitschaft geregelt ist (siehe auch M 6.59 *Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen*).

Ergänzende Kontrollfragen:

- Wann wurde die Eskalationsstrategie letztmalig aktualisiert?
- Wurden die Eskalationswege in Übungen erprobt?

M 6.62 Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Ein Sicherheitsvorfall entsteht erfahrungsgemäß durch eine Verkettung verschiedener Ursachen. Daraus ergibt sich meist, dass die resultierenden potentiellen Schäden verschiedenen Schadenskategorien zugerechnet werden können. Daher ist es wichtig, die Prioritäten für die Problembeseitigung möglichst vorab festzulegen. Von dieser Prioritätensetzung hängt unter anderem ab, in welcher Reihenfolge die Probleme angegangen werden sollen.

Sicherheitsvorfälle stehen in Konkurrenz zu anderen Problemen

Eine Prioritätensetzung hängt dabei stark von den Gegebenheiten der jeweiligen Organisation ab. Für die Prioritätensetzung sind folgende Fragen zu bearbeiten:

- Welche Schadenskategorien sind für die Organisation relevant?
- In welcher Reihenfolge sollten Schäden der einzelnen Schadenskategorien behoben werden?

Hilfestellung für die Bearbeitung der Fragen bietet eine nach IT-Grundschutz durchgeführte Schutzbedarfsfeststellung. In dieser Schutzbedarfsfeststellung werden die für die Organisation relevanten Schadenskategorien definiert.

Wie schwerwiegend sind die Schäden?

Beispiel: Relevante Schadenskategorien sind:
- Verstoß gegen Gesetze, Vorschriften oder Verträge,
- Beeinträchtigung des informationellen Selbstbestimmungsrechts,
- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,
- Negative Außenwirkung und
- Finanzielle Auswirkungen.

Ebenso wird im Rahmen der Schutzbedarfsfeststellung eine Definition erarbeitet, wie zu jeder Schadenskategorie die Schadenshöhe definiert wird.

Beispiel: Schadensdefinition Finanzielle Auswirkungen

Schadenskategorie Finanzielle Auswirkungen	
Schaden mittel	Schaden kleiner 25.000.- €
Schaden hoch	Schaden zwischen 25.000.- und 5.000.000.- €
Schaden sehr hoch	Schaden höher als 5.000.000.- €

Tabelle: Finanzielle Auswirkungen von Schäden

Priorisierung in drei Stufen oder durch Reihenfolge

Anhand dieser Kategorien und Schadenshöhenbestimmung kann man die Prioritätensetzung wie folgt durchführen. In einer Tabelle werden in der ersten Spalte die Schadenskategorien aufgeführt. Die drei anschließenden Spalten erhalten als Überschrift die Schadenshöhen mittel, hoch und sehr hoch. Anschließend wird jeder Kombination von Schadenskategorie und Schadenshöhe eine Priorität zugeordnet. Die Prioritätensetzung kann einerseits durch eine Prioritätenklassifizierung mit Einteilungen wie

1 = besonders wichtig,
2 = wichtig,
3 = nachrangig

oder durch die Festlegung einer Reihenfolge stattfinden.

Beispiel:

Betrachtet wird als Organisation eine Stadtverwaltung, die dem Bürger ihre Dienstleistungen auch über das Internet anbietet. Dazu kann der Bürger Anträge per E-Mail an die Stadtverwaltung senden und über das Internet die Bearbeitungsfortschritte seines Antrags beobachten. Als Informationsdienst bietet diese Stadtverwaltung einen Internet-Server an.

Schadenskategorie	**Schaden mittel**	**Schaden hoch**	**Schaden sehr hoch**
Verstoß gegen Gesetze, Vorschriften oder Verträge	2	2	2
Beeinträchtigung des informationellen Selbstbestimmungsrechts	2	2	1
Beeinträchtigung der persönlichen Unversehrtheit	2	1	1
Beeinträchtigung der Aufgabenerfüllung	3	3	2
Negative Außenwirkung	3	2	1
Finanzielle Auswirkungen	3	3	2

Tabelle: Beispielergebnis mit Prioritätenklassifizierung

Schadenskategorie	Schaden mittel	Schaden hoch	Schaden sehr hoch
Verstoß gegen Gesetze, Vorschriften oder Verträge	13	12	11
Beeinträchtigung des informationellen Selbstbestimmungsrechts	8	6	3
Beeinträchtigung der persönlichen Unversehrtheit	5	2	1
Beeinträchtigung der Aufgabenerfüllung	15	14	7
Negative Außenwirkung	17	9	4
Finanzielle Auswirkungen	18	16	10

Tabelle: Beispielergebnis mit Prioritätensetzung durch Reihenfolge

Genehmigung durch die Leitungsebene

Diese Prioritätensetzung muss durch die Behörden- bzw. Unternehmensleitung gebilligt und in Kraft gesetzt werden. Die Prioritätensetzung ist allen Entscheidungsträgern bei der Behandlung von Sicherheitsvorfällen bekannt zu geben.

Tritt ein Sicherheitsvorfall ein, so kann die Prioritätensetzung wie folgt verwendet werden. Nach der Untersuchung und Bewertung des Sicherheitsvorfalls kann eingeschätzt werden, welche Schäden zu erwarten wären. Diese Schäden können den bekannten Schadenskategorien zugeordnet werden. Anschließend sind diese Schäden in die Klassen "mittel", "hoch" und "sehr hoch" einzuteilen. Aus der tabellarischen Übersicht der Prioritätensetzung kann dann abgelesen werden, in welcher Reihenfolge die einzelnen Schäden behoben werden sollten. Hierbei sollte allerdings beachtet werden, dass die vorab vorgenommene Prioritätensetzung nur eine erste Orientierung bietet. Gegebenenfalls muss sie im individuellen Fall angepasst werden.

Beispiel:

Angenommen wird, dass es in der obigen Beispiel-Stadtverwaltung einem Hacker gelungen ist, die Informationen auf dem Internet-Informationsserver zu manipulieren, so dass die Stadtverwaltung verunglimpft wird. Dies wird frühzeitig bemerkt, das IT-Sicherheitsmanagement eingeschaltet und die obige Schadenseinschätzung durchgeführt. Diese hätte zum Ergebnis, dass folgende Schäden zu erwarten sind:

Schadenskategorie	Schaden mittel	Schaden hoch	Schaden sehr hoch
Verstoß gegen Gesetze, Vorschriften oder Verträge	S1		
Beeinträchtigung des informationellen Selbstbestimmungsrechts			
Beeinträchtigung der persönlichen Unversehrtheit			
Beeinträchtigung der Aufgabenerfüllung	S2		
Negative Außenwirkung			S3
Finanzielle Auswirkungen	S4		

Tabelle: Schadenskategorieneinteilung

Den Schäden S1, ..., S4 werden anhand der Prioritätensetzung folgende Prioritäten zugeordnet:

Prioritätenklassifizierung: S1 = 2, S2 = 3, S3 = 1, S4 = 3

Prioritätenreihenfolge: S1 = 13, S2 = 15, S3 = 4, S4 = 18

In beiden Fällen würde deutlich, dass die Anstrengungen der Schadensbegrenzung sich zunächst auf den Schaden S3 (negative Außenwirkung) konzentrieren müssten, bevor die anderen Schäden angegangen würden. Im Beispiel würde man, um die negative Außenwirkung zu begrenzen, den manipulierten Internet-Server vom Netz nehmen, um anschließend weitere Maßnahmen zu ergreifen. Hätte man die Schäden der negativen Außenwirkung niedriger priorisiert und hingegen die Beeinträchtigung der Aufgabenerfüllung in den Vordergrund gestellt, würde man gegebenenfalls von der Abschaltung des Internet-Servers als Sofortmaßnahme absehen.

Ergänzende Kontrollfragen:

- Ist die getroffene Prioritätensetzung mit der Behörden- bzw. Unternehmensleitung abgestimmt?
- Ist die Prioritätensetzung allen Entscheidungsträgern des Managementsystems zur Behandlung von Sicherheitsvorfällen bekannt?
- Wann wurde die Prioritätensetzung aktualisiert?

M 6.63 Untersuchung und Bewertung eines Sicherheitsvorfalls

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator, Notfall-Verantwortliche, Verantwortliche der einzelnen IT-Anwendungen

Nicht jeder Sicherheitsvorfall ist unmittelbar als solcher zu erkennen. Viele Sicherheitsvorfälle, insbesondere wenn es sich um gezielte vorsätzliche Angriffe auf IT-Systeme handelt, fallen erst nach Tagen oder Wochen auf. Oftmals kommt es auch zu Fehlalarmen, z. B. weil Hard- oder Software-Probleme als Infektion mit Computer-Viren fehlinterpretiert werden.

Um jedoch eine sicherheitsrelevante Unregelmäßigkeit untersuchen und bewerten zu können, muss vorausgesetzt werden können, dass bestimmte Vorabfeststellungen schon durchgeführt wurden. Dazu zählen

- die Erhebung der vorhandenen IT-Struktur und IT-Vernetzung,
- die Erhebung der Ansprechpartner bzw. Benutzer der IT-Systeme,
- die Erhebung der IT-Anwendungen auf den jeweiligen IT-Systemen und
- die Schutzbedarfsfeststellung der IT-Systeme.

Diese Untersuchungen werden im ersten Schritt der Anwendung des IT-Grundschutzes durchgeführt und müssten daher dem IT-Sicherheitsmanagement im Ergebnis vorliegen.

Was ist alles betroffen?

Anhand dieser Informationen kann bei einer eingehenden Meldung kurzfristig entschieden werden, welches IT-System mit welchen IT-Anwendungen und mit welchem Schutzbedarf betroffen ist. Gleichzeitig ist bekannt, wer als Ansprechpartner benannt ist und kurzfristig zur Entscheidungsfindung hinzugezogen werden kann.

Stellt sich dabei heraus, dass ein IT-System oder eine IT-Anwendung mit einem hohen Schutzbedarf betroffen ist, so liegt ein Sicherheitsvorfall vor und die festgelegten Schritte zu dessen Behandlung sind einzuleiten. Sind hingegen nur IT-Anwendungen und IT-Systeme mit geringem Schutzbedarf betroffen, kann versucht werden, das Sicherheitsproblem lokal zu beheben.

Mobilisieren des Sicherheitsvorfall-Teams

Zeichnet es sich ab, dass der Sicherheitsvorfall schwerwiegende Folgen haben könnte und eine hinreichend große Komplexität besitzt, kann es sinnvoll sein, das Sicherheitsvorfall-Team (siehe M 6.59 *Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen*) kurzfristig einzuberufen.

Zur Untersuchung und Bewertung des Sicherheitsvorfalls sind als Nächstes folgende Einflussfaktoren zu erheben:

- Welche IT-Systeme und IT-Anwendungen können von dem Sicherheitsvorfall zusätzlich betroffen sein?
- Können Folgeschäden auch durch die Vernetzung der IT-Systeme entstehen?

- Für welche IT-Systeme und IT-Anwendungen können Schäden und Folgeschäden ausgeschlossen werden?
- Wie hoch kann der durch den Sicherheitsvorfall verursachte direkte Schaden oder Folgeschaden sein? Dabei ist insbesondere die Abhängigkeit der verschiedenen IT-Systeme und IT-Anwendungen zu beachten.
- Wodurch wurde der Sicherheitsvorfall ausgelöst (z. B. durch Unachtsamkeit, Angreifer oder Ausfall der Infrastruktur)?
- Wann und an welcher Stelle hat sich der Sicherheitsvorfall ereignet? Dies kann auch weit vor der ersten Beobachtung des Sicherheitsvorfalls liegen. Auch bei dieser Untersuchung sind gut geführte Protokolldateien eine wertvolle Hilfe, aber nur, wenn man sich darauf verlassen kann, dass sie nicht manipuliert worden sind.

Protokolle zu Rate ziehen

- Sind durch den Sicherheitsvorfall nur interne IT-Benutzer oder auch externe Dritte betroffen?
- Wie viele Informationen über den Sicherheitsvorfall sind bereits an die Öffentlichkeit gedrungen?

Stellt sich dabei heraus, dass der Sicherheitsvorfall schwerwiegende Folgen nach sich ziehen kann, ist zumindest die nächste Eskalationsebene zu beteiligen.

Aktionen festlegen

Nach dieser Erhebung der Einflussfaktoren sind die Handlungsoptionen zu erarbeiten, die aus Sofortmaßnahmen und ergänzenden Maßnahmen bestehen. Hierbei sind die getroffenen Prioritätenfestlegungen zu beachten (siehe M 6.62 *Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen*). Dazu ist auch die notwendige Zeit für die Durchführung dieser Maßnahmen und die erforderlichen Kosten und Ressourcen für die Problembehebung und Wiederherstellung abzuschätzen.

Übersteigen Schadenshöhe, Zeit und Kosten eine vorbestimmte Grenze, ist vor der Entscheidung über die Maßnahmenauswahl die nächsthöhere Eskalations- und Entscheidungsebene miteinzubeziehen. Im Ergebnis liegen nach einer so strukturierten Untersuchung und Bewertung eines Sicherheitsvorfalls die Handlungsoptionen vor.

Ergänzende Kontrollfragen:

- Liegen die erforderlichen Informationen aus der Schutzbedarfsfeststellung den Meldestellen und den nachfolgenden Eskalationsebenen vor?
- Sind Hilfsmittel vorhanden, um die Auswertung von Sicherheitsvorfällen technisch zu unterstützen, beispielsweise Tools zur Auswertung von Protokolldaten?

M 6.64 Behebung von Sicherheitsvorfällen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Administrator, Leiter IT

Sobald die Ursache eines Sicherheitsvorfalls identifiziert worden ist, sollten die erforderlichen Maßnahmen zu dessen Behebung ausgewählt und umgesetzt werden. Dazu muss zunächst das Problem eingegrenzt und beseitigt werden und anschließend der "normale" Zustand wiederhergestellt werden.

Bereitstellung des notwendigen Expertenwissens

Liste mit Experten-Adressen

Die unabdingbare Voraussetzung für die Untersuchung und Beseitigung einer Sicherheitslücke ist das entsprechende Fachwissen. Daher muss das Personal entsprechend geschult sein oder es müssen Experten zu Rate gezogen werden. Dafür sollte eine Liste mit den Kontaktadressen von einschlägigen internen und externen Experten aus den verschiedenen Themenbereichen vorbereitet sein, damit diese schnell zu Rate gezogen werden können. Zu den externen Experten gehören unter anderem

- Computer Emergency Response Teams (CERTs) (siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*),
- Hersteller bzw. Vertreiber der betroffenen IT-Systeme (siehe auch M 4.107 *Nutzung von Hersteller-Ressourcen*),
- Hersteller bzw. Vertreiber der eingesetzten Sicherheitssysteme, wie Computer-Viren-Schutzprogramm, Firewall, Zutrittskontrolle, etc.,
- externe Berater mit sicherheitsspezifischem Fachwissen.

Wiederherstellung des sicheren Zustands

Untersuchung der betroffenen IT-Systeme

Zur Beseitigung von Sicherheitslücken müssen die betroffenen IT-Systeme vom Netz genommen und alle Dateien gesichert werden, die Aufschluss über die Art und Ursache des aufgetretenen Problems geben könnten. Hierzu gehören insbesondere alle relevanten Protokolldateien. Da das gesamte IT-System als unsicher oder manipuliert betrachtet werden sollte, müssen das Betriebssystem und alle Applikationen auf Veränderungen untersucht werden. Neben Programmen müssen aber auch Konfigurationsdateien und Benutzerdateien auf Manipulationen untersucht werden. Sinnvollerweise sollten hierfür Prüfsummenverfahren eingesetzt werden. Dies setzt allerdings voraus, dass die Prüfsummen des "sicheren" Zustandes im Vorfeld erhoben und auf schreibgeschützte Datenträger ausgelagert wurden (siehe auch M 4.93 *Regelmäßige Integritätsprüfung*).

Vorsicht beim Einspielen von Datensicherungen!

Um sicherzugehen, dass von einem Angreifer hinterlassene trojanische Pferde wirklich beseitigt worden sind, sollten die Original-Dateien von schreibgeschützten Datenträgern wiedereingespielt werden. Dabei muss darauf geachtet werden, dass alle sicherheitsrelevanten Konfigurationen und Patches mitaufgespielt werden. Wenn Dateien aus Datensicherungen wiedereingespielt werden, muss sichergestellt sein, dass diese vom Sicherheitsvorfall nicht betroffen waren, also z. B. nicht bereits mit dem Computer-Virus infiziert sind. Die Untersuchung der Datensicherungen kann andererseits hilfreich sein,

um den Beginn eines Angriffs oder einer Computer-Virusinfektion festzustellen.

Passwörter ändern!

Vor der Wiederinbetriebnahme nach einem Angriff sollten alle Passwörter auf den betroffenen IT-Systemen geändert werden. Dies schließt auch die IT-Systeme ein, die nicht unmittelbar durch Manipulationen betroffen waren, von denen aber der Angreifer vielleicht bereits Informationen über die Benutzer und/oder Passwörter eingeholt hat.

Überwachung der betroffenen IT-Systeme

Es sollte damit gerechnet werden, dass nach dem Wiederherstellen des "sicheren" Zustands der Angreifer eine erneute Attacke versucht. Deshalb sollten die IT-Systeme, insbesondere die Netzübergänge, mit den entsprechenden Überwachungstools beobachtet werden (siehe auch M 5.71 *Intrusion Detection und Intrusion Response Systeme*).

Dokumentation

Während der Behebung eines Sicherheitsproblems sollten alle durchgeführten Aktionen möglichst detailliert dokumentiert werden,

- um den Überblick zu behalten,
- um die aufgetretenen Probleme nachvollziehbar zu machen,
- um einen Fehler, der bei der meist zügigen Umsetzung der Gegenmaßnahmen erfolgen kann, wieder beheben zu können,
- um bereits bekannte Probleme bei einem erneuten Auftreten schneller bereinigen zu können,
- um die Sicherheitslücken schließen und vorbeugende Maßnahmen ausarbeiten zu können und
- um für eine mögliche Strafverfolgung Beweise zu sammeln.

Zu einer solchen Dokumentation gehören nicht nur eine Beschreibung der durchgeführten Aktionen inklusive der Zeitpunkte, sondern auch die Protokolldateien der betroffenen IT-Systeme.

Reaktion auf vorsätzliche Handlungen

Bei Sicherheitsvorfällen, die durch einen Angreifer ausgelöst wurden, muss eine Entscheidung darüber getroffen werden, ob der entdeckte Angriff beobachtet oder möglichst schnell Gegenmaßnahmen durchgeführt werden sollen. Natürlich kann versucht werden, den Angreifer "auf frischer Tat" zu ertappen, aber dies birgt auch das Risiko, dass der Angreifer in der Zwischenzeit Daten zerstört, manipuliert oder ausliest.

Umgang mit Innentätern

Leider stellt sich bei der Untersuchung von Sicherheitsproblemen häufig heraus, dass diese von eigenen Mitarbeitern verursacht worden sind. Dies kann durch Versehen, fehlerhafte Arbeitsabläufe oder technische Probleme passieren, aber auch durch Nichtbeachtung von Sicherheitsmaßnahmen oder vorsätzliche Handlungen.

Es muss bei allen intern verursachten Sicherheitsproblemen der Auslöser untersucht werden. In vielen Fällen wird sich zeigen, dass die Probleme aus fehlerhaften oder missverständlichen Regelungen resultieren. Dann müssen

die Regelungen entsprechend geändert oder um weitere, z. B. technische Maßnahmen, ergänzt werden.

Sind Sicherheitsprobleme vorsätzlich oder aus Nachlässigkeit verursacht worden, sollten angemessene disziplinarische Maßnahmen ergriffen werden.

Ergänzende Kontrollfragen:

- Wann wurde die Liste der Sicherheitsexperten letztmalig aktualisiert?
- Sind schon vorsätzliche Angriffe durch Innentäter beobachtet worden?

M 6.65 Benachrichtigung betroffener Stellen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, IT-Sicherheitsmanagement, Leiter IT, Pressestelle

Wenn ein Sicherheitsvorfall eingetreten ist, müssen alle davon betroffenen internen und externen Stellen darüber informiert werden. Dies sind insbesondere diejenigen Stellen, die direkt durch den Sicherheitsvorfall Schäden erleiden könnten, Gegenmaßnahmen ergreifen müssen oder solche, die Informationen über Sicherheitsvorfälle aufbereiten und bei der Vorbeugung oder Behebung helfen können. Bei Bedarf sollte auch die Öffentlichkeit aufgeklärt werden, insbesondere wenn schon Informationen durchgesickert sind.

Wer informiert wen?

Hierzu muss individuell für den Sicherheitsvorfall ein klares Konzept entwickelt werden, wer durch wen in welcher Reihenfolge in welcher Tiefe informiert wird. Dazu muss sichergestellt sein, dass Auskünfte über den Sicherheitsvorfall ausschließlich durch benannte Verantwortliche, wie zum Beispiel das IT-Sicherheitsmanagement oder die Pressestelle, gegeben werden.

Nichts beschönigen!

Wer Informationen in welchem Detaillierungsgrad erhält, hängt natürlich insbesondere vom fachlichen Hintergrund ab. Es sollten keine falschen oder schöngefärbten Informationen weitergegeben werden, da dies zu Verwirrung, Fehleinschätzungen und Imageverlust führen kann.

Beispielhaft soll nachfolgend aufgezeigt werden, welche Stellen typischerweise über welche Inhalte aufgeklärt werden:

Interne Stellen

Besteht noch Unklarheit darüber, ob ein Sicherheitsvorfall vorliegt oder wie schwerwiegend er ist, sollten die potentiell betroffenen internen Kräfte gebeten werden, ihre Arbeitsbereiche auf Unregelmäßigkeiten zu prüfen.

Sind die erforderlichen Gegenmaßnahmen bei einem Sicherheitsvorfall bekannt, müssen die betroffenen internen Stellen kurzfristig darüber informiert werden, was sie tun müssen, um die Auswirkungen eines Sicherheitsvorfalls zu minimieren oder um den sicheren Zustand wiederherzustellen.

Zu berücksichtigen sind dabei u. a. folgende Gruppen:

- Leiter IT,
- Leiter von betroffenen Fachabteilungen,
- IT-Benutzer,
- IT-Administratoren,
- IT-Benutzerservice,
- Haustechnik
- Überwachungspersonal,
- interne Sicherheitskräfte und
- Pförtner.

Externe Stellen

Falls der Sicherheitsvorfall nicht intern begrenzt ist, sollten alle externen Stellen, die ebenfalls betroffen sind oder sein können, darüber informiert werden, welches Sicherheitsproblem aufgetreten ist, welche Gegenmaßnahmen notwendig sind und wie die Auswirkungen eingedämmt werden können.

Sollte diese Informationsweitergabe nicht erfolgen, kann dies im Falle des Bekanntwerdens eine weitere konstruktive Zusammenarbeit nachhaltig schädigen und ein bestehendes Vertrauensverhältnis beeinträchtigen.

Zu berücksichtigen sind dabei folgende Gruppen:

- Kunden,
- Lieferanten,
- freie Mitarbeiter,
- Subunternehmen,
- IT-Service-Dienstleister,
- Stellen, zu denen Kommunikationsverbindungen existieren,
- Software-Entwicklungsunternehmen und
- Netzbetreiber.

Je nach Art des Vorfalls kann es außerdem notwendig sein, die Polizei bzw. einen Rechtsbeistand hinzuzuziehen.

Öffentlichkeit

öffentliche Aussagen nur durch den Pressesprecher

Bei größeren oder komplexeren Sicherheitsvorfällen kann es notwendig sein, die Öffentlichkeit aufzuklären. Alle Pressekontakte sollten hierbei ausschließlich über den Pressesprecher laufen. Dazu ist sicherzustellen, dass der Pressesprecher über den Sicherheitsvorfall, über Schadenshöhe und erforderliche Gegenmaßnahmen und über benachrichtigte Stellen ausreichend vorab informiert wird.

Die Informationen für die Öffentlichkeit sollten jedoch so weit abstrahiert werden, dass keine Nachahmer animiert werden.

Bei allen Personen, die Informationen über Sicherheitsvorfälle einholen wollen, ist es wichtig, deren Identität zu überprüfen, damit sich der Angreifer nicht über den Erfolg seiner Attacke auf dem Laufenden halten kann.

IT-Sicherheitsgemeinde

Warnung vor Sicherheitslücke weiterleiten

Ist der Sicherheitsvorfall auf eine noch nicht bekannte Sicherheitslücke zurückzuführen, sollte diese Erkenntnis nicht verheimlicht, sondern an weitere Stellen geleitet werden, damit vor der Sicherheitslücke gewarnt wird und Gegenmaßnahmen entwickelt werden können. Als Adressaten kommen dabei typischerweise folgende Stellen in Betracht:

- Hersteller des Computer-Viren-Suchprogramms, wenn der Verdacht besteht, dass ein neuartiger Computer-Virus IT-Systeme infiziert hat, aber der Viren-Scanner diesen nicht erkennt,
- Hersteller des Betriebssystems oder der Applikationssoftware, falls die Sicherheitslücke darin aufgetreten ist,

- Computer Emergency Response Team (CERT, siehe auch M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*), wenn der Sicherheitsvorfall auf system- oder applikationsspezifischen Sicherheitslücken beruht,
- IT-Sicherheitsfachpresse oder
- für IT-Sicherheit zuständige öffentliche Stellen wie das BSI.

Beispiel:

Es wurde bemerkt, dass sporadisch Daten auf PCs manipuliert oder unauffindbar waren. Nach Meldung und anschließender Untersuchung stellte sich heraus, dass ein bislang unbekannter Makro-Virus aufgetreten ist. Dieser Virus verbreitet sich über an E-Mail angehängte Dateien. In diesem Fall sollten folgende Stellen umgehend benachrichtigt werden:

- Leiter IT,
- IT-Benutzer,
- IT-Administratoren,
- IT-Benutzerservice,
- sämtliche Stellen, mit denen seit dem ersten Auftreten des Computer-Virus Daten ausgetauscht wurden,
- Hersteller des Computer-Viren-Suchprogramms, da der Viren-Scanner diesen nicht erkannt hat und
- ein Computer Emergency Response Team.

Ergänzende Kontrollfragen:

- Wer gibt Informationen über Sicherheitsvorfälle an Dritte weiter?
- Wie wird sichergestellt, dass keine unautorisierte Person Informationen über den Sicherheitsvorfall weitergibt?

M 6.66 Nachbereitung von Sicherheitsvorfällen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Revisor

Aus jedem Sicherheitsvorfall kann man etwas lernen. Um aus einem eingetretenen Sicherheitsvorfall den maximalen Lerneffekt ziehen zu können, darf die Nachbereitung nicht vernachlässigt werden. Oftmals lassen sich daraus Verbesserungen im Umgang mit Sicherheitsvorfällen herausarbeiten oder Rückschlüsse auf die Wirksamkeit des IT-Sicherheitsmanagements bzw. der vorhandenen IT-Sicherheitsmaßnahmen ziehen. Dabei sind unter anderem folgende Aspekte zu beachten:

Reaktionszeit

Untersucht werden sollte, wie schnell der Sicherheitsvorfall bemerkt wurde. Dabei ist zu prüfen, ob es sinnvoll ist, technische Detektionsmaßnahmen nachzurüsten.

Darüber hinaus sollte auch der Frage nachgegangen werden, wie lange es dauerte, bis die Meldung den erforderlichen Meldeweg durchlaufen hat. Schließlich sollte der Aspekt betrachtet werden, wie schnell die Entscheidungen über die zu treffenden Maßnahmen erfolgte, wie lange deren Umsetzung dauerte und wann die Benachrichtigung der betroffenen internen und externen Stellen erfolgte.

Hat der Informationsfluss funktioniert?

Bei der Rückverfolgung des Meldewegs sollte überprüft werden, ob der Meldeweg jedem bekannt war oder ob zusätzliche Sensibilisierungsmaßnahmen und Informationen notwendig sind.

Wirksamkeit der Eskalationsstrategie

Anhand des konkreten Sicherheitsvorfalls sollte untersucht werden, ob die festgelegte Eskalationsstrategie eingehalten wurde, welche zusätzlichen Informationen notwendig sind und ob eine Anpassung der Eskalationsstrategie notwendig ist.

