FERCHAU ENGINEERING

<atFERCHAU #16>

DAS IT-MAGAZIN VON FERCHAU ENGINEERING

<06>

<DAS ROTKÄPPCHEN-SYNDROM>

IT-Schwachstelle Mensch: freundlich, neugierig, hilfsbereit

FERCHAU IST TOP ARBEITGEBER

VIELFACH AUSGEZEICHNET

Best of Corporate Publishing 2015

Live long and prosper!

Liebe Leserinnen, liebe Leser,

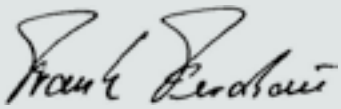
1966, im Gründungsjahr von FERCHAU, entwickelte Professor Joseph Weizenbaum ein experimentelles Programm namens »Eliza«. Dadurch konnten Menschen Sätze natürlicher Sprache in die Tastatur tippen, und der Computer »antwortete« im Stile eines Psychiaters über Wörterbücher und vorab definierte Phrasen. Eliza war ein Erfolg, einige Probanden erkannten sogar ein tiefes menschliches Verständnis in den Aussagen der Software. Weizenbaum hingegen war entsetzt über das große Maß an »Maschinengläubigkeit« – vor allem bei Psychiatern, die mit dem Programm ihr Geschäftsmodell automatisieren wollten.

Auch 50 Jahre später haben viele Menschen anscheinend noch ein Urvertrauen gegenüber Computern. Sie kommunizieren etwa auf Dating-Seiten mit Chatbots, die nach dem Prinzip von Eliza funktionieren. Sie reagieren auf Phishing-Mails, klicken kryptische Links an oder laden Dateianhänge unbekannter Absender herunter. Ein Großteil der erfolgreichen IT-Angriffe läuft heute über Menschen, die sich der Gefahren der Digitalisierung und ihrer Folgen nicht bewusst sind. Ohne Maßnahmen zur Sensibilisierung wird die Lücke immer größer, die der »menschliche Faktor« in die Verteidigung öffnet, wie unsere Autoren bei den Recherchen zur Titelgeschichte herausgefunden haben (Seite 6). Hinzu kommt: Laut Schätzungen des Hightech-Verbandes Bitkom waren 2015 in Deutschland erstmals mehr als eine Million Menschen in den Bereichen ITK und Unterhaltungselektronik beschäftigt. Damit sind in den fünf Jahren zuvor rund 135.000 neue Arbeitsplätze in der Branche entstanden.

Ich bin mir sicher, dass sich im Zusammenspiel von Mensch und Maschine die spannendste Perspektive für die kommenden 50 IT-Jahre zeigt. Dieses wird sich verändern, indem die Maschine einen immer aktiveren Part übernimmt. Fragen werden sein: Wer analysiert die Vielzahl der verfügbaren Daten, wer trifft künftig welche Entscheidungen, wer legt die ethischen Grundlagen für maschinelles Verhalten fest? Diese Fragen müssen offen diskutiert, beantwortet und technisch umgesetzt werden. Die Maschinen reagieren künftig nicht mehr nur auf die menschlichen Vorgaben, sie gestalten das System aktiv mit, in dem sie sich mit den Menschen gemeinsam bewegen. Wie industrielle Klebeprozesse durch IT optimiert werden, zeigt unser Projektbericht »400.000 Zeilen Code für perfektes Kleben« anhand des Einsatzes von FERCHAU-IT-Consultants bei SCA Schucker (Seite 25).

Und noch ein historisches Datum: 1966 flog zum ersten Mal die »USS Enterprise« in Gegenden, in denen nie zuvor ein Mensch gewesen ist. Auch wenn einige interessante Technologien der TV-Serie »Star Trek« wie das »Beamen« bislang leider noch nicht entwickelt wurden, haben die Filme für jeden Technik-Enthusiasten die Tür in eine neue Welt aufgestoßen. Es liegt an uns, hindurchzugehen und die eigene Zukunft mitzugestalten.

Viel Spaß bei der Lektüre wünscht Ihnen



IMPRESSUM

atFERCHAU
Ausgabe 01 | 2016
Auflage: 32.000
8. Jahrgang

HERAUSGEBER
FERCHAU
Engineering GmbH
Steinmüllerallee 2
51643 Gummersbach
Fon +49 2261 3006-0
Fax +49 2261 3006-99
zeitungen@ferchau.com
ferchau.com

CHEFREDAKTION
(V. I. S. D. P.)
Martina Gebhardt

REDAKTIONSTEAM
Katharina Bischoff
Dirk Cornelius
Nando Förster
Wibke Kötter
Kerstin Kraft
Dietmar Schönherr
Rolf Schultheis
Christoph Sedlmeir
Nicole Walter

GESTALTUNG
Matthias Müller
Fon +49 211 63559150
grafish.de

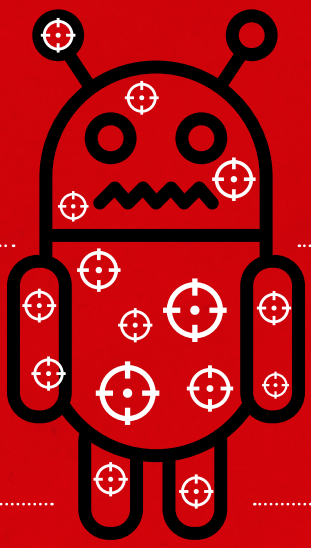
REDAKTION EXTERN
Bernd Seidel & Friends
Fon +49 89 890683620
seidelfriends.de

DRUCK
Gronenberg
Druck & Medien
51674 Wiehl
Fon +49 2261 9683-0

IHR WEG ZU UNS

<atFERCHAU #16>

DAS IT-MAGAZIN VON FERCHAU ENGINEERING



88 PROZENT
ALLER ANDROID-GERÄTE
SIND DURCH SCHWACHSTELLEN
ANGREIFBAR.[1]

IM DURCHSCHNITT BLEIBT EIN ANGRIFF AUF EINE IT-UMGEBUNG 205 TAGE UNENTDECKT.[2]

DIE DREI BELIEBTESTEN PASSWÖRTER IN DEN USA UND WESTEUROPA:[3]

123456789 PASSWORD 123456

IN DEUTSCHLAND SUMMIERT SICH DER SCHADEN DURCH CYBER-KRIMINALITÄT AUF 51 MILLIARDEN EURO PRO JAHR.[4]

DIE WELTWEITEN AUSGABEN FÜR IT-SECURITY BELAUFEN SICH IM JAHR 2015 AUF ÜBER 75 MILLIARDEN DOLLAR.[5]

VOR GENAU 30 JAHREN KAM DER ERSTE MS-DOS-VIRUS IN UMLAUF.[6]

ANTEIL DER DEUTSCHEN, DIE PERSÖNLICHE DATEN GEGEN EINE MONETÄRE VERGÜTUNG ZUR VERFÜGUNG STELLEN WÜRDEN: 20 PROZENT.

ANTEIL DER DEUTSCHEN, DIE EINE TELEMATIK-BOX NUTZEN WÜRDEN, UM GÜNSTIGERE VERSICHERUNGSTARIFE ZU ERHALTEN: 32 PROZENT.[7]

Quellen: [1] Universität Cambridge, Oktober 2015 [2] Mandiant M-Trends 2015 [3] Splashdata, Zdnet, 2015
[4] Bitkom-Verband [5] Gartner [6] Wikipedia [7] Forsa Data Monitor 2015

Die Welt ist böse

SCHWACHSTELLE MENSCH: FREUNDLICH, NEUGIERIG, HILFSBEREIT

Der Mensch gilt als größte Schwachstelle in der IT-Sicherheit. Meist ist er sich dessen nicht bewusst, oder es ist ihm egal. Darum arbeiten Experten daran, Menschen für die Bedeutung von IT-Security zu sensibilisieren. Schließlich ist schon das Trojanische Pferd nicht von allein in die Stadt gelaufen.

Wenn Tobias Schrödel mal wieder als Hacker arbeitet und Unternehmen angreift, lässt er gerne präparierte USB-Sticks in Firmen liegen, etwa auf der Toilette, an den Fahrstühlen und am Parkplatz. Dieses »Social Engineering« mit Ködern ist beileibe kein neuer Trick, aber immer noch extrem erfolgreich: »Es ist schön, wenn ihnen die Wache das Burgtor aufmacht, um sie hereinzulassen.« Stecken ahnungslose Mitarbeiter einen der USB-Sticks in ihren Rechner, erscheint ein Warnhinweis – es hätte aber auch ein bösartiger Trojaner sein können, der es erlaubt, die IT-Systeme auszuspionieren. Die »Lücke Mensch« sucht Schrödel gezielt und stets im Auftrag des Managements: »Weil die Technik immer besser wird«, so seine Bilanz, »hat sich der Mensch zur Schwachstelle in der Verteidigung entwickelt.«

Das war kein Rückblick auf das Jahr 2002, sondern immer noch ein aktuelles Beispiel: Rund 15 Jahre nach dem Aufkommen von Phishing-Mails und 34 Jahre nach Gründung der Hacker-Vereinigung Chaos Computer Club (CCC) klicken Menschen auf schadhafte Links und Dateianhänge, sie tippen ihre Passwörter in beliebige Masken ein und antworten bereitwillig auf Fragen des vermeintlichen User-Supports. Auch in das Netz des Deutschen Bundestags sind die Eindringlinge über eine gefälschte E-Mail eingedrungen, Abgeordnete oder Mitarbeiter waren dem darin enthaltenen Link auf eine infektiöse Website gefolgt. Mal wurde Angela Merkel, mal die Vereinten Nationen als Absender genannt. Social Engineering lebt davon, Vertrauen zu erzeugen und auszunutzen – solange dies gelingt, kann es keine wirksame Sicherheitsstrategie geben. Das Märchen vom bösen Wolf und vom arglosen Rotkäppchen kommt nicht von ungefähr.

Der Mensch ist der stärkste Hebel, um in eine Organisation einzudringen. Die Erkenntnis ist seit Jahren bekannt, und jedes Jahr erscheinen neue Studien, die diese These bestätigen. Zuletzt berichtete eine PwC-Untersuchung aus Großbritannien, dass 75 Prozent der Konzerne im vergangenen Jahr Sicherheitsverstöße ausgehend von Mitarbeitern zu verzeichnen hatten. Schlimmer noch: Jeder zweite der Security-Vorfälle mit den größten Auswirkungen für das jeweilige Unternehmen war durch menschliche Unachtsamkeit verursacht worden. Es liegt am mangelnden Problembewusstsein, an der Bequemlichkeit und an der Neugier. »Menschen sind freundlich und gutgläubig, darum kann man sie einfach überlisten«, sagt Schrödel, der als »Comedy-Hacker«, Sicherheitsberater und Buchautor arbeitet. Zudem sei der einfachere Weg immer verlockend, was Trampelpfade über einst akkurate Rasenflächen zeigen.

Siebenmal am Tag einloggen, einhändig, weil die andere Hand einen Kaffee oder das Telefon hält? »Da wählen viele Menschen einfache Passwörter, aber Sicherheit in der IT basiert nun mal auf Komplexität.« Das Problem zeigt sich am Dreieck mit den Vektoren Funktionalität, Nutzbarkeit und Sicherheit: Je sicherer ↘




Von links: **Frank von Stetten**, Sicherheitsberater, schaltet den gesunden Menschenverstand ein. **Michael Ochs** vom Fraunhofer-IESE federt den »menschlichen Faktor« technisch ab. **Hans Pongratz**, CIO der TU München, sensibilisiert Mitarbeiter und Studenten. Und Comedy-Hacker **Tobias Schrödel** verteilt USB-Sticks als Köder.

die IT-Anwendung, desto schlechter werden Funktionalität und Usability. Wer ohnehin schon viel zu tun hat, will von der IT nicht noch Knüppel zwischen die Beine bekommen. »Der Mensch muss arbeiten können und Zugang zu Systemen haben«, berichtet Schrödel. »Da sind bequeme, gutgläubige oder eingeschüchterte Mitarbeiter eine große Hilfe und ein wunderbares Angriffsziel.«

Einigen Menschen ist dies egal, was als »Security Fatigue« bezeichnet wird. Andere hingegen sind sich des Problems immer noch nicht bewusst, die sogenannte »Security Awareness« fehlt. Hier können adäquate Investitionen in die Sensibilisierung der Mitarbeiter helfen: was für Angriffe möglich sind, welche Folgen diese haben können und wie man gegensteuern kann. Doch laut der Initiative »Deutschland sicher im Netz« (DsiN) verzichten im Jahr 2015 knapp drei Viertel aller kleineren und mittelständischen Unternehmen (KMU) auf IT-Schulungen ihrer Mitarbeiter. Sensibilisierung, so viel ist sicher, muss im Top-Management beginnen.