Effektivität der Untersuchung

In einer Rückschau sollte betrachtet werden, ob die Einschätzung der Schadenshöhe des Sicherheitsvorfalls korrekt war, ob die berücksichtigten Prioritäten angemessen waren und ob ein für die Untersuchung geeignetes Sicherheitsvorfall-Team eingesetzt wurde.

Benachrichtigung betroffener Stellen

Überprüft werden sollte, ob tatsächlich sämtliche betroffenen Stellen benachrichtigt wurden und ob die Benachrichtigung zeitlich ausreichend schnell war. Unter Umständen müssen schnellere Wege der Benachrichtigung gefunden werden.

Rückmeldung an meldende Stelle

Diejenigen Stellen, die einen Sicherheitsvorfall entdeckt haben und diesen an die zuständigen Experten weitergemeldet haben, sollten nach dessen Behebung auch über die entstandenen Schäden und ergriffenen Maßnahmen informiert werden. Dies zeigt, dass solche Meldungen ernst genommen werden und fördert die Motivation. Zusätzlich könnte auch eine Belobigung oder Belohnung für die korrekte Weitermeldung ausgesprochen werden, um für das Betriebsklima ein Signal zu setzen, wie wichtig das Meldewesen für Sicherheitsvorfälle ist.

Tätermotivation

Stellt sich heraus, dass der Sicherheitsvorfall auf eine vorsätzliche Handlung zurückzuführen ist, sollte die Motivation des Täters untersucht werden. Handelt es sich dabei um einen Innentäter, kommt der Motivation eine besondere Bedeutung zu. Stellt sich heraus, dass die Ursache im Bereich des Betriebsklimas zu sehen ist, sollte dies auch der Leitungsebene bekanntgegeben werden, da zu erwarten ist, dass Fehlhandlungen und vorsätzliche Handlungen wiederholt auftreten werden.

Je nach Relevanz der Nachbereitungsergebnisse sollte die Leitungsebene unterrichtet werden, um Verbesserungen zu veranlassen. Daher kann es sinnvoll sein, diese Nachbereitung durch eine Organisationseinheit durchzuführen, die nicht Teil des Meldeplans ist.

Entwicklung einer Handlungsanweisung

Im Rahmen der Nachbereitung eines Sicherheitsvorfalls ist es sinnvoll, aus den Erfahrungen heraus eine Handlungsanweisung zu erstellen bzw. zu überarbeiten, wie bei Auftreten eines vergleichbaren Sicherheitsvorfalls zu verfahren ist. Da jetzt die Probleme real bearbeitet wurden, können Handlungsanweisungen noch effizienter ausgearbeitet werden als bei der Erstellung auf einer theoretischen Basis. Darüber hinaus beweist der aufgetretene Sicherheitsvorfall, dass ein Bedarf für eine Handlungsanweisung konkret für diese Art von Sicherheitsvorfall gegeben ist. Eine derart erstellte Handlungsanweisung ist den relevanten Personengruppen in geeigneter Weise bekannt zu geben.

Ergänzende Kontrollfragen:

- Wurde eine Nachbereitung der letzten Sicherheitsvorfälle durchgeführt?
- Findet eine jährliche Unterrichtung der Leitungsebene über die Sicherheitsvorfälle statt?
- Wie werden die konkreten Handlungsanweisungen aktualisiert und bekanntgegeben?

M 6.67 Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement

Aufdecken von Sicherheitsvorfällen

Neben der Prävention kommt auch der Detektion von Sicherheitsvorfällen große Bedeutung zu. Es gibt eine Reihe von sicherheitsrelevanten Unregelmäßigkeiten, die mit entsprechender technischer Unterstützung automatisiert und daher frühzeitig erkannt werden können. Diese Detektionsmaßnahmen erhöhen meist die Zuverlässigkeit der Feststellung und verkürzen die Zeit zwischen Auftreten und Erkennen einer Unregelmäßigkeit drastisch. Dem Gewinn an Reaktionsfähigkeit und -zeit steht jedoch der Aufwand zur Implementation und Kontrolle gegenüber, der vorher abgeschätzt werden sollte. Praktisch unverzichtbar sind solche Detektionsmaßnahmen, wenn im Schadensfall sehr große Schäden bis hin zum Personenschaden zu erwarten sind.

Beispiele für solche technischen Detektionsmaßnahmen sind:

- Gefahrenmeldeanlage (siehe M 1.18 *Gefahrenmeldeanlage*),
- Fernanzeige von Störungen (siehe M 1.31 *Fernanzeige von Störungen*),
- Computer-Viren-Suchprogramme (siehe M 2.157 *Auswahl eines geeigneten Computer-Viren-Suchprogramms*),
- Intrusion Detection und Intrusion Response Systeme (siehe M 5.71 *Intrusion Detection und Intrusion Response Systeme*),
- Kryptographische Checksummen (siehe M 4.34 *Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen*) oder
- Einsatz eines Security-Realtime-Monitors für z/OS-Systeme, um Sicherheitsverletzungen schneller feststellen zu können.

Kombination von technischen und organisatorischen Maßnahmen

Nicht alle Sicherheitsvorfälle lassen sich durch rein technische Maßnahmen rechtzeitig feststellen. Häufig müssen zusätzlich organisatorische Maßnahmen hinzukommen. Die Zuverlässigkeit von technischen Detektionsmaßnahmen ist im Allgemeinen davon abhängig, wie aktuell diese sind und wie gut diese auf die tatsächlichen Gegebenheiten angepasst sind. Die Zuverlässigkeit von organisatorischen Detektionsmaßnahmen hängt stark davon ab, wie zuverlässig die mit deren Umsetzung beauftragten Personen sind, aber auch, in wie weit die Maßnahmen sich im laufenden Betrieb tatsächlich umsetzen lassen.

Typische Beispiele von Detektionsmaßnahmen, die ganz oder teilweise organisatorischer Natur sind, sind:

- Informationsbeschaffung über Sicherheitslücken (siehe M 2.35 *Informationsbeschaffung über Sicherheitslücken des Systems*)
- Regelmäßiger Sicherheitscheck ausgewählter IT-Systeme (siehe z. B. M 2.92 *Durchführung von Sicherheitskontrollen im Windows NT Client-Server-Netz*, M 4.93 *Regelmäßige Integritätsprüfung*, M 5.8 *Regelmäßiger Sicherheitscheck des Netzes*)

- Regelmäßige Auswertung von Protokoll-Dateien (siehe z. B. M 2.64 *Kontrolle der Protokolldateien*, M 4.5 *Protokollierung der TK-Administrationsarbeiten*, M 4.25 *Einsatz der Protokollierung im Unix-System*, M 4.47 *Protokollierung der Sicherheitsgateway-Aktivitäten*, M 4.54 *Protokollierung unter Windows NT*, M 5.9 *Protokollierung am Server*)
- Auswertung von SMF-Datensätzen unter z/OS (siehe M 2.291 *Sicherheits-Berichtswesen und -Audits unter z/OS*). Informationen aus diesen SMF-Datensätzen können entweder für Batch-Reports oder als Quelle für Security-Realtime-Monitore benutzt werden, die ihrerseits eine zentrale Kontroll-Konsole ansteuern können. Solche zentralen Konsolen werden von verschiedenen Herstellern im Rahmen von Automationsprodukten angeboten.

Ergänzende Kontrollfragen:

- Welche Detektionsmaßnahmen kommen zum Einsatz?
- Ist sichergestellt, dass Auffälligkeiten in Protokoll-Dateien gemeldet werden?

M 6.68 Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Revisor

Das Managementsystem zur Behandlung von Sicherheitsvorfällen muss regelmäßig auf seine Aktualität und Wirksamkeit geprüft werden. Daneben sollten auch die darin formulierten Maßnahmen regelmäßig daraufhin getestet werden, ob sie

- den betroffenen Mitarbeitern bekannt sind,
- unter Stress umsetzbar sind, also auch bei einem Sicherheitsvorfall, der einen ungeordnet ablaufenden Betrieb zur Folge hat, und
- in den Betriebsablauf integrierbar sind.

Überprüfung des Managementsystems

Um die Wirksamkeit zu testen, sollte durch simulierte Schadensereignisse überprüft werden, ob der festgelegte Handlungsablauf eingehalten wird bzw. überhaupt eingehalten werden kann. Ist er das nicht, müssen entsprechende Änderungen eingebracht werden.

Dazu könnten sowohl angekündigte als auch unangekündigte Übungen durchgeführt werden.

Durch Übungen darf kein Schaden eintreten!

Bei allen unangekündigten Übungen dürfen auf keinen Fall irgendwelche Aktionen ausgelöst werden, die zu irgendeinem nicht oder nur schwer behebbaren Schaden an IT-Systemen, Daten oder sonstigem führen können.

Sehr genau sollte vor dem Beginn jeder Übung überlegt werden, wer alles vorab darüber informiert wird. Es ist immer unbedingt sicherzustellen, dass die Übung durch die Behörden- bzw. Unternehmensleitung autorisiert ist. Manchmal kann es nützlich sein, bestimmte Personengruppen nicht zu informieren, z. B. die Pförtner oder die Administratoren. Es sollte aber sichergestellt sein, dass dabei die Situation unter Kontrolle bleibt. Es sollte also vermieden werden, dass z. B. Polizei oder Feuerwehr alarmiert oder alle Netzverbindungen der Behörde bzw. des Unternehmens gekappt werden.

Beispiele:

simulierte Schadensereignisse

- Rufen Sie bei der Telefonzentrale ihres Unternehmens bzw. Behörde an und geben Sie sich als Hacker aus, der in das interne Netz eingebrochen ist. Wahlweise kann man sich auch als Journalist ausgeben, der darüber informiert sein will, dass ein Hacker ins interne Netz eingebrochen ist und sensitive Daten kopiert hat. Es können auch solche Mitarbeiter angerufen werden, an die typischerweise in solchen Fällen verwiesen wird, also beispielsweise der Pressesprecher oder der Leiter IT. Bei einem solchen Anruf sollte sich zeigen, ob intern Panik ausbricht oder ob gezielt die Aktionen eingeleitet werden, die in einem solchen Fall adäquat wären.
- An einem beliebigen Tag könnten alle bei einer Computer-Viren-Infektion durchzuführenden Handlungen und Meldewege getestet werden. Hierbei müssen nicht unbedingt alle Beteiligten vorher informiert werden, spätestens aber in dem Moment, wo sie in die Handlungskette integriert werden.

Ergänzende Kontrollfragen:

- Welche Übungen wurden zuletzt durchgeführt?
- Werden Übungen vorher mit der Leitungsebene abgestimmt?

M 6.69 Notfallvorsorge und Ausfallsicherheit bei Faxservern

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Fax-Poststelle

Die Maßnahmen für Notfallvorsorge und Ausfallsicherheit von Faxservern sind abhängig vom Volumen, das über den oder die Faxserver abgewickelt wird und von den Anforderungen an die Verfügbarkeit dieses Dienstes.

Konfigurationsparameter dokumentieren

Zunächst ist grundsätzlich sicherzustellen, dass alle Konfigurationsparameter der benutzten Kommunikationskarten, des Betriebssystems und der Faxserver-Applikation dokumentiert werden. Bei Veränderungen an der Konfiguration ist die Dokumentation entsprechend zu aktualisieren. Nur so kann sichergestellt werden, dass im Notfall ein Faxserver in kürzester Zeit neu installiert werden kann.

regelmäßige Datensicherung

Weiterhin sollten in regelmäßigen Abständen gemäß den Festlegungen des Datensicherungskonzeptes und der Sicherheitspolitik Datensicherungen durchgeführt werden. Dabei sollten neben den Datenpartitionen auch die Partitionen, auf denen sich das Betriebssystem und die Faxserver-Applikation befinden, mit in die Datensicherung einbezogen werden.

Die auf dem Faxserver gespeicherten Faxsendungen müssen regelmäßig gesichert werden. Sofern eine dauerhafte Archivierung von Faxdaten gewünscht ist, sollte diese nicht auf dem Faxserver sondern auf externen Datenmedien erfolgen.

herkömmliche Faxgeräte vorhalten

Um bei einem Ausfall des Faxservers bzw. des Netzes auch weiterhin Faxe versenden und empfangen zu können, sollten ggf. ein oder mehrere herkömmliche Faxgeräte vorgehalten werden. Die Anzahl der benötigten Geräte ist vom Volumen an ein- und ausgehenden Faxsendungen im Notfall abhängig. Sinnvoll ist, als Notfallreserve die Faxgeräte zu verwahren, die schon vor Installation des Faxservers verwendet wurden.

Alle weiteren Maßnahmen zur Erhöhung der Ausfallsicherheit verursachen z. T. erhebliche Kosten und werden daher wohl nur bei höheren Anforderungen an die Verfügbarkeit in Betracht kommen und müssen einzeln erwogen werden.

Einsatz von RAID-Systemen

Zunächst kann das IT-System, auf dem der Faxserver installiert ist, mit einem RAID-System ausgerüstet werden. Dabei werden mehrere Festplatten zu einem Stapel zusammengefasst und die darauf befindlichen Daten unter Bildung von Redundanzen auf die verschiedenen Festplatten verteilt. Dies führt z. B. bei einem so genannten RAID Level 5 dazu, dass auch beim Ausfall einer Festplatte keine Datenverluste auftreten. Allerdings verringert sich beim Einsatz der RAID-Technologie die freie Gesamtkapazität der Festplatten wegen der Redundanzbildung. Außerdem muss berücksichtigt werden, dass diese Lösung kein Ersatz für die externe Datensicherung ist und auch nicht vor dem Gesamtausfall des Systems schützt.

Einsatz mehrerer Faxserver

Ausfallsicherheit kann auch durch den Einsatz mehrerer Faxserver erreicht werden. Sofern ein Server ausfällt, kann die Last auf die anderen Server verteilt werden. Vorteilhaft an dieser Lösung ist zudem, dass auch eine Last-

trennung erreicht wird und die Gefahr einer Überlastung eines einzelnen Faxservers vermindert wird. Nachteilig ist allerdings, dass eingegangene Faxsendungen, die sich auf dem ausgefallenen Server befinden, zumindest für die Dauer des Ausfalls nicht mehr verfügbar sind.

Einsatz redundanter Faxserver

Sofern Ausfälle bei Faxservern aufgrund der Verfügbarkeitsanforderungen allenfalls im Minutenbereich tolerierbar sind, bietet sich der Einsatz redundanter Server an. Für jeden Faxserver, der in ein solches Redundanzkonzept eingebunden wird, ist dann ein zweiter Server verfügbar, auf den die entsprechenden Daten repliziert werden. Diese Lösung bietet - ggf. in Kombination mit RAID-Systemen - die höchstmögliche Ausfallsicherheit, verursacht aber auch erhebliche Kosten.

Ergänzende Kontrollfragen:

- Ist die Dokumentation der Konfiguration aktuell?
- Wer ist für die Durchführung der Datensicherung zuständig?
- Stehen herkömmliche Faxgeräte als Notfallreserve zur Verfügung?

M 6.70 Erstellen eines Notfallplans für den Ausfall des RAS-Systems

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement-Team

Verantwortlich für Umsetzung: Administrator

Je nach Anforderungen an die Verfügbarkeit kann der Ausfall oder das Nichtzustandekommen von RAS-Verbindungen zu erheblichen Beeinträchtigungen führen. Dabei sind die Fehlerquellen jedoch sehr vielfältig, so dass sich die Ursachenforschung oft als sehr schwierig erweist. Neben dem Ausfall der Verbindungsinfrastruktur (siehe dazu auch G 1.10 *Ausfall eines Weitverkehrsnetzes*) stellen RAS-Clients und RAS-Server - neben den zur Verbindung benutzten Netzkoppelelementen (siehe dazu auch G 4.31 *Ausfall oder Störung von Netzkomponenten*) - naturgemäß weitere Ausfallpunkte in einem RAS-System dar.

Als Folge des Ausfalles einer Komponente des RAS-Systems (Client, Server, Netzkoppelelemente) ergibt sich, dass u. U. wichtige Daten und Informationen nicht ausgetauscht werden können und Arbeitsabläufe unterbrochen werden, bis die Verbindung wieder zustande kommt oder Ausweichlösungen gefunden werden konnten.

Beim Ausfall des RAS-Systems ist die Anbindung externer Rechner (z. B. einzelner Telearbeitsplätze oder ganzer LANs von Filialen) nicht mehr gewährleistet, so dass beispielsweise auch kein Datenaustausch mehr stattfinden kann. Je nach Einsatzszenario kann dies zu erheblichen Beeinträchtigungen des IT-Betriebs führen. Der Notfallvorsorge und der Erstellung eines Notfallplans für den teilweisen (z. B. Ausfall des Authentisierungs-Servers) oder totalen Ausfall des RAS-Systems kommt daher eine wichtige Rolle zu.

Im Rahmen der Notfallvorsorge für das RAS-System sind die generellen Maßnahmen des Bausteins B 1.3 *Notfallvorsorge-Konzept* relevant. Zusätzlich sollten noch die Maßnahmen

- M 6.18 *Redundante Leitungsführung*
- M 6.31 *Verhaltensregeln nach Verlust der*
- M 6.37 *Dokumentation der*
- M 6.54 *Verhaltensregeln nach Verlust der Netzintegrität*

betrachtet werden. Diese Maßnahmen sind jeweils für die im Umfeld des RAS-Systems angesiedelten Komponenten und Daten zu konkretisieren und umzusetzen.

Im Rahmen des Notfallsplans sollten insbesondere folgende Aspekte behandelt werden:

- Welche Störungen, Schäden und Folgeschäden ergeben sich konkret bei Ausfall einer RAS-Verbindung?
- Für welche RAS-Verbindungen muss eine Hochverfügbarkeit gewährleistet werden?
- Wie schnell kann der Ausfall eines RAS-Systems festgestellt werden?

- Können Fehler in den zur Verbindung benutzten Telekommunikationsnetzen schnell als solche erkannt werden oder werden diese dem zuständigen Administrator mitgeteilt (beispielsweise Verbindungsprobleme, Probleme bei der Rufnummernübertragung, Probleme mit der Schaltung von geschlossenen Benutzergruppen)?
- Wie schnell kann eine RAS-Verbindung wieder hergestellt werden (Ersatz von Geräten, Hochfahren des Systems)?
- Beim Ausfall welcher Komponenten muss das RAS-System abgeschaltet werden, obwohl technisch noch RAS-Verbindungen aufgebaut werden können (z. B. Ausfall der Protokollierung, der Kommunikationsverschlüsselung oder des Authentisierungsservers)?

Notfallrufnummer einrichten

Für entfernte Mitarbeiter sollte eine Notfallrufnummer angeboten werden, damit sie RAS-Probleme zeitnah an verantwortliche Stellen kommunizieren können. Außerdem sollte das RAS-System in den kritischen Zeitabschnitten (z. B. Bürozeiten, Zeiten in denen vornehmlich Daten per RAS ausgetauscht werden) permanent überwacht werden.

Notfalldokumentation erstellen

Für einzelne Schadensszenarien sollten geeignete Vorgehensweisen in Form einer Notfalldokumentation erarbeitet werden. Darin sollten alle für die Behebung eines Notfalls notwendigen Daten erfasst und so dargestellt sein, dass auch das Vertretungspersonal damit arbeiten kann. Die Notfalldokumentation sollte außerdem Informationen über alternative Verbindungswege enthalten, z. B. alternative Telekommunikationsanbieter oder alternative Übertragungsmedien.

Wiederanlaufplan erarbeiten

Je nach Anforderungen an die Verfügbarkeit des RAS-Systems müssen u. U. Ersatzgeräte für den sofortigen Austausch vorgehalten werden. Für die erneute Inbetriebnahme des RAS-Systems nach einem Austausch oder einem Systemabsturz muss die Notfalldokumentation einen Wiederanlaufplan enthalten. Ggf. ist es sogar erforderlich, dass bestimmte Komponenten im laufenden Betrieb ausgetauscht werden können. Dieses so genannte Hot-Swap muss von den beteiligten Komponenten unterstützt werden.

Datenintegrität nach Störungen überprüfen

Je nach RAS-System kann die Konsistenz der per RAS übertragenen Daten bei einem Systemabsturz nicht gewährleistet werden. Nach jeder Störung sollte daher die Integrität dieser Daten überprüft und eine Problemanalyse durchgeführt werden, um Wiederholungen möglichst zu vermeiden.

sichere Notfallkonfiguration

In bestimmten Situationen kann es erforderlich sein, das RAS-System mit eingeschränkter Funktionalität oder Leistungsfähigkeit zu betreiben. In diesem Fall muss eine entsprechende Notfallkonfiguration aktiviert werden (siehe auch M 4.111 *Sichere Konfiguration des RAS-Systems*). Diese dient dazu, die Sicherheit des RAS-Systems (Zugangssicherheit, Zugriffssicherheit, Kommunikationssicherheit) auch bei eingeschränktem Betrieb aufrechtzuerhalten.

Ergänzende Kontrollfrage:

- Gibt es einen Notfallplan für RAS-Systeme?
- Erfüllt dieser die geforderten Anforderungen?

M 6.71 Datensicherung bei mobiler Nutzung des IT-Systems

Verantwortlich für Initiierung: IT-Sicherheitsmanagement-Team, Leiter IT

Verantwortlich für Umsetzung: Administrator, Benutzer

IT-Systeme im mobilen Einsatz (z. B. Laptops, Notebooks) sind in aller Regel nicht permanent in ein Netz eingebunden. Der Datenaustausch mit anderen IT-Systemen erfolgt üblicherweise über Datenträger oder über temporäre Netzanbindungen. Letztere können beispielsweise durch Remote Access oder direkten Anschluss an ein LAN nach Rückkehr zum Arbeitsplatz realisiert sein. Anders als bei stationären Clients ist es daher bei mobilen IT-Systemen meist unvermeidbar, dass Daten zumindest zeitweise lokal anstatt auf einem zentralen Server gespeichert werden. Dem Verlust dieser Daten muss durch geeignete Datensicherungsmaßnahmen vorgebeugt werden.

Generell bieten sich folgende Verfahren zur Datensicherung an:

1. **Datensicherung auf externen Datenträgern**

   Der Vorteil dieses Verfahrens ist, dass die Datensicherung an nahezu jedem Ort und zu jeder Zeit erfolgen kann. Nachteilig ist, dass ein geeignetes Laufwerk und genügend Datenträger mitgeführt werden müssen und dass für den Benutzer zusätzlicher Aufwand für die ordnungsgemäße Handhabung der Datenträger entsteht. Die Datenträger sollten eine ausreichende Speicherkapazität besitzen, so dass der Benutzer nicht mehrere Datenträger pro Sicherungsvorgang in das Laufwerk einlegen muss. Bei unverschlüsselter Datenhaltung ergibt sich außerdem die Gefahr, dass Datenträger abhanden kommen und dadurch sensitive Daten kompromittiert werden können. Die Datenträger und das mobile IT-System sollten möglichst getrennt voneinander aufbewahrt werden, damit bei Verlust oder Diebstahl des IT-Systems die Datenträger nicht ebenfalls abhanden kommen.

   Die Speicherung auf externen Datenträgern zur Datensicherung bietet sich insbesondere an, wenn auch der Datenaustausch mit anderen IT-Systemen über externe Datenträger erfolgt. Diese beiden Prozesse können u. U. kombiniert werden. Nach Rückkehr zum Arbeitsplatz müssen die Datensicherungen auf den Datenträgern in das Backup-System oder in das Produktivsystem bzw. die zentrale Datenhaltung der Institution eingepflegt werden.

2. **Datensicherung über temporäre Netzverbindungen**

   Wenn die Möglichkeit besteht, das IT-System regelmäßig an ein Netz anzuschließen, beispielsweise über Remote Access, kann die Sicherung der lokalen Daten auch über die Netzanbindung erfolgen. Vorteilhaft ist hier, dass der Benutzer keine Datenträger verwalten und auch kein entsprechendes Laufwerk mitführen muss. Weiterhin lässt sich das Verfahren weitgehend automatisieren, beispielsweise kann die Datensicherung beim Einsatz von Remote Access nach jedem Einwahlvorgang automatisch gestartet werden.

Entscheidend bei der Datensicherung über eine temporäre Netzverbindung ist, dass deren Bandbreite für das Volumen der zu sichernden Daten ausreichen muss. Die Datenübertragung darf nicht zu lange dauern und nicht zu übermäßigen Verzögerungen führen, wenn der Benutzer gleichzeitig auf entfernte Ressourcen zugreifen muss. Bei gängigen Zugangstechnologien (z. B. ISDN, Modem, Mobiltelefon) bedeutet dies, dass nur geringe Datenmengen pro Sicherungsvorgang transportiert werden können. Einige Datensicherungsprogramme bieten daher die Möglichkeit an, lediglich Informationen über die Änderungen des Datenbestands seit der letzten Datensicherung über die Netzverbindung zu übertragen. In vielen Fällen kann hierdurch das zu transportierende Datenvolumen stark reduziert werden.

Eine wichtige Anforderung an die zur Datensicherung verwendete Software ist, dass unerwartete Verbindungsabbrüche erkannt und ordnungsgemäß behandelt werden. Die Konsistenz der gesicherten Daten darf durch Verbindungsabbrüche nicht beeinträchtigt werden.

Bei beiden Verfahren zur Datensicherung ist es wünschenswert, das Volumen der zu sichernden Daten zu minimieren. Neben dem Einsatz verlustfreier Kompressionsverfahren, die in viele Datensicherungsprogrammen integriert sind, können auch inkrementelle oder differentielle Sicherungsverfahren zum Einsatz kommen (siehe auch M 6.35 *Festlegung der Verfahrensweise für die Datensicherung*). Hierdurch erhöht sich jedoch u. U. der Aufwand für die Wiederherstellung einer Datensicherung.

Die Datensicherung sollte möglichst weitgehend automatisiert werden, so dass die Benutzer möglichst wenig Aktionen selbst durchführen müssen. Wenn die Mitarbeit der Benutzer erforderlich ist, sollten sie zur regelmäßigen Durchführung der Datensicherung verpflichtet werden (siehe M 2.41 *Verpflichtung der Mitarbeiter zur Datensicherung*). Schließlich sollte sporadisch geprüft werden, ob angelegte Datensicherungen wiederhergestellt werden können (siehe M 6.22 *Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen*).

Ergänzende Kontrollfragen:

- Werden alle Daten, die auf mobilen IT-Systemen lokal gespeichert werden, regelmäßig gesichert?
- Ist das gewählte Verfahren zur Datensicherung für das Volumen des Datenbestands geeignet?
- Sind bei der Datensicherung möglichst wenig Aktionen des Benutzers erforderlich?

M 6.72 Ausfallvorsorge bei Mobiltelefonen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Benutzer

Ein Mobiltelefon kann aus verschiedenen Gründen ausfallen oder in seiner Funktionsfähigkeit gestört sein. Dies ist natürlich besonders ärgerlich, wenn es dringend benötigt wird oder dadurch wichtige Daten verloren gehen. Daher sollten von vorne herein entsprechende Vorkehrungen getroffen werden, um einem Ausfall vorzubeugen bzw. die Probleme zu minimieren.

Energieversorgung

Der Ladezustand und die Funktionsfähigkeit des Mobiltelefon-Akkus sollten regelmäßig überprüft werden (siehe auch M 4.115 *Sicherstellung der Energieversorgung von Mobiltelefonen*).

regelmäßige Datensicherung

Alle auf dem Mobiltelefon gespeicherten Daten wie Telefonbucheintragungen, Nachrichten, etc. sollten in regelmäßigen Abständen auf einem anderen Medium gespeichert werden, damit sie im Zweifelsfall rekonstruiert werden können. Hierzu gibt es mehrere Möglichkeiten:

- Die wichtigsten Einstellungen wie PINs und die Konfiguration von Sicherheitsmechanismen sollten schriftlich dokumentiert und entsprechend ihres Schutzbedarfs sicher aufbewahrt werden.
- Alle Daten, die auf der SIM-Karte gespeichert sind, also z. B. Telefonbücher, können über SIM-Kartenleser und entsprechende Software in einen PC eingelesen und dort verwaltet werden. Dies hat außerdem den Vorteil, dass Adressdaten auf dem PC leichter gepflegt und mit anderen Adressdatenbanken synchronisiert werden können. Insbesondere bei der Nutzung mehrerer Mobiltelefone (siehe auch M 2.190 *Einrichtung eines Mobiltelefon-Pools*) ist ein Abgleich der Telefonbücher auf diesem Weg sinnvoll. Wenn nur die Daten auf der SIM-Karte gesichert werden, sind alle Benutzer darauf hinzuweisen, dass sie auch nur dort Rufnummern und Ähnliches speichern sollten.
- Das Mobiltelefon kann auch mit einem weiteren IT-System, z. B. einem Notebook oder einem Organizer, gekoppelt und die zu sichernden Daten auf diesem Weg ausgetauscht werden (siehe auch M 5.81 *Sichere Datenübertragung über Mobiltelefone*). Dabei können sowohl die auf der SIM-Karte als auch die im Gerät gespeicherten Daten gesichert werden.

Ersatz vorrätig halten

Wenn ein Mobiltelefon kontinuierlich verfügbar sein soll, sollte ein Ersatz-Mobiltelefon, mindestens aber ein Ersatz-Akku mitgeführt werden.

Wenn Mobiltelefone im Rahmen von Alarmierungen eingesetzt werden, also wenn z. B. die Einbruchmeldeanlage Alarmmeldungen über GSM absetzt oder Notfallpersonal über Mobiltelefone benachrichtigt werden soll, muss immer eine Ausweichmöglichkeit vorgesehen sein.

Reparatur

Bei einem Mobiltelefon kann das komplette Gerät oder auch nur einzelne Komponenten defekt sein. Die Reparatur sollte nur von vertrauenswürdigen Fachbetrieben durchgeführt werden. Daher sollte eine Übersicht über entsprechende Fachbetriebe vorhanden sein.

Viele Händler bieten auch für die Dauer der Reparatur Ersatzgeräte an. Bei schnelllebigen Geräten wie Mobiltelefonen lohnt sich eine Reparatur häufig nicht, so dass auch manchmal ein Tauschgerät angeboten wird. Da gerade ein Mobiltelefon kontinuierlich zur Verfügung stehen sollte, ist bei der Auswahl des Mobiltelefons bzw. des Händlers darauf zu achten, dass solche Dienstleistungen angeboten werden.

Bevor das Mobiltelefon zur Reparatur gegeben wird, sollten alle personenbezogenen Daten, also z. B. der Anrufspeicher, gespeicherte E-Mails und das Telefonbuch im Gerät gelöscht werden (siehe auch M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*), soweit das noch möglich ist. Vorher sollten sie selbstverständlich gesichert werden. Außerdem sollte die SIM-Karte entfernt werden.

Ergänzende Kontrollfragen:

- Existiert eine Liste der Fachhändler für Mobiltelefone im Notfallplan?
- Werden die auf Mobiltelefonen gespeicherten Daten regelmäßig gesichert?

M 6.73 Erstellen eines Notfallplans für den Ausfall des Lotus Notes-Systems

Verantwortlich für Initiierung: Leiter IT, Behörden-/Unternehmensleitung

Verantwortlich für Umsetzung: Administrator

Der teilweise oder komplette Ausfall eines Notes-Systems hat in vielen Fällen gravierende Auswirkungen auf die Arbeitsmöglichkeiten der Benutzer, da alle Server-basierten Aktionen nicht mehr ausgeführt werden können. Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind.

Folgende Aspekte müssen dabei berücksichtigt werden:

- Die Notfallplanung für das Notes-System muss in den existierenden Notfallplan integriert werden (siehe auch Baustein B 1.3 *Notfallvorsorge-Konzept*).
- Durch einen System-Ausfall kann es auch zu Datenverlusten kommen. Daher ist ein Datensicherungskonzept für Lotus Notes zu erstellen, das in das existierende Datensicherungskonzept integriert werden sollte (siehe auch Baustein B 1.4 *Datensicherungskonzept*). Hierin sollten alle Komponenten eines Lotus Notes Systems berücksichtigt sein, insbesondere auch die Clients.

Datensicherungskonzept

- Wichtige Datenbanken sollten durch das Anlegen von Replikaten auf mehrere Server verteilt werden, damit beim Ausfall einzelner Server auf die Replikate zugegriffen werden kann.

Replikation

- Notes bietet durch das sogenannte Clustering eine Möglichkeit, mehrere physikalische Server als einen virtuellen Server zu betreiben. Beim Ausfall eines Servers erfolgt ein automatisches "Failover" und die restlichen Server des Clusters übernehmen die Aufgaben des ausgefallenen Servers. Ob dies eine sinnvolle Option im Rahmen des Betriebskonzepts für Lotus Notes ist, muss im Einzelfall entschieden werden.

Clustering

- Für Notes-IDs bietet Lotus Notes einen Wiederherstellungsmechanismus an. Dieser kann auf zwei Arten verwendet werden: Einerseits kann die gesamte Notes-ID-Datei wiederhergestellt werden, wenn sie unbrauchbar oder gelöscht worden ist. Andererseits besteht die Möglichkeit, vergessene Notes-ID-Passwörter durch den Wiederherstellungsmechanismus für Passwörter zurückzusetzen. In diesem Fall muss der Benutzer von einem oder mehreren Administratoren sogenannte Wiederherstellungspasswörter anfordern und kann dann ein neues Notes-ID-Passwort vergeben.

Wiederherstellung von Notes-IDs

- Wichtige System-Notes-IDs (Root-Certifier, Certifier, Server, Administrator) sind immer in mindestens einer ausgelagerten Kopie zu verwahren (siehe M 4.129 *Sicherer Umgang mit Notes-ID-Dateien*).

Kopien wichtiger System-Notes-IDs vorhalten

- Die Systemkonfiguration ist zu dokumentieren. Wichtige Aufgaben müssen so beschrieben sein, dass sie im Notfall auch von technisch versierten Laien durchgeführt werden können.

Dokumentation muss notfalltauglich sein

- Es muss ein Wiederanlaufplan erstellt werden, der das geregelte Hochfahren des Systems gewährleistet. **Wiederanlaufplan**
- Die Notfallplanung muss die Besonderheiten wichtiger Notes-Server (z. B. einer Zertifizierungsstelle) in Betracht ziehen und darauf eingerichtet sein.
- Im Rahmen der Notfallvorsorge sollten auch unterschiedliche Szenarien von Kompromittierung (z. B. der Root-Certifier-ID) und entsprechende Reaktionen berücksichtigt werden.

Ergänzende Kontrollfragen:

- Existiert ein Notfallplan für den Ausfall des Lotus Notes-Systems?
- Existiert ein Datensicherungskonzept für Lotus Notes, das alle Komponenten beinhaltet?

M 6.74 Notfallarchiv

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, Leiter IT

Verantwortlich für Umsetzung: Leiter IT

Ein Notfallarchiv enthält diejenigen Sicherungsdaten, mit denen das Gesamtsystem in sich konsistent wiederhergestellt werden kann.

Aufbewahrung der gesicherten Daten in anderen Gefahrenbereichen

Keinesfalls darf dieser Datensicherungsbestand aus der gleichen Schadensursache heraus untergehen wie die Produktionsdaten. Er muss auch nach einem Katastrophen-Fall verfügbar bzw. zugänglich sein, d. h., der Zugriff auf die Backup-Datenträger und ihr Transport muss zeitlich in das Fenster passen, das als Rahmen für den Wiederanlauf planmäßig zur Verfügung steht. Die Unterbringung in einem Datenträgersafe oder einem Datenträgersicherheitsarchiv allein ist nicht ausreichend, da

- der Zugang beispielsweise durch Schutt verwehrt sein könnte,
- die vom Schaden betroffene Lokation durch die Feuerwehr oder ermittelnde Stellen für mehrere Tage gesperrt werden könnten oder
- ein Betreten schlichtweg nicht mehr möglich sein kann, beispielsweise aufgrund beeinträchtigter Statik.

Um diese Probleme zu lösen, sollten die Backup-Datenträger ausgelagert werden.

Hier kommen folgende Möglichkeiten in Betracht:

Datenträger ins Notfallarchiv transportieren

1. In einem anderen Bauteil (in der Regel zwei Brandabschnitte entfernt) oder in einem anderen Gebäude kann ein Notfallarchiv eingerichtet werden. Die Datenträger mit den Sicherungen müssen dann zeitnah dorthin transportiert werden. Die dort gelagerten Datensicherungen müssen außerdem gegen unberechtigten Zugriff und vor Sabotage geschützt werden. Je nach Risikolage muss auch an den Schutz vor Feuer, Brandgasen, Wasser und die Zerstörung durch Magnetfelder gedacht werden. Daher kommt eine Unterbringung in einem Datensafe einer geeigneten Klasse oder einem Datenträgersicherungsarchiv in Frage.

Datenbestände über Netze übermitteln

2. Es werden keine Datenträger zum Auslagerungsort transportiert, stattdessen wird die Datensicherung über Kommunikationsstrecken entweder in ein Roboterarchiv oder auf entfernt unterhaltene gespiegelte Plattenbestände übertragen. Für große Datenvolumina bieten sich hierzu Lichtwellenleiter an, die eine hohe Datenrate und lange Verbindungsstrecken erlauben. Um die Verfügbarkeit zusätzlich zu erhöhen, sollten bei dieser Lösung redundante Leitungswege in Betracht gezogen werden (siehe auch M 6.18 *Redundante Leitungsführung*).

Der Betrieb eines Notfallsarchivs kann auch von externen Dienstleistern übernommen werden, die sowohl den Datentransfer als auch die Datenspeicherung anbieten. Für den Notfall stellen diese Unternehmen auch bei Bedarf Hardware-Komponenten zur kurzfristigen Übernahme der Informationsverarbeitung zur Verfügung. Bei der Wahl externer Dienstleister müssen mit

diesen genaue Vereinbarungen und Regelungen über den Leistungsumfang und die zu beachteten Sicherheitsmaßnahmen getroffen werden (siehe M 5.87 *Vereinbarung über die Anbindung an Netze Dritter*).

Ergänzende Kontrollfragen:

- Wurde untersucht, ob ein Notfallarchiv erforderlich ist?
- Werden die Datensicherungsmedien in einem anderen Brandabschnitt als die IT-Systeme aufbewahrt?
- Ist es erforderlich, redundante Leitungswege zum Notfallarchiv vorrätig zu halten?

M 6.75 Redundante Kommunikationsverbindungen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement-Team

Verantwortlich für Umsetzung: Administrator

Je nach Anforderungen an die Verfügbarkeit kann der Ausfall oder das Nichtzustandekommen von Kommunikationsverbindungen zu erheblichen Beeinträchtigungen führen. Dies gilt sowohl für Telefon- wie LAN- oder WAN-Verbindungen. Die Fehlerquellen können dabei sehr vielfältig sein, so dass sich die Ursachenforschung oft als sehr schwierig erweist.

Da die typischen Arbeitsumgebung immer stärker vernetzt wird, kann der Ausfall von Kommunikationsverbindungen dazu führen, dass wichtige Daten und Informationen nicht ausgetauscht werden können. Dadurch werden unter Umständen Arbeitsabläufe unterbrochen, bis die Verbindung wieder zustande kommt oder bis Ausweichlösungen gefunden werden konnten.

Daher ist es sinnvoll, für die verschiedenen Kommunikationsverbindungen Ausweichlösungen bereitzuhalten (abhängig von deren Schutzbedarf).

Beispiele:

- Die telefonische Anbindung einer Einsatzzentrale sollte nicht nur über Festnetz, sondern auch über ein Mobiltelefon gewährleistet sein.
- Für die Anbindung des E-Mail-Servers an die Außenwelt sollte neben dem normalen Internet-Provider ein zweiter vorgesehen sein.
- Neben der E-Mail-Anbindung bzw. neben einem Faxserver sollte auch ein Faxgerät vorhanden sein, für den Fall, dass die Netzanbindung oder der Server ausfällt.

Dabei muss nicht immer ein weiterer Anschluss mit derselben Bandbreite und denselben Qualitätsanforderungen vorgehalten werden. In vielen Fällen reicht es, für den Notfall einen eingeschränkten IT-Betrieb aufrechterhalten zu können (siehe dazu auch Baustein B 1.3 *Notfallvorsorge-Konzept*).

Ergänzende Kontrollfragen:

- Gibt es Ausweichlösungen für wichtige Kommunikationsverbindungen?
- Werden die Ausweichlösungen regelmäßig der technischen Weiterentwicklung angepasst?

M 6.76 Erstellen eines Notfallplans für den Ausfall von Windows 2000/XP/2003-Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Notfalldokumente müssen vertraulich behandelt werden

Der Ausfall von einem oder mehreren Windows-Systemen kann bei entsprechender Serverrolle gravierende Auswirkungen auf die IT-Umgebung haben, da Benutzer nicht auf das Serversystem zugreifen können. Es ist festzulegen, welche Maßnahmen zu treffen sind, um eine Notfallsituation zu vermeiden, die Folgen des Ausfalls zu minimieren und den schnellen, erfolgreichen Wiederanlauf zu gewährleisten. Die bei einem Ausfall (des Servers) benötigten Dokumentationen und Handlungsanweisungen können schützenswerte Informationen enthalten. Sie sind sicher aufzubewahren, um dem Missbrauch der Informationen vorzubeugen. Schützenswerte Informationen können hier z. B.

- Konfigurationsdaten,
- Lizenzschlüssel, gegebenenfalls Volumenlizenz-Datenträger,
- (administrative) Benutzerkonten und Kennwörter

sein. Gleichzeitig muss organisatorisch gewährleistet werden, dass diese Informationen bei einem Ausfall den Personen zur Verfügung stehen, welche für die Wiederherstellung verantwortlich sind. Der Notfallplan für Windows-Systeme muss in das Notfallkonzept integriert werden (siehe B 1.3 *Notfallvorsorge-Konzept*) und mit der Maßnahme M 6.96 *Notfallvorsorge für einen Server* kompatibel sein.

Notfallplanung schon bei Systemplanung beginnen

Die Notfallplanung sollte bereits in die Planung der Systeme einbezogen werden, da bestimmte Verfügbarkeitsvorgaben, die beispielsweise redundante Server erforderlich machen, frühzeitig beachtet werden müssen (siehe M 6.1 *Erstellung einer Übersicht über Verfügbarkeitsanforderungen*). Im Notfallplan sollten eindeutige Kriterien niedergelegt sein, für welche Windows-Systeme der Notfallplan angewendet werden soll.

Datensicherung

Im Notfallplan für Windows-Systeme ist darauf hinzuweisen, dass die Umsetzung der Maßnahmen von B 1.4 *Datensicherungskonzept* für die Bewältigung eines Notfalls realisiert sein muss. Bei Windows-Server-2003-Systemen ist auf die Umsetzung der Maßnahme M 6.99 *Regelmäßige Sicherung wichtiger Systemkomponenten für Windows Server 2003* zu achten.

Dokumentation der Datensicherung

Die Dokumentation zur Datensicherung ist für den Notfallplan von besonderer Bedeutung. Die Aktualität sollte regelmäßig im Rahmen von Wartungsarbeiten überprüft werden. Insbesondere muss der Dokumentation zu entnehmen sein, welchen Umfang die Datensicherung hat, wann die letzte erfolgreiche Datensicherung erstellt wurde und welche Soft- und Hardware für die Datensicherung verwendet wurde. Das gewählte Datensicherungsverfahren und die dafür verwendete Hard- und Software muss den Anforderungen an eine Wiederherstellung innerhalb der geforderten Wiederherstellungszeit entsprechen.

Technische Dokumentation

Bei einem Ausfall muss eine angemessene technische Dokumentation der Systeme vorliegen. Sie sollte mindestens folgende Punkte beinhalten:

- BIOS- und Firmware-Versionen
- Hardwareausstattung
- installierte Windows-Komponenten
- installierte Zusatz-Software
- Netzkonfiguration (siehe *Eigenschaften* der LAN-Verbindungen, zu finden unter den Netzverbindungen in der Systemsteuerung)
- Dienste (siehe Dienstekonsole)
- Partitionierung der Festplatten oder des angeschlossenen Festplatten-Systems
- Benutzerkonten und Gruppen mit Berechtigungen
- Freigaben und Freigabeberechtigungen, NTFS Berechtigungen
- Einstellungen in den Sicherheitsrichtlinien (mittels Vorlagen)

Alle Dokumentationsunterlagen zur Erstellung des Notfallplans heranziehen

Grundsätzlich sollten im Rahmen der Notfallplanung alle Dokumentationsunterlagen berücksichtigt und gegebenenfalls vervollständigt werden, damit nicht im Notfall wichtige Funktionen vergessen werden. Die Dokumentation ist zum Beispiel bei Wartungsarbeiten und bei Veränderungen an Hard- und Software sowie der Systemkonfiguration anzupassen.

Alle Dokumentationsunterlagen offline bereitstellen

Die Aktualisierung der technischen Dokumentation und damit auch des Notfallplans ist Teil des Änderungsmanagements. Es sollte erkennbar sein, durch welche Person Änderungen durchgeführt wurden und wer die Dokumentation aktualisiert hat. Für den Notfallplan müssen alle Dokumentationen, auch Herstellerdokumentationen in gedruckter Form vorliegen, da der elektronische Zugriff im Notfall nicht gewährleistet werden kann.

Ausweichbetrieb

Können nur kurze Ausfallzeiten toleriert werden, so ist ein Ausweichbetrieb zu ermöglichen (siehe M 6.6 *Untersuchung interner und externer Ausweichmöglichkeiten*). Beim Ausfall eines einzelnen Systems sollte die Kapazitätsplanung für die Gesamtheit der Systeme so gestaltet sein, dass andere in Betrieb befindliche Systeme die Rollen und Funktionen des ausgefallenen Systems weitgehend übernehmen können. Hierbei ist M 4.276 *Planung des Einsatzes von Windows Server 2003* zu beachten.

Vorhaltung von Ersatzgeräten

Für Windows-Server sollte die Beschaffung von Ersatzgeräten überlegt werden, deren Ausstattung den Betrieb eines Windows-Servers inklusive einiger Anwendungen zulässt, falls mehrere Server ausfallen. Um die Umschaltzeit zu minimieren, sollten diese Geräte vorinstalliert und regelmäßig hochgefahren und gewartet werden.

konkrete Handlungsanweisungen für den Ausweichbetrieb

Die Entwicklung von Ausweichszenarien kann hohen Aufwand erzeugen. Es empfiehlt sich, Ausweichszenarien schon in der Planungsphase für den

Einsatz des Servers zu berücksichtigen. Es sollten konkrete Handlungsanweisungen für die Aufnahme des Ausweichbetriebs vorliegen.

Wiederanlaufplan

In Abhängigkeit von der Serverrolle und der IT-Umgebung ergeben sich nach einem Ausfall für das Wiederanlaufen bestimmte Anforderungen an Windows-Systeme. Hierbei sind neben dem betrachteten Server auch Anlaufzeiten der angebundenen IT-Umgebung zu beachten (z. B. Router, andere Server, Standortkonnektoren). Ein Anlaufplan ist mit zunehmender Größe des IT-Verbunds zunehmend komplex und muss individuell in Abhängigkeit von der Domänenstruktur und den verwendeten Serverrollen erstellt werden. Ein Mitgliedsserver sollte erst neu gestartet werden, nachdem mindestens ein Domänencontroller mit globalem Katalog, ein Zertifikatsserver zum Abrufen von Zertifikatssperrlisten (falls vorhanden) und alle Infrastrukturserver gestartet sind.

Test des Notfallplans

Im Rahmen des Wartungsplans sollte der Notfallplan regelmäßig (z. B. einmal pro Quartal) in einer Testumgebung getestet werden, aber auch gelegentlich in der Produktivumgebung, hierbei ist natürlich besondere Sorgfalt erforderlich. Je häufiger Konfigurationsänderungen zu erwarten sind, desto häufiger sollten Tests durchgeführt werden, um die Aktualität des Notfallplans sicherzustellen. Die Ergebnisse müssen dokumentiert werden und führen gegebenenfalls zu Änderungen am bestehenden Notfallplan. Grundsätzlich sind Wiederherstellungsszenarien zu proben und die Ergebnisse zu dokumentieren (siehe M 6.41 *Übungen zur Datenrekonstruktion*).

Wiederherstellung

Im Notfallplan sind die notwendigen Vorraussetzungen zur Wiederherstellung durch Neuinstallation festzuhalten. Das Bereitstellungskonzept oder vorhandene Installationskonzepte (im Falle eines Windows-Server-2003-Systems M 4.281 *Sichere Installation und Bereitstellung von Windows Server 2003*) sind zu berücksichtigen. Kritisch sind zum Beispiel einzusetzende Hardware und notwendige Treiber. Es kann bei bestimmten RAID-Controllern erforderlich werden, während der Installation Treiber zu installieren. In der Regel werden hierfür vom Hersteller Treiber auf einem Datenträger mitgeliefert oder im Internet auf den Herstellerseiten bereitgestellt. Eine aktuell verwendete Version dieses Treibers muss auf einem Datenträger vorliegen.

Installationsquellen und Lizenzen

Für die Wiederherstellung muss die Originalsoftware mit den Originaldatenträgern inklusive Produktschlüssel sowie Lizenzinformationen vorhanden sein. Falls kein Volumenlizenzprogramm verwendet wird, ist hinsichtlich der möglicherweise erforderlichen Aktivierung von Windows-Systemen darauf hinzuweisen, dass mehrfache Aktivierungen per Internet mit Hilfe desselben Produktschlüssels auf verschiedenen Festplatten fehlschlagen können. Infolgedessen kann der direkte telefonische Kontakt mit Microsoft erforderlich werden. Microsoft ist dann auf den Systemausfall hinzuweisen.

Bereitstellen von Replikaten

Durch das Anlegen von Replikaten wichtiger Informationen und Dateien auf mehreren Servern kann beim Ausfall einzelner Server auf diese Replikate

zugegriffen werden. Damit ist es möglich, Benutzern kurzfristig eine Kopie von Daten anzubieten. Im Rahmen der Notfallplanung sollte geprüft werden, ob und für welche Daten dies notwendig ist. Windows-Server bieten dazu den *File Replication Service* (FRS) an, der auch in Verbindung mit dem DFS (*Distributed File Service*) genutzt werden kann. In den Versionen vor Windows Server 2003 R2 sind diese Dienste jedoch nur eingeschränkt für ein Notfallkonzept geeignet und meist mit hohem Aufwand für Test und Wartung verbunden.

Die Notfallplanung ist im Hinblick auf bestimmte Rollen von Windows-Systemen, zum Beispiel DNS-Server und Zertifikatsserver, zu differenzieren, um die vollständige Wiederherstellung gewährleisten zu können. Dazu gehört die Sicherung von rollenspezifischen Systemkomponenten (z. B. Datenbanken des DNS-Dienstes oder der Zertifizierungsstelle) sowie eine umfassende Dokumentation der mit den betreffenden Rollen verbundenen Einstellungen.

Ergänzende Kontrollfragen:

- Existiert ein Notfallplan für Windows-Systeme?
- Ist der Notfallplan konform zur Maßnahme M 6.96 *Notfallvorsorge für einen Server*?
- Ist eine umfassende Systemdokumentation vorhanden?
- Werden Wiederanlauf- und Wiederherstellungsvorgänge regelmäßig getestet?

M 6.77 Erstellung von Rettungsdisketten für Windows 2000

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: Administrator

Für jedes unter Windows 2000 betriebene System, das über ein Diskettenlaufwerk verfügt, sollte eine Notfalldiskette erstellt werden, mit der sich der auf der Diskette gespeicherte Status wiederherstellen lässt, wenn Dateien beschädigt werden. Für jeden Rechner muss eine eigene Notfalldiskette erstellt werden, da diese Disketten nicht zwischen verschiedenen Rechnern ausgetauscht werden können.

Während des Windows Setup wird der Benutzer gefragt, ob er eine Notfalldiskette erstellen will. Zur Erstellung der Notfalldiskette muss eine leere 3,5-Zoll-Diskette auf Anforderung in Laufwerk A: eingelegt werden, auf der dann die zur Reparatur des Systems benötigten Informationen gespeichert werden.

Sofern bei der Installation keine Notfalldiskette erstellt wurde, kann diese auch nachträglich mit dem Dienstprogramm *NTBACKUP* erzeugt werden. Dieses befindet sich im Windows-Systemverzeichnis *%SystemRoot%\SYSTEM32*, z. B. *\WINNT\SYSTEM32*, und kann auch über das Start-Menü unter *Start/Programme/Zubehör/Systemprogramme/Sicherung* gestartet werden. Unter der Registerkarte *Willkommen* befindet sich die Schaltfläche *Notfalldiskette*, mit der die Erstellung angestoßen wird.

aktueller Systemzustand

Hinweis: Dieser Prozess sollte nach jeder Veränderung der Systemkonfiguration wiederholt werden, damit die Notfalldiskette stets den aktuellen Systemzustand widerspiegelt. Die Erstellung der Notfalldiskette sollte nach dem nächsten erfolgreichen Systemstart durchgeführt werden, um sicherzustellen, dass eine lauffähige Systemversion gesichert wird.

Ergänzende Kontrollfragen:

- Sind die Informationen auf der Notfalldiskette aktuell?
- Werden die Reparaturdisketten unter Verschluss gehalten, um eventuellen Missbrauch zu vermeiden?
- Ist für jedes Windows 2000 System eine Notfalldiskette erstellt worden?

M 6.78 Datensicherung unter Windows 2000/XP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Unter Windows 2000/XP kann die Datensicherung mit dem zum System gehörigen Dienstprogramm *NTBACKUP.EXE* durchgeführt werden, wobei zu beachten ist, dass dieses Programm nicht in der Lage ist, die Sicherungsmedien generell zu verschlüsseln, so dass diese geschützt aufbewahrt werden müssen. Über EFS verschlüsselte Dateien werden jedoch verschlüsselt gesichert. Im Unterschied zur in Windows NT mitausgelieferten Version unterstützt das Backup-Programm auch die Sicherung der Daten in eine Datei, so dass damit z. B. lokale Dateien auf einen Server gesichert werden können, von wo aus sie dann durch die Serversicherung auf ein Backup-Medium geschrieben werden.

Bei der Durchführung der Datensicherung sind die folgenden Punkte zu beachten:

wichtige Systemdateien sichern

- Die Sicherungssoftware ist in der Lage, wichtige Systemdateien, wie die Registrierung des lokalen Rechners, die COM+ Registrierungen sowie die Startdateien, zu sichern. Dies sollte in regelmäßigen Abständen und nach größeren Änderungen der Konfiguration durchgeführt werden. Dazu sind unter der Option *Systemstatus* die jeweiligen Auswahlboxen zu aktivieren.
- Auf Domänen-Controllern können zusätzlich auch die Active Directory Daten sowie die Daten des SYSVOL-Ordners gesichert werden. Dies sollte bei jedem Backup durchgeführt werden. Die relevanten Optionen sind auf Domänen-Controllern ebenfalls unter der Option *Systemstatus* zu finden.

Protokolldatei anlegen

- Bei der Durchführung der Sicherung sollte unbedingt eine Protokolldatei angelegt werden. Nach Abschluss der Operation ist die Protokolldatei daraufhin zu überprüfen, ob alle zu sichernden Daten auch tatsächlich gesichert werden konnten oder ob während der Sicherung Fehler aufgetreten sind. Dabei ist es empfehlenswert, die Option *Details* unter *Extras/Optionen/Sicherungsprotokoll* zu aktivieren, da damit auch festgestellt werden kann, ob alle zu sichernden Daten gesichert wurden und ob überhaupt die Verzeichnisse in die Datensicherung einbezogen wurden, die gesichert werden sollten.

Zugriffsschutz wiederherstellen

- Bei der Wiederherstellung gesicherter Dateien kann deren Zugriffsschutz wiederhergestellt werden, sofern dies in den Eigenschaften des Wiederherstellungsauftrages (Schaltfläche *Wiederherstellung starten/ Erweitert*) spezifiziert wurde. Standardmäßig ist diese Option aktiviert. Dabei kann dies nur für Daten erfolgen, die von einem Windows NTFS-Dateisystem stammen.
- Die Auswahl der zu sichernden Dateien und Verzeichnisse kann, im Gegensatz zur Windows NT Version des Programms, in einer Datei gespeichert werden, die später wieder geladen werden kann. Durch diesen Mechanismus ist es auch möglich, mehrere Sicherungsvarianten zu erzeugen, durch die unterschiedliche Daten erfasst werden.