Ist der Groschen oben gefallen, arbeiten immer mehr Organisationen gegen das mangelnde Sicherheitsbewusstsein unten an. »Sensibilisieren bedeutet Überzeugungsarbeit leisten, nicht Vorschriften machen«, sagt Hans Pongratz, Vizepräsident und CIO der Technischen Universität München (TUM). Sein Problem: »Universitäten sind für Hacker grundsätzlich interessant, da ihre IT-Infrastruktur als Sprungbrett für weitere Angriffe oder als Zwischenlager für illegale Inhalte dienen kann.« Pongratz hat in der TUM Kampagnen für Studierende und Mitarbeiter gestartet: Nach einem großen Sicherheitswettbewerb folgte das volle Awareness-Programm mit Vorträgen, Infoständen, Postern, Flyern, Passwortkarten und Give-aways, speziellen Webseiten, einer Live-Hacking-Veranstaltung im Audimax, Newslettern und einer Phishing-Beratung. Zentraler Grundsatz: »Nach der Kampagne ist vor der Kampagne«, sagt CIO Pongratz, »denn steter Tropfen höhlt den Stein.«

Neben der Sensibilisierung brauchen die Nutzer eine zentrale Stelle in der Organisation, um IT-Sicherheitsvorfälle zu melden. »Hier werden alle Anfragen und Nachrichten gesammelt und an die zuständigen Experten weitergeleitet«, erläutert Pongratz. Zudem hilft noch eine eigene Referentin für IT-Sicherheit und Datenschutz dabei, die Vorfälle systematisch aufzuarbeiten. Wichtig ist dem CIO eine Botschaft: »Die IT darf trotz der Sicherheitsbedürfnisse nicht als Blockierer auftreten, aus dem Zeitalter sind wir raus.« Stattdessen verstehe er seine Organisation als Partner, der Verständnis weckt und die Nutzer berät. »Bei Reglementierungen suchen sich die Menschen sofort einen Workaround, da sind sie ganz findig.«

Mehr Security macht das Leben komplizierter, sagt auch Frank von Stetten, Vorstand der Sicherheitsberatung HvS-Consulting AG in München. »Der eine Klick mehr bremst den flüssigen Arbeitsalltag – für den zusätzlichen Schritt müssen Sie Verständnis erzeugen.« Das sei wie mit dem Anschnallen beim Autofahren, das inzwischen zum normalen Alltag gehöre. Seiner Meinung nach sollten Security-Awareness-Kampagnen primär dazu dienen, ohne erhobenen Zeigefinger den gesunden Menschenverstand einzuschalten und eine grundsätzliche Skepsis aufbauen – speziell im Büro, wo man niemals ganz unter sich sei. »Sie müssen Betroffenheit erzeugen, indem sie den Mitarbeitern zeigen, dass die Welt böse ist.«

Es sei kein Beinbruch, ein Passwort zu verlieren oder auf einen Phishing-Link zu klicken, argumentiert Sicherheitsberater von Stetten. »Es ist schlimm, den Fehler nicht zu bemerken und zu melden.« Die Sensibilisierung der Mitarbeiter verhält sich dabei wie Werbung: Man könne zwar kurzfristig einen hohen Werbedruck erzeugen und eine hohe Aufmerksamkeit erreichen, langfristig werde aber damit noch keine Verankerung geschaffen. »Deswegen ist die ›Security Awareness‹ ein kontinuierlicher Prozess, bei dem sie am Anfang viel investieren, um die Aufmerksamkeitsschwelle zu überschreiten, und dann stetig neue Impulse setzen, um die Aufmerksamkeit hoch zu halten«, berichtet von Stetten.

»Security-Awareness-Kampagnen müssen Betroffenheit erzeugen, indem sie den Mitarbeitern zeigen, dass die Welt böse ist.«

Frank von Stetten

Derweil arbeitet das Fraunhofer-Institut für Experimentelles Software Engineering IESE in Kaiserslautern daran, den »menschlichen Faktor« durch Software abzufangen. Beispielsweise das versehentliche Versenden von E-Mails mit sensiblen Anhängen an Adressaten, die nicht zum Kreis der gedachten Empfänger gehören, erläutert Michael Ochs vom IESE: »Wir wollen Sicherheitsarchitekturen tief in die Systeme einbauen, in denen bestimmte Richtlinien für Daten, Objekte, Informationstypen oder Dateitypen hinterlegt sind.« Erkennt das System, dass etwa persönliche oder andere sensible Daten nach außen geschickt werden sollen, kann es zum Beispiel einen Freigabe-Workflow mit Vier-Augen-Prinzip anstoßen. »Was einmal im Internet ist, kriegen Sie praktisch nicht mehr weg.«

In einem zweiten IESE-Szenario werden sensible Kundendaten am Bildschirm ausgeblendet, wenn sich der Anwender im öffentlichen Bereich aufhält, so Ochs: »Der Policy Decision Point entscheidet dann in Echtzeit, ob Kundendaten auf dem Tablet oder Notebook im Bus anonymisiert werden.« Mit derartigen Lösungen der Datennutzungskontrolle könne man zumindest an einigen Stellen menschliche Fehler eindämmen. »Der Hauptzweck ist, die Grauzone zwischen der Vollsperrung und der totalen Offenheit der Daten nutzbar zu machen, um auch neue Geschäftsmodelle zu ermöglichen.«

Diese Ansätze zeigen, dass sich die Fehlerquote der Menschen durchaus reduzieren lässt. Rein technisch wird sich das gesamte Sicherheitsproblem aber nicht lösen lassen, denn bislang sind den Angreifern immer noch Mittel und Wege eingefallen, um Hardware und Software zu umgehen und direkt auf den Menschen zu zielen: das Lindenblatt auf dem Rücken der IT-Sicherheitsverantwortlichen. Wenn der Mensch sich jedoch bewusst ist, dass sein Verhalten die Sicherheit eines Unternehmens gewährleistet, ist ein großer Schritt getan. //

MEHR INFORMATIONEN

Tipps gegen Social Engineering
bit.ly/1M9W7gE

Kampagne der TU München
it.tum.de/it-sicherheit

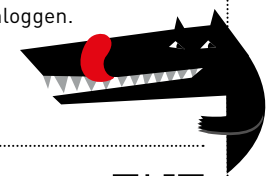
Rückblick: 10. Cyber-Sicherheits-Tag – »Security Awareness – Wege aus der digitalen Sorglosigkeit«
bit.ly/1o3fRIO

Tobias Schrödel – Homepage
sichere.it

Fraunhofer IESE – Datennutzungskontrolle
bit.ly/Od7CNo

WEB-SPECIAL

Auf der FERCHAU-Homepage finden Sie einen aktuellen Artikel über sichere Passwörter – was man beachten muss und wie man sich kryptische Buchstabenkombinationen merkt. Sie müssen sich dazu nur mit Ihren Windows-Anmeldedaten einloggen.

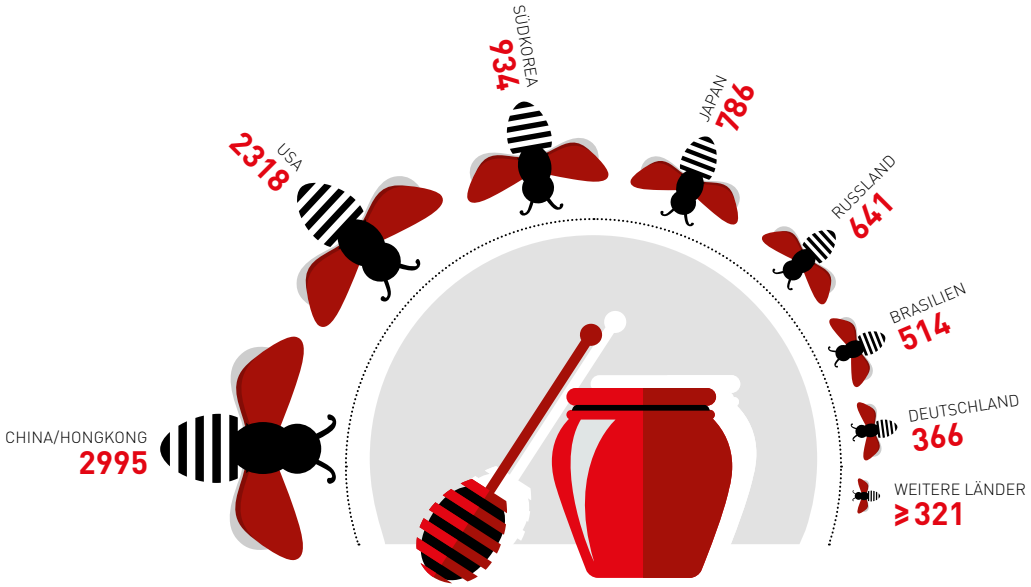


bit.ly/1Z0Pnsi

Honeynets

DIGITALE LOCKVÖGEL ENTLARVEN HACKER

Immer häufiger werden scheinbar unspektakuläre Mittelständler mit Low-Tech-Produkten gehackt. Versuche mit digitalen Lockvögeln, genannt Honeypots und Honeynets, zeigen, woher die Angreifer kommen und wie sie vorgehen.



Die weitaus meisten Attacken kamen aus nur zwei Ländern: China und USA. Quelle: TÜV Süd

Kürzlich stellte der TÜV Süd das Wasserwerk einer Kleinstadt zu Versuchszwecken ins Internet. Natürlich nur zum Schein: Als mittelständischer Betrieb getarnt, sollte es Zu- und Angriffe aus dem Cyberspace protokollieren. Ähnlich ging Sophos vor: Auf der CeBit hatte das IT-Sicherheitsunternehmen ein Honeynet gezeigt, das eine Ablaufsteuerung für den Eisenbahnverkehr mimte, in Wirklichkeit aber ein Scheinziel für Hacker war. In beiden Fällen trieben die Sicherheitsspezialisten einen hohen Aufwand, um Angreifern eine »echte« IT-Umgebung vorzugaukeln. Sophos hatte dazu Originalkomponenten aus dem Bahnbetrieb eingesetzt. Das Honeynet des TÜV Süd emulierte den Betrieb des Wasserwerks ebenfalls mit realistischen Software- und Hardwarekomponenten.

Abwehrstrategien entwickeln

Der Grundgedanke bei der Einrichtung vorgetäuschter IT-Installationen ist einleuchtend. Um Abwehrstrategien und -techniken gegen Attacken aus dem Cyberspace zu entwickeln, müssen Sicherheitsunternehmen zunächst einmal die Schlupflöcher der Eindringlinge identifizieren und deren Techniken studieren. Sie setzen dabei zunehmend auf den Einsatz von Lockmitteln, sogenannten Honeynets und Honeypots.

Genutzt werden diese auch von IT-Sicherheitsfirmen. »Wir tun das, um uns ein Bild von der Sicherheitslage machen zu können«, erläutert Udo Schneider, Security Evangelist beim Sicherheitsunternehmen Trend Micro. »Aber auch für IT-Anwender kann sich der Einsatz lohnen, wenn damit eine konkrete Kosten-Nutzen-Betrachtung verbunden

ist.« Untersuchungen an Systemen der Shopfloor-IT und ähnlichen Echtzeit-Steuerungssystemen können indessen für den Honeynet-Betreiber stärker ins Geld gehen als bei Standard-IT, so Schneider. Denn es sei mindestens eine Fachkraft zu kalkulieren, die Know-how aus beiden Feldern mitbringt. Auch Dienstleister können helfen. So bietet die Telekom mit dem »T-Pot« eine Plattform, die sich mit wenig Aufwand betriebsbereit konfigurieren lassen soll.