- Sicherungen sollten in regelmäßigen Abständen durchgeführt werden. Mit dem Backup-Programm von Windows 2000/XP ist es möglich,

  Sicherungsaufträge für bestimmte Zeiten zu planen. Damit kann die Sicherung auch automatisiert erfolgen.

Soll für umfangreichere Installationen bzw. bei hohen Verfügbarkeitsanforderungen zusätzliche Software zur Durchführung von Datensicherungen eingesetzt werden, so ist bei der Auswahl derartiger Sicherungssoftware darauf zu achten, dass sie die folgenden Anforderungen erfüllt:

- Die eingesetzten Dateisysteme, also FAT, NTFS und ggf. auch HPFS, sollten bei der Sicherung und Wiederherstellung unterstützt werden.
- Es muss möglich sein, auch Active Directory Daten sowie die Daten des SYSVOL-Ordners zu sichern.
- **automatische Rückmeldung**

  Es sollte möglich sein, Sicherungen automatisch zu vorwählbaren Zeiten bzw. in einstellbaren Intervallen durchführen zu lassen, ohne dass hierzu manuelle Eingriffe (außer dem eventuell notwendigen Bereitstellen von Sicherungsdatenträgern) erforderlich wären.
- Es sollte möglich sein, einen oder mehrere ausgewählte Benutzer automatisch über das Sicherungsergebnis und eventuelle Fehlermeldungen per E-Mail oder ähnliche Mechanismen zu informieren.
- Die Sicherungssoftware sollte den Schutz des Backup-Mediums durch ein Passwort oder noch besser durch Verschlüsselung unterstützen. Weiterhin sollte sie in der Lage sein, die gesicherten Daten in komprimierter Form abzuspeichern.
- **Include- und Exclude-Listen**

  Durch Vorgabe geeigneter Include- und Exclude-Listen bei der Datei- und Verzeichnisauswahl sollte genau spezifiziert werden können, welche Daten zu sichern sind und welche nicht. Es sollte möglich sein, diese Listen zu Sicherungsprofilen zusammenzufassen, abzuspeichern und für spätere Sicherungsläufe wieder zu benutzen.
- Es sollte möglich sein, die zu sichernden Daten in Abhängigkeit vom Datum ihrer Erstellung bzw. ihrer letzten Modifikation auszuwählen.
- **automatischer Vergleich**

  Die Sicherungssoftware sollte die Erzeugung logischer und physischer Vollkopien sowie inkrementeller Kopien (Änderungssicherungen) unterstützen.
- Die Sicherung sollte auch auf Festplatten und Netzlaufwerken erfolgen können.
- Die Sicherungssoftware sollte in der Lage sein, nach der Sicherung einen automatischen Vergleich der gesicherten Daten mit dem Original durchzuführen und nach der Wiederherstellung von Daten einen entsprechenden Vergleich zwischen den rekonstruierten Daten und dem Inhalt des Sicherungsdatenträgers durchzuführen.

- Bei der Wiederherstellung von Dateien sollte ausgewählt werden können, ob die Dateien am ursprünglichen Ort oder auf einer anderen Platte bzw. in einem anderen Verzeichnis wiederhergestellt werden. Ebenso sollte es möglich sein, das Verhalten der Software für den Fall zu steuern, dass am Zielort schon eine Datei gleichen Namens vorhanden ist. Dabei sollte einstellbar sein, ob diese Datei immer, nie oder nur in dem Fall überschrieben wird, dass sie älter als die zu rekonstruierende Datei ist, oder dass in diesem Fall eine explizite Anfrage erfolgt.

Zusätzlich zur Durchführung der normalen Datensicherungen ist es unter Windows 2000 empfehlenswert, die aktuelle Systemkonfiguration nach jeder größeren Änderung auf eine Notfalldiskette zu sichern, um sie bei eventuellen Inkonsistenzen wiederherstellen zu können (siehe auch M 6.77 *Erstellung von Rettungsdisketten für Windows 2000*).

Die Systemwiederherstellung wurde in Windows XP eingeführt und stellt eine neue Funktionalität dar, die das Wiederherstellen von alten Systemzuständen möglich macht. Die Systemwiederherstellung erstellt einen Zustandsschnappschuss wichtiger Systemdateien und einiger Programm-dateien. Dieser bildet einen Wiederherstellungspunkt, auf welchen das System später zurückgesetzt werden kann. Der Einsatz der automatischen Systemwiederherstellung kann in Abhängigkeit von lokalen Umständen und insbesondere von der implementierten Softwareverteilungs-Strategie vorteilhaft sein.

Ergänzende Kontrollfragen:

- Wird der Datensicherungsvorgang dokumentiert?
- Ist der Datensicherungsvorgang konform zum vorhandenen Datensicherungskonzept?

M 6.79 Datensicherung beim Einsatz von Internet-PCs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Internet-PCs können in unterschiedlichen Einsatzszenarien verwendet werden. Einerseits können Internet-PCs als Ergänzung zu anderen Zugriffsmöglichkeiten auf das Internet installiert werden, z. B. wenn am Arbeitsplatz-PC zwar ein Internet-Zugang vorhanden ist, aus Sicherheitsgründen jedoch keine aktiven Inhalte wie JavaScript ausgeführt werden dürfen. Andererseits stellen Internet-PCs in vielen Fällen die einzige Möglichkeit dar, das World Wide Web, E-Mail oder andere Internet-Dienste zu nutzen.

Erhöhung der Verfügbarkeit

Aus diesen Einsatzszenarien ergeben sich auch unterschiedliche Anforderungen an die Verfügbarkeit von Internet-PCs. Hohen oder sehr hohen Verfügbarkeitsanforderungen kann unter anderem durch redundante Auslegung des Internet-PCs und der Internet-Anbindung Rechnung getragen werden. Um bei einem Ausfall des Internet-PCs, z. B. durch technisches Versagen oder durch einen erfolgreichen Angriff, das System zeitnah wiederherstellen zu können, sollte auf jeden Fall ein Konzept für die Datensicherung erstellt werden. Dabei muss unterschieden werden zwischen den System-, Programm- und Konfigurationsdateien einerseits und den Anwendungsdaten andererseits.

Backup der System-, Programm- und Konfigurationsdateien

Image als Grundlage der Datensicherung

Um den Internet-PC nach einem Ausfall möglichst schnell wiederherstellen zu können, sollte nach der Installation aller benötigten Betriebssystem- und Software-Komponenten und anschließender Konfiguration ein Abbild ("Image") des Systems gespeichert werden.

Hierzu werden entweder alle System-, Programm- und Konfigurationsdateien mit Hilfe eines Backup-Programms gesichert, oder es wird ein spezielles Tool eingesetzt, das den gesamten Inhalt der Festplatte Byte für Byte abspeichert. Im letztgenannten Fall sollten sich währenddessen keine Anwendungsdaten auf der Festplatte befinden.

Es wird empfohlen, ein Image des Systems zu sichern,

- erstmalig, sobald die Installation und Konfiguration des Internet-PCs abgeschlossen ist,
- jedes Mal, wenn Betriebssystem- oder Software-Komponenten installiert, entfernt oder aktualisiert wurden, beispielsweise durch die Installation von Patches,
- jedes Mal, wenn wesentliche oder sicherheitsrelevante Änderungen an der Konfiguration vorgenommen wurden.

Dadurch wird vermieden, dass nach einem Ausfall des Internet-PCs alle Software-Komponenten einzeln installiert und konfiguriert werden müssen. Stattdessen kann das System als Ganzes wiederhergestellt werden.

Backup der Anwendungsdaten

Wenn das Nutzungskonzept eine lokale Datenhaltung vorsieht, müssen außer dem System auch die Anwendungsdaten *regelmäßig* gesichert werden.

Verzeichnisse festlegen

Hierzu wird empfohlen, auf dem Internet-PC ein oder mehrere Verzeichnisse festzulegen, in denen Anwendungsdateien gespeichert werden dürfen. Der Inhalt dieser Verzeichnisse wird in das Backup einbezogen. Die Benutzer müssen darüber unterrichtet werden, welche Verzeichnisse gesichert werden, und wie sie Dateien dort abspeichern können.

Die zu sichernden Anwendungsdaten können u. U. schnell anwachsen. Im Datensicherungskonzept ist daher auch festzulegen, welche Volumenbeschränkungen es für das Backup gibt und wie bei Überschreitung vorzugehen ist.

Datensicherungskonzept

Die Vorgehensweise zur Datensicherung sollte in einem Konzept dokumentiert werden. Das Konzept sollte mindestens folgende Punkte umfassen:

- Umfang der Datensicherung (Verzeichnisse, Partitionen, usw.),
- Häufigkeit und Zeitpunkt der Datensicherung,
- Datensicherungsmedium,
- Verantwortlichkeit für die Datensicherung und
- Aufbewahrungsort der Backup-Datenträger.

Benutzer informieren

Das Datensicherungskonzept muss allen Benutzern des Internet-PCs zur Kenntnis gegeben werden. Weitere Empfehlungen zur Entwicklung eines Datensicherungskonzepts finden sich in Maßnahme M 6.33 *Entwicklung eines Datensicherungskonzepts*.

Beispiele:

- Szenario 1:

  Der Internet-PC wird in einem Unternehmen als Zusatzangebot zur Verfügung gestellt, da beim Surfen über das Hausnetz keine aktiven Inhalte ausgeführt werden dürfen. Das System wird mit Hilfe eines Image wöchentlich neu installiert. Die Benutzer sind darüber informiert, dass sie Anwendungsdaten auf dem Internet-PC selbst sichern müssen, wenn sie diese weiter benötigen.

- Szenario 2:

  Das Hausnetz in einem Unternehmen ist nicht an das Internet angeschlossen. Es werden daher mehrere Internet-PCs für die Nutzung von E-Mail installiert und untereinander vernetzt. Ein- und ausgehende E-Mails werden täglich über einen CD-Writer gesichert, der in einen der Internet-PCs eingebaut ist. Ein Administrator und ein Vertreter sind dafür verantwortlich, entsprechende CD-R- bzw. CD-RW-Medien einzulegen und die Datensicherung zu starten.

Ergänzende Kontrollfragen:

- Wurde ein Konzept für die Datensicherung für den Internet-PC erstellt?
- Berücksichtigt das Datensicherungskonzept evtl. lokal abgespeicherte Anwendungsdaten?
- Ist das Datensicherungskonzept allen Benutzern bekannt?

M 6.80 Erstellen eines Notfallplans für den Ausfall eines Novell eDirectory Verzeichnisdienstes

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Der teilweise oder komplette Ausfall eines eDirectory-Verzeichnisdienstes hat in der Regel gravierende Auswirkungen auf die Arbeitsmöglichkeiten von Benutzern, da je nach Schadensfall alle Server-basierten Aktionen nicht mehr ausgeführt werden können. Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind.

Folgende Aspekte müssen dabei berücksichtigt werden:

- Die Notfallplanung für das eDirectory-System muss in den existierenden Notfallplan integriert werden (siehe auch Baustein B 1.3 *Notfallvorsorge-Konzept*).
- Durch einen Systemausfall kann es auch zu Datenverlusten kommen. Daher ist ein Konzept für die Datensicherung der eDirectory-Verzeichnisdatenbank zu erstellen, das in das bisherige Backup-Konzept integriert werden kann oder dieses ablöst. Weitere Hinweise hierzu finden sich in Baustein 3.4 Datensicherungskonzept sowie in Maßnahme M 6.81 *Erstellen von Datensicherungen für Novell eDirectory*.
- Werden von wichtigen Informationen und Dateien Replikate auf mehreren Servern angelegt, so kann beim Ausfall einzelner Server auf diese Replikate zugegriffen werden. eDirectory bietet dazu einen eigenen Replikationsmechanismus an. Damit ist es möglich, Benutzern eine jeweils räumlich nahe Replik von Daten zur Verfügung zu stellen, umso gute Zugriffszeiten und eine hohe Verfügbarkeit der Server zu erreichen (siehe M 2.237 *Planung der Partitionierung und Replikation im Novell eDirectory*).
- eDirectory bietet die Möglichkeit, die Verzeichnisdatenbank auf mehrere eDirectory-Server zu verteilen (partitionieren), so dass jeder Server nur einen Teil der Daten hält. Bei Ausfall eines eDirectory-Servers ist somit nur die dort gespeicherte Partition des Verzeichnisses betroffen (siehe M 2.237 *Planung der Partitionierung und Replikation im Novell eDirectory*). Bei der Erstellung eines Notfallplans muss darauf geachtet werden, dass alle Partitionen einer eDirectory-Installation berücksichtigt werden.

Partitionierung der Verzeichnisdatenbank

- Die gesamte Systemkonfiguration ist zu dokumentieren. Alle Aufgaben zur Wiederherstellung des Systems müssen so beschrieben werden, dass sie im Notfall auch von Personal durchgeführt werden können, das keine detaillierten Kenntnisse der vorher vorhandenen Systemkonfiguration hat.

Sorgfältige Dokumentation der Systemkonfiguration

- Durch die Notfallplanung muss sichergestellt sein, dass im Notfall entsprechend geschultes Personal zur Verfügung steht.
- Es muss ein Wiederanlaufplan erstellt werden, der das geregelte Hochfahren des Systems gewährleistet.

- Die Notfallplanung muss die Besonderheiten wichtiger eDirectory-Server in Betracht ziehen und darauf eingerichtet sein.

Notfälle nicht nur planen, sondern auch üben!

Im Rahmen der Notfallvorsorge sollten auch unterschiedliche Szenarien betrachtet werden, bei denen das eDirectory-System oder Teile davon kompromittiert werden. Für diese Szenarien sollte im Notfallplan möglichst präzise beschrieben werden, wie jeweils zu reagieren ist und welche Aktionen auszuführen sind. Die Reaktionen sollten regelmäßig geübt werden.

Die rechtzeitige Notfallplanung mit vorgegebenen Handlungsanweisungen, die auch durch Personen durchgeführt werden können, die nicht mit der Systemadministration vertraut sind, kann im Schadensfall die Auswirkungen abmildern. Es ist zu beachten, dass die entsprechenden Dokumente für die Notfallsituation wichtige und schützenswerte Informationen beinhalten, so dass diese geschützt aufbewahrt werden müssen. Trotzdem müssen die berechtigten Personen im Notfall darauf zugreifen können.

Ergänzende Kontrollfragen:

- Wurde eine bedarfsgerechte Notfallplanung durchgeführt?
- Liegen Notfallpläne für den Ausfall wichtiger Systeme vor?
- Wurden alle Notfallprozeduren dokumentiert?
- Ist das Notfallkonzept mit dem Datensicherungskonzept abgestimmt?

M 6.81 Erstellen von Datensicherungen für Novell eDirectory

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Die Datensicherung eines eDirectory-Verzeichnisdienstes sollte zusammen mit einem generellen Server-Backup vorgenommen werden, damit später der Gesamtzustand der Server wiederhergestellt werden kann. Somit hängt der Backup-Prozess auch von dem unterliegenden Betriebssystem ab.

Um konsistente Datensicherungen des eDirectory-Datenbestandes auf einem Server zu erhalten, sollte ein spezielles Backup-Werkzeug verwendet werden. Folgende Werkzeuge hält eDirectory für die Datensicherung bereit:

- unter Netware: *SBCON.NLM*
- unter Windows NT/2000: *SMSENGN.EXE*
- unter Linux, Sun Solaris: *ndsbackup utility*

Neben einer Vollsicherung des Verzeichnisses bieten die Novell-Werkzeuge auch die Möglichkeit, nur Teile des eDirectory zu sichern. Um einzelne eDirectory-Objekte zu archivieren oder wiederherzustellen, muss der vollständige *distinguished name* des Objektes spezifiziert werden. Um den gesamten Baum zu sichern, muss das jeweilige *Tree*-Objekt angegeben werden. Es kann auch gesondert das Schema gesichert werden, hierzu muss das *Schema*-Objekt selektiert werden. Schließlich können auch Teile eines eDirectory-Baums gesichert werden, hierzu muss der entsprechende Container des Baumes ausgewählt werden. Es werden dann sämtliche Objekte unterhalb dieses Containers gesichert.

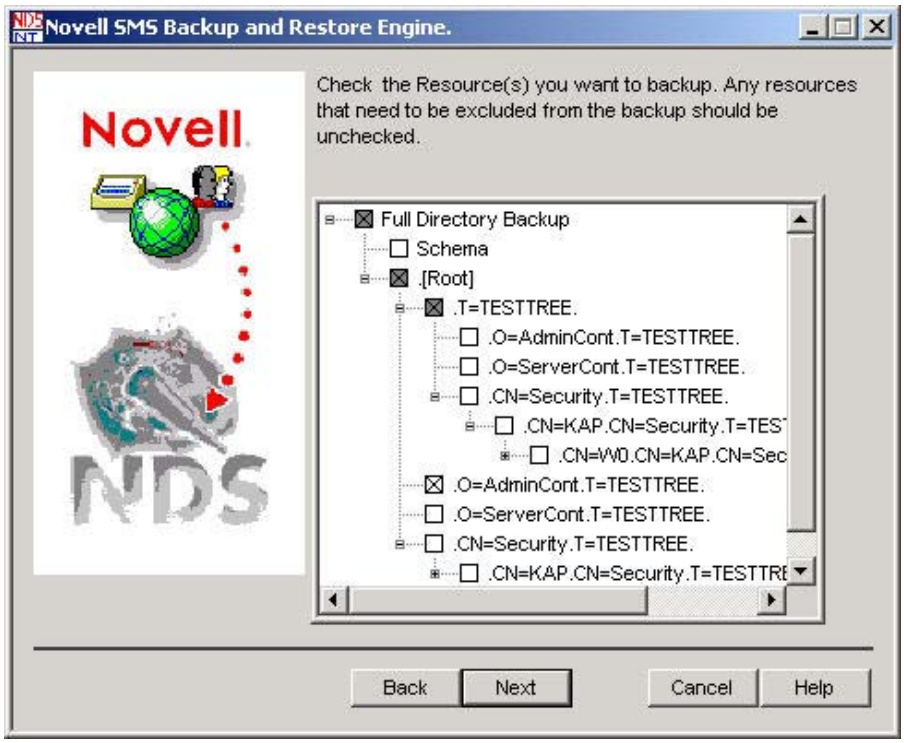


Abbildung: Novell SMS Backup and Restore Engine

Partitionsinformationen können mit diesen Backup-Werkzeugen nicht gesichert werden. Im Wiederherstellungsfall müssen die entsprechenden Teile dann nachträglich partitioniert werden. Zu diesem Zweck sollten unbedingt gedruckte Kopien der Baumstruktur und der Partitionen angefertigt und regelmäßig aktualisiert werden.

Dokumentation auch ausdrucken!

Der Backup-Prozess der eDirectory-Utilities kann an die Bedürfnisse der Benutzer angepasst werden. Insbesondere können mittels der Option *Exclude/Include* spezielle eDirectory-Objekte aus der Datensicherung ausgenommen bzw. darin einbezogen werden.

Sicherungskopien sollten in der Regel einmal wöchentlich oder öfter angelegt werden. Dies richtet sich danach, wie häufig sich wichtige Verzeichnisinformationen ändern. Der Backup-Prozess sollte stets nachvollziehbar protokolliert werden, und anhand des Protokolls sollte nachgeprüft werden, ob tatsächlich sämtliche Daten fehlerfrei gesichert wurden.

Datensicherung protokollieren

Backup unter Netware

Teil des Netware-Betriebssystems ist *SBCON.NLM*, eine so genannte *Storage Management Engine* (SME). Sie stellt das Back-End dar, welches die Backup/Restore-Requests umsetzt. Vor der Nutzung von *SBCON.NLM* muss zuerst jedoch *QMAN.NLM* geladen werden, damit die von *SBCON.NLM* erzeugten Backup/Restore-Jobs verarbeitet werden können.

Alternativ dazu kann auch mit SMS-kompatiblen Backup/Restore-Utilities gearbeitet werden. Der *Storage Management Data Requester* (SMDR) kommuniziert zwischen der SME und der *Target Service Agent* (TSA)-Software. Das erste Mal, wenn *SMDR.NLM* geladen wird, wird der Benutzer nach diversen Konfigurationsoptionen gefragt, unter anderem, ob ein SMDR-Objekt im eDirectory-Verzeichnisbaum angelegt werden soll.

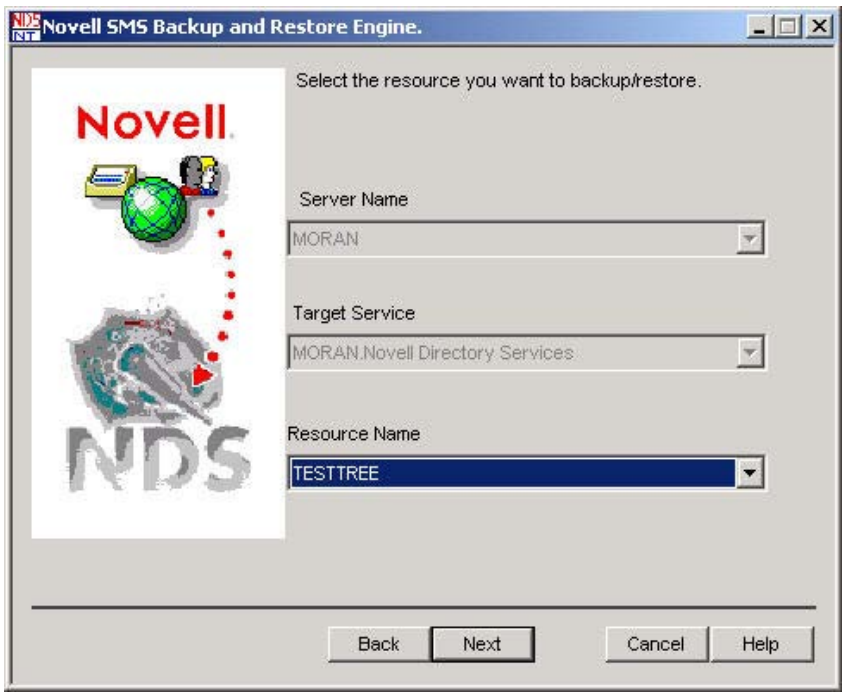


Abbildung: Ressource Name

Die SME und der TSA können sich auf dem selben oder auf verschiedenen Computern befinden. Im verteilten Fall muss auf beiden Seiten SMDR installiert sein. Die *Target Service Agents for NDS* (TSANDS) reichen die Requests zwischen dem SMDR und der eDirectory-Datenbank weiter.

Backup unter Windows NT/2000

Von Novell wird für die Datensicherung unter Windows NT/2000 die Applikation *SMSENGN.EXE* zur Verfügung gestellt. *SMSENGN.EXE* erzeugt für Daten und Index jeweils eine Datei (*.DAT* beziehungsweise*.IDX*).

Alternativ kann auch hier ein SMS-kompatibles Backup/Restore-Werkzeug verwendet werden. Die oben beschriebenen Komponenten SMDR, TSA und TSANDS kommen dann analog zum Einsatz. Hierbei sind SMDR und TSANDS standardmäßig als NT-Services verfügbar. Sofern diese nicht aktiviert sind, können sie explizit mittels *W32MDR.EXE* unter dem NDS\SMS-Verzeichnis gestartet werden.

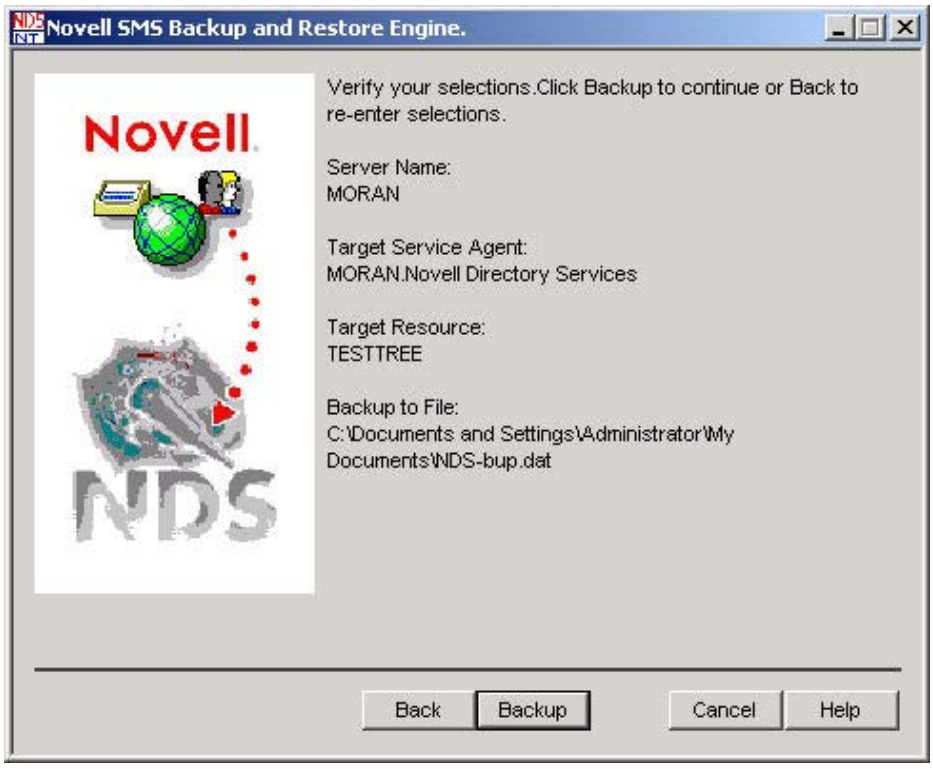


Abbildung: Verify Backup Einstellungen

Backup unter Linux und Sun Solaris

Unter Linux und Sun Solaris gibt es für die Datensicherung das Werkzeug *ndsbackup*. Dieses wird über die Kommandozeile gestartet und erlaubt es, eDirectory-Objekte in einer einzelnen Datei *ndsbackupfile* zu speichern. Um eDirectory-Objekte zu sichern, muss deren *full distinguished name* (FDN) spezifiziert werden. Um den gesamten Baum zu speichern, muss das entsprechende Baum-Objekt ausgewählt werden.

Auf der Kommandozeile akzeptiert das Tool eine Reihe von Funktionsbuchstaben, z. B. *c* für *create*, *r* für *restore*, etc., sowie einen Satz von Parametern. Einzelheiten sind dem Administrationshandbuch zu entnehmen.

Ergänzende Kontrollfragen:

- Ist die Partitionierung des eDirectory schriftlich dokumentiert, so dass sie nach einem Systemausfall manuell wieder rekonstruiert werden kann?
- Wird der Datensicherungsvorgang dokumentiert?
- Ist der Datensicherungsvorgang konform zum vorhandenen Datensicherungskonzept?

M 6.82 Erstellen eines Notfallplans für den Ausfall von Exchange-Systemen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der teilweise oder komplette Ausfall eines Exchange-Systems hat in vielen Fällen gravierende Auswirkungen auf die Arbeitsmöglichkeiten der E-Mail-Benutzer, da alle Server-basierten Aktionen nicht mehr ausgeführt werden können. Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten bei einem Ausfall durchzuführen sind.

Die Notfallplanung für das Exchange-System muss den existierenden Notfallplan der Organisation berücksichtigen (siehe auch Baustein B 1.3 *Notfallvorsorge-Konzept*). Außerdem muss sich die Notfallplanung für Exchange 2000 dabei auch in die Notfallplanung des jeweiligen Windows 2000 Netzes (siehe M 6.76 *Erstellen eines Notfallplans für den Ausfall eines Windows 2000/XP Netzes*) integrieren.

Systemkonfiguration dokumentieren

Die Systemkonfiguration ist zu dokumentieren. Dazu gehört die Beschreibung der Festplattenpartitionen und deren Verwendungszwecke (System, Transaktionsprotokoll, Datenbank etc.) sowie die Dokumentation der Hardware und des Betriebssystems. Wichtige Aufgaben müssen so beschrieben sein, dass sie im Notfall direkt von entsprechend geschultem Personal durchgeführt werden können. Der notwendige Detailgrad der Dokumentation richtet sich hierbei nach den Kenntnissen des Personals, das im Notfall zur Verfügung steht. Ist z. B. eine mehrköpfige Gruppe von geschulten Exchange-Administratoren in der Organisation beschäftigt, so können entsprechende Kenntnisse in der Notfalldokumentation vorausgesetzt werden. Ist dagegen nur ein einzelner geschulter Exchange-Administrator in der Organisation tätig, so sollte die Notfalldokumentation wichtige Maßnahmen so beschreiben, dass sie auch von technisch versierten Laien durchgeführt werden können.