Nicht für Vernetzung konzipiert

Spannend wird es bei der Sicherheit von Maschinensteuerungen und Fabrikanlagen: Einerseits sollen diese Anlagen künftig verstärkt ins Internet integriert werden, andererseits aber gibt es hier eine riesige installierte Basis, die überhaupt nicht für vernetzte Umgebungen konzipiert wurde. Welche Überlebenschancen werden diese Anlagen also in der freien Wildbahn des Internet of Things haben?

Die aufgestellten Honigtöpfe von Sophos und TÜV Süd wurden jedenfalls überraschend schnell als Hackerziel angenommen. Der erste Zugriff auf das simulierte Wasserwerk erfolgte »praktisch im Moment des Einschaltens«, wie ein Sprecher des TÜV Süd anmerkt. Die klebrige Honigfalle »Honeytrain« von Sophos verzeichnete bereits innerhalb der ersten vier Stunden mehrere Tausend Besucher.

Zugriffe aus der ganzen Welt

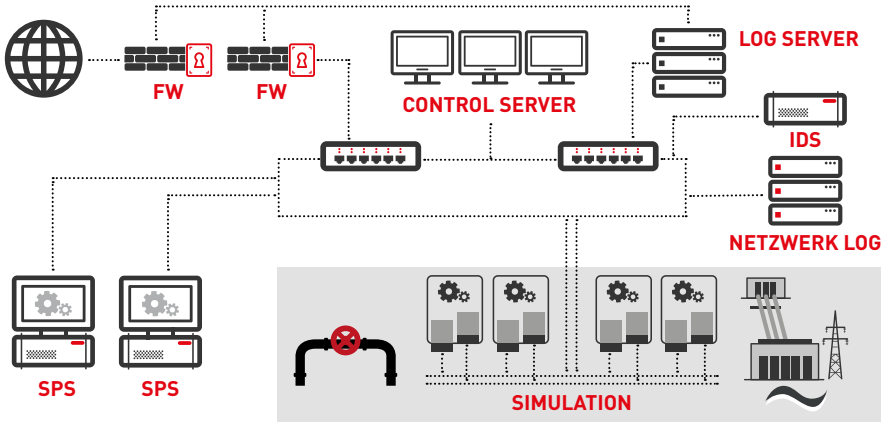
Die Erkenntnisse zeigten, dass die verwendeten Komponenten der Fertigungslandschaften einem ernsthaften Cyber-Angriff nicht viel entgegensetzen können. Die Hacker nutzten nicht nur die gängigen IT-Protokolle, sie zeigten sich auch versiert im Umgang mit Echtzeitsystemen und den in Fertigungsindustrie oder Bahnverkehr gängigen Protokollen wie Modbus TCP oder S7Comm. »Diese Zugriffe waren zwar nicht so häufig, aber sie kamen aus der ganzen Welt«, erklärt Thomas Störtkuhl, Teamleiter IT Security beim TÜV Süd. Nach Ansicht des Sicherheitsexperten wird damit deutlich, dass Fertigungssysteme, so wie sie heute sind, nicht ausreichend gegen Hacker geschützt sind. Auch verstecken geht nicht: Spezielle Suchmaschinen im Internet zeigen dem wissensdurstigen Hacker jedes vernetzte Echtzeit-Gerät an, egal ob es sich um einen Home-Router oder eine Chemiefabrik handelt.

Die meisten Zugriffe kamen bei den drei genannten Honeynet-Projekten aus China. Auf Platz zwei rangieren mit deutlichem Abstand Attacken aus den USA, gefolgt von Südkorea. Ganz eindeutig ist die Situation nicht, denn die geografische Zuordnung der Angreifer erfolgte anhand der IP-Adressen, und die lassen sich ebenso faken wie die Honeynets. Zwischen den Besuchern aus China und jenen aus den USA hat Trend Micro aus eigener Praxis mit Honeynets einen deutlichen Unterschied ausgemacht: Während die US-Hacker gerne ausprobieren, was sie mit den vorgefundenen Steuerungen anstellen können, zeigen sich ihre Kollegen aus dem Reich der Mitte einfach neugierig. »Die luden alle möglichen Daten herunter und sahen sich alles an«, so Schneider. »US-Hacker versuchen auch schon einmal, Parameter zu verändern oder eine Maschine über ihre Grenzwerte hinauszusteuern.«

Warnglocken läuten

Wenn selbst relativ unkritische Ziele wie ein Kleinstadt-Wasserwerk Angreifer in Scharen anlocken, sollten bei den Protagonisten der vernetzten Produktionen jedenfalls die Warnglocken läuten, so die Quintessenz der Honeynet-Betreiber. »Aus einfachen Zugriffen können Angriffe mit hohem Schadenspotenzial werden«, warnt Sicherheitsexperte Schneider. //

LOGISCHE STRUKTUR DES HONEYNETS



Sieht wie ein normaler Betrieb aus, ist aber nur ein digitaler Lockvogel: das Honeynet des TÜV Süd. Bild: TÜV Süd

HONIGTÖPFE FÜR HACKER

In der IT werden Rechner als Honeypots bezeichnet, die Hacker anlocken sollen, um deren Verhalten zu studieren. Nach außen erwecken sie den Anschein, als würden sie einem normalen betrieblichen Zweck dienen. Ihr eigentlicher Zweck ist jedoch das Sammeln von Daten über Zugriffe und Angriffe von außen. Erfasst werden beispielsweise genutzte Protokolle, Ports, Verfahren und IP-Adressen. Genauso lässt sich auch ein komplettes Unternehmen oder eine maßgeschneiderte IT-Umgebung als Scheinziel für Cyber-Angreifer präparieren. In einem solchen Fall sprechen die Sicherheitsexperten von einem Honeynet.

MEHR INFORMATIONEN

honeynet.org bit.ly/1GwWoOL

Bild: ABB, Dual-Arm-Konzeptroboter

Wie Roboter und Mensch
künftig sicher zusammenarbeiten

DIE WILDEN KERLE

Bisher standen Roboter hinter Schutzzäunen.
In Zukunft arbeiten sie mit Menschen auch im Team. Sie reichen das Werkzeug, helfen beim Schrauben oder tragen Lasten. Wie sicher ist die Zusammenarbeit mit den neuen »Kollegen«, wenn sie aus dem Käfig gelassen werden?

»Roboter tötet Arbeiter« – diese Schlagzeile ging im Sommer 2015 durch die Presse. Im Werk eines deutschen Autoherstellers war ein Techniker von einem Roboter tödlich verletzt worden. Der 22-Jährige hatte die Maschine neu einstellen wollen und war zum Zeitpunkt des Unfalls im sonst abgesperrten Bereich. Auch wenn Experten das Ereignis als tragischen Arbeitsunfall und menschliches Versagen einstuften, entfachte erneut die Diskussion über Automatisierung. Denn zur Sorge, dass Maschinen den Mensch überflüssig machen, kam eine Frage hinzu: Wie sicher ist die Zusammenarbeit mit Kollege Roboter? Bisher stehen die meisten Systeme in der Produktion hinter Schutzzäunen. Doch in Zukunft werden kollaborative Roboter direkt mit dem Menschen zusammenarbeiten.

Künstliche Roboter-Haut erkennt Berührungen

»Es wird weltweit intensiv an neuen Technologien geforscht, um den Einsatz von Robotern ohne Schutzzaun zu ermöglichen«, sagt Dr. Norbert Elkmann. Er leitet das Geschäftsfeld Robotersysteme am Fraunhofer-Institut für Fabrikbetrieb und -automatisierung IFF in Magdeburg. Sicherheit bedeutet zum einen, Kollisionen zu vermeiden, also Abstand zu halten. Dazu entwickelten Elkmann und sein Team einen taktilen Fußboden sowie optische Sensorsysteme, die erkennen, wenn ein Mensch dem Roboter zu nahe kommt. Der Roboter stoppt daraufhin oder verringert seine Geschwindigkeit.

Direkter Kontakt zwischen Mensch und Roboter ist bei vielen Anwendungen jedoch unumgänglich. Eine vom IFF entwickelte maßgeschneiderte Taktilsensorik mit Dämpfungsschicht wird dem Roboter übergezogen. Die künstliche Haut erkennt leichteste Berührungen, so dass der Roboter sofort stoppen kann. Diese Technologie kann auch zum gefühlvollen Greifen von zerbrechlichen Objekten eingesetzt werden. »BROMMI« heißt ein Roboterarm in Form eines Elefantenrüssels. Anders als ein herkömmlicher Roboter hat er keine Klemm- und Scherstellen, die Bauweise verhindert Verletzungen. Ein weiterer Ansatz der sicheren Mensch-Roboter-Kollaboration ist die Handführung, das heißt, der Mensch bedient die Apparatur zum Beispiel per Joystick.

Kollaborative Roboter im Einsatz

Im Vergleich zu bisherigen Industrierobotern, die im Karosserie-Bau oder bei der Lackierung eingesetzt wurden, halten die Leichtbausysteme Einzug in der Montage. Im BMW-Werk in Spartanburg, USA, gibt es einen Roboterarm, der Türdichtungen andrückt. Bisher ein Job, der für die Arbeiter anstrengend war und Präzision erforderte. Auch Mercedes-Benz hat die Arbeit mit Leichtbaurobotern für die Serienanfertigung erprobt. Der gelenkige Roboterarm iiwa des Herstellers Kuka hilft den Arbeitern hier unter anderem beim Schrauben. Er verfügt über Kollisions- und Krafterkennung, kann seine Geschwindigkeit reduzieren, bewegt sich innerhalb eines Überwachungsraums und hat keine Ecken und Kanten, an denen man sich stoßen könnte.

Auch der Zweiarmroboter YuMi, dem 2015 auf der Hannover Messe sogar Bundeskanzlerin Angela Merkel die Greifhand schüttelte, soll besonders sicher sein. Der Leichtbauroboter sei laut Hersteller ABB so designt, dass man sich nicht verletzen könne. Ein Sensor misst Kraft und Drehmoment des Roboters und verhindert dadurch schmerzhafte Kollisionen. Die Arme sind zusätzlich gepolstert. Auch YuMis Aussehen, das an einen Oberkörper mit zwei muskulösen Armen erinnert, soll dem Anwender ein Sicherheitsgefühl geben.

Wie viel Schmerz ist erträglich?

Der ein oder andere blaue Fleck lässt sich bei der Zusammenarbeit mit Robotern wahrscheinlich nicht vermeiden. Aber wie stark darf ein Roboter einen Menschen überhaupt berühren, ohne dass er ihn verletzt oder ihm Schmerzen zufügt? Das erforschen das Fraunhofer IFF und die Universitätsklinik Magdeburg. Mit freiwilligen Teilnehmern werden Daten erhoben, wie viel Druck oder Kraft an unterschiedlichen Körperstellen maximal auftreten darf, um die Schmerz- oder Verletzungseintrittsschwelle nicht zu überschreiten. Die Daten sollen in die weltweit gültigen Normen einfließen, so Dr. Norbert Elkmann.

Doch wer ist für einen Unfall verantwortlich? Das ist die Frage, die sich nicht nur beim autonomen Auto, sondern auch bei Robotern in der Fabrikhalle stellen wird. Und wie können Maschinen sozial verträglich handeln? Maschinenethik und soziale Robotik spielen in der Entwicklung eine wichtige Rolle. Der Philosoph und promovierte Wirtschaftsinformatiker Oliver Bendel beschäftigt sich an der Hochschule für Wirtschaft der Fachhochschule Nordwestschweiz intensiv mit dem Thema. Er sagt: »In Zukunft müssen wir auch nach der Moral von Maschinen fragen, weil immer mehr autonome und teilautonome Maschinen Entscheidungen mit moralischen Implikationen treffen. Dabei geht es nicht nur darum, dass Roboter nach bestimmten Regeln handeln, sondern auch darum, dass sie Folgen abwägen.« //

Dr. Norbert Elkmann
Geschäftsfeldleiter Robotersysteme am Fraunhofer Institut für Fabrikbetrieb und -automatisierung
Bild: Fraunhofer IFF

MEHR INFORMATIONEN

Eine im September 2015 veröffentlichte Studie der Boston Consulting Group (BCG) bestätigt, dass einfache Tätigkeiten durch den Roboter ersetzt werden. Jedoch würden gleichzeitig neue Jobprofile entstehen. In Deutschland stünden laut Studie 610.000 Jobs, die bis 2025 verschwinden, rund einer Million Jobs, die entstehen könnten, gegenüber.

Laut Roboter-Weltstatistik 2015 der International Federation of Robotics soll der Absatz von Industrie-Robotern bis 2018 jährlich um 15 Prozent zunehmen. Die verkauften Einheiten sollen sich bis dahin auf rund 400.000 Stück verdoppeln. Die fünf größten Märkte sind China, Japan, USA, Südkorea und Deutschland.

WEB-SPECIAL

DIE ROBOTER LERNEN MORAL
Das komplette Interview mit dem Maschinenethiker Professor Oliver Bendel auf ferchau.com.

bit.ly/1OuOTcr

Auto-Software: der neue Angriffsvektor Internet

GEHACKT IM STRASSENGRABEN

Die rollende Killer-App des 21. Jahrhunderts heißt »connected car«. Aber das vernetzte Automobil an der langen Leine des Internets wird auch zur Zielscheibe von Hackern und somit zum Risiko für Fahrer und Insassen. Wie wollen Hersteller und Zulieferer solche Sicherheitslücken künftig schließen und illegale Zugriffe verhindern?

Früher musste man die Bremsleitung durchtrennen oder die Verteilerkappe abziehen, um ein Fahrzeug zu manipulieren. Heute macht man sich die Finger nicht mehr schmutzig. So wie die beiden Hacker Charlie Miller und Chris Valasek in den USA. Das Duo nutzte eine Sicherheitslücke in der Elektronik eines Jeep Cherokee, um die Kontrolle zu übernehmen. Vom heimischen Sofa aus betätigten sie per Fernsteuerung die Scheibenwischer und schalteten das Getriebe in den Leerlauf. Als Höhepunkt der Aktion deaktivierten sie die Bremsen. Mitsamt seinem Fahrer, der in die Aktion eingeweiht war, landete das Zwei-Tonnen-Gefährt im Straßengraben – der bisher wohl spektakulärste Hack eines Fahrzeugs. Schon wenige Tage später machte ein ähnlicher Fall Schlagzeilen. Diesmal war es Hackern gelungen, per Smartphone die Bremsen eines Sportwagens des Typs Chevrolet Corvette zu deaktivieren. Keine Frage: Autos werden allmählich zur Zielscheibe von Hackern.

Vollgestopft mit Elektronik

Die steigende Zahl derartiger Meldungen hat eine Ursache: Moderne Autos sind vollgestopft mit Elektronik. Der Softwareumfang einer Limousine übersteigt bereits die Marke von 100 Millionen Codezeilen, wie das Magazin MIT Technology Review berichtet. Und dass Software nie fehlerfrei ist, ist hinlänglich bekannt. Alles also gute Angriffspunkte für Hacker. Beim Auto kommt als Risikofaktor noch die verschachtelte Bordelektronik mit Dutzenden vernetzter Echtzeitrechner dazu, welche viele Funktionen steuern, vom elektrischen Fensterheber bis hin zu ABS und Sportfahrwerk. Nicht selten tun sich selbst die Architekten und Entwickler dieses Dickichts schwer, den Überblick zu behalten. Für Hacker bietet sich damit ein weites Feld für Experimente. So sind bei manchen Fahrzeugen die Reifen mit Drucksensoren ausgestattet, die ihre Messergebnisse per Funk an einen Empfänger in der Karosserie senden. Auf dem Hacker-Treff Black-Hat-Konferenz wurde vor Jahren schon ein Angriff über dieses Einfallstor vorgestellt. Sogar Hacks über das CD-Laufwerk des Autoradios, bei denen eine maßgeschneiderte Schadsoftware eingeschleust werden konnte, sind bekannt.

Und die Bedrohungslage dürfte sich in Zukunft weiter verschärfen: Ab April 2018 soll das Notrufsystem »eCall« in allen Neuwagen zur Pflicht werden und somit alle Fahrzeuge via eigener Mobilfunk-Nummer netzfähig machen. Von Rechts wegen. Sicherheitsexperten warnen, dass der EU-Notruf nicht nur den Krankenwagen alarmiert, sondern eventuell auch Hacker auf den Plan rufen wird. »eCall ist ein trojanisches Pferd«, konstatiert denn auch der wissenschaftliche Leiter des Forschungszentrums Energiewirtschaft und Energierecht (fee) der Hochschule Osnabrück, Professor Volker Lüdemann. Dieses System sei eine technische Plattform, die Zusatzdiensten aller Art offenstehe. Die Europäische Union nehme es in Kauf, dass eCall unter dem Deckmantel der Lebensrettung zum Türöffner für weitreichende Datennutzung werde, kritisiert der Wissenschaftler. Illegale Verwendungen nicht ausgeschlossen!

Zeitreise in die Vergangenheit

Beim Zugriff eines Smartphones auf die Autoelektronik prallen nicht nur die Welten von Autoelektronik und Consumer-IT aufeinander. Es findet eine Zeitreise statt. Denn während Smartphones und Apps fast im Monatsrhythmus aus den Shops purzeln, dauert es immer noch vier bis fünf Jahre, ein Auto zu entwickeln. Als die Steuergeräte und Elektronik-Architekturen für die heutigen Autos konzipiert wurden, standen Konnektivität und Internet-Anbindung noch gar nicht auf den To-do-Listen der Designer; ein Zugriff auf die Software von außerhalb war nicht vorgesehen – und deswegen auch keine Sicherheitsmaßnahmen. Genauso wenig übrigens wie eine Möglichkeit, die Software beim Bekanntwerden von Sicherheitslücken schnell und automatisch zu aktualisieren. Software-Updates werden in der Autobranche immer noch händisch durchgeführt, und zwar erst dann, wenn das Auto zufällig wieder einmal in der Werkstatt auftaucht. Das kann Monate dauern. Immerhin: inzwischen arbeiten auch die Auto-Entwickler hierzulande daran, ihre Fahrzeuge updatefähig zu machen, wie Rudolf von Stokar anmerkt, Sales Director von Redbend Software, einer Firma, die sich das Software-Update »Over the Air« (OTA) auf ihre Fahnen geschrieben hat.

> »Während Smartphones und Apps fast im Monatsrhythmus aus den Shops purzeln, dauert es vier bis fünf Jahre, ein Auto zu entwickeln.«

In Sachen Sicherheit hätten Autohersteller inzwischen einiges getan, um die zuvor offenen Schnittstellen der Fahrzeugdiagnosesysteme abzusichern, wie der IT-Sicherheitsexperte Thilo Schumann in seinem Vortrag auf dem Chaos Communication Camp sagte. Fragt man über die offiziellen Kanäle der Unternehmen nach Sicherheitsstrategien, geben sich die Autobauer allerdings meist zugeknöpft.

Protokolle nicht standardisiert

Das Grundproblem: Die auf Controller Area Network (CAN) aufgebauten Protokolle seien nicht standardisiert, wie Thilo Schumacher weiter angibt. ↘

Jeder Hersteller nutze seine eigene Implementierung. Und die Hersteller geben nur ungern Einblicke in ihre Protokolle. Dazu müsse man ständig Vertraulichkeitsvereinbarungen unterschreiben, sagte Schumann. Das auf CAN aufbauende Fahrzeugdiagnosesystem ODB II hingegen ist in der ISO-Norm 15031-6 festgelegt und wird in Europa eingesetzt. Sein Pendant IVN (In-Vehicle-Network) wird in den USA verwendet. Per Gesetz müssen sämtliche Fahrzeuge eine solche Schnittstelle besitzen.

Recherchen bei den Automobilzulieferern sind dagegen ergiebiger. »Alle diese Hacks, die in jüngster Zeit durch die Presse gingen, wurden über Telematiksysteme ausgeführt, die nicht über einen zeitgemäßen Schutz gegen Eindringlinge verfügten«, sagt beispielsweise Lars Reger, CTO des Chipherstellers NXP. Gegen übergriffige Hacker empfiehlt Reger, ein zentrales Kommunikations-Gateway in die Autos einzubauen, welches wie eine Grenzpolizei den Datenverkehr zwischen der Außen- und der Innenwelt des Fahrzeugs überwacht. Eine weitere Sicherheitsmaßnahme wäre die Verschlüsselung und Signierung des Datenverkehrs zwischen den Steuergeräten.

Gegen Manipulationen geschützt

Erfahrung mit der Sicherung der Integrität kritischer Daten und Infrastrukturen besitzen Halbleiterhersteller wie NXP, Atmel oder Infineon unter anderem aufgrund ihrer Entwicklungen von Chips für Reisepässe und Chipkarten. Indessen ist Security aber immer auch »ein Performance-Thema«, bemerkt Hans Adlkofer, bei Infineon als Vice President für das Geschäft mit Automobilhalbleitern zuständig. Die aktuellen, speziell für den

Chris Valasek (links) und **Charlie Miller** auf der Sicherheitskonferenz Black Hat 2015 in Las Vegas. Bild: Corbis

Betrieb im Auto entwickelten Prozessoren der Münchner Chipschmiede sind bereits mit einem entsprechenden Hardwarebeschleuniger bestückt, unterstreicht der Infineon-Manager. Diese Beschleuniger sind von außen nicht zugänglich und daher gegen Manipulationen geschützt.

Das Wissen um Sicherheitstechniken und -Verfahren ist bei den Zulieferern also vorhanden. Nur können – oder dürfen – sie nichts darüber sagen, inwieweit diese Techniken bereits in die Autoelektronik Eingang gefunden haben. Die Entwickler bei den Fahrzeugherstellern brauchen das Rad nicht neu zu erfinden, so die Quintessenz, denn die gesuchten Techniken werden in der kommerziellen IT längst eingesetzt.

Uber mischt die Branche auf

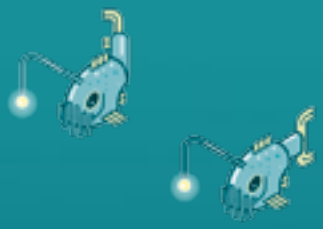
Das hat auch der auf über 50 Milliarden Dollar Marktwert taxierte ehemalige Limousinenservice Uber erkannt und mischt die Branche der Selbstfahrer mächtig auf. Damit ihre autonomen Fahrzeuge künftig vor Daimler, Audi, BMW oder Google rangieren, heuerte das Unternehmen eben mal das Know-how von 40 Eliteuniforschern an. Diesem aggressiven Abwerbungsgebaren konnten offensichtlich auch die beiden Jeep-Hacker Charlie Miller und Chris Valasek nicht mehr widerstehen und wechselten unlängst von Twitter beziehungsweise von der IT-Sicherheitsfirma IOActive hinüber ins Uber-Technikzentrum. So schließt man Sicherheitslücken heute. //

WEB-SPECIAL

DAMIT AUTO-HACKER KEINE CHANCE HABEN.

Maßnahmen und Techniken zur Abwehr der Eindringlinge sind verfügbar.

bit.ly/1JSVFmQ



Seekabel – es werde Licht

DIE NERVENBAHNEN DES INTERNETS

Unterseekabel gelten als »Nervenbahnen des Internets« und als unverzichtbarer Bestandteil der globalen Vernetzung. Mehr als 95 Prozent des weltweiten Datenverkehrs werden darüber abgewickelt, Satelliten übernehmen den spärlichen Rest. Das zarte Geflecht der Seekabel ist fortwährend bedroht.