Die Notfallplanung muss neben Exchange/Outlook 2000 auch die Besonderheiten anderer wichtiger Windows 2000 Server, z. B. einer Zertifizierungsstelle, in Betracht ziehen und darauf eingerichtet sein.

Datensicherungskonzept erstellen

Durch einen Systemausfall kann es auch zu Datenverlusten kommen. Daher ist ein Datensicherungskonzept für Exchange 2000 zu erstellen, das in das existierende Datensicherungskonzept integriert werden sollte (siehe auch Baustein B 1.4 *Datensicherungskonzept*). Hierbei sollten nicht nur Exchange-Server, sondern auch Exchange-Clients berücksichtigt sein, insbesondere also die Outlook 2000 Clients. Weitere Informationen zum Thema Datensicherung finden sich in M 4.166 *Sicherer Betrieb von Exchange/Outlook 2000*.

Wiederanlaufplan erstellen

Es muss ein Wiederanlaufplan erstellt werden, der das geregelte Hochfahren des Systems nach einem Ausfall gewährleistet. Dazu kann auch das Setup-Programm von Exchange 2000 Server im *Disaster-Recovery-Modus* verwendet werden.

Im Rahmen der Notfallvorsorge sollten unterschiedliche Kompromittierungsszenarien berücksichtigt und spezifische Handlungsanweisungen für den Fall

der Kompromittierung der Server, einzelner Dienste oder einzelner Benutzerkonten gegeben werden.

Notfallübungen durchführen

Die regelmäßige Durchführung von Notfallübungen zur Systemwiederherstellung wird dringend empfohlen. Die Notfallübungen sollten alle Aspekte eines Systemausfalls bzw. einer Kompromittierung berücksichtigen. Die Verantwortlichen sollten in einer speziellen Testumgebung vor allem die Wiederherstellung von Daten, das Reparieren einzelner Dienste oder ihre Neukonfiguration (z. B. nach einer Kompromittierung) üben. Das Testsystem sollte dem Produktivsystem so ähnlich wie möglich sein.

In einigen Fällen sind für die Wiederherstellung von Daten oder für die Reparatur eines Systems sensitive Zugangsinformationen, wie z. B. kryptographische Schlüssel oder Kennwörter, notwendig. Es ist darauf zu achten, dass der Notfallplan eine Vorgehensweise für solche Fälle definiert. Weiterhin ist durch die Datensicherung oder andere Maßnahmen zu gewährleisten, dass diese Informationen bei einem Notfall verfügbar sind.

Ergänzende Kontrollfragen:

- Existiert ein Notfallplan für das Exchange-System?
- Existiert ein Datensicherungskonzept für Exchange/Outlook 2000, das alle relevanten Komponenten berücksichtigt?
- Finden regelmäßig Notfallübungen statt?

M 6.83 Notfallvorsorge beim Outsourcing

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung: IT-Sicherheitsmanagement, Leiter IT, Administrator

Für die Notfallvorsorge beim Outsourcing gelten grundsätzlich die gleichen Anforderungen wie beim nicht ausgelagerten Betrieb von IT-Systemen. Die Besonderheiten beim Outsourcing-Betrieb ergeben sich dadurch, dass auch die Notfallvorsorge auf unterschiedliche Parteien aufgeteilt ist und durch die Verteilung der IT-Komponenten auch zusätzliche Komponenten neu hinzukommen.

Verteilung der Notfallvorsorgekonzepte

Generell müssen Notfallvorsorgekonzepte für die Systeme beim Auftraggeber, beim Outsourcing-Dienstleister sowie für die Schnittstellen zwischen Auftraggeber und Dienstleister (z. B. Netzverbindung, Router, Telekommunikationsprovider) existieren. In M 2.253 *Vertragsgestaltung mit dem Outsourcing-Dienstleister* sind einige Hinweise gegeben, welche Aspekte bereits im Service Level Agreement geregelt werden sollten. Im Notfallvorsorgekonzept müssen diese Vorgaben genau spezifiziert und im Detail beschrieben werden:

Detailregelungen

- Zuständigkeiten, Ansprechpartnern und Abläufe müssen klar geregelt und vollständig dokumentiert werden.
- Detailregelungen für die Datensicherung sind zu erstellen (z. B. getrennte Backup-Medien für jeden Klienten, Verfügbarkeit, Vertretungsregelungen, Eskalationsstrategien, Virenschutz).
- Detaillierte Arbeitsanweisungen mit konkreten Anordnungen für bestimmte Fehlersituationen sind zu erstellen.
- Ein Konzept für Notfallübungen, die regelmäßig durchgeführt werden müssen, muss erarbeitet werden.

Bedeutung von Arbeitsanweisungen

Die IT-Sicherheit hängt in Notfällen entscheidend von der Qualität der Arbeitsanweisungen für das Personal des Outsourcing-Dienstleisters ab. Oftmals werden die Systeme des Auftraggebers von Personal des Dienstleisters betrieben, das keine Detailkenntnisse über die Anwendungen besitzt, die auf den IT-Systemen betrieben werden. Die Verantwortung für die Anwendung liegt dennoch ausschließlich beim Auftraggeber. Tritt ein Fehler in der Anwendung auf, muss der Outsourcing-Dienstleister unter Umständen eine Fehlerbehebung herbeiführen, ohne umfangreiche Kenntnisse über das System zu besitzen. Durch das Notfallvorsorgekonzept müssen dem Outsourcing-Dienstleister daher genaue Anweisungen zur Verfügung gestellt werden, wie er dabei vorgehen darf. Es kann dabei auch sinnvoll sein, Aktionen zu definieren, die explizit verboten sind (z. B. Reboot einer Maschine).

Ein Fehlverhalten einer Anwendung kann technische Ursachen haben (z. B. Datenträger voll, Netzprobleme) oder anwendungsspezifische (z. B. Verarbeitung eines falschen Datensatzes, Programmfehler, falsche Parametereinstellung).

Bei technischen Fehlern ohne Auswirkungen auf andere Anwendungen wird der Outsourcing-Dienstleister den Fehler zwar selbst beheben können. Meist

ist aber dennoch eine Kooperation mit dem Auftraggeber notwendig, um ungewünschte Seiteneffekte auf Applikationsebene zu verhindern.

Liegen anwendungsspezifische Probleme vor, benötigt der Outsourcing-Dienstleister detaillierte und umfangreiche Anweisungen sowie Listen mit Ansprechpartnern auf Seiten des Auftraggebers, damit er richtig reagieren kann. Besonders bei Problemen mit komplizierten Anwendungen oder bei umfangreichen Batch-Prozessen sind häufig Kenntnisse erforderlich, die nur beim Auftraggeber vorhanden sind.

Wichtig ist in diesem Fall auch, dem Dienstleister Informationen bezüglich des Schutzbedarfs der betroffenen Daten und Systeme zur Verfügung zu stellen, damit mit angemessener Umsicht gehandelt werden kann.

Ergänzende Kontrollfragen:

- Sind alle Notfallvorsorgekonzepte (Auftraggeber, Dienstleister, Schnittstelle) festgelegt?
- Sind die Notfallvorsorgekonzepte von denjenigen, die sie anwenden müssen, auf Verständlichkeit und Anwendbarkeit geprüft worden?
- Liegen dem Dienstleister alle notwendigen Information vor, um in Notsituationen sinnvoll handeln zu können?
- Sind die Notfallkonzepte von Auftraggeber und Dienstleister aufeinander abgestimmt?
- Wird das Verhalten im Notfall durch Notfallübungen trainiert?

M 6.84 Regelmäßige Datensicherung der System- und Archivdaten

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Leiter IT, Administrator

Elektronische Archivsysteme unterliegen denselben Risiken hinsichtlich eines Datenverlustes wie andere IT-Systeme auch. Die Auswahl geeigneter Datenträger, z. B. optischer Archivmedien, allein bietet keinen ausreichenden Schutz vor Verlust, beispielsweise bei Zerstörung oder Diebstahl des Archivmediums selbst.

Eine redundante Speicherung der Archivdaten, der zugehörigen Index-Datenbank und der Systemdaten ist daher unerlässlich. Für die Datensicherung ist grundsätzlich die im Baustein B 1.4 *Datensicherungskonzept* genannte Vorgehensweise zu verwenden.

Alternativ zu einer Datensicherung der Archivdaten kann auch eine redundante Speicherung auf physikalisch getrennten und in unterschiedlichen Brandabschnitten aufgestellten Archivsystemen erfolgen. Einige Hersteller von Archivsystemen bieten hierzu Hochverfügbarkeitslösungen an. Trotzdem muss auch in diesem Fall eine Datensicherung des Archivsystems selbst sowie der Index-Datenbank erfolgen.

Folgende Vorgaben sind für die Sicherung der Daten und die Handhabung der Speichermedien zu beachten:

- Es ist eine regelmäßige Datensicherung der archivierten Dokumente und der dazugehörigen Index-Datenbank anzulegen. Dazu kann z. B. folgendes Verfahren angewandt werden:
  - Tagessicherung (automatische Differenzsicherungen werktags),
  - Wochensicherung (automatische Differenzsicherungen) und
  - Gesamtsicherung einmal monatlich und bei der Einrichtung und Änderungen der Konfiguration.
- Es sollten ausschließlich Speichermedien gemäß Herstellerangaben verwendet werden. **Herstellerangaben beachten**
- Wird eine Jukebox als Speichereinheit zur Archivierung eingesetzt, ist darauf zu achten, dass die Speichermedien nur programmgesteuert der Jukebox entnommen und darin eingelegt werden können. Ein manuelles und somit unkontrolliertes Entnehmen oder Einlegen der Medien sollte ausgeschlossen werden.
- Es ist zu dokumentieren, welche Medien zu welchem Zeitpunkt im Archivsystem eingesetzt (online) und entnommen (offline) sind, um zu vermeiden, dass Daten unautorisiert auf entnommenen Medien gelöscht oder hinzugefügt werden.
- Alle Medien sind verwechselungssicher zu beschriften. **Medien beschriften**
- Offline-Medien sind sorgfältig aufzubewahren, also so, dass sie einerseits nur für Administratoren zugänglich und andererseits vor schädigenden Umwelteinflüssen geschützt sind. Dies kann beispielsweise durch Aufbe-

wahrung in einem verschlossenen feuersicheren und einbruchgeschützten Stahlschrank (S 120 DIS, VdS Klasse III) erreicht werden.

- Sicherheitskopien der einzelnen Medien sind direkt nach ihrer Erstellung derart räumlich vom Archivsystem zu trennen, dass auch nach einer Zerstörung des Archivs dessen Daten vollständig rekonstruiert werden können. Die Räumlichkeiten sind vor dem Zutritt Unbefugter zu schützen.
- Die gewählte Verfahrensweise für die Datensicherung ist zu dokumentieren. Außerdem ist zu dokumentieren, wann welche Sicherheitskopien erstellt worden sind und wohin sie ausgelagert wurden (siehe auch M 6.37 *Dokumentation der Datensicherung*).

Datensicherung dokumentieren

- Da alle Sicherungsmedien nur eine begrenzte Lebensdauer haben, müssen sie regelmäßig entsprechend den Herstellerempfehlungen durch neue ersetzt werden.
- Alle angelegten Datensicherungen sind regelmäßig auf Lesbarkeit zu testen und gegebenenfalls auf neue Speichermedien zu übertragen.
- In regelmäßigen Abständen und bei Konfigurationsänderungen ist die Verwendbarkeit der Sicherungen und die Restart- und Recovery-Fähigkeit des Systems zu prüfen. Dieser Test geht über das reine Lesen der Sicherungsmedien hinaus und prüft, ob das Archiv anhand der gesicherten Daten ohne Datenverlust neu aufgesetzt werden kann. Das Ergebnis ist zu dokumentieren.

Restart- und Recovery-Fähigkeit prüfen

- Bei einer Neuverschlüsselung von Archivdaten (siehe hierzu M 2.264 *Regelmäßige Aufbereitung von verschlüsselten Daten bei der Archivierung*) müssen auch die auf Backup-Medien vorgehaltenen Daten neu verschlüsselt und alte Medien gelöscht oder vernichtet werden.
- Wenn Datensicherungen wieder in das Archivsystem eingespielt werden, ist zu überprüfen, ob dadurch Datenverluste aufgetreten sind, also ob zu archivierende Daten erneut erfasst werden müssen. Außerdem muss kontrolliert werden, ob für die wieder eingespielten Daten Löschvermerke vorliegen, die berücksichtigt werden müssen.

Ergänzende Kontrollfragen:

- Ist eine redundante Speicherung der zu archivierenden Dokumente vorgesehen - auf redundanten Archivsystemen oder auf Backup-Systemen?
- Können bei einem Defekt eines Archivmediums einzelne Daten aus der Datensicherung wieder hergestellt werden?
- Werden die Sicherungsmedien vom Archivsystem räumlich getrennt gelagert?

M 6.85 Erstellung eines Notfallplans für den Ausfall des IIS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der teilweise oder komplette Ausfall eines IIS hat in vielen Fällen gravierende Auswirkungen auf die Arbeitsmöglichkeiten der Benutzer und ggf. das Ansehen in der Öffentlichkeit, da z. B. der Internet-Auftritt einer Behörde bzw. eines Unternehmens nicht mehr verfügbar ist. Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind.

Folgende Aspekte müssen dabei berücksichtigt werden:

- Die Notfallplanung für den IIS muss in den existierenden Notfallplan integriert werden (siehe auch Baustein B 1.3 *Notfallvorsorge-Konzept*).
- Durch einen Systemausfall kann es auch zu Datenverlusten kommen. Daher ist ein Datensicherungskonzept für alle IIS zu erstellen, das in das existierende Datensicherungskonzept integriert werden sollte (siehe auch Baustein B 1.4 *Datensicherungskonzept*). Dabei sollten alle Komponenten eines IIS berücksichtigt sein, insbesondere auch ggf. angebundene Datenbank-Server.

Datensicherungskonzept

- Hochverfügbarkeit
- Die Verfügbarkeit und Performance sind für den Erfolg eines Internet-Angebots von entscheidender Bedeutung. Lange Wartezeiten werden von keinem Anwender auf Dauer akzeptiert, deshalb muss ein Internet-Server ständig verfügbar und seine Reaktionszeit möglichst kurz sein. Um die Verfügbarkeit und die Performance von Server-Diensten zu erhöhen, können sowohl einfache Standby-Lösungen als auch komplexe Verfahren für eine optimale Lastverteilung auf mehrere Server implementiert werden. Bei einer hochverfügbaren Lösung ist auch die Netzanbindung zu betrachten. In der Regel befindet sich ein Web-Server hinter einer Firewall in einer so genannten demilitarisierten Zone (DMZ). Das bedeutet für die Firewall, dass sie ebenfalls hochverfügbar und performant auszulegen ist, wenn entsprechende Anforderungen an den Web-Server bestehen.
- Die Systemkonfiguration ist zu dokumentieren. Wichtige Aufgaben müssen so beschrieben sein, dass sie im Notfall auch von technisch versierten Laien durchgeführt werden können.

Dokumentation muss notfalltauglich sein

- Es muss ein Wiederanlaufplan erstellt werden, der das geregelte Hochfahren des Systems gewährleistet.

Wiederanlaufplan

- Die Notfallplanung muss die Besonderheiten wichtiger Internet-Server, z. B. eines Zertifikats-Servers, in Betracht ziehen.

Ergänzende Kontrollfragen:

- Existiert ein Notfallplan für den Ausfall des IIS?
- Existiert ein Datensicherungskonzept für den IIS, das alle Komponenten berücksichtigt?

M 6.86 Schutz vor schädlichem Code auf dem IIS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Systemspezifische Schwachstellen

Für einen Web-Server, der nur Informationen über das HTTP-Protokoll zur Verfügung stellt, ist die Bedrohung durch Computer-Viren, Würmer und Trojanische Pferde eher gering. Dennoch zeigen aktuelle Ereignisse, dass auch reine Informations-Server auf Basis von HTTP unter Ausnutzung systemspezifischer Schwachstellen mit schädlichem Code infiziert und für weitere Angriffe ausgenutzt werden können.

Ein Beispiel für eine solche Attacke ist der Computer-Virus bzw. Wurm *Code Red*, der seit Juli 2001 in verschiedenen Varianten auftritt. Dieser Wurm ist ein selbstreplizierendes, schädliches Programm, das sich eine Schwachstelle im Microsoft Internet Information Server zu Nutze macht, indem es einen Pufferüberlauf erzeugt. Gefährdet sind alle Computer, auf denen IIS 4.0 oder 5.0 und Index Server 2.0 (bzw. Indexing-Service bei Windows 2000) installiert sind. Dazu kommen diverse Produkte von Cisco, die mit dem IIS arbeiten.

Ein wirksamer Schutz vor Programmen, die systemspezifische Schwachstellen ausnutzen, kann nur durch zeitnahes Einspielen von Sicherheits-Patches erreicht werden. Gegen *Code Red* sind bei Microsoft entsprechende Patches sowohl für Windows NT als auch für Windows 2000 verfügbar (siehe *http://www.microsoft.com/technet/security/bulletin/MS01-033.asp*).

Prüfwerkzeuge

Um ein IIS-System auf bestehende Schwachstellen zu prüfen, werden sowohl von Microsoft wie auch von Drittherstellern verschiedene Prüfwerkzeuge und Scanner angeboten. Mit dem Tool *HFCHECK.WSF* von Microsoft (siehe *http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24168*) kann beispielsweise der aktuelle Patchstatus für Windows NT und Windows 2000 sowie die aktuellen Hotfixes für IIS 4.0 und IIS 5.0 untersucht werden. Ein spezieller Scanner für den *Code Red* wird von der Firma eEye Digital Security kostenlos bereit gestellt (siehe *http://www.eeye.com/html/Research/Tools/codered.html*).

Die Gefahr einer Virusinfektion eines Web-Servers steigt bei zusätzlich angebotenen Diensten und veränderbaren Datenbeständen. Fungiert der Web-Server z. B. auch als FTP-Server oder ist ein HTTP-Download möglich, muss natürlich sichergestellt sein, dass die angebotenen Dateien vertrauenswürdig sind und keine Viren enthalten. Zum Schutz gegen Computer-Viren werden eine Reihe von Virenschutzprogrammen angeboten. Maßgeblich für die Effektivität dieser Programme ist ihre kontinuierliche Aktualisierung, da immer neue Computer-Viren auftauchen. Weitere Hinweise hierzu finden sich im Baustein B 1.6 *Computer-Viren-Schutzkonzept*.

Uploads

Ab IIS 4.0 wird HTTP 1.1 unterstützt, so dass ein Upload von Dateien mit der HTTP-Methode PUT unter Verwendung eines kompatiblen Browsers möglich ist. Durch die Möglichkeit von Uploads auf einem Web-Server ensteht eine weitere Gefahr, dass schädlicher Code in das System eingebracht wird. Um das Risiko für Uploads auf den IIS zu minimieren, sollten folgende Empfehlungen beachtet werden:

- Wenn keine Möglichkeit zum Datei-Upload benötigt wird, ist die gesamte Unterstützung für Uploads zu deaktivieren. Beispielweise sind die Frontpage Server-Erweiterungen zu entfernen (siehe auch M 4.187 *Entfernen der FrontPage Server-Erweiterung des IIS*).
- Die Zugriffsrechte auf Dateien und Verzeichnisse sollten möglichst restriktiv vergeben werden (siehe auch M 4.185 *Absichern von virtuellen Verzeichnissen und Web-Anwendungen beim IIS-Einsatz)*. Ein allgemeines Schreibrecht der Gruppe *Jeder* ist zu vermeiden.
- Uploads sollten nur auf einer separaten Festplatte bzw. Partition ermöglicht werden.
- Voraussetzung zum Upload ist eine Authentisierung des Benutzers (siehe auch M 4.180 *Konfiguration der Authentisierungsmechanismen für den Zugriff auf den IIS*).
- Die Verzeichnisse im Upload-Bereich sollten nur über Schreibrecht (kein Ausführungsrecht) verfügen.
- Die Inhalte sind auf schädlichen Code zu prüfen, z. B. durch Einsatz eines Content-Scanners.
- Alle Uploads sind zu protokollieren.

Ergänzende Kontrollfragen:

- Wurden die aktuellen Patches und Hotfixes eingespielt?
- Werden auf den Servern geeignete Virenschutzprogramme eingesetzt?
- Wird der Server vor unberechtigten Uploads geschützt?

M 6.87 Datensicherung auf dem IIS

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Ein wichtiges Kriterium für die Verfügbarkeit und Integrität der durch den Web-Server bereitgestellten Informationen ist die Möglichkeit, Daten im Fehlerfall, z. B. bei einem Festplattendefekt, in einem angemessenen Zeitraum wiederherstellen zu können. Die Besonderheit eines Web-Servers ist, dass Datenbestände mit unterschiedlichen Sicherheitsanforderungen vorhanden sind:

- Daten, auf die in der Regel Unbekannte von extern zugreifen dürfen, z. B. virtuelle Verzeichnisse
- Daten, deren Vertraulicheit und Integrität gewährleistet sein muss, z. B. Konfigurations- und Protokolldateien sowie administrative Programme

Partitionen

Für die sichere Installation eines IIS wird das Einrichten von mindestens zwei Partitionen empfohlen, so dass das *Webroot*-Verzeichnis auf einer anderen Partition als das Systemverzeichnis installiert werden kann (siehe M 4.174 *Vorbereitung der Installation von Windows NT/2000 für den IIS*). Diese Konfiguration ist bei der Datensicherung des IIS zu berücksichtigen.

IIS-Metabasis

Die meisten Konfigurationseinstellungen für den IIS befinden sich in der IIS-Metabasis. Dies ist ein Datenspeicher, der der Windows-Registrierung ähnelt. Die Metabasis ist hierarchisch organisiert und spiegelt die Struktur der IIS-Installation wider. Die Konfigurationsparameter werden durch sogenannte Schlüssel definiert, denen ein aber auch mehrere Werte zugeordnet werden können. Einige Einstellungen zur sicheren Konfiguration des IIS lassen sich in der Metabasis vornehmen, z. B. das Unterbinden der Content-Location. Die Metabasis kann mit Hilfe der Microsoft Management Console (MMC) mit einem Rechtsklick auf den entsprechenden Server und Auswahl des Menüpunktes *Sicherungskopie/Wiederherstellen der Konfiguration* gesichert bzw. wiederhergestellt werden.

Konfigurationsdaten

Zur Sicherung der vollständigen Konfigurationsdaten ist es sinnvoll, eine Image-Datei zu erstellen, mit deren Hilfe die Funktionalität des IIS nach einem Systemausfall in sehr kurzer Zeit wiederhergestellt werden kann. Eine Sicherung der Konfigurationsdaten sollte nach jeder Änderung durchgeführt werden. Veränderbare Daten, z. B. Protokolldateien und Dateien im *Webroot*-Verzeichnis, sind gesondert und konform zum Datensicherungskonzept (siehe *M 6.33* Entwicklung eines Datensicherungskonzepts) zu sichern.

Ergänzende Kontrollfragen:

- Werden alle Daten des IIS sowie eventuell nachgeordnete Datenbanken gesichert?
- Ist der Datensicherungsvorgang dokumentiert?
- Ist der Datensicherungsvorgang konform zum vorhandenen Datensicherungskonzept?

M 6.88 Erstellen eines Notfallplans für den Webserver

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der teilweise oder komplette Ausfall eines Webservers hat in vielen Fällen gravierende Auswirkungen. So kann der Webserver etwa wesentlicher Bestandteil innerbetrieblicher Arbeitsabläufe oder eines E-Commerce-oder E-Government-Systems sein.

Ein Ausfall des Webservers hat dann auch den Ausfall des Gesamtsystems zur Folge. Falls der Webserver ein öffentliches Webangebot beherbergt, so wird ein Ausfall oder eine Störung auch schnell öffentlich bekannt werden.

Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind.

Folgende Aspekte müssen dabei berücksichtigt werden:

Allgemeine Notfallplanung

- Die Notfallplanung für den Webserver muss in den existierenden Notfallplan integriert werden (siehe Baustein B 1.3 *Notfallvorsorge-Konzept*).

regelmäßige Datensicherung

- Durch einen Systemausfall kann es auch zu Datenverlusten kommen. Daher ist ein Datensicherungskonzept für den Webserver zu erstellen, das in das existierende Datensicherungskonzept integriert werden sollte (siehe auch Baustein B 1.4 *Datensicherungskonzept*). Hierin sollte nicht nur der Webserver selbst, sondern auch das Gesamtsystem, innerhalb dessen der Webserver eingesetzt wird, berücksichtigt werden. Dazu gehören unter Umständen Datenbanken, Applikationsserver oder Proxy-Installationen zur Lastverteilung.
- Bestehen besondere Anforderungen an die Verfügbarkeit des Webservers, so sollten benötigte Komponenten redundant ausgelegt werden. Beispielsweise kann der Webserver selbst in manchen Anwendungen durch die Verwendung eines gemeinsamen, externen Speichersystems redundant ausgelegt werden.
- Zum Betrieb des Webservers im Internet ist eine funktionierende Internet-Anbindung Voraussetzung. Bei bestimmten Konfigurationen ist auch ein korrekt funktionierender DNS-Server nötig. Ein Ausfall dieser Komponenten muss daher ebenfalls in Betracht gezogen werden.
- Wird SSL auf dem Webserver eingesetzt, so muss beim Wiederanlauf des Systems auch der private Schlüssel des SSL-Zertifikates zugreifbar sein. Da dieser durch ein Passwort geschützt sein sollte, muss dieses sicher hinterlegt sein, damit es für den Wiederanlauf verfügbar ist (siehe auch M 2.22 *Hinterlegen des Passwortes*).
- Die Systemkonfiguration ist zu dokumentieren. Wichtige Aufgaben müssen so beschrieben sein, dass das Gesamtsystem im Notfall auch ohne vorherige Kenntnis dieser Systemkonfiguration wiederhergestellt werden kann.
- Es muss ein Wiederanlaufplan erstellt werden, der das geregelte Hochfahren des Systems gewährleistet.

Ergänzende Kontrollfragen:

- Existiert ein Notfallplan für den Ausfall des Webservers?
- Gibt es entsprechende Notfallpläne für die anderen Systeme, die zum Betrieb des Webservers benötigt werden?
- Existieren Notfallpläne für den Ausfall der Internet-Anbindung, falls der Webserver im Internet genutzt wird?
- Existiert ein Datensicherungskonzept für den Webserver?

M 6.89 Notfallvorsorge für einen Apache-Webserver

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Bei der Erstellung eines Notfallplans für einen Apache-Webserver sollten zunächst die allgemeinen Punkte, die in der Maßnahme M 6.88 *Erstellen eines Notfallplans für den Webserver* beschrieben wurden, umgesetzt werden. Dazu gehören insbesondere:

- Die Einbindung in ein existierendes allgemeines Notfallkonzept.
- Die Entwicklung eines Datensicherungskonzepts und dessen Einbindung in ein existierendes allgemeines Datensicherungskonzept.
- Die Dokumentation der Systemkonfiguration und aller wichtigen Schritte zur Wiederherstellung des Systems, so dass das System im Notfall auch ohne vorherige Kenntnis der Systemkonfiguration wiederhergestellt werden kann.
- Gegebenenfalls die redundante Auslegung wichtiger System- und Netzkomponenten.
- Die Erstellung eines Wiederanlaufplans, der das geregelte Hochfahren des Systems gewährleistet.

Für einen Apache-Webserver sollten insbesondere folgende Punkte berücksichtigt werden:

Sicherungskopie der eingesetzten Software

- Die Pakete (etwa Quelltextarchive oder Distributionspakete), mit denen der Apache-Webserver installiert wurde, sollten an einem definierten Ort verfügbar gehalten werden, etwa auf einer entsprechenden CD-ROM. Dort sollten auch alle benötigten externen Module und verwendeten Programme vorhanden sein.

gewählte Konfiguration dokumentieren

- Wurde der Apache-Webserver aus den Quelltexten übersetzt, so sollte die Dokumentation der Systemkonfiguration sämtliche beim Übersetzen verwendeten Optionen (insbesondere die Optionen, mit denen das configure-Skript aufgerufen wurde) enthalten.
- Wurden externe Module (etwa *mod_perl* oder PHP) ebenfalls aus den Quelltexten installiert, so müssen die entsprechenden Quelltextpakete ebenfalls vorhanden sein und zusätzlich zu den entsprechenden Konfigurationsoptionen sollte auch dokumentiert sein, in welcher Reihenfolge die Übersetzung erfolgt ist.

Installation dokumentieren

- Wurde der Apache-Webserver aus einem Binärpaket installiert, so sollten analog die Schritte dokumentiert werden, mit denen die Installation nachvollzogen werden kann.
- Jede Änderung an einer Konfigurationsdatei, insbesondere der Datei *httpd.conf*, sollte dokumentiert werden. Alle Konfigurationsdateien sollten regelmäßig gesichert werden.

SSL-Serverzertifikat sicher hinterlegen

- Wird SSL verwendet, so müssen das Serverzertifikat und der dazu gehörende private Schlüssel sowie die Passphrase an einer sicheren Stelle so hinterlegt werden, dass im Notfall darauf zugegriffen werden kann.

Ergänzende Kontrollfragen:

- Sind die notwendigen Pakete und Informationen vorhanden, um den Apache-Webserver im Notfall schnell neu installieren zu können?
- Wie werden Änderungen an der Konfiguration dokumentiert? Wo werden Konfigurationsdateien gesichert?

M 6.90 Datensicherung und Archivierung von E-Mails

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Benutzer, Administrator

Die Bedeutung von E-Mail für die interne und externe Kommunikation nimmt ständig zu, daher ist es wichtig, dass die gesendeten bzw. empfangenen Nachrichten auch längerfristig zur Verfügung stehen. Während die Datensicherung der Fileserver im allgemeinen gut geregelt ist, bestehen häufig große Regelungslücken bei der Frage der Datensicherung und Archivierung von E-Mails.

E-Mails auf Clients sichern

Typischerweise werden E-Mails von einem zentralen E-Mail-Server zunächst auf Benutzer-PCs oder in Benutzerverzeichnisse verlagert, wo sie bearbeitet und weitergeleitet bzw. abgelegt werden. Während Daten auf E-Mail-Servern im allgemeinen regelmäßig gesichert werden, werden die auf den Clients gespeicherten E-Mails häufig nicht oder unzureichend gesichert. Es sollte auch hierfür eine geregelte Vorgehensweise geben.

Beispiel:

Bei Microsoft Outlook werden die meisten Informationen in Dateien mit der Erweiterung *.pst* gespeichert, nur die Adressbücher werden in *.pab*-Dateien geführt. Wo persönliche Ordner gespeichert werden, können Benutzer unter *Extras* | *Dienste* | *Persönliche Ordner* | *Eigenschaften* anzeigen lassen. Jeder Benutzer sollte überprüfen, wo seine E-Mail-Informationen gespeichert werden und ob diese in das Datensicherungskonzept mit einbezogen wurden.

Zusätzlich kann für jeden einzelnen persönlichen Ordner eine andere Datei festgelegt werden, in dem die in diesem Ordner enthaltenen E-Mails archiviert werden. Dies kann über das *Eigenschaften*-Menü des jeweiligen Ordners (rechte Maustaste) auf der Registerkarte *AutoArchivierung* eingestellt werden.

Projektverzeichnisse

Für den Empfang von E-Mails können benutzer- oder aufgabenbezogene E-Mail-Adressen eingerichtet werden. Viele E-Mails, die an eine benutzerbezogene E-Mail-Adresse gerichtet sind, sollten aber einer Reihe von Mitarbeitern zugänglich sein, z. B. in Projektgruppen. Daher ist es wichtig, diese in entsprechenden Projektverzeichnissen auf Servern zu speichern. Häufig müssen bei der Speicherung solcher E-Mails als offizielle Dokumente auch Mindest- bzw. Höchstfristen der Speicherung beachtet werden (siehe Baustein B 1.12 *Archivierung*).

Es sollte grundsätzlich geregelt sein, wie, wann und wo sowohl gesendete als auch empfangene E-Mails archiviert werden, beispielsweise ob zentral oder dezentral von den Benutzern.

Archivieren von verschlüsselter E-Mail

Beim Archivieren von verschlüsselter E-Mail müssen einige Punkte beachtet werden (siehe auch M 6.56 *Datensicherung bei Einsatz kryptographischer Verfahren*):

- E-Mails, die über eine beträchtliche Zeitspanne gespeichert werden sollen, können unlesbar sein, wenn die benutzten kryptographischen Schlüssel nicht mehr vorhanden sind.
- Das Archivieren und das Wiedereinspielen verschlüsselter E-Mails muss sorgfältig geplant werden. Eine Möglichkeit ist z. B., die Nachrichten im

Klartext zu speichern. Dabei muss die Vertraulichkeit auf andere Weise sichergestellt werden.

Ergänzende Kontrollfragen:

- Ist die Datensicherung und Archivierung von E-Mails geregelt?
- Wissen alle Benutzer, wie E-Mails aus dem E-Mail-Client heraus zu speichern und zu sichern sind?

M 6.91 Datensicherung und Recovery bei Routern und Switches

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Auch Router und Switches sollten in das übergeordnete Datensicherungskonzept einbezogen werden. Dabei kommt insbesondere der Sicherung der Konfigurationsdateien eine hohe Bedeutung zu.

Eine Sicherung von Dateisystemen ist bei aktiven Netzkomponenten nicht möglich. Da im Rahmen einer zentralen Administration Konfigurationsdateien oftmals auf separaten Servern gehalten und auch von dort geladen werden, kann die Sicherung über diese Server erfolgen. Die Konfigurationsdateien auf diesen Servern sind vor unberechtigtem Zugang zu schützen. Dies gilt insbesondere dann, wenn in den Konfigurationsdateien Passwörter im Klartext gespeichert sind.

Falls zur Sicherung der Konfigurationsdateien ein TFTP-Server eingesetzt wird, so darf dieser nur im Administrationsnetz erreichbar sein. Alternativ kann bei einigen Systemen eine Datensicherung auch über die Verwendung von PCMCIA-Speichereinschüben erfolgen.

Um auf die Nutzung der Datensicherung vorbereitet zu sein, müssen regelmäßig Recovery-Übungen zum Wiederherstellen der Sicherung durchgeführt werden (siehe hierzu auch M 6.41 *Übungen zur Datenrekonstruktion*).

Weiterführende Maßnahmen:

M 6.36 *Festlegung des Minimaldatensicherungskonzeptes*

M 6.37 *Dokumentation der Datensicherung*

M 6.35 *Festlegung der Verfahrensweise für die Datensicherung*

M 6.41 *Übungen zur Datenrekonstruktion*

Ergänzende Kontrollfragen:

- Wird eine regelmäßige Datensicherung der Konfigurationsdateien durchgeführt?
- Wird eine regelmäßige Datensicherung in der Sicherheitsrichtlinie vorgeschrieben?
- Werden die gesicherten Konfigurationsdateien sicher und zentral verwaltet?

M 6.92 Notfallvorsorge bei Routern und Switches

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Fehlerbehandlung bei Routern und Switches

In jedem IT-Betrieb treten Störungen auf, die von sporadisch auftretenden Fehlverhalten von Komponenten bis zum klar abzugrenzenden Ausfall eines Geräts und dadurch verursachten Netzausfällen reichen können. Grundlage eines sicheren Betriebs ist die Vorbereitung auf Störungssituationen. Hierzu gehören Ausfälle oder Beeinträchtigungen von Hardware und Software beispielsweise auf Grund von Defekten oder Kompromittierungen.

Um in derartigen Situationen effektiv und schnell reagieren zu können, müssen Diagnose und Fehlerbehebung bereits im Vorfeld geplant und vorbereitet werden. Für typische Ausfallszenarien und als Ergebnis von bereits aufgetretenen Störungen sollten Handlungsanweisungen erstellt werden. Kochbuchartige Dokumentationen aller notwendigen Kommandos, ihrer Anwendung mit den zu erwartenden Ausgaben sind in Situationen, die schnelles Handeln erfordern, besonders hilfreich. Hierzu gehören neben Diagnose und Fehlerbehandlung auch die im normalen Betrieb notwendigen Administrationstätigkeiten. Letztere können typischerweise bereits in der vom Hersteller gelieferten Dokumentation enthalten sein. Für die tägliche Praxis ist es allerdings sinnvoll, eine Gesamtdokumentation in Form eines Betriebshandbuchs zu erstellen.

Protokollierung

Zu den Voraussetzungen für den Erfolg der Diagnosearbeiten gehört auch eine geeignete Protokollierung während des Betriebs (siehe auch M 4.205 *Protokollierung bei Routern und Switches*). Weiterhin sollten für die Fehlerbehandlung geeignete Werkzeuge genutzt werden. Dazu existieren sowohl frei verfügbare als auch kommerzielle Programme, oft auch vom Hersteller der Geräte. Die Verwendung geeigneter Werkzeuge ist umso wichtiger, da mit den Systemkommandos nicht immer alle Konfigurationseinstellungen angezeigt werden. Teilweise werden lediglich die von den Standardeinstellungen abweichenden Daten erfasst.

Die Vorgehensweise bei der Fehlerbehandlung lässt sich in die Bereiche Administration, Performancemessung und Diagnose unterteilen. Nachfolgend werden die jeweils zu berücksichtigenden Aspekte dargestellt:

Administration

In einem Betriebshandbuch sollten alle notwendigen Kommandos zu Administration und Konfiguration dokumentiert werden.

Folgende Bereiche sind zu berücksichtigen:

- Einrichten von Nutzern, Vergabe von Berechtigungen
- Update des Betriebssystems
- Konfiguration
  - Interface
  - Line-Ports

  - Access-Control-Lists
  - Routing
- Protokollierung

Performance

Folgende Aspekte sollten für Aussagen über die Performance berücksichtigt werden:

- Eingehender und ausgehender Verkehr (pro Interface oder Port)
- Durchsatz oder Verkehr pro Interface
- Statistikinformationen der verwendeten Protokolle

Diagnose

Für die Diagnose sollten alle notwendigen Kommandos und die zu erwartenden Ausgaben zur Anzeige der Zustände des Gesamtsystems, der Interfaces und ihrer Konfiguration dokumentiert sein. Viele Kommandos ermöglichen zudem einen Debug-Modus zu Ausgabe umfangreicher Statusinformationen.

Unter anderem sind folgende Informationen für die Fehlerdiagnose relevant:

- Status der Netz-Interfaces und der sonstigen Anschlüsse
- Status der TCP- und UDP-Netzdienste
- Gesamtkonfiguration als Überblick
- Prozesse
- Routing Tabelle und genutzte Routing Protokolle
- ARP-Tabelle
- Angemeldete Nutzer
- DNS und nslookup-Informationen
- Protokollierung (Nutzung der Log-Level, Interpretation der Log-Informationen)

Als weiterführende Maßnahmen sollte M 2.215 *Fehlerbehandlung* betrachet werden.

Notfallvorsorge zur Steigerung der Verfügbarkeit

Durch eine Planung des Vorgehens bei Störungen kann die Zeit zur Wiederherstellung minimiert und unter Umständen eine Lösung überhaupt erst ermöglicht werden. Die Planungen sind mit der übergreifenden Störungs- und Notfallvorsorge abzustimmen und sollten sich am allgemeinen Notfallvorsorgekonzept orientieren (siehe Baustein B 1.3 *Notfallvorsorge-Konzept*). Hier werden generelle Vorgaben für Notfalldokumente im gesamten IT-Betrieb formuliert. Diese legen idealerweise einheitliche und verbindliche Anforderungen bez. Aufbau, Inhalt und Form fest.

Folgende Fragestellungen sind für die Notfallvorsorge relevant:

- Welche Anforderungen bestehen an das Monitoring?

- Zusammenstellung der Informationen, die von den für den Betrieb der Netzkomponenten verantwortlichen Stellen immer ausgewertet werden (siehe auch Abschnitt Protokollierung)
  - Wie kann eine frühzeitige Störungserkennung sicher gestellt werden?
- Was sind Gründe für mögliche Störungen?
  - Hardware-Defekte
  - Zu geringe Dimensionierung (Ausfall bei Steigerung der Last)
- Welche Vorsorgemaßnahmen können getroffen werden?
  - Ersatzgeräte
  - Ersatzteile
  - Implementierung von Failover-Lösungen, die im laufenden Betrieb ein Umschalten auf ein Alternativgerät ermöglichen
  - Wartungsverträge
  - Ausbildung der Mitarbeiter
- Welche Service Level Agreements bestehen oder sollten getroffen werden?
  - Hardware-Lieferanten (beispielsweise Vor-Ort-Austausch mit Zeitgarantie für bestimmte Komponenten)
  - Interne Service Level Anforderungen
- Wie ist eine Diagnose durchzuführen?
  - Statusabfragen
  - Anzeige der Konfiguration
  - Prozesse
  - Routing
  - Angemeldete Nutzer
  - Protokollierung
- Welche Entstörprozeduren müssen durchgeführt werden?
  - Vorgehen bei Ausfall des Komplettsystems (Wiederherstellen von Betriebssystem und Konfiguration)
  - Vorgehen bei Ausfall von Teilkomponenten, bspw. Speicher
- Wer ist im Schadensfall zu benachrichtigen?
  - Server- und Anwendungsadministration
  - Hardware-Lieferant/Ansprechpartner für den Wartungsvertrag
- Welche Dokumente müssen im Schadensfall verfügbar sein?
  - Konfiguration
  - ACLs (Regelwerk)
  - Eingerichtete Nutzer und Berechtigungen

- Passwörter

Die Dokumentation sollte keinesfalls ausschließlich elektronisch vorliegen. Handlungsanweisungen sollten mindestens auch in Papierform existieren. Gegebenenfalls können Konfigurationsdateien auch auf CD-ROMs oder anderen Datenträgern gesondert hinterlegt werden.

Dokumentation auch in Papierform

- Wie verläuft der Wiederanlauf?
  - Abhängigkeiten zu anderen Netzkomponenten bzw. Bereichen des IT-Verbunds
  - Neuinstallation des Betriebssystems und Konfiguration
  - Zurückspielen einer gesicherten Konfiguration
  - Möglichkeiten eines eingeschränkten Betriebs

Die für die Notfallvorsorge notwendigen Vorgehensbeschreibungen sind möglichst sorgfältig zu erstellen und regelmäßig zu erproben. Eventuell müssen variierende Vorgehensweisen bei unterschiedlichen Gerätetypen und Betriebssystemen berücksichtigt werden.

Vorgehens-beschreibungen auch erproben

Die wahrscheinlich wichtigste Maßnahme zur Steigerung der Verfügbarkeit ist die Vorhaltung von Ersatzteilen, um bei Hardware-Defekten die Ausfallzeiten zu minimieren. Alternativ oder auch als Ergänzung hierzu können Wartungsverträge mit dem Hersteller abgeschlossen werden, die durch garantierte Reaktions- oder sogar Reparaturzeiten die Verfügbarkeit sicherstellen. Hierdurch lassen sich Kosten für die Lagerhaltung reduzieren oder eine noch höhere Hardwareverfügbarkeit erreichen. Im Rahmen eines solchen Vertrages kann auch die Versorgung mit Software-Updates geregelt werden.

Ergänzende Kontrollfragen:

- Sind Störungs- und Notfallprozeduren in der Sicherheitsrichtlinie beschrieben?
- Wurden Verantwortlichkeiten im Notfall definiert?
- Werden Störungs- und Notfallprozeduren regelmäßig getestet?

M 6.93 Notfallvorsorge für z/OS-Systeme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Zu einem sicheren z/OS-Betrieb gehört es, für verschiedene Notfälle vorbereitet zu sein. Dazu zählen z. B.

- ein Notuser-Verfahren, das notwendig wird, wenn keine Kennung mehr mit bestimmter Funktionalität verfügbar ist,
- ein Verfahren zur Wiederherstellung einer funktionierenden RACF-Datenbank,
- ein z/OS-Backup-System, das sofort aktiviert werden kann und
- ein Notfall-System, das bei Einzelsystemen u. U. benötigt wird, um Fehlerkorrekturen vornehmen zu können.

Die verschiedenen Handlungsempfehlungen zur Notfallvorsorge sind nachfolgend näher beschrieben:

Notuser-Verfahren

Zur Notfallvorsorge muss ein Notuser-Verfahren eingerichtet werden. Dieser Notuser kann verwendet werden, falls in einer Notsituation kein RACF-Administrator (*Resource Access Control Facility*) zur Verfügung steht, bzw. falls alle Kennungen mit *SPECIAL*-Rechten gesperrt sind. Es können eine oder mehrere Notuser-Kennungen eingerichtet werden.

Es sind folgende Regeln zu beachten:

Zugang zur Notuser-Kennung

Da die Notuser-Kennung sehr hohe Berechtigungen (*SPECIAL*) im System besitzt, muss die Herausgabe der Notuser-Kennung restriktiv gehandhabt werden.

Der Notuser darf nur vorher festgelegten Personen zugänglich sein. Er sollte nur RACF-Administratoren und Systemprogrammierern mit RACF-Ausbildung zur Verfügung stehen.

Meldung und Dokumentation der Verwendung des Notusers

Bei Verwendung des Notusers sind sobald als möglich die RACF-Administration, der Auditor und das IT-Sicherheitsmanagement zu unterrichten. Folgende Informationen müssen gemeldet werden:

- Wer hat den Notuser benutzt?
- Weshalb wurde der Notuser benötigt?
- Wann erfolgte der Zugriff?
- Was wurde mit der Berechtigung des Notuser durchgeführt?

Alle Vorgänge zur Notuser-Kennung sind nachvollziehbar zu dokumentieren und zu archivieren.

Passwort der Notuser-Kennung

Beim Login mit der Notuser-Kennung ist das Passwort durch den Benutzer sofort auf ein neues zu ändern. Dies wird durch RACF erzwungen, wenn der Notuser mit einem neuen *Initial-Passwort* versehen wurde.

Nach dem Gebrauch der Notuser-Kennung muss das zugehörige Passwort durch die RACF-Administration wieder neu gesetzt und hinterlegt werden.

Missbrauch des Notuser-Verfahrens

Das Notuser-Verfahren darf nicht zur Berechtigungserweiterung im Nicht-Notfall missbraucht werden. Es muss verhindert werden, dass der Notuser aus Bequemlichkeit verwendet wird, um definierte Administrations- und Entscheidungswege zu umgehen.

Verhindern der Notuser-Sperrung

Alle Kennungen können nach einer vorgegebenen Zeit wegen Inaktivität gesperrt werden. Die entsprechende Einstellung erfolgt in den *SETROPTS*-Parametern von RACF. Eine solche Sperrung kann auch Notuser-Kennungen betreffen, wenn diese längere Zeit nicht verwendet werden. Es ist zu überlegen, diese automatische Sperrung durch den Einsatz eines Batch-Jobs zu verhindern. Der Batch-Job sollte regelmäßig die Notuser-Kennungen benutzen (z. B. einmal im Monat). Dadurch werden die Zeitstempel in der RACF-Datenbank aktualisiert. Dieser Batch-Job kann über einen Job-Scheduler initiiert werden. Es muss sichergestellt werden, dass das Passwort des Notusers außer den explizit hierzu autorisierten Mitarbeitern niemandem bekannt wird. Hierfür sollte die RACF-Klasse *SURROGAT* zum Einsatz kommen, damit kein Passwort in die *Job Control Language* eingestellt werden muss.

Verfahren zur Wiederherstellung von z/OS-RACF-Datenbanken

Die RACF-Datenbank ist der wichtigste und zentrale Speicherort für die Sicherheitseinstellungen eines z/OS-Systems. Soll ein sicherer Betrieb gewährleistet werden, muss die RACF-Datenbank korrekt funktionieren. Um Problemen durch nicht zur Verfügung stehende oder defekte RACF-Datenbanken zu begegnen, sind die folgenden Empfehlungen zu beachten:

Sicherung der RACF-Datenbanken

Es ist wichtig, dass die Synchronisierung der RACF-Datenbanken einwandfrei funktioniert. Deshalb muss zur Sicherung aktiver Datenbanken (die Datenbanken, die beim *RVARY*-Display als aktiv gekennzeichnet sind) immer entweder das RACF-Utility *IRRUT200* (von IBM empfohlen) oder *IRRUT400* eingesetzt werden.

Während der Sicherung werden zahlreiche *LOCK*-Funktionen ausgeführt. Deshalb sollte der Batch-Job, der die Sicherung durchführt, in ein Zeitfenster mit möglichst geringer Auslastung gelegt werden.

Die Sicherungen dürfen nicht auf der gleichen Festplatte gespeichert werden, auf der die RACF-Datenbanken im Betrieb liegen.

Es sollte überlegt werden, mehrere Generationen der Sicherungen aufzubewahren. Dabei ist das Wochenende mit zu berücksichtigen.

Die Sicherungskopien der Datenbanken sind - ebenso wie die RACF-Datenbanken selbst - über entsprechende RACF-Profile zu schützen (siehe M 4.211 *Einsatz des z/OS-Sicherheitssystems RACF*).

RACF-Datenbankwiederherstellung

Im z/OS-System gibt es eine *Primary* und eine *Backup* RACF-Datenbank. Diese können im Betrieb umgeschaltet werden. Aus Sicherheitsgründen sind die beiden Datenbanken auf verschiedenen Platten zu speichern. Treten Fehler in der *Primary* Datenbank auf, so kann durch ein *RVARY SWITCH* Kommando die *Backup* zur *Primary* und die *Primary* zur *Backup* RACF-Datenbank gemacht werden. Die defekte *Backup* RACF-Datenbank kann daraufhin in der Regel gelöscht und durch eine neue ersetzt werden.

Sind beide RACF-Datenbanken fehlerhaft, so ist es in diesem Notfall möglich, die defekte RACF-Datenbank durch eine gültige Sicherungskopie zu ersetzen und hierdurch den Systembetrieb wieder herzustellen (u. U. von einem anderen System aus). Bei Einzelsystemen ist hierfür eventuell ein Notfallsystem notwendig (siehe unten: *Erstellung eines z/OS-Notfallsystems*).

Nachvollziehbarkeit im Fehlerfall

Es ist ein Verfahren zur Sicherung und zum Zurückspielen der RACF-Datenbank einzurichten.

Es ist ein Verfahren einzurichten, so dass Änderungen in der RACF-Datenbank in der Zeit zwischen der letzten Sicherung der RACF-Datenbank und dem Zeitpunkt des eingetretenen Notfalls nachvollzogen werden können. Eine Möglichkeit hierfür ist beispielsweise, dass RACF-Änderungen nur durch dokumentierte Batch-Jobs durchgeführt werden dürfen. Eine andere Möglichkeit ist, dass direkt nach RACF-Änderungen die SMF-Datensätze ausgewertet werden. Beide Verfahren müssen nachvollziehbar dokumentiert sein. Die Dokumentation muss den Administratoren vorliegen.

z/OS-Backup-System

Bei Systemfehlern, bei denen das z/OS-System (oder auch ein kompletter *Parallel Sysplex Cluster*) nicht mehr gestartet werden kann, ist es wichtig, möglichst schnell das System bzw. die Systeme wieder in einen betriebsbereiten Zustand zu bringen. Solche Ausfälle können beispielsweise auf Grund eines technischen Fehlers oder auch auf Grund fehlerhafter manueller Eingaben vorkommen. Deshalb sollte ein separater Satz von Festplatten vorgehalten werden, der eine Kopie des aktuellen Betriebssystems enthält. Durch einfache Änderung der IPL-Adresse (*Initial Program Load*) kann auf diese Weise ein z/OS-Betriebssystem in den meisten Fällen schnell reaktiviert werden. Die folgenden Empfehlungen sind dabei zu beachten:

Festplatten-Konzept

Das Festplatten-Konzept für das z/OS-Betriebssystem und die dazugehörenden Programmprodukte (wie Scheduler, Output-Manager und weitere) muss logisch aufgebaut und klar erkennbar sein. Zusammengehörende Dateien, z. B. des Betriebssystems, dürfen nicht verteilt auf viele unterschiedliche Festplatten gespeichert werden. Es sollten möglichst wenig Festplatten verwendet

werden, damit relativ einfach vollständige Sicherungen erstellt werden können.

Cloning-Prozess

Für das Erstellen der Backup-Festplatten sollte ein *Cloning*-Prozess entwickelt werden, der mindestens die folgenden Aktionen durchführt:

- Kopieren der System-Residenzen,
- Kopieren der Programmprodukt-Festplatten,
- Kopieren der HFS-Festplatten (*Hierarchical File System*),
- Kopieren der SMP/E-Festplatten (*System Modification Program*),
- Verändern der Volume-Angaben in SMP/E durch die *ZONEEDIT*-Funktion (alte Volume-Angabe durch neue ersetzen) und
- Anpassen der Volume-Angabe im Member *IEASYMnn* der *Parmlib.*

Wartungskonzeption

Um den laufenden Betrieb nicht zu gefährden, wird zur Pflege des z/OS-Betriebssystems in der Regel ein separater Festplattensatz verwendet. Es ist zu überlegen, diesen nach erfolgter Wartung als neuen aktiven Plattensatz und die vorherigen Platten als Backup-Satz zu benutzen.

Einsatz von System-Variablen

Zur Erleichterung der Definitionen sollten, wo immer technisch möglich und sinnvoll, symbolische Variablen benutzt werden (ab z/OS 1.4 sind bis zu 800 solcher Variablen definierbar). Es sollte überlegt werden, die Katalogeinträge des Masterkatalogs und dessen *ALIAS*-Einträge über solche Techniken variabel zu gestalten, damit ein Wechsel ohne zusätzliche Eingriffe jederzeit möglich ist. Die Benutzung symbolischer Variablen ist in vielen Definitionen möglich, es sollte jedoch berücksichtigt werden, dass einige Definitionen die Variablen noch nicht unterstützen.

Führung von Arbeitsdateien

Um unnötigen Wartungsaufwand zu vermeiden, sollten Arbeitsdateien, wie Kataloge, *Parmlibs*, *Proclibs* und Datenbanken von Programmprodukten, nicht doppelt oder sogar mehrfach geführt werden.

Erstellung eines z/OS-Notfallsystems

Durch Fehler in maßgeblichen Software-Komponenten, z. B. RACF (*Resource Access Control Facility*) oder Master-Katalog, kann es vorkommen, dass das gesamte System ausfällt. Bei Einzelsystemen muss für diesen Fall kurzfristig ein Notfallsystem zur Verfügung stehen, das ohne große Probleme gestartet werden kann und eine Reparatur des defekten Systems ermöglicht.

Im Gegensatz zu Backup-Systemen ist das Notfallsystem nicht für den Produktivbetrieb gedacht. Bei der Erstellung von Notfallsystemen sind die folgenden Hinweise zu berücksichtigen:

Unabhängigkeit

Das Notfallsystem muss komplett unabhängig von den Dateien und Definitionen der Produktionssysteme eingerichtet werden.

Reduktion auf das Wesentliche

Das Notfallsystem sollte nicht mehr Software-Funktionen enthalten, als unbedingt für eine Reparatur notwendig sind, damit für das System nicht mehr als eine Festplatte benötigt wird. Dazu gehören die Programme JESx (*Job Entry Subsystem*), VTAM (*Virtual Telecommunication Access Method*) und TSO (*Time Sharing Option*) mit den dazugehörenden ISPF-Dateien (*Interactive Support Programming Facility*). Es ist zu überlegen, ob ein System ohne JES ausreicht. Dann können jedoch keine Batch-Jobs eingesetzt werden.

Volume-Angaben

Alle Prozeduren sind mit *Volume*-Angaben zu versehen, um Abhängigkeiten von Katalogen zu vermeiden. Es sollten deshalb auch keine SMS-Dateien (*System Managed Storage*) verwendet werden.

VTAM-Terminals

Es muss eine möglichst einfache VTAM-Prozedur angelegt werden, bei der mindestens ein VTAM *Local Node* vorgesehen ist, der die Adresse einer MCS-Konsole (*Multiple Console Support*) beinhaltet. Damit ist es möglich, eine VTAM-Verbindung aufzubauen und sich an dem defekten System anzumelden. Bei Änderungen in den VTAM-Konfigurationen ist die Definition des VTAM *Local Node* entsprechend zu aktualisieren.