Deutschlands größte Auffahrt auf die Datenautobahn liegt im ostfriesischen Städtchen Norden. Die Einrichtung hieß in Postbehördenzeiten »Seekabelendstelle«, heute »Competence Center Submarine Cables« (CCSC). Hier kommt das »Trans Atlantic Transmission Cable 14« an Land, kurz TAT-14, das Deutschland seit 2001 mit Großbritannien, Frankreich und den USA verbindet. Das ringförmige und 15.000 Kilometer lange Netzwerk soll um die Jahrtausendwende rund 1,3 Milliarden Dollar gekostet haben und kann neben 15 Millionen Telefonaten gleichzeitig auch geschätzte 160 Gigabit übertragen – pro Sekunde und in jedem der vier Glasfaserpaare. Umgerechnet sind das über 250 DVDs. Technisch sind heute bei Glasfasern Übertragungen im Terabit-Bereich machbar. Aktuell gibt es über 230 Seekabel mit einer Gesamtlänge von weit mehr als 300.000 Kilometern. Die Kabel verbinden einzelne Länder, aber auch Kontinente miteinander. Und es werden immer noch neue Verbindungen gelegt: Google will sich beispielsweise an Kabeln zwischen den USA und Japan beziehungsweise Brasilien beteiligen, Microsoft verlegt Richtung Europa. Auch zwischen Finnland und Rostock liegt bald ein neues Kabel. Die Cloud schwebt im Wasser.

Und wenn ein Kabel reißt, werden die Datenströme automatisch umgeleitet. Reißen jedoch mehrere Kabel in einer Region, wird es eng: Dann kommen Daten verzögert beim Empfänger an, das Internet wird langsam. Jetzt muss ein Reparaturschiff auslaufen, die Bruchstelle suchen und das Kabel vom Meeresboden hochfischen. Die Reparatur kann Wochen dauern. ↘

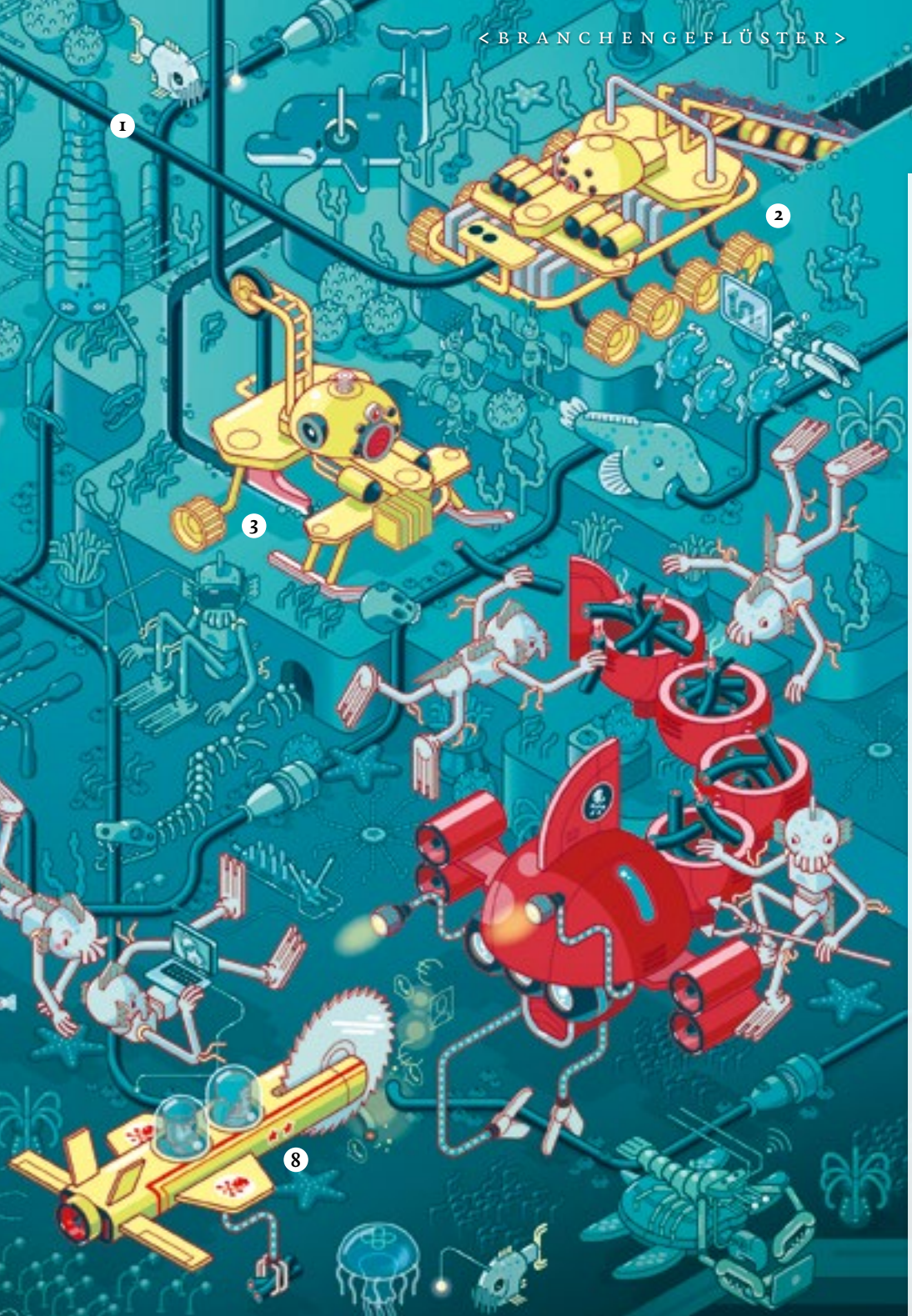
KABEL-TECHNIK

1 DAS KABEL
Seekabel sind zwischen zwei und acht Zentimeter dick, wiegen rund drei bis zehn Kilogramm pro Meter und bestehen aus mehreren Schichten. Die Lichtteilchen (Photonen) treffen in der Glasfaser kaum auf Widerstand und verlieren nur wenig Schwung. Dennoch führt das Kabel alle 40 bis 100 Kilometer durch torpedoförmige Verstärker und Repeater, welche die optischen Signale aufbereiten und weiterschicken.

2 ROBOTEREINSATZ
In Küstennähe und bis auf 2.000 Metern Tiefe kommt ein »Pflug« zum Einsatz, der eine metertiefe Rinne für das Kabel mechanisch oder mit Wasserdruck in den Boden schneidet. Der Verlegepflug schafft hinter dem Verlegeschiff rund fünf bis 35 Kilometer pro Tag. An tieferen Stellen liegt das Kabel auf dem Meeresgrund auf.

3 KABELROLLEN
Das neue Google-Kabel von den USA nach Japan hat einen Durchmesser von nur zwei Zentimetern. Es liegt vor der Verlegung horizontal in drei riesigen Spulen im Bauch des Kabellegers »René Descartes«. Jeder dieser Kabeltanks ist 16 Meter breit und rund acht Meter hoch. Die 9.000 Kilometer Strecke soll in einem Stück verlegt werden.

4 REPARATUREN
Bruchstellen lassen sich von Land aus bis auf wenige Meter orten. Ein Spezialschiff holt die Enden mit einem Schleppanker (Grapnel) oder einem Tauchroboter herauf, an Bord werden die Lichtwellenleiter getestet, ersetzt und der Bruch wird schließlich geflickt.



DIE GRÖSSTEN FEINDE DER SEEKABEL

5 HAIE
Elektromagnetische Wellen der Stromleitungen an den Kabeln machen Haie wild. Metallarmierungen oder spezielle Kunststoffe sollen die wertvollen Kabel schützen.

6 ANKER UND NETZE
Im Küstenbereich haben ankernde Schiffe und Fischernetze immer wieder Seekabel gekappt. Daher gibt es zunehmend Verbotszonen, und die Kabel werden bis in große Tiefe mit einem »Pflug« im Seeboden vergraben.

7 ERDBEBEN
Die armdicken Kabel sind anfällig gegen Erdstöße und Steinschlag. An Weihnachten 2006 wurden neun Seekabel im Gebiet zwischen den Philippinen und Taiwan in mehreren Tausend Metern Tiefe getrennt, die Reparaturen durch elf Spezialschiffe dauerten mehrere Wochen.

8 MENSCHEN
Mal sind es Saboteure, dann wieder Diebe, zuletzt haben sich verstärkt russische »Forschungsschiffe« für die fragilen Adern interessiert – im Fall von Konflikten lässt sich die Kommunikation des Gegners mit einem gezielten Schnitt lahmlegen.

1850
Das erste Seekabel wurde zwischen England und Frankreich verlegt. Es brach nach einem Telegramm und wurde ein Jahr später ersetzt.

1858
Queen Victoria und US-Präsident James Buchanan kommunizierten durch eine 4.000 Kilometer lange Leitung miteinander.

1866
Eine haltbare Telegrafie-Verbindung besteht zwischen Amerika und Europa.

1956
Das erste Transatlantik-Telefonkabel (TAT-1) zwischen Schottland und Kanada wird in Betrieb genommen. Es konnte 36 Telefonate parallel übertragen.

1988
Das erste Glasfaserkabel wird angebunden (TAT-8), es übertrug 40.000 Telefongespräche gleichzeitig.

2001
Zwischen Deutschland, UK und den USA geht das TAT-14-Glasfaserkabel in Betrieb.

2013
Es wird bekannt, dass der britische Geheimdienst GCHQ das Seekabel TAT-14 sowie rund 200 weitere Glasfaserkabel systematisch abhört.

MEHR INFORMATIONEN

Weltkarte der wichtigsten Seekabel
submarinecablemap.com

Illustration: Christoph Hoppenbrock, bildbauer.de

E-Sport in Deutschland

ERFOLG IM STEALTH-MODUS

Jahrelang spielte sich der elektronische Sport (E-Sport) in einer Nische ab, und die Protagonisten träumten vom großen Durchbruch. Inzwischen strömen Tausende Zuschauer in die Hallen, und Millionen schauen Gaming im Internet. E-Sport hat sich zu einem Big Business entwickelt, ohne dass es draußen groß aufgefallen ist.

Wo sonst die Kölner Haie ihre Bahnen über das Eis ziehen, trafen sich im August 2015 insgesamt 16 qualifizierte Clans aus aller Welt, um ein Major-Turnier in der E-Sport-Disziplin »Counter-Strike: Global Offensive« auszutragen. Neben der Ehre ging es in der »Lanxess Arena« um ein Preisgeld von 250.000 Dollar. Mehr als 10.000 Zuschauer waren vor Ort und über eine Million Fans an den Schirmen. Ein Einzelphänomen? Nicht wirklich, denn schon 2014 und 2015 strömten Zehntausende in die Frankfurter Commerzbank-Arena, um das Turnier »ESL One« mit dem Spiel »DotA« zu verfolgen. Die Nische des E-Sports ist in Deutschland zu einer kritischen Größe angewachsen.

Großer Aufwand, große Träume

Auch Alexander Holzhammer war mal »Pro-Gamer«, ein professioneller Spieler, der Weltmeister wurde, Europameister, und auch noch die E-Bundesliga im Fußballspiel »FIFA« gewann. Sein Spielername war »gamerno1«: »Das war zwischen 2001 und 2008, als Zuschauerzahlen und Preisgelder noch viel kleiner waren als heute.« Nur die Träume nicht, »und auch nicht der Trainingsaufwand«, erinnert sich der Kölner. Während der Schule und des Studiums war viel Zeit, um stundenlang mit Freunden Spielzüge und Tricks einzuüben. »Am Schluss habe ich ganz gut vom E-Sport leben können«, sagt Holzhammer, »und neben dem Studium so viel verdient wie ein normaler Berufsanfänger.«

Heute fließt wesentlich mehr Geld in das Segment, das von einigen großen Multigaming-Clans (= Sportvereine) sowie internationalen Veranstaltern dominiert wird, die eigene Ligen und Wettbewerbe aus dem Boden stampfen. Linear verlief der Aufstieg des E-Sports nicht, viele Umbrüche prägten die Szene. In den Clans herrscht eine Hire&Fire-Mentalität, neue Spiele werden aufgenommen und wieder abgesetzt, Ligen ganz geschlossen oder umgestaltet. »In den beiden vergangenen Jahren hat sich die Vermarktung jedoch enorm weiterentwickelt«, berichtet Holzhammer, der sich inzwischen aus dem aktiven E-Sport zurückgezogen und ein Start-up in der Reisebranche gegründet hat.