Komponenten des Notfall-Systems

Das Notfallsystem sollte auf einer Festplatte liegen, die mindestens die folgenden Dateien und Komponenten enthält:

- IPL-Text,
- Master-Katalog,
- JESx-Checkpoint und Spool-Datei,
- Page-Dataset,
- System-Dateien (MANx, STGINDEX, LOGREC, DAE),
- Parmlib, Proclib (Logon-Prozedur nicht vergessen),
- SMF-Dateien (SYS1.MANx),
- BROADCAST- und UADS-Dateien und
- RACF-Datenbank.

User-IDs für den Notfall

Es müssen mindestens zwei *User-IDs* auf dem Notfallsystem vorhanden sein, die wie die Notuser behandelt werden.

Permanente Pflege

Der Zutritt und der Zugang zum Notfallsystem müssen geschützt werden. Änderungen im normalen System müssen zeitnah auf dem Notfallsystem nachvollzogen werden, falls sie für das Notfallsystem relevant sind. Die Funktionsfähigkeit des Notfallsystems ist in periodischen Zeitabständen zu überprüfen.

Ergänzende Kontrollfragen:

- Gibt es ein Notuser-Verfahren?
- Ist die Festplatte bekannt, auf der die Sicherungskopie der RACF-Datenbank liegt?
- Gibt es ein z/OS-Backup-System?
- Gibt es bei Einzelsystemen ein Notfallsystem?

M 6.94 Notfallvorsorge bei Sicherheitsgateways

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Fehlerbehandlung bei Sicherheitsgateways

Sicherheitsgateways spielen eine zentrale Rolle im Hinblick auf die Verfügbarkeit der Netzanbindung einer Organisation. Fehler oder Ausfälle des Sicherheitsgateways oder einzelner Komponenten (von sporadisch auftretenden Fehlverhalten bis zum klar abzugrenzenden Ausfall eines Geräts und dadurch verursachten Netzausfällen) können unmittelbare und schwerwiegende Auswirkungen haben, wenn keine ausreichende Vorsorge für Notfälle getroffen wurde.

Um in derartigen Situationen effektiv und schnell reagieren zu können, müssen Diagnose und Fehlerbehebung bereits im Vorfeld geplant und vorbereitet werden. Für typische Ausfallszenarien und als Ergebnis von bereits aufgetretenen Störungen sollten Handlungsanweisungen erstellt werden. Kochbuchartige Dokumentationen aller notwendigen Schritte sind in Situationen, die schnelles Handeln erfordern, besonders hilfreich. Hierzu gehören neben Diagnose und Fehlerbehandlung auch die im normalen Betrieb notwendigen Administrationstätigkeiten. Letztere können typischerweise bereits in der vom Hersteller gelieferten Dokumentation enthalten sein. Für die tägliche Praxis ist es allerdings sinnvoll, eine Gesamtdokumentation in Form eines Betriebshandbuchs zu erstellen.

Protokollierung

Zu den Voraussetzungen für den Erfolg der Diagnosearbeiten gehört auch eine geeignete Protokollierung während des Betriebs (siehe auch M 4.47 *Protokollierung der Sicherheitsgateway-Aktivitäten*). Weiterhin sollten für die Fehlerbehandlung geeignete Werkzeuge genutzt werden.

Die Vorgehensweise bei der Fehlerbehandlung kann in die Bereiche Administration, Performancemessung und Diagnose unterteilt werden. Nachfolgend werden die jeweils zu berücksichtigenden Aspekte dargestellt. Für Router, die als Paketfilter Teil eines Sicherheitsgateway sind, sollte M 6.92 *Notfallvorsorge bei Routern und Switches* herangezogen werden.

Administration

In einem Betriebshandbuch für die einzelnen Komponenten des Sicherheitsgateways sollten alle notwendigen Kommandos und Arbeitsschritte zu Administration und Konfiguration dokumentiert werden. Aus Gründen der Übersichtlichkeit ist es empfehlenswert, dies für jede Komponente getrennt zu machen und zusätzlich ein Übersichtsdokument zu erstellen.

Folgende Bereiche sind zu berücksichtigen:

- Konfiguration des Betriebssystems, insbesondere die Konfiguration der Netzschnittstellen
- Update des Betriebssystems
- Konfiguration der "Funktionskomponenten" (Paketfilter, Sicherheitsproxies, Virenscanner usw.), insbesondere
  - wichtige Kommandos zum Starten und Beenden der Dienste

  - Speicherort und Format der Konfigurationsdateien oder -datenbanken, gegebenenfalls Benutzung der betreffenden Konfigurationswerkzeuge
  - bei Sicherheitsproxies (beispielsweise HTTP-Proxy, E-Mail-Gateway) auch Lage (Partition / Filesystem) der Datenverzeichnisse
- Protokollierung

Performance

Folgende Aspekte sollten für Aussagen über die Performance berücksichtigt werden:

- Eingehender und ausgehender Verkehr über die Paketfilter sowie für jedes der Protokolle, für die ein Sicherheitsproxy eingesetzt wird
- Statistikinformationen der verwendeten Protokolle

Diagnose

Für die Diagnose sollten alle notwendigen Kommandos und die zu erwartenden Ausgaben zur Anzeige des Betriebszustands aller Komponenten des Sicherheitsgateways und ihrer Konfiguration dokumentiert sein. Unter anderem sind folgende Informationen für die Fehlerdiagnose relevant:

- Gesamtkonfiguration als Überblick
- Status und Konfiguration der Netz-Interfaces und der sonstigen Anschlüsse
- Status der vorhandenen Netzdienste
- Prozesse
- Angemeldete Benutzer
- Protokollierung (Nutzung der Log-Level, Interpretation der Log-Informationen)

Weiterführende Maßnahmen sind in M 2.215 *Fehlerbehandlung* beschrieben.

Notfallvorsorge zur Steigerung der Verfügbarkeit

Durch eine Planung des Vorgehens bei Störungen kann die Zeit zur Wiederherstellung minimiert und unter Umständen eine Lösung überhaupt erst ermöglicht werden. Die Planungen sind mit der übergreifenden Störungs- und Notfallvorsorge abzustimmen und sollten sich am allgemeinen Notfallvorsorgekonzept orientieren (siehe Baustein B 1.3 *Notfallvorsorge-Konzept*). Hier werden generelle Vorgaben für Notfalldokumente im gesamten IT-Betrieb formuliert. Diese legen idealerweise einheitliche und verbindliche Anforderungen bezüglich Aufbau, Inhalt und Form fest.

Folgende Fragestellungen sind für die Konzeption der Notfallvorsorge relevant:

- Welche Anforderungen bestehen an das Monitoring?
  - Zusammenstellung der Informationen, die von den für den Betrieb der Netzkomponenten verantwortlichen Stellen immer ausgewertet werden (siehe auch Abschnitt Protokollierung)

  - Wie kann eine frühzeitige Störungserkennung sicher gestellt werden? Gibt es eventuell Tools, die eine automatische Alarmierung ermöglichen?
- Was sind Gründe für mögliche Störungen?
  - Angriffe
  - Hardware-Defekte
  - Zu geringe Dimensionierung (Ausfall bei Steigerung der Last)
- Welche Vorsorgemaßnahmen können getroffen werden?
  - Erarbeitung von Alternativkonfigurationen und "Fallback-Strategien" für bestimmte Ausfall- oder Angriffsszenarien (beispielsweise geändertes Routing, alternative Paketfilterregeln)
  - Ersatzgeräte- Implementierung von Failover-Lösungen, die im laufenden Betrieb ein Umschalten auf ein Alternativgerät ermöglichen
  - Wartungsverträge
  - Ausbildung der Mitarbeiter
- Welche Service Level Agreements bestehen oder sollten getroffen werden?
  - Hardware-Lieferanten (beispielsweise Vor-Ort-Austausch mit Zeitgarantie für bestimmte Komponenten, insbesondere bei Appliances)
  - Interne Service Level Anforderungen
- Wie ist eine Diagnose durchzuführen?
  - Statusabfragen
  - Anzeige der Konfiguration
  - Protokollierung
- Welche Entstörprozeduren müssen durchgeführt werden?
  - Vorgehen bei Ausfall des Komplettsystems (Wiederherstellen von Betriebssystem und Konfiguration)
  - Vorgehen bei Ausfall von Teilkomponenten (beispielsweise Speicher, Festplatten, Netzkarten)
- Wer ist im Schadensfall zu benachrichtigen?
  - Server- und Anwendungsadministration
  - Hardware-Lieferant / Ansprechpartner für den Wartungsvertrag
- Welche Dokumente müssen im Schadensfall verfügbar sein?
  - Konfiguration
  - Paketfilterregeln, Konfiguration für Sicherheitsproxies
  - Passwörter

Die Dokumentation sollte keinesfalls ausschließlich elektronisch vorliegen. Handlungsanweisungen sollten mindestens auch in Papierform existieren. Gegebenenfalls können Konfigurationsdateien auch auf CD-ROMs oder anderen Datenträgern gesondert hinterlegt werden.

Dokumentation auch in Papierform

- Wie verläuft der Wiederanlauf?
  - Abhängigkeiten zu anderen Bereichen des IT-Verbunds
  - Neuinstallation des Betriebssystems und Konfiguration
  - Zurückspielen einer gesicherten Konfiguration
  - Möglichkeiten eines eingeschränkten Betriebs.

Vorsicht beim eingeschränkten Betrieb

Bei der Planung für einen eingeschränkten Betrieb muss berücksichtigt werden, dass ein eingeschränkter Betrieb des Sicherheitsgateways nicht zur Folge haben darf, dass während dieser Zeit keine ausreichende Absicherung des eigenen Netzes gewährleistet ist. Im Zweifelsfall sollte lieber eine längere Ausfallzeit eines Dienstes hingenommen werden als die Gefahr, dass es wegen "eingeschränkter Sicherheit" zu weiteren Problemen kommt.

Vorgehensbeschreibungen auch erproben

Die für die Notfallvorsorge notwendigen Vorgehensbeschreibungen sind möglichst sorgfältig zu erstellen und regelmäßig zu erproben. Eventuell müssen unterschiedliche Vorgehensweisen bei unterschiedlichen Geräten und Betriebssystemen berücksichtigt werden.

Bei zentralen Komponenten wie beispielsweise den Paketfiltern des Sicherheitsgateways, der zwischen dem eigenen Netz und dem Internet eingerichtet ist, kann der Ausfall einer Komponente des Sicherheitsgateways den Ausfall der gesamten Internetanbindung nach sich ziehen. Die wahrscheinlich wichtigste Maßnahme zur Steigerung der Verfügbarkeit ist daher die Vorhaltung von Ersatzteilen oder Ersatzgeräten, um bei Hardware-Defekten die Ausfallzeiten zu minimieren. Alternativ oder auch als Ergänzung hierzu können Wartungsverträge mit dem Hersteller abgeschlossen werden, die durch garantierte Reaktions- oder sogar Reparaturzeiten die Verfügbarkeit sicherstellen. Hierdurch lassen sich Kosten für die Lagerhaltung reduzieren oder eine noch höhere Hardwareverfügbarkeit erreichen. Im Rahmen eines solchen Vertrages kann auch die Versorgung mit Software-Updates geregelt werden.

Ergänzende Kontrollfragen:

- Sind Störungs- und Notfallprozeduren in der Sicherheitsrichtlinie beschrieben?
- Wurden Verantwortlichkeiten im Notfall definiert?
- Werden Störungs- und Notfallprozeduren regelmäßig getestet?

M 6.95 Ausfallvorsorge und Datensicherung bei PDAs

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Ein PDA kann aus verschiedenen Gründen ausfallen oder in seiner Funktionsfähigkeit gestört sein. Dies ist natürlich besonders ärgerlich, wenn er dringend benötigt wird oder dadurch wichtige Daten verloren gehen. Daher sollten von vorne herein entsprechende Vorkehrungen getroffen werden, um einem Ausfall vorzubeugen bzw. die Probleme zu minimieren.

Energieversorgung

Der Ladezustand und die Funktionsfähigkeit des PDA-Akkus sollten regelmäßig überprüft werden (siehe auch M 4.31 *Sicherstellung der Energieversorgung im mobilen Einsatz*).

regelmäßige Datensicherung

Alle auf dem PDA gespeicherten Daten wie Telefonbucheintragungen, Notizen, etc. sollten in regelmäßigen Abständen auf einem anderen Medium gespeichert werden, damit sie im Zweifelsfall rekonstruiert werden können. Hierzu gibt es mehrere Möglichkeiten:

- Die wichtigsten Einstellungen wie Passwörter und die Konfiguration von Sicherheitsmechanismen sollten schriftlich dokumentiert und entsprechend ihres Schutzbedarfs sicher aufbewahrt werden.
- Der PDA sollte regelmäßig mit einem PC synchronisiert werden, dadurch werden schnell und bequem Kalendereinträge, Adressen und ähnliches mit denen auf dem PC abgeglichen. Dies ersetzt allerdings keine vollständige Datensicherung.
- Es sollte daher regelmäßig auch eine komplette Datensicherung des PDAs mit einem weiteren IT-System, z. B. einem Notebook oder einem Desktop, durchgeführt werden.
- Der PDA kann auch mit einem weiteren IT-System, z. B. einem Notebook oder einem Desktop, gekoppelt und die zu sichernden Daten auf diesem Weg ausgetauscht werden (siehe auch M 5.121 *Sichere Kommunikation von unterwegs*).
- Da bei PDAs der vorhandene Speicherplatz beschränkt ist, können die meisten Modelle mit externen Speichermedien erweitert werden (siehe auch M 4.232 *Sichere Nutzung von Zusatzspeicherkarten*). Verbreitet sind hierfür Speicherkarten, z. B. Memory-Cards, die den Vorteil haben, schnell wechselbar zu sein. Diese können auch eingesetzt werden, um unterwegs Backups durchzuführen, was vor allem dann sinnvoll ist, wenn ein PDA-Benutzer häufig lange abwesend ist und somit für längere Zeit keine Synchronisation zwischen IT-System und PDA stattfindet. Wie generell für Datensicherungen gilt auch hier, dass diese sicher verwahrt werden müssen. Wenn die Memory-Cards im PDA oder anderswo unbeaufsichtigt zurückgelassen werden können, können Unbefugte diese benutzen, um die darauf gespeicherten Daten auf einem ähnlichen System wiederaufzuspielen. Wenn anschließend die Memory-Card wieder zurückgelegt wird, werden dabei nicht einmal Spuren hinterlassen.

- Alle Daten, die auf austauschbaren Speicherkarten gespeichert sind, müssen ebenfalls gesichert werden, spätestens bei der nächsten Synchronisation.

Sicherheit der Daten im Flash-Speicher

Bei den meisten PDAs liegt das Betriebssystem in einem Flash-Speicher, der häufig auch genügend Platz für eine Datensicherung wenigstens der wichtigsten Daten wie die des Personal Information Manager bieten. Um dies komfortabel durchzuführen, gibt es je nach Hersteller mitgelieferte oder zusätzliche Tools. Hierbei sollte beachtet werden, dass nach einem kompletten Reset alle Daten außerhalb des Flash-Speichers gelöscht werden, also auch alle Passwörter zum Zugriffsschutz. Ein Angreifer kann damit leicht Zugriff auf den Flash-Speicher und die dort gespeicherten Daten erhalten. Bevor ein PDA weitergegeben wird, z. B. zur Reparatur oder an andere Benutzer, sollten daher alle Daten inklusive der im Flash-Speicher gelöscht werden.

Ersatz vorrätig halten

Wenn ein PDA kontinuierlich verfügbar sein soll, sollte immer ein Ersatz-Akku mitgeführt werden.

Reparatur

Bei einem PDA kann das komplette Gerät oder auch nur einzelne Komponenten defekt sein. Die Reparatur sollte nur von vertrauenswürdigen Fachbetrieben durchgeführt werden. Daher sollte eine Übersicht über entsprechende Fachbetriebe vorhanden sein.

Viele Händler bieten auch für die Dauer der Reparatur Ersatzgeräte an. Bei schnelllebigen Geräten wie PDAs lohnt sich eine Reparatur häufig nicht, so dass auch manchmal ein Tauschgerät angeboten wird. Da gerade ein PDA kontinuierlich zur Verfügung stehen sollte, ist bei der Auswahl des PDAs bzw. des Händlers darauf zu achten, dass solche Dienstleistungen angeboten werden.

Bevor ein PDA zur Reparatur gegeben wird, sollten alle personenbezogenen Daten, also z. B. gespeicherte E-Mails und das Telefonbuch im Gerät gelöscht werden (siehe auch M 2.4 *Regelungen für Wartungs- und Reparaturarbeiten*), soweit das noch möglich ist. Vorher sollten sie selbstverständlich gesichert werden. Außerdem sollten Zusatzkarten entfernt werden.

Ergänzende Kontrollfragen:

- Existiert eine Liste der Fachhändler für PDAs im Notfallplan?
- Werden die auf PDAs gespeicherten Daten regelmäßig gesichert?

M 6.96 Notfallvorsorge für einen Server

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der teilweise oder komplette Ausfall eines Servers kann gravierende Auswirkungen haben, wenn der Server wesentlicher Bestandteil innerbetrieblicher Arbeitsabläufe ist oder ein öffentlich zugängliches Angebot unterstützt (etwa in E-Commerce- oder E-Government-Anwendungen).

Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind.

Folgende Aspekte müssen dabei berücksichtigt werden:

Allgemeine Notfallplanung

- Die Notfallplanung für den Server muss in den existierenden Notfallplan integriert werden (siehe auch Baustein B 1.3 *Notfallvorsorge-Konzept*).

Regelmäßige Datensicherung

- Durch einen Systemausfall kann es auch zu Datenverlusten kommen. Daher ist im Rahmen des allgemeinen Datensicherungskonzepts (siehe auch B 1.4 *Datensicherungskonzept*) ein Datensicherungskonzept für den Server zu erstellen. Darin muss nicht nur der Server selbst berücksichtigt werden, sondern auch die Systeme, von denen der Betrieb des Servers abhängt.
- Im Rahmen von Wartungs- und Serviceverträgen oder durch eigene Lagerhaltung muss die Versorgung mit Ersatzteilen innerhalb einer Frist sichergestellt werden. Die Ausfallzeit ist daher auf ein tragbares Maß zu reduzieren. Bei besonderen Anforderungen an die Verfügbarkeit des Servers muss gegebenenfalls eine Hochverfügbarkeitslösung eingesetzt werden.

Dokumentation ist wichtig

- Die Systemkonfiguration muss dokumentiert werden. Wichtige Aufgaben müssen so beschrieben sein, dass das Gesamtsystem im Notfall auch ohne vorherige Kenntnis dieser Systemkonfiguration wiederhergestellt werden kann. Die Dokumentation sollte keinesfalls ausschließlich elektronisch vorliegen, sondern Handlungsanweisungen sollten auch in Papierform existieren. Gegebenenfalls können Konfigurationsdateien auch auf CD gesondert hinterlegt werden.
- Es muss ein Wiederanlaufplan erstellt werden, der das geregelte Hochfahren des Systems gewährleistet.

Vorgehensbeschreibungen überprüfen

- Alle notwendigen Vorgehensbeschreibungen müssen regelmäßig überprüft und geprobt werden. Eventuell müssen variierende Vorgehensweisen bei unterschiedlichen Betriebssysteme berücksichtigt werden.

Ergänzende Kontrollfragen:

- Existiert ein Notfallplan für den Ausfall des Servers?
- Gibt es entsprechende Notfallpläne für die anderen Systeme, die zum Betrieb des Servers benötigt werden?
- Existiert ein Datensicherungskonzept für den Server?
- Werden Störungs- und Notfallprozeduren regelmäßig getestet?

M 6.97 Notfallvorsorge für SAP Systeme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Wie für jedes andere IT-System muss auch für ein SAP System Notfallvorsorge betrieben werden. Damit die Vorbereitung zielgerichtet erfolgt, muss im Rahmen der Planungs- und Konzeptionsphase ein Notfallkonzept erstellt worden sein (siehe M 2.341 *Planung des SAP Einsatzes*), in dem auch die Notfälle definiert sind, die im Rahmen der Notfallvorsorge berücksichtigt werden sollen. Generell unterscheidet sich ein SAP System im Hinblick auf die Notfallvorsorge nicht von anderen IT-Systemen. Daher sind auch die Notfallvorsorge-Maßnahmen anderer relevanter Bausteine umzusetzen, die auf die IT-Systeme (z. B. Server-Rechner, Client-Rechner, Datenbank) anwendbar sind, aus denen das SAP System besteht.

Die Notfallvorsorge sollte mindestens folgende Maßnahmen umfassen und entsprechend der individuellen Anforderungen erweitert werden:

- Ein Notfall-Administrator sollte eingerichtet und Regelungen für den Einsatz festgelegt werden.
- Es müssen regelmäßige Datensicherungen des SAP Systems durchgeführt werden. Die Verfahrensweise und Häufigkeit ist im Datensicherungskonzept festzuhalten.
- Verfahren für das Wiederherstellen eines SAP Systems müssen festgelegt werden.
- Ein Ausweichsystem sollte bei entsprechend hohen Verfügbarkeitsansprüchen vorgehalten werden.

Je nach Einsatzszenario kann auch der Schutz vor Computer-Viren (siehe M 4.271 *Virenschutz für SAP Systeme*) zur Notfallvorsorge gehören.

Notfall-Administration

Für den Fall, dass mit normalen Administrator-Benutzerkennungen nicht mehr auf ein SAP System zugegriffen werden kann, wird ein Notfall-Administrator-Konto benötigt. Da ABAP- und Java-Stack jeweils mit einer eigenen Benutzerverwaltung ausgestattet ist, muss in jedem Stack ein Notfall-Administrator-Konto definiert werden.

Im ABAP-Stack kann dieses mit Berechtigungen ausgestattet werden, die der Summe der Profile SAP_ALL und SAP_NEW entsprechen. Damit besitzt der Notfall-Administrator vollständige Kontrolle über den ABAP-Stack des SAP Systems.

Im Java-Stack muss das Konto der Gruppe der Administratoren zugeordnet sein. Standardmäßig besitzt die Gruppe der Administratoren vollständige Kontrolle über den Java-Stack.

Seit NetWeaver 04 (Java 6.40) ist die Benutzerverwaltung in Java über die User Management Engine (UME) realisiert (siehe auch M 4.267 *Sicherer Einsatz der SAP Java-Stack Benutzerverwaltung*). Diese ist gruppen- und

rollenbasiert und unterstützt unterschiedliche Ablageorte für Benutzerkonten. Die Gruppe der Administratoren ist je nach Ablageort unterschiedlich benannt. Werden Benutzerkonten in einer Datenbank oder einem LDAP-Verzeichnis gespeichert, so heißt sie "Administrators". Werden die Benutzerkonten im ABAP-Stack gespeichert, so heißt sie "SAP_J2EE_ADMIN". Benutzer in dieser Gruppe haben keine kompletten administrativen Rechte, sondern nur Rechte für die Basisadministration und Benutzerverwaltung des Java-Stacks. Der generelle Notfallbenutzer für den Java-Stack ist das von SAP vorgegebene Benutzerkonto "SAP*", das aber nur dann verwendet werden kann, wenn der Java-Stack in den so genannten Single-User-Modus geschaltet wurde. In diesem Modus kann sich jedoch ausschließlich der Benutzer "SAP*" anmelden. Daher ist ein weiterer Notfallbenutzer erforderlich, der auch im Normalbetrieb einsetzbar ist.

Die Konten, die zur Notfall-Administration genutzt werden, sind mit starken Passwörtern auszustatten. Die verantwortlichen Personen müssen über den Aufbewahrungsort der Passwörter informiert sein. Nach einem Notfall sind die Passwörter so zu ändern, dass diese nur dann bekannt werden, wenn die Verfahren zur Notfall-Administration angewendet werden.

Es ist zu bedenken, dass die Konten, die zur Notfall-Administration verwendet werden, immer zugreifbar sein müssen. Sie dürfen also auch nicht deaktiviert oder gesperrt werden. Aus diesem Grund müssen die Zugangsdaten stark geschützt sein.

Wird ein Konto zur Notfall-Administration genutzt, ist nicht mehr nachzuvollziehen, welche Person auf das SAP System zugegriffen hat. Daher müssen die System-Administratoren und das IT-Sicherheitsmanagement über den Notfall zeitnah unterrichtet werden. Dabei sind folgende Informationen mitzuteilen:

- Welcher Notfall lag vor?
- Durch wen und wann erfolgte der Zugriff?
- Welche Aktivitäten und Änderungen sind erfolgt?

Backup

Zu den regelmäßig durchzuführenden Maßnahmen der Notfallvorsorge gehört die Datensicherung eines SAP Systems. Im Rahmen des institutionsweiten Backup-Konzeptes muss während der Planungsphase auch die Datensicherung für ein SAP System konzipiert werden.

Die Daten eines SAP Systems werden zwar vornehmlich in der Datenbank abgelegt, die Datensicherung reduziert sich jedoch nur bei reinen ABAP-Stack-Installationen (z. B. bei SAP R/3 Systemen) darauf, lediglich die Datenbank zu sichern. Insbesondere der Java-Stack erfordert, dass weitere Daten gesichert werden. Dies sind vor allem die Daten aus dem SAP Verzeichnisbaum des Dateisystems.

Für den Java-Stack sind außerdem Sicherungen der Daten (z. B. weitere Datenbanken oder Dateien) durchzuführen, auf die die installierten Applikationen zurückgreifen. Werden diese nicht gesichert, kann es zu Inkonsistenzen in den Applikationsdaten kommen. Die verantwortlichen Administratoren müssen außerdem über den Aufbewahrungsort der Backup-Medien und über den Prozess der Wiederherstellung informiert sein.

und über den Prozess der Wiederherstellung informiert sein.

SAP Informationsquellen

Weitere Dokumentationen werden in M 2.346 *Nutzung der SAP Dokumentation* beschrieben.

Ausweichsystem

Kleine Unternehmen und Behörden betreiben unter Umständen ein SAP System, bei dem alle Komponenten auf einem Rechner (Single-Server-Installation) installiert sind. Liegt ein Notfall vor, der nicht durch das Einspielen gesicherter Daten behoben werden kann, z. B. bei einem Hardware-Defekt, so ist ein Ersatzsystem zu beschaffen. Da eine Ersatzbeschaffung in der Regel Zeit kostet, kann es zu langen Ausfallzeiten kommen. Daher wird empfohlen, ein Ausweichsystem vorzuhalten, das so weit vorbereitet ist, dass nur noch die letzte Datensicherung eingespielt werden muss, um den Betrieb wieder aufzunehmen.

Ergänzende Kontrollfragen:

- Gibt es ein Notfallvorsorge-Konzept für SAP Systeme?
- Ist ein Notfall-Administrator eingerichtet?
- Ist den verantwortlichen Mitarbeitern bekannt, wo die Zugangsdaten für den Notfall-Administrator aufbewahrt werden?
- Werden regelmäßig Datensicherungen des SAP Systems durchgeführt?
- Ist bekannt, wo die Backup-Medien aufbewahrt werden und wie ein SAP System aus einem Backup wiederhergestellt wird?
- Existiert ein Ausweichsystem?

M 6.98 Notfallvorsorge für Speichersysteme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, Administrator

Fehlerbehandlung bei Speichersystemen

In jedem IT-Betrieb treten Störungen auf, die vom sporadischen Fehlverhalten von Komponenten bis zum klar abzugrenzenden Ausfall eines Geräts reichen können. Grundlage eines sicheren Betriebs ist die Vorbereitung auf Störungssituationen. Hierzu gehören Ausfälle oder Beeinträchtigungen von Hardware und Software beispielsweise auf Grund von Defekten oder Kompromittierungen.

Um in derartigen Situationen effektiv und schnell reagieren zu können, müssen Diagnose und Fehlerbehebung bereits im Vorfeld geplant und vorbereitet werden. Für typische und für bereits aufgetretene Ausfallszenarien sollten Handlungsanweisungen erstellt werden. Eine kochbuchartige Dokumentationen von Maßnahmen und Kommandos, die die Fehleranalyse und Fehlerkorrektur unterstützen, ist besonders hilfreich.

Gerade bei komplexen Systemen wie einem Speichersystem ist die Darstellung von Verknüpfungen und Abhängigkeiten, die individuell für die Institution sind, entscheidend für die Beurteilung von Störungen und schnelles und sicheres Eingreifen.