Stattliche Summen

Vor allem in den USA und in Asien hat sich E-Sport schon auf breiter Front durchgesetzt, in Korea genießen die Profis und Live-Kommentatoren Starstatus. So liegt das Preisgeld für die LoL-WM 2015 bei über zwei Millionen Dollar, und im Finale »The International 2015«, in dem »DotA 2« gespielt wird, summierten sich die Prämien auf stattliche 18,4 Millionen Dollar. Der Sieger, der US-Clan »Evil Geniuses«, konnte 6,6 Millionen Dollar einstreichen. Kein Wunder, dass einige Spieler angeblich Aufputschmittel nehmen und das »digitale Doping« ein ernstes Problem ist – für Cheat-Programme wie Zielhilfen oder Wallhacks gibt es Märkte im Internet und Dark Web.

Gut laufen auch die Geschäfte von Live-Streaming-Plattformen wie Twitch, zu der die »Evil Geniuses« gehören. Mitte 2014 hat Amazon die Seite, die in Spitzenzeiten einen signifikanten Teil des US-Internet-Verkehrs ausmacht, für knapp eine Milliarde Dollar gekauft. Die Marktforschungsfirma Superdata Research schätzt allein den weltweiten Markt für E-Sport auf über 600 Millionen Dollar pro Jahr sowie die Zielgruppe auf 134 Millionen Menschen. Und neben realen T-Shirts, Bechern und Figuren zieht das Geschäft mit Software-Merchandising an: Auf der ESL One in Köln wurden über 4,2 Millionen Dollar aus den Einnahmen von virtuellen Sticker-Verkäufen an die Teams ausgeschüttet, die sich die Zuschauer auf der Veranstaltung zur Verschönerung ihrer eigenen E-Spielfiguren und zur Unterstützung der Lieblings-Clans gekauft haben.

Rasante Veränderungen

»Der Wandel im Medienkonsum bei Jugendlichen ist krass«, sagt Ex-Profi Holzhammer, »und Gaming ist inzwischen ein bedeutender Teil davon.« Die Veränderung hat sich jedoch weitgehend unbemerkt vollzogen, da viele Erwachsene und Jugendliche keinen Kontakt zur Szene haben. Dies liegt auch daran, dass sich Technik, Spiele und die Branche selbst rasant verändern. Und von unten drängen permanent neue Spieler nach, die schneller klicken und entscheiden können. Auch Holzhammer sieht sich selbst nicht mehr als »Teil der Online-Avantgarde, seit der YouTube-Trend komplett an mir vorbeigegangen ist«. Heute geht der 30-Jährige lieber ins Stadion zum echten Fußball – wo ein Clan noch Club heißt. Allerdings scheint es nur eine Frage der Zeit zu sein, bis die ersten Hologramme über den Rasen laufen und man sich als Fan einen virtuellen Geißbock kaufen kann. //

MEHR INFORMATIONEN

DotA = »Defense of the Ancients« ist ein Action-Echtzeit-Strategiespiel, genannt »Multiplayer Online Battle Arena« (»Moba«).

LoL = »League of Legends« ist ebenfalls ein Moba-Spiel.

Multigaming-Clan = ein (professioneller) Zusammenschluss von Spielern mit Teams für verschiedene Games

E-Sport beim Kicker
esport.kicker.de

E-Sport live
twitch.tv

Diese Seite: ESL One Cologne, Counter-Strike: Global Offensive
Linke Seite: ESL One Frankfurt, DotA 2

Bilder: H. Kristiansson, ESL, eslgaming.com

Big Data – der Ruf nach immer mehr Daten

FUTTER FÜR DEN TRUTHAHN

Prof. Dr. Gerd Gigerenzer

Bild: Dirk Beichert BusinessPhoto

Glaubt man den Prognosen der Marktforscher von IDC, sollen sich bis zum Jahre 2018 die weltweiten Investitionen für Big-Data-Technik auf 41,5 Milliarden US-Dollar belaufen. »Aber diese ungebremste Datensammelei kann zur Illusion von Sicherheit führen und dadurch zum Problem werden«, erklärt der Direktor des Max-Planck-Instituts für Bildungsforschung, Prof. Dr. Gerd Gigerenzer. atFERCHAU befragte den Berliner Risikoforscher zu Risiken und Nebenwirkungen von falsch angewandten »Big-Data-Präparaten«.

Braucht die Wissenschaft eigentlich den Begriff des Risikos, Herr Professor Gigerenzer, beschreibt er letztlich doch nur eine Wahrscheinlichkeit?

Der Begriff Risiko besitzt verschiedene Facetten. Auf der einen Seite, ja, die Definition als Wahrscheinlichkeit. Risiken beinhalten andererseits aber immer auch Chancen – eine Bedeutung, die in Deutschland so nicht im Vordergrund steht, weil man hier eben die Gefahr, die man vermeiden möchte, mit dem Risiko verbindet.

Und dann kennen die Deutschen auch noch das Restrisiko ...

Restrisiko wird oft in einem Zusammenhang verwendet, als gäbe es noch etwas, was man beseitigen könnte. Aber es gibt kein Nullrisiko! Das ist absolut irreführend und der künstliche Begriff versprüht eine trügerische Illusion der Sicherheit.

Deshalb das menschliche Verlangen, die Risiken durch immer mehr Daten – also Big Data – zu minimieren?

Noch so ein moderner Begriff: Aber Big Data gibt es doch schon seit Jahrhunderten, etwa in der Astronomie. Wenn man eine stabile Welt hat, wie zum Beispiel die Bewegungen der Himmelskörper, lohnt sich der Einsatz von Big Data. Wenn die Welt aber instabil und ungewiss ist, wie etwa im Finanzbereich, kann Big Data zur Illusion von Sicherheit führen und zum Problem werden.

Inwiefern?

Wenn Sie die Prognosen von Wechselkursen anschauen und analysieren, werden Sie feststellen, das ist reines Unterhaltungsprogramm, aber bestimmt keine seriöse Vorhersage!

Man könnte also auch zur Wahrsagerin gehen, sagen Sie ...

... ja, oder selbst aus der Glaskugel lesen!

Ohne sogenanntes Fachwissen bin ich eventuell erfolgreicher?

Und manchmal sogar weniger gefährlich! Wechselkursprognosen sind weniger kritisch; aber denken Sie an die allgemeinen Prognosen vor der letzten großen Finanzkrise, als das Vertrauen in die laufenden Systeme immer weiter stieg und die Banken-Ratings diesem verhängnisvollen Trend folgten. In einer stabilen Welt, frei von unvorhersehbaren Ereignissen, schaffen viele Daten eine bessere Vorhersage. Dort aber, wo der Zufall eine große Rolle spielt und Überraschungen eintreten können, gilt diese Regel eben nicht mehr. In unseren Forschungen haben wir gezeigt, dass man durch einfache Heuristiken – Strategien, die versuchen, das Wesentliche zu erfassen und den Rest zu ignorieren – bessere Vorhersagen erzielen kann.

Big Data hilft bei komplexen Verhältnissen also nicht wirklich weiter?

Ein einfaches Beispiel ohne viel Big Data: Nehmen Sie an, Sie wären ein Truthahn. Am ersten Tag Ihres Lebens kommt ein Mann zu Ihnen, und Sie fürchten, er könnte Sie umbringen. Aber er füttert Sie. Am nächsten Tag kommt er wieder, und er füttert Sie wieder. Jetzt fangen Sie an zu rechnen und kommen zum Schluss, dass die Wahrscheinlichkeit, dass er Sie umbringen wird, mit jedem Tag sinkt. Am hundertsten Tag sind Sie sich fast sicher, dass der Mann Sie wieder füttern wird. Was der Truthahn nicht weiß: Dies ist der Tag vor Thanksgiving, wo der Truthahnbraten auf den Tisch kommt. Hätte man nun ein Vorhersageprogramm verwendet, um diese Datenreihe bis zum hundertsten Tag fortzusetzen, wäre wohl immer mehr Futter für den Truthahn angesagt worden.

Mit Big Data kann man überraschende Wendungen des Lebens nicht vorhersagen.

Richtig, denn Big Data arbeitet in der Regel ohne jede Theorie und ein Verständnis für Ursachen. In unserem Projekt »Einfache Heuristiken für eine sichere Welt der Finanzen« untersuchen wir zusammen mit der Bank of England, wie man die irreführende Komplexität von Analysemethoden und Regulierungen reduzieren kann. Wie man mit einfachen Methoden mehr Sicherheit schafft. Denn die sehr komplexen Berechnungen beruhen oft auf Schätzungen, die alle miteinander verknüpft sind. Das ergibt eine unüberschaubare Korrelationsmatrix mit Millionen Verknüpfungen. Und das schafft zweierlei Probleme. Zum einen: Die Ausgangsschätzungen sind notwendigerweise höchst fehlerbehaftet. Und zum anderen: Jeder kann seine Schätzungen wiederum so modifizieren, dass das gewünschte Ergebnis angenähert wird. Bankenaufsichten können diesen Millionen von Schätzungen überhaupt nicht mehr folgen, geschweige denn sie kontrollieren. Wir dürfen nicht wieder den Fehler machen, komplizierte Verhältnisse mit noch komplizierteren Analysemethoden und Big Data abzubilden. Wir brauchen nicht mehr ↘

Illusionen, sondern mehr Kompetenz im Umgang mit Risiken.

Das bestätigt auch eine Umfrage von Forrester Consulting, laut der meist schlechte Datenqualität und fehlende Kompetenz im Umgang mit den Daten als Hinderungsgründe für den Einsatz von Big Data stehen. Steigen denn selbst die Fachleute nicht mehr durch?

Fragen Sie doch einmal Ihren Steuerberater, ob er die Finanzgesetze versteht! Meiner tut's nicht. Die Bank of England hat einmal ein Experiment gemacht und Informationen einer hypothetischen Bank an verschiedene Banken geschickt, mit der Aufgabe, das Risikokapital der fiktiven Bank zu berechnen. Nun sollte man meinen, dass mit den komplexen Berechnungen alle Banken ein zumindest ähnliches Ergebnis erzielt hätten, aber dem war nicht so: Die Ergebnisse variierten um bis zu 100 Prozent.

» Wenn die Welt aber instabil und ungewiss ist, wie etwa im Finanzbereich, kann Big Data zur Illusion von Sicherheit führen und zum Problem werden. «

Und auf dieser Basis werden Entscheidungen getroffen.

Natürlich. Komplexität schafft keine Klarheit, sondern Schlupflöcher. Wir haben viele große Unternehmen zu ihren Entscheidungskriterien befragt, und in der Hälfte aller Fälle waren es »Bauchentscheidungen«. Erfolgreiche Top-Manager spüren, in welche Richtung es gehen soll, können es aber selbst nicht begründen. In der Öffentlichkeit würden sie eine solche Bauchentscheidung wegen der Vorurteile gegen intuitive Entscheidungen niemals zugeben. Aber solche intuitiven Entscheidungen sind keine Willkür, sondern basieren auf viel Erfahrung.

Kann man denn Intuition lernen?

Durchaus. Indem wir lernen, unserer Intuition und den dahintersteckenden Faustregeln zu vertrauen; aber auch gleichzeitig lernen, wann und wie wir ihr vertrauen können.

Intuitive Entscheidungen lassen sich aber nicht erklären, weil ...?

... weil nicht alles, was im Gehirn entschieden wird, der Sprache fähig ist! Die Erfahrung, die nicht sprachlich repräsentiert ist, ist eben nicht irrelevant. Jeder gute Experte braucht gute Intuitionen! Wer auf seinen Bauch hört, nutzt eine unbewusste Form von Intelligenz. Er greift auf Erfahrungen zurück, die er bereits gemacht hat, nutzt Faustregeln und sogenannte soziale Heuristiken, also sein Gespür, auf welche Urteile er sich verlassen, wen er um Rat fragen kann. Wenn jemand in einer Entscheidungssituation ein schlechtes Bauchgefühl hat, dann kann dies ein verlässliches Warnsignal sein, das mit körperlichen Veränderungen einhergeht. Intuition ist keine impulsive Laune des Geistes und auch keine Willkür. Sie macht sich Eigenschaften des Gehirns zunutze, die der Mensch im Zuge der Evolution erworben hat, und speist sich aus den Erfahrungen im ständigen Austausch mit der Umwelt.

Welche Intuition hatte denn Neil Armstrong bei seiner Mondlandung geholfen?

Um gute Intuitionen zu haben, brauchen Sie nicht zum Mond zu reisen. Intuitive Entscheidungen passieren ständig. Und es gibt Lebensbereiche, wo sie auch erwartet werden. Wenn ein Fußballspieler aus einem unmöglichen Winkel ein Tor schießt, kommt der Schiedsrichter ja auch nicht auf den Stürmer zu und sagt: Erst erklären Sie mir, wie Sie es gemacht haben, sonst gilt das Tor nicht! Das wäre absurd! Aber in vielen anderen Bereichen wird erwartet, dass man die Intuition erklären kann. Ein Spieler weiß, wie er den Ball treten muss, kann es aber nicht erklären. Analytisch lassen sich die Regeln für diese Vorgehensweise herausarbeiten, um Anfängern zu helfen, es auch schnell zu lernen.

Oder um es einem Computer beizubringen?

Ja, wenn diese intuitiven Urteile analysiert sind, können die Regeln auch Computern beigebracht werden. Es darf aber nicht dazu führen, dass in einer Welt, in der immer mehr Menschen Angst vor Verantwortung haben, Big Data als ein willkommener Ausweg angesehen wird, diese Verantwortung zu delegieren. So kann man als Verantwortlicher den Fehler zwar auf die falschen Analysen schieben, aber dann ist Big Data ein teures Risikogeschäft mit einem ungewissen Ausgang! //

ÜBER PROF. DR. GERD GIGERENZER

Prof. Dr. Gerd Gigerenzer (Jahrgang 1947 – Psychologe und Risikoforscher) leitet seit 1997 das Max-Planck-Institut für Bildungsforschung sowie das 2009 gegründete Harding-Zentrum für Risikokompetenz in Berlin. Darüber hinaus ist Gigerenzer auch Mitglied der Deutschen Akademie der Wissenschaften (Leopoldina) sowie der Berlin-Brandenburgischen Akademie der Wissenschaften, Ehrendoktor der Universität Basel und der Open University of the Netherlands sowie Batten Fellow an der Darden Business School der Universität von Virginia.

MEHR INFORMATIONEN

Max-Planck-Institut Berlin
bit.ly/1Na2lxJ

RWI Essen
bit.ly/1IVMKmc

International Data Corporation
bit.ly/1oUba3e

Studie Xerox
bit.ly/1izPoVy

SCA Schucker GmbH & Co. KG:
Klebesysteme für die Industrie

400.000 ZEILEN CODE FÜR PERFEKTES KLEBEN

Damit zusammenfindet, was zusammengehört, setzt die SCA Schucker GmbH & Co. KG auf höchste Präzision ihrer Klebesysteme und individuelle Problemlösungen für ihre Kunden. Die Systeme werden vordringlich für die Applikation von Klebstoffen im Automobilbau eingesetzt. Eine ebenso zuverlässige wie variable Software liefert die Basis dafür.

Alexander Haupenthal,
IT-Consultant von FERCHAU

»Die Software spielt in unseren Produkten eine entscheidende Rolle, weil sie entscheidenden Einfluss auf die Qualität der Klebstoffapplikation hat.«

Kleben ist nicht gleich kleben. Und Alleskleber ist, wie die Alltagserfahrung zeigt, ein Mythos. Dennoch ist Kleben »die Fügetechnik des 21. Jahrhunderts«, wie Professor Dr. Andreas Groß vom Fraunhofer Institut für Fertigungstechnik und Angewandte Materialforschung (IFAM) auf den Kundentagen des Klebetechnikspezialisten SCA Anfang Mai in Bretten erklärte. Allerdings kommt es auf die Verarbeitung der Klebstoffe an. Das gilt gerade im industriellen Umfeld. Insbesondere in der Automobilindustrie und im Flugzeugbau werden höchste Anforderungen an Klebeverbindungen gestellt.

Einer, der mit dafür sorgt, dass Millionen von Autofahrern von den Vorteilen der Klebeverbindungen profitieren, ist Alexander Haupenthal. Der IT-Consultant von FERCHAU programmiert bei SCA in Bretten die Steuerung von Klebesystemen für industrielle Ansprüche. »Herausfordernd ist diese Aufgabe vor allem aufgrund der hohen Anforderungen der SCA-Kunden, die überwiegend aus der Automobilbranche kommen«, erklärt Haupenthal.

Seit einem halben Jahr unterstützt der 34-jährige Diplom-Nachrichtentechniker das 15-köpfige Software-Engineering-Team von Abteilungsleiter Michael Ebert beim Entwickeln von Mikrocontroller-Firmware für die Steuerung SYS 6000. Die Bedeutung der Software für den Geschäftserfolg von SCA beschreibt Ebert so: »Die Software spielt in unseren Produkten eine entscheidende Rolle, weil sie entscheidenden Einfluss auf die Qualität der Klebstoffapplikation hat.«

Die SYS 6000 regelt hochpräzise den Volumenstrom des Klebstoffauftrags. Gleichzeitig regelt sie die Temperatur in den verschiedenen Komponenten der Anlage. Die Steuerung über Feldbusse, um mit dem Roboter interagieren zu können, ist ebenfalls ein Muss. So erhält die Steuerung vom Roboter die Signale, wann Kleber dosiert werden soll, und wann nicht. Ebenso steuert die SYS 6000 das Füllen des Dosierers oder das Füllen zu Beginn der Applikation.

Die Bandbreite der Anwendungen von Klebesystemen reicht von dem Verbinden von Komponenten im Karosserierohbau über das Abdichten der Verbindungsstellen bis hin zum flächigen Aufbringen von flüssigen Dämmstoffen oder Unterbodenschutz. Entsprechend umfangreich ist auch die Software, an der Alexander Haupenthal arbeitet: Sie umfasst mehr als 400.000 Zeilen Code in einer Vielzahl unterschiedlicher Module für die einzelnen Aufgabenbereiche. Beim Klebevorgang kommt es darauf an, dass die Steuerung millisekundengenau arbeitet. Schon kleinste Fehler können teure Produktionsausfälle oder Qualitätsmängel verursachen.

Bei der Steppnaht-Applikation kommt es darauf an, dass die Steuerung millisekundengenau arbeitet.

Weltweit befinden sich mehr als 12.500 Anlagen mit SYS-Steuerung von SCA im Einsatz.

Die SCA-Software erfüllt höchste Qualitätsstandards in jedem Einsatzbereich.

Ein Schwerpunkt von Haupenthals Arbeit liegt unter anderem deshalb auf dem Entwerfen von Test-Cases für die Software-Validierung. Selbstverständlich hat er auf seinem Schreibtisch eine SYS 6000 stehen. »So kann ich schnell überprüfen, was ich neu programmiert habe. Aber manche Dinge lassen sich natürlich nur mit Peripherie ausprobieren, und dafür haben wir bei den Kollegen der Abteilung Test und Validierung eine eigene Versuchsumgebung«, erklärt Haupenthal. Dort werden die Funktionen der Software vor der Auslieferung geprüft.

Bei der Programmierung kann Haupenthal seine Erfahrung aus früheren Projekten einbringen: »In der Lkw-Entwicklung bei Daimler habe ich als Messtechnik-Ingenieur auch selbst Versuchsfahrten betreut. Daher kenne ich mich in der Analyse von Steuergeräten aus.« Diese Erfahrung weiß Michael Ebert zu schätzen: »In der Regel reicht es, wenn ich ein Problem grob beschreibe. Herr Haupenthal forscht dann im Quellcode nach den Ursachen, entwickelt selbständig eine Lösung und probiert sie auch soweit möglich aus, so dass sie anschließend direkt in die Abteilung Test und Validieren gehen kann.« Ein weiterer Tätigkeitsbereich von Alexander Haupenthal ist eine PC-gestützte, ergonomische Visualisierungssoftware, mit der Anwender die SYS 6000 zentral bedienen können.

Generell, da sind Ebert und Haupenthal sich einig, gewinnt die Software bei SCA auch weiterhin an Bedeutung. »Durch Industrie 4.0 sehen wir eindeutig einen Trend in Richtung Prozessdatenmanagement. Das heißt, wir werden noch mehr Informationen über den Klebeprozess und den Zustand der Anlagenkomponenten gewinnen und auswerten. Ziel ist es dabei, die Qualität des Applikationsprozesses jederzeit transparent zu machen. Ohne Software geht da nichts.« //

WEITBLICK

Kleben hat in den letzten dreißig Jahren in der Industrie erheblich an Bedeutung gewonnen. Weltweit werden pro Jahr mehr als 13 Mio. Tonnen Klebstoffe verbraucht, berichten die Marktforscher von Ceresana. Laut Industrieverband Klebstoffe e. V. entfällt fast ein Zehntel (neun Prozent) der jährlichen Klebstoffproduktion auf die Fahrzeugbranche. Ein Auto enthält heute rund 15 bis 18 Kilogramm Klebstoff. Kein Wunder: Crash-Tests in der Automobilindustrie haben gezeigt, dass Klebeverbindungen in der A-Säule bessere Resultate beim Überschlag erzielen als geschweißte Teile. Der Trend, im Karosseriebau leichtere und crashsichere Karossen zu entwickeln, führt zu einer Mischbauweise aus unterschiedlichen Werkstoffen. Diese Bauweise unterstützt die hybride Fügetechnik, also die Kombination unterschiedlicher Fügetechnologien. Die Klebetechnologie spielt in diesem Zusammenhang eine zentrale Rolle.

ÜBER SCA

SCA wurde 1986 gegründet und hat sich als Spezialist für Klebesysteme und Dosiertechnologie vor allem in der Automobilindustrie einen Namen gemacht. Seit 2011 gehört SCA zum schwedischen Industriekonzern Atlas Copco. Heute beschäftigt SCA über 500 Mitarbeiter in rund 27 Ländern und erzielt mehr als 141 Millionen Euro Umsatz in 2014.
// www.sca-solutions.com

MEHR INFORMATIONEN

KERSTIN KRAFT
Business Manager IT
FERCHAU Karlsruhe

karlsruhe@ferchau.com
ferchau.com/go/karlsruhe

FERCHAU-Mitarbeiter Holger Lindner arbeitet derzeit für directonline an der Umsetzung von Neu- und Weiterentwicklungen eines CRM-Systems für McFIT.

directonline: CRM-System für 1,2 Millionen Mitglieder

VERSTECKTE KOMPLEXITÄT

Mit über 1,2 Millionen Mitgliedern in fünf Ländern ist McFIT Europas Nr. 1 in der Fitnessbranche. Die einheitliche Kundenpflege der aktuell 235 Standorte erledigt ein von directonline entwickeltes CRM-System, das quasi ständig angepasst und aktualisiert wird. FERCHAU-Mitarbeiter Holger Lindner erläutert, was die Software leisten muss.

Seit Juni 2015 arbeiten Sie bei directonline. Was ist Ihr Aufgabenbereich?

Ich bin als Softwareentwickler im Team »Zentrale« tätig. Wir entwickeln zusammen mit dem Team »Studio« das CRM-System für McFIT. Meine Aufgabe besteht sowohl in der Umsetzung von Neu- und Weiterentwicklungen in allen Bereichen der Software, die die Verwaltungszentrale betreffen, als auch in Supporttätigkeiten im First- und Second-Level-Bereich. Außerdem prüfe ich die Anforderungen des Kunden aus technischer Sicht und bewerte ihre Umsetzbarkeit.

Was muss ein Customer-Relationship-Management für rund 1,2 Millionen Kunden alles können?