Fehlerbehandlung

Zu den Voraussetzungen für den Erfolg der Diagnosearbeiten gehört eine geeignete Protokollierung während des Betriebs (siehe auch M 2.359 *Überwachung und Verwaltung von Speichersystemen*). Weiterhin sollten für die Fehlerbehandlung geeignete Werkzeuge genutzt werden. Dazu existieren sowohl frei verfügbare als auch kommerzielle Programme, oft auch vom Hersteller der Geräte. Die Verwendung geeigneter Werkzeuge ist umso wichtiger, da bei komplexen Systemen nicht die Kontrolle und Steuerung der einzelnen Komponente, sondern die Übersicht über das Zusammenwirken von Hard- und Software des oftmals sehr heterogenen Gesamtsystems gefordert ist.

Es muss klar sein, dass gerade bei Speichersystemen nach Störungen und Notfällen eine Rückführung in den Normalbetrieb nur dann möglich ist, wenn eine brauchbare Datensicherung bereit steht. Eine Prüfung der Wiederherstellbarkeit von Datensicherungen (siehe M 6.22 *Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen*) muss regelmäßig durchgeführt werden.

Die Vorgehensweise bei der Fehlerbehandlung von Speichersystemen lässt sich in die Bereiche Administration, Performancemessung und Diagnose unterteilen. Nachfolgend werden die jeweils zu berücksichtigenden Aspekte dargestellt:

Administration

In einem Betriebshandbuch sollten alle notwendigen Kommandos zu Administration und Konfiguration dokumentiert werden.

Folgende Bereiche sind zu berücksichtigen:

- Einrichten von (administrativen) Nutzern, Vergabe von Berechtigungen
- Update von Firmware und Betriebssystem
- Konfiguration
  - der Speicherressourcen
  - der administrativen Zugänge
  - der angeschlossenen Server und Sicherungsgeräte
- Protokollierung

Performance

Folgende Aspekte sollten für Beobachtungen und Aussagen über die Performance berücksichtigt werden:

- Belegung der Medien (pro logischem oder physischem Gerät)
- Durchsatz pro Interface
- Statistikinformationen zur Benutzung

Diagnose

Alle für die Fehlerdiagnose notwendigen Kommandos sowie die zu erwarteten Aussagen und ihre Bedeutung sollten dokumentiert sein. Dazu zählen beispielsweise Aussagen über die Zustände der verschiedenen Systemkomponenten, Schnittstellen sowie Aussagen über die aktuellen Konfigurationen.

Unter anderem sind folgende Informationen für die Fehlerdiagnose relevant:

- Status der Netz-Interfaces und der sonstigen Anschlüsse
- Status der Netzdienste (TCP/IP bei NAS-Systemen, spezifische Informationen beim SAN, z. B. Status der SAN-Switches)
- Gesamtkonfiguration als Überblick
- Prozesse
- Zuordnung
- Angemeldete Benutzer
- Protokollierung (Nutzung der Log-Level, Interpretation der Log-Informationen)

Notfallvorsorge zur Steigerung der Verfügbarkeit

Durch eine Planung des Vorgehens bei Störungen kann die Zeit zur Wiederherstellung minimiert und unter Umständen eine Lösung überhaupt erst ermöglicht werden. Die Planungen sind mit der übergreifenden Störungs- und Notfallvorsorge abzustimmen und sollten sich am allgemeinen Notfallvorsorgekonzept orientieren (siehe Baustein B 1.3 *Notfallvorsorge-Konzept*). Hier werden generelle Vorgaben für Notfalldokumente im gesamten IT-Betrieb formuliert. Diese legen idealerweise einheitliche und verbindliche Anforderungen beziehungsweise Aufbau, Inhalt und Form fest.

Die genauen Verfügbarkeitsanforderungen an die Speichersysteme müssen klar definiert sein.

Folgende Fragestellungen sind für die Notfallvorsorge relevant:

- Was sind Gründe für mögliche Störungen?
  - Hardware-Defekte
  - Zu geringe Dimensionierung (Störung oder Ausfall bei Steigerung der Nutzung)
- Welche Anforderungen bestehen an das Monitoring?
- Wie kann eine frühzeitige Störungserkennung sicher gestellt werden?
- Zusammenstellung der Informationen, die von den für den Betrieb der Speichersysteme verantwortlichen Stellen immer ausgewertet werden
- Welche Vorsorgemaßnahmen können getroffen werden?
  - Ersatzgeräte
  - Ersatzteile
  - Implementierung von Failover-Lösungen, die im laufenden Betrieb ein Umschalten auf ein Alternativgerät ermöglichen
  - Wartungsverträge
  - Ausbildung der Mitarbeiter
- Welche Service Level Agreements (SLAs) sollten getroffen werden?
  - Hardware-Lieferanten (beispielsweise Vor-Ort-Austausch mit Zeitgarantie für bestimmte Komponenten)
  - Verwaltung der Service Level Agreements: Es muss sichergestellt werden, dass SLAs rechtzeitig verlängert werden beziehungsweise rechtzeitig an die aktuellen Anforderungen angepasst werden.

Verwaltung von Service Level Agreements:

SLAs werden in der Regel für einen begrenzten Zeitraum abgeschlossen und nicht immer automatisch verlängert. Darüber hinaus passiert es häufig, dass die Preise für die Verlängerung von SLAs für längere Zeiträume deutlich steigen oder dass diese für veraltete Systeme gar nicht mehr angeboten werden, so dass möglicherweise eine Investition in neuen Speichersystemen günstiger ist. Dies muss rechtzeitig bedacht und geplant werden.

Dokumentation zur Notfallvorsorge

Das genaue Vorgehen in bestimmten Notfallsituationen muss in einem Notfallplan beschrieben werden. Dies beinhaltet folgende Punkte:

- Wie ist eine Diagnose durchzuführen? Folgende Informationen können dabei behilflich sein:

  - Statusabfragen
  - Anzeige der Konfiguration
  - Anzeige der laufenden Prozesse
  - Angemeldete Nutzer
  - Protokollierung
- Welche Entstörungsprozeduren müssen durchgeführt werden?
  - Vorgehen bei Ausfall des Komplettsystems (Wiederherstellen von Betriebssystem und Konfiguration)
  - Vorgehen bei Ausfall von Teilkomponenten, beispielsweise Speicher
- Wer ist im Schadensfall zu benachrichtigen?
  - Server- und Anwendungsadministration
  - Hardware-Lieferant/Ansprechpartner für den Wartungsvertrag
  - Alle notwendigen Informationen zu den Wartungsverträgen und Service Level Agreements, Hotline-Nummern, Kunden- oder Geräteidentifikationsnummern
- Welche Dokumente müssen im Schadensfall verfügbar sein?
  - Grundkonfiguration zur (Wieder-)Inbetriebnahme
  - Änderungen der Grundkonfiguration um die aktuelle Betriebskonfiguration einzurichten
  - Regelwerk für die Zugriffskontrolle (Access Control Lists)
  - Eingerichtete Benutzer und Berechtigungen
  - Passwörter für Notfall-Zugriffe
- Wie verläuft der Wiederanlauf?
  - Abhängigkeiten zu anderen Systemen des IT-Verbunds
  - Neuinstallation des Betriebssystems und Konfiguration
  - Zurückspielen einer gesicherten Konfiguration
  - Möglichkeiten eines eingeschränkten Betriebs
  - Remote-Betrieb an einem anderen Standort

Vorgehensbeschreibungen auch erproben

Die für die Notfallvorsorge notwendigen Vorgehensbeschreibungen sind möglichst sorgfältig zu erstellen und regelmäßig zu erproben. Eventuell müssen variierende Vorgehensweisen bei unterschiedlichen Gerätetypen und Betriebssystemen berücksichtigt werden.

Dokumentation auch in Papierform

Die Dokumentation sollte keinesfalls ausschließlich elektronisch vorliegen. Handlungsanweisungen sollten mindestens auch in Papierform existieren. Gegebenenfalls können Konfigurationsdateien auch auf CD-ROM gesondert hinterlegt werden.

Die wahrscheinlich wichtigste Maßnahme zur Steigerung der Verfügbarkeit ist die Vorhaltung von Ersatzteilen, um bei Hardware-Defekten die Ausfallzeiten

zu minimieren. Alternativ oder auch als Ergänzung hierzu können Wartungsverträge mit dem Hersteller abgeschlossen werden, die durch garantierte Reaktions- oder sogar Reparaturzeiten die Verfügbarkeit sicherstellen. Hierdurch lassen sich Kosten für die Lagerhaltung reduzieren oder eine noch höhere Hardwareverfügbarkeit erreichen. Im Rahmen eines solchen Vertrages kann auch die Versorgung mit Software-Updates geregelt werden.

Ergänzende Kontrollfragen:

- Gibt es einen schriftlichen Notfallplan für die Speichersysteme?
- Ist dieser zugänglich aufbewahrt, besonders auch im Falle eines Katastrophe, welcher den Zugang zum Rechenzentrum erschwert oder behindert?
- Ist der Notfallplan aktuell? Wie wird die Aktualität sichergestellt?
- Wurden Verantwortlichkeiten im Notfall definiert?
- Werden Störungs- und Notfallprozeduren regelmäßig getestet?
- Kann der Notfallplan auch von einem anderen Mitarbeiter (der den Plan nicht selbst geschrieben hat oder der kein entsprechender Systemspezialist ist) ausgeführt werden?

M 6.99 Regelmäßige Sicherung wichtiger Systemkomponenten für Windows Server 2003

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Verantwortliche für die Datensicherung

Datensicherungskonzept

Die Systemkomponenten des Windows Server 2003 sind regelmäßig zu sichern, da der Server in Abhängigkeit von seiner Serverrolle ständigen Konfigurationsänderungen unterliegt. Unbeabsichtigte Änderungen, die Fehler im System provozieren können, z. B. fehlerhaftes Einspielen von Updates, können die Wiederherstellung wichtiger Systemkomponenten erforderlich machen. Wichtige Systemkomponenten sind nicht nur die eigentlichen Systemdateien, sondern auch Konfigurationsdaten (z. B. Registrierdatenbank, IIS-Metabase, Konfigurationsdateien), Statusinformationen (Registrierdatenbank, Datenbanken von DHCP, WINS usw.) und Protokolldaten. Die Sicherung kann von einem Sicherungsprogramm durchgeführt werden oder selektiv über das Dateisystem erfolgen, zum Beispiel per Skript. Generell müssen zumindest Statusinformationen und Protokolldaten täglich im Rahmen der Vorgaben eines Datensicherungskonzepts (siehe Baustein B 1.4 *Datensicherungskonzept*) gesichert werden.

Systemstatussicherung (*System State*)

Sicherungsprogramm

Das Sicherungsprogramm von Windows Server 2003 (*Sicherung*) enthält den vordefinierten Sicherungsvorgang *Systemstatussicherung* (engl. *System State*). Er deckt in der Regel alle wichtigen Systemkomponenten aller Serverrollen ab, die in Windows Server 2003 mitgeliefert werden.

Systempartition und Festplattenpartitionen

Wichtige Systemkomponenten können sich sowohl in der Systempartition als auch auf anderen Festplattenpartitionen befinden. Dies hängt unter anderem davon ab, ob bei der Installation einer Komponente alternative Installationspfade konfiguriert wurden, z. B. für Protokolldateien.

Systemstatussicherung

Die Systemdaten können mit dem Sicherungsprogramm gesichert werden. Dabei ermöglicht die Verwendung der Systemstatussicherung des Sicherungsprogramms

- das Sichern von Active Directory, während der Domänencontroller online ist,
- das Sichern mithilfe von Skripten oder Batchdateibefehlen,
- den regelmäßigen Aufruf der Sicherung unter Verwendung von *Geplante Tasks*,
- das Sichern auf Wechselmedien, auf einem Netzlaufwerk oder in einer Datei,
- das Sichern anderer System- und Datendateien mit Konfigurationsinformationen von installierten Serverrollen.

Wenn das Sicherungsprogramm z. B. auf einem Domänencontroller verwendet wird, werden mit Auswahl des Systemstatus unabhängig vom bei der Installation gewählten Speicherort alle Systemkomponenten und alle verteilten Dienste gesichert, auf die Active Directory angewiesen ist.

Beispiele für Systemstatusdaten:

Systemstatusdaten nach Grundinstallation:

- Systemstartdateien
- Systemregistrierung
- Klassenregistrierungsdatenbank von COM+ (einer Erweiterung zu Component Object Model)
- Protokollierungsdateien
- Zusätzliche Systemstatusdaten auf einem Domaincontroller (exemplarisch):
  - Verzeichnis SYSVOL
  - DNS-Datenbank
  - Active Directory

Beispiele für weitere rollenspezifische Systemstatusdaten:

- Clusterdienststatus (soweit installiert)
- Zertifikatsdienste-Datenbank (soweit installiert)

Es ist zu prüfen, ob entsprechend der Serverrolle und der installierten Serverprodukte auf Basis von Windows Server 2003 noch weitere System- und/oder Programmordner außerhalb des vordefinierten Systemstatus gesichert werden müssen. Hierfür kann es erforderlich sein, die gesamte Systempartition sowie weitere Partitionen zu sichern.

Sicherungsprogramme

Programme anderer Hersteller

Das Sicherungsprogramm *Sicherung* beinhaltet nur Grundeigenschaften eines Datensicherungsprogramms und genügt nur einem geringen Schutzbedarf. Das Programm *Sicherung* bzw. die NT-Backup-API-Schnittstelle ist lediglich für die Sicherung der Windows Server 2003-eigenen Systemstatusdateien ausreichend. Es ist unter anderem bei der Zuverlässigkeit (Prüfungsmechanismen führen keine Checksummenbildung durch) und Hardwareunterstützung eingeschränkt und bietet nur rudimentäre Protokollierung, Überwachung, und Zeitplanung. Es ist entsprechend der Serverrolle und den Anforderungen an die Datensicherung zu prüfen, ob Programme anderer Hersteller zu bevorzugen sind. Diese sollten die NT-Backup-API unterstützen.

Wiederherstellen von Systemstatusdaten

Komplette Systemstatussicherung und die teilweise Wiederherstellung

Das Windows-Sicherungsprogramm kann nur die komplette Systemstatussicherung wiederherstellen. Programme von Drittanbietern ermöglichen z. T. die Wiederherstellung von Konfigurationsdaten einzelner Rollen, z. B. Active Directory. In jedem Fall muss vor der Wiederherstellung das Basisbetriebssystem identisch eingerichtet worden sein, sonst schlägt die Wiederherstellung entweder ganz fehl oder hinterlässt ein System mit nicht lauffähigen Parametern. Es ist zu klären:

Basisparameter

- Welches Service Pack wird verwendet?
- Welche Edition von Windows Server 2003 ist im Einsatz?

- Welcher Lizenzierungstyp wurde gewählt?
- Auf welche Weise muss die Produktaktivierung durchgeführt werden?
- Wie lautet der Computername?
- Wie wurde die Hardware konfiguriert? (Geringe Änderungen der Hardware können durch Plug and Play kompensiert werden.)

Wiederherstellung auf separatem Testsystem

Die Wiederherstellung des Systemstatus sollte niemals auf einem produktiven Server durchgeführt werden, auch nicht zu Überprüfungszwecken. Zur Umsetzung von M 6.41 *Übungen zur Datenrekonstruktion* kommt nur ein separates Testsystem in Frage. Genügt dies nicht dem Schutzbedarf des Systems, muss über alternative Sicherungsstrategien für den Systemstatus nachgedacht werden (z. B. Festplatten-Abbilder, Servervirtualisierung).

Beispiel für ein Überprüfungsszenario:

Die Systempartition befindet sich auf einem Laufwerk mit RAID-Level 1 (Spiegelung). Eine Festplatte wird aus dem RAID-Verbund entfernt und offline geschaltet, so dass der Originalzustand des Systems konserviert wird. Anschließend wird die Wiederherstellung des Systemstatus probeweise durchgeführt und das System auf seine Lauffähigkeit hin überprüft. Nach Abschluss des Tests wird die zuvor entfernte Platte wieder online geschaltet und zurückgespiegelt, so dass der Originalzustand wiederhergestellt ist.

Notfallwiederherstellung (Disaster Recovery)

ASR: Sicherungsfunktion und Wiederherstellungsfunktion

Die in dem Datensicherungsprogramm von Windows Server 2003 enthaltene Sicherungskomponente *Automatische Systemwiederherstellung* (Automated System Recovery, ASR) besteht aus zwei Funktionen. Zum einen gibt es eine Sicherungsfunktion, die aus dem Programm *Sicherung* aufgerufen wird, und zum anderen eine Wiederherstellungsfunktion, die bei der Windows-Server-2003-Installationsroutine mit *F2* aufgerufen werden kann. Bei der vorbereitenden Erstellung des ASR-Datensatzes werden die Systemstatusdaten, Systemdienste und alle mit den Betriebssystemkomponenten verknüpften Datenträger in eine Datei gesichert. Weiterhin wird bei der Erstellung eine Diskette mit Informationen zur Sicherung, zu Datenträgerkonfigurationen, wie Basisvolumen und dynamische Volumen und zu Informationen über die Wiederherstellung erstellt. Bei der Wiederherstellung mit ASR werden keine Nutzdaten wiederhergestellt. Die ASR-Wiederherstellung stellt lediglich das Grundbetriebssystem bereit. Die Nutzdaten und andere serverrollenabhängige, wichtigen Systemkomponenten müssen mit einer separaten Sicherung gesichert und gegebenenfalls wiederhergestellt werden. Sollte es entsprechend der Serverrolle Systemkomponenten geben, die nicht in einer Standardsicherung enthalten sind, ist zu prüfen, welches Verfahren zur Sicherung der wichtigen Systemkomponenten geeignet ist. ASR ist in so einem Falle nicht ausreichend. Weiterhin ist zu beachten, dass bei dem Verfahren Disketten (und damit ein unzuverlässiges Wechselmedium) notwendig sind und keine automatische regelmäßige Sicherung möglich ist. Daher ist zu empfehlen, die für die Serverrolle geeignete Variante zur Sicherung wichtiger Systemdaten zu wählen und

dieses Verfahren regelmäßig zu testen. Hierbei sind nicht nur Erfolg der Wiederherstellung, sondern insbesondere auch die benötigte Wiederherstellungszeit ausschlaggebend (siehe M 6.76 *Erstellen eines Notfallplans für den Ausfall von Windows 2000/XP/2003-Systemen*).

Ergänzende Kontrollfragen:

- Werden Protokoll- und Systemstatusdaten des Windows Server 2003 Systems täglich gesichert?
- Wurde geprüft, ob die vordefinierte Systemstatussicherung vom Umfang her ausreichend ist?
- Wurde geprüft ob der Einsatz von Sicherungsprodukten von Drittherstellern notwendig ist?
- Ist sichergestellt, dass vor der Wiederherstellung von Systemstatusdaten das Basisbetriebssystem identisch eingerichtet wird und eine Wiederherstellung nicht auf einem produktiven System erfolgt?
- Werden entsprechend der Serverrolle und der Verfügbarkeitsanforderungen die Wiederherstellung und die Wiederherstellungsdauer im Rahmen eines Notfallplans für den Server getestet und verbessert?

M 6.100 Erstellung eines Notfallplans für den Ausfall von VoIP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Der teilweise oder komplette Ausfall der VoIP-Architektur hat in vielen Fällen gravierende Auswirkungen, denn die Telefonie ist meist einer der wichtigsten Dienste in einer Institution. Ein Ausfall kann viele Ursachen haben. Neben VoIP-typischen Problemen kann auch eine Störung einzelner Netzkomponenten zum vollständigen Ausfall des VoIP-Dienstes führen.

Im Rahmen der Notfallvorsorge ist daher ein Konzept zu entwerfen, wie die Folgen eines Ausfalls minimiert werden können und welche Aktivitäten im Falle eines Ausfalls durchzuführen sind.

Folgende Aspekte müssen dabei berücksichtigt werden:

- Die Notfallplanung für VoIP muss in den existierenden Notfallplan integriert werden (siehe auch Baustein B 1.3 *Notfallvorsorge-Konzept*).
- Bei einem Ausfall von VoIP muss eine Telekommunikation weiter möglich sein. Daher ist zu klären, ob beim VoIP-Ausfall zumindest eine Notfall-Kommunikation möglich ist (zumindest zu Polizei, Feuerwehr). Außerdem muss es möglich sein, einen (externen) Support-Dienstleister zeitnah über den Ausfall zu informieren, damit der Fehler behoben werden kann. Bei einem Ausfall können beispielsweise Mobiltelefone zur Kommunikation genutzt werden, hierfür ist aber Vorsorge zu treffen.
- Durch einen Systemausfall kann es auch zu Datenverlusten kommen. Daher sind im Rahmen des allgemeinen Datensicherungskonzepts (siehe auch B 1.4 *Datensicherungskonzept*) Regelungen für die VoIP-Komponenten zu erstellen. Darin muss nicht nur die VoIP-Middleware selbst berücksichtigt werden, sondern auch die Endgeräte mit den von Benutzern vorgenommen Einstellungen, wie beispielsweise Telefonbücher.
- Es müssen Vorkehrungen für den Fall getroffen werden, dass ein IT-System, auf dem ein Softphone betrieben wird, repariert werden soll. Müssen die Anwender für die Erfüllung ihrer Aufgaben telefonisch erreichbar sein, sind entsprechende Maßnahmen zu treffen.

Ergänzende Kontrollfragen:

- Existiert ein Notfallplan für den Ausfall von VoIP?
- Gibt es redundante Telefonlösungen, wie zum Beispiel Mobiltelefone?

M 6.101 Datensicherung bei VoIP

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Um bei Fehlkonfigurationen oder einem Ausfall, der nur durch den Austausch einer Komponente behoben werden kann, den VoIP-Betrieb schnell wieder aufnehmen zu können, müssen regelmäßig Sicherungen aller wichtigen Konfigurationsdateien angefertigt werden. Für die Datensicherung ist grundsätzlich die im Baustein B 1.4 *Datensicherungskonzept* genannte Vorgehensweise zu verwenden. Der Umfang der zu sichernden Dateien muss anhand der eingesetzten VoIP-Komponente ermittelt werden. Hierzu gehören unter anderem

- alle VoIP-spezifischen Konfigurationseinstellungen,
- übergeordnete Konfigurationseinstellungen, wie IP-Adressen, Passwörter und alle relevanten Konfigurationen des eingesetzten Betriebssystems,
- Protokolldaten und
- vom Benutzer individuell vorgenommene Einträge, wie persönliche Telefonbücher.

Diese Konfigurationseinstellungen müssen regelmäßig gesichert werden. Vor und nach jeder Änderung der Konfiguration ist ebenfalls eine Sicherung durchzuführen. Dabei ist darauf zu achten, dass mehrere Versionen (Generationen) der Sicherungsdateien gepflegt werden. Eine fehlerhafte Konfiguration kann durch das Einspielen der Version, die davor generiert wurde, oft behoben werden.

Es muss berücksichtigt werden, dass nach einem Release-Wechsel die vorhandenen Konfigurationsdateien eventuell nicht übernommen werden können. Wird nach einem Hardware-Ausfall ein Gerät mit einem aktuelleren oder älteren Release eingesetzt, können die vorhandenen Konfigurationsdateien eventuell nicht direkt übernommen werden. Daher sind bei einem Austausch aktuelle Hersteller-Informationen, beispielsweise aus Changelog-Dateien, zu sichten und zu berücksichtigen. Müssen die Konfigurationsdateien bei einem Release-Wechsel angepasst werden, muss sowohl die alte als auch die neue Version gesichert werden. Bei Problemen mit dem neueren Release kann auf diese Weise auch zu einem späteren Zeitpunkt auf die alte, eventuell stabilere Version gewechselt werden.

Die Datensicherung ist auf IT-Systemen und Medien durchzuführen, die von den für den Betrieb verwendeten IT-Systemen und Medien unabhängig sind. Dies können zum Beispiel Bandlaufwerke, CD-RWs oder andere IT-Systeme sein. Bei der Übertragung auf ein anderes System über ein Netz sollte überlegt werden, die Daten zu verschlüsseln oder über eigenes Administrationsnetz zu übertragen, um sie vor Abhören und Manipulationen zu schützen.

Es müssen regelmäßig Recovery-Übungen durchgeführt werden, um die Wiederherstellbarkeit der Sicherung zu prüfen (siehe hierzu auch M 6.41 *Übungen zur Datenrekonstruktion*).

Ergänzende Kontrollfragen:

- Werden die Konfigurationsdateien regelmäßig gesichert?
- Wird regelmäßig überprüft, ob die gesicherten Daten wiederhergestellt werden können?

M 6.102 Verhaltensregeln bei WLAN-Sicherheitsvorfällen

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Falls sich das WLAN in nicht vorgesehener Weise verhält (z. B. WLAN ist längere Zeit nicht verfügbar, Zugriff auf Netzressourcen ist nicht möglich, Netzperformance bricht dauerhaft ein), kann dies durch einen Sicherheitsvorfall verursacht worden sein. Dieser kann durch einen Angreifer, Fehlkonfigurationen oder Systemfehler herbeigeführt worden sein.

Das sollten Benutzer beachten

Dann sollten die Benutzer folgende Punkte beachten:

- Sie sollten ihre Arbeitsergebnisse sichern, den WLAN-Zugriff beenden und die WLAN-Schnittstelle ihres Clients deaktivieren.
- Sollten Fehlermeldungen erscheinen oder sich der Client nicht normal verhalten haben, so sollten diese durch die Benutzer genau dokumentiert werden. Ebenso sollte dokumentiert werden, was der Benutzer getan hat bevor bzw. während der Sicherheitsvorfall eingetreten ist. Dadurch kann der Grund für den Vorfall durch die Administratoren eventuell schneller eingegrenzt und schneller Gegenmaßnahmen eingeleitet werden.
- Die Administratoren müssen über eine geeignete Eskalationsstufe (z. B. User Help Desk) von den Benutzern benachrichtigt werden. Dabei ist sicherzustellen, dass der Administrator durch den Benachrichtigungsprozess in seiner Arbeit nicht wesentlich behindert wird.

Gegenmaßnahmen durch die Administratoren

Die Administratoren sollten bei einem Sicherheitsvorfall passende Gegenmaßnahmen einleiten. Mögliche Aktionen sind z. B.:

- Abschaltung von Access Points
- Sperren der Kommunikation am Übergabepunkt zwischen Distribution System und LAN / Internet
- Herunterfahren von Servern (Web-Server oder Steuerungsserver im Produktionsumfeld oder ähnliches)
- Deaktivierung der WLAN-Schnittstelle des WLAN-Clients
- Überprüfung der Konfigurationen der Access Points
- Sicherung aller Dateien, die Aufschluss über die Art und Ursache des aufgetretenen Problems geben könnten (z. B. ob tatsächlich ein Angriff erfolgt ist und auf welche Weise der Angreifer eindringen konnte), d. h. insbesondere Sicherung aller relevanten Protokolldateien
- gegebenenfalls Wiedereinspielen der Original-Konfigurationsdaten (siehe M 6.52 *Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten*)
- Benachrichtigung der Benutzer mit der Bitte, ihre Arbeitsbereiche auf Unregelmäßigkeiten zu prüfen.

Falls Access Points gestohlen worden sind, müssen gezielte Sicherheitsmaßnahmen ergriffen werden, wie z. B.:

- Änderung aller eingesetzten kryptographischen Schlüssel, also z. B. der PSKs im Falle der Verwendung von WPA-PSK bzw. WPA2-PSK
- Konfigurationsänderung auf RADIUS-Servern zum Ausschluss des entwendeten Access Point (IP, Name, RADIUS-Client, Shared Secret, IPSec)

Die möglichen Konsequenzen sicherheitskritischer Ereignisse müssen untersucht werden. Letztlich sind alle erforderlichen Maßnahmen zu ergreifen, um eine missbräuchliche Verwendung von entwendeten Geräten zum Zugriff auf das Netz der Institution auszuschließen. Falls ein WLAN-Client entwendet worden ist, müssen bei der Verwendung einer zertifikatsbasierten Authentisierung auch die Client-Zertifikate gesperrt werden.

Ergänzende Kontrollfragen:

- Ist sichergestellt, dass ein Administrator effektiv benachrichtigt wird?
- Kennen Benutzer und Administratoren alle erforderlichen Verhaltensregeln bei WLAN-Sicherheitsvorfällen?
- Werden die möglichen Konsequenzen sicherheitskritischer Ereignisse analysiert?