Das Softwarepaket automatisiert die Mitglieder- und Mitarbeiterverwaltung sowie die Mitgliederkommunikation per E-Mail und Post. Des Weiteren beinhaltet es die Vertragsabwicklung, die Finanzbuchhaltung, das SEPA-Lastschriftverfahren, die Kontoauszugsverarbeitung, Einwohnermeldeamtsanfragen und den Mahnprozess bis hin zum Datenaustausch mit Inkassounternehmen. Zusätzlich ist die Erstellung und Auswertung von Statistiken möglich.

»Es ist eine Herausforderung, ein über mehr als zehn Jahre gewachsenes System übersichtlich und homogen zu halten.«

Das hört sich nach einer recht umfangreichen Software an ...

Stimmt. Es ist eine speziell an McFIT angepasste »Riesensoftware«. Und man kann sich sicherlich vorstellen, dass es eine Herausforderung ist, ein über mehr als zehn Jahre gewachsenes System übersichtlich und homogen zu halten.

Wie behalten Sie dabei den Überblick?

Zum einen werden die Lösungen sehr speziell an das bestehende System angepasst und meist lokal vorgenommen. Das heißt, die Änderungen werden so umgesetzt, dass sie möglichst wenig Einfluss auf das Kernsystem haben. Die Komplexität versteckt sich sozusagen. Zum anderen kann einer allein natürlich nicht alles wissen. Vielmehr kommt es darauf an zu wissen, wen man zu welchem Thema befragen muss. Aus diesem Grund steht bei uns die Teamarbeit absolut im Vordergrund. Und letztlich muss das Rad ja auch nicht jedes Mal neu erfunden werden: Die Wiederverwendung von vorhandenen Lösungen beseitigt viele Hürden.

»Die Änderungen werden so umgesetzt, dass sie möglichst wenig Einfluss auf das Kernsystem haben.«

Wie gehen Sie im Detail vor, um ein Problem zu lösen?

In der Regel gibt es zu jedem neuen Projekt ein Meeting, in dem die Anforderungen besprochen sowie Korrektur- und Änderungsvorschläge erarbeitet werden. Daraufhin wird ein Lösungskonzept ausgearbeitet – je nach Größe des Projekts entweder allein oder im Team – und mit der Umsetzung begonnen. Anschließend testen wir die neue Version erst in der Entwicklungsumgebung, bevor wir sie auf das Testsystem des Kunden einspielen. Nach der Auswertung der Testergebnisse werden etwaige Fehler bereinigt und die Tests erneut durchgeführt. Hierfür wurden automatisierte Testsysteme eingerichtet, die für uns die Softwareanpassungen überprüfen. Passt alles, wird die neue Version in das Live-System übertragen.

Was reizt Sie an der Tätigkeit?

Das Reizvollste sind die kurzen Entwicklungszyklen. Oftmals sind neue Funktionen oder Bugfixes innerhalb von wenigen Tagen im Live-System und werden von den Sachbearbeitern für die Verwaltung von über 1,2 Millionen Mitgliedern eingesetzt. Es ist ein tolles Gefühl, die eigene Arbeit im professionellen Einsatz zu sehen. Und jedes Projekt bietet die Möglichkeit, sich mit einem anderen Bereich der Software auseinanderzusetzen: Gestern war es die Aufbereitung von Daten für eine Statistik, heute ist es der Export von Daten zum Inkassounternehmen, morgen die Erstellung von Vertragsdokumenten.

Wie sind Sie dazu gekommen, Software zu entwickeln?

Schon früh habe ich durch Videospiele meine Affinität zur Computersoftware entdeckt. Ich wollte immer verstehen, wie eine Maschine dazu fähig sein konnte, die virtuellen Welten zu simulieren, die ich erleben durfte. So fing ich an, mir das Programmieren beizubringen und an kleineren privaten Projekten zu arbeiten.

Herr Lindner, vielen Dank für das Gespräch. //

WEITBLICK

IT im Sportbereich

In vielen Sportarten werden mittlerweile Daten gesammelt, die unter anderem Auskunft geben über die Leistungsfähigkeit der Sportler. Auch im Breitensport findet die Vermessung des Sports statt, zum Beispiel in Form von Pulsmessgeräten, Schritt- und Kalorienzählern oder Fitness-Apps. Laut einer YouGov-Studie hatten Ende 2014 rund 41 Prozent der Befragten eine Gesundheits-App auf dem Smartphone. Zudem hat sich der weltweite Absatz von Smartwatches und Fitness-Trackern laut statista.com in den vergangenen Jahren verdreifacht – von 17 auf 51 Millionen Stück.

METHODEN UND TOOLS

Programmiersprache: Delphi XE7; Datenbanken: MSSQL und MySQL; Anwendungen: Jira und Confluence von Atlassian.

ÜBER DIRECTONLINE

directonline wurde 1999 von Thorsten Schultheis als Software-Start-up mit dem Schwerpunkt Informationssysteme im Bereich Versicherungswesen gegründet. Bereits ein Jahr später erfolgte die Verlagerung des Kerngeschäfts auf die Sport- und Freizeitindustrie. Mittlerweile beschäftigt die Firma directonline über 40 Mitarbeiter. Seit November 2015 finden Sie die Firma an ihrem neuen Standort in Würzburg. // directonline.de

MEHR INFORMATIONEN

UFUK SEN
Account Manager IT
FERCHAU Schweinfurt

schweinfurt@ferchau.com
ferchau.com/go/schweinfurt

AES: Softwaretest für neue Triebwerkgeneration

30.000 TEILE UND ZIGTAUSEND PARAMETER

Wer einem Flugzeugtriebwerk nahe gekommen ist und es nackt, ohne bedeckende Verkleidungsschalen gesehen hat, der wird dessen imposante Erscheinung nicht vergessen. Wie steuert man diese aus über 30.000 Teilen bestehenden technischen Wunderwerke? Und wie testet man die Funktionssicherheit? Bei AES Aerospace Embedded Solutions GmbH geben zwei IT-Consultants von FERCHAU Antworten.

»Preiskampf ruiniert Luftfahrtbranche«, titelte das Nachrichtenmagazin FOCUS im vergangenen Jahr. Die Branche sei im Umbruch. Ruinöser Konkurrenzkampf, Überkapazitäten, geizige Kunden, hohe Fixkosten setzten Airline-Manager unter Druck.

Im Wettbewerb um geringere Costs per Seat setzen Flugzeugbauer heute daher verstärkt am Herzstück der Flieger an: den Triebwerken. Weniger Emissionen und Treibstoffverbrauch heißt die Vorgabe für die Luftfahrtindustrie. Höhere Reichweiten sollen bei gleicher Tankfüllung erreicht werden und die Betriebskosten sinken. Der US-amerikanische Triebwerkspezialist Pratt & Whitney erfüllt mit der neuen Getriebefan-Triebwerksfamilie PurePower® PW1000G, an der die MTU Aero Engines mit ihren Schlüsselkomponenten beteiligt ist, exakt diese Forderungen. Das moderne Getriebefan-Triebwerk (siehe Infokasten Weitblick) ist leiser, stößt weniger Stickoxide und rund 15 Prozent weniger CO_2 aus und verbraucht 15 Prozent weniger Treibstoff. Die Antriebsfamilie kommt im Airbus A320neo, aber auch in Fliegern von Bombardier, Mitsubishi, Embraer und Irkut zum Einsatz.

Neue Werkstoffe und technische Komponenten sowie konstruktive Neuerungen sind nur so wirkungsvoll, wie sie eine intelligente Steuerung in Szene setzen. Hier kommt die Münchner Softwareschmiede Aerospace Embedded Solutions GmbH (AES) ins Spiel. Die Münchner sind Spezialisten für Entwicklung und Test von sicherheitskritischen Hard- und Softwarekomponenten im Luft- und Raumfahrtbereich. Im Auftrag der MTU Aero Engines testet AES verschiedene Softwarekomponenten für die Steuerung des Electronic Engine Control (EEC) Systems, das in den neuen Pratt & Whitney-Antrieben eingesetzt wird.

»Kern unserer Arbeit ist es, alle Parameter zu testen, die zur Steuerung des Triebwerks erforderlich und definiert sind«, erklärt Norbert Vogel, Director Quality bei AES. Reagiert das EEC des Triebwerks auf Parameter – das können schon mal mehrere 10.000 sein –, so wie es in den vom Kunden gelieferten Requirements beschrieben ist? »Dabei geht es darum, die geforderte Funktion der Software zu überprüfen und alle möglichen Fehlerzustände zu identifizieren und zu eliminieren. Softwaretest ist eine – wenn auch sehr wichtige – Methode, um die Steuerungssoftware zu verifizieren«, so Vogel weiter. Um jede Codezeile der Steuerungssoftware genau zu prüfen, hat AES sein eigenes Testteam durch IT-Consultants von FERCHAU München verstärkt.

Thorsten Pfeifer und Khanh Nguyen erarbeiten Testszenarien, führen Checks durch und dokumentieren die Ergebnisse. »Wir stellen sicher, dass die hohen Qualitätsstandards und Vorgaben des Kunden und der Überwachungsbehörden eingehalten werden«, erklärt Thorsten Pfeifer, Master für Luft- und Raumfahrt. Was das konkret bedeuten kann, erklärt der Elektro- und Informationstechnikingenieur Khanh Nguyen: Code-Reviews und Softwaremodul-Reviews auf der untersten Ebene. Im Einzelnen sind das Normal Range Test Cases, Robustness Test Cases, Test-Coverage-Analyse, Structural-Coverage-Analysen sowie Überprüfen von Anforderungen am Simulator und etwaige Fehler oder Abweichungen minutiös dokumentieren. »Es besteht auch die Möglichkeit, nicht durchlaufene Code-Sequenzen, so genannte ›deactivated codes‹, gewollt zu deaktivieren«, fügt Pfeifer hinzu. Dieser wird im normalen Zustand des Systems zwar nicht angesteuert, in einem unbeabsichtigten Fehlerzustand befürchtet man hier jedoch ein ungewolltes und unvorhersehbares Verhalten des Systems. Tools wie »Notepad++«, »Unigraph« und »Eclipse« unterstützen die beiden bei ihrer Arbeit.

Basis für die Tests und Prüfungen bildet die RTCA-Norm DO-178B, ein Standard zur Softwareentwicklung im sicherheitskritischen Bereich der Luftfahrt. »Der Nachweis erfolgt anhand der Dokumentierung und ist Voraussetzung für eine Zertifizierung von Software für den Einsatz in der Luftfahrt«, erläutert Testexperte Nguyen die Kerninhalte der Norm. Grundsätzlich ist es dem Anwender überlassen, welches Lebenszyklus-Modell er verwendet. »Bei AES kommt das bewährte und strenge V-Modell, das auch viele unserer Kunden benutzen, zum Einsatz«, resümiert Qualitätsmanager Vogel, »so dass jede Phase der Entwicklung und des Tests nachvollziehbar und transparent ist.« //

STECKBRIEF ZU DEN EXPERTEN

Thorsten Pfeifer
Master Luft- und Raumfahrttechnik

Aufgabe: Erstellung von Testszenarien, Dokumentation der Ergebnisse nach RTCA/DO-178B; Sichten der Input-Dokumente, Umsetzen der Requirements in testbare Sequenzen, Analysieren der Ergebnisse aus den erstellten Tests, Dokumentieren der Ergebnisse.
Stärken: Kommunikative Teamarbeit, Lernbereitschaft, selbst organisiertes Arbeiten, Nachvollziehen komplizierter Zusammenhänge
Leidenschaft: Sport, Informatik, Technik, handwerkliche Tätigkeiten

Khanh Nguyen
Elektro- und Informationstechnikingenieur

Aufgabe: Erstellung, Durchführung und Dokumentation von Testszenarien nach RTCA/DO-178B; Sicherstellung von Qualitäts-Standards, Erstellung von anforderungsbasierenden Testszenarien, Auswertung und Dokumentation der Testergebnisse.
Stärken: Strukturierte und ergebnisorientierte Arbeitsweise, Verständnis für komplexe System-Prozesse, Teamfähigkeit und Kommunikation im Team.
Leidenschaft: Technik, Informatik, Sport, Reisen

MEHR INFORMATIONEN

DANIEL KRÖNER
Senior Account Manager IT
FERCHAU München

muenchen@ferchau.com
ferchau.com/go/muenchen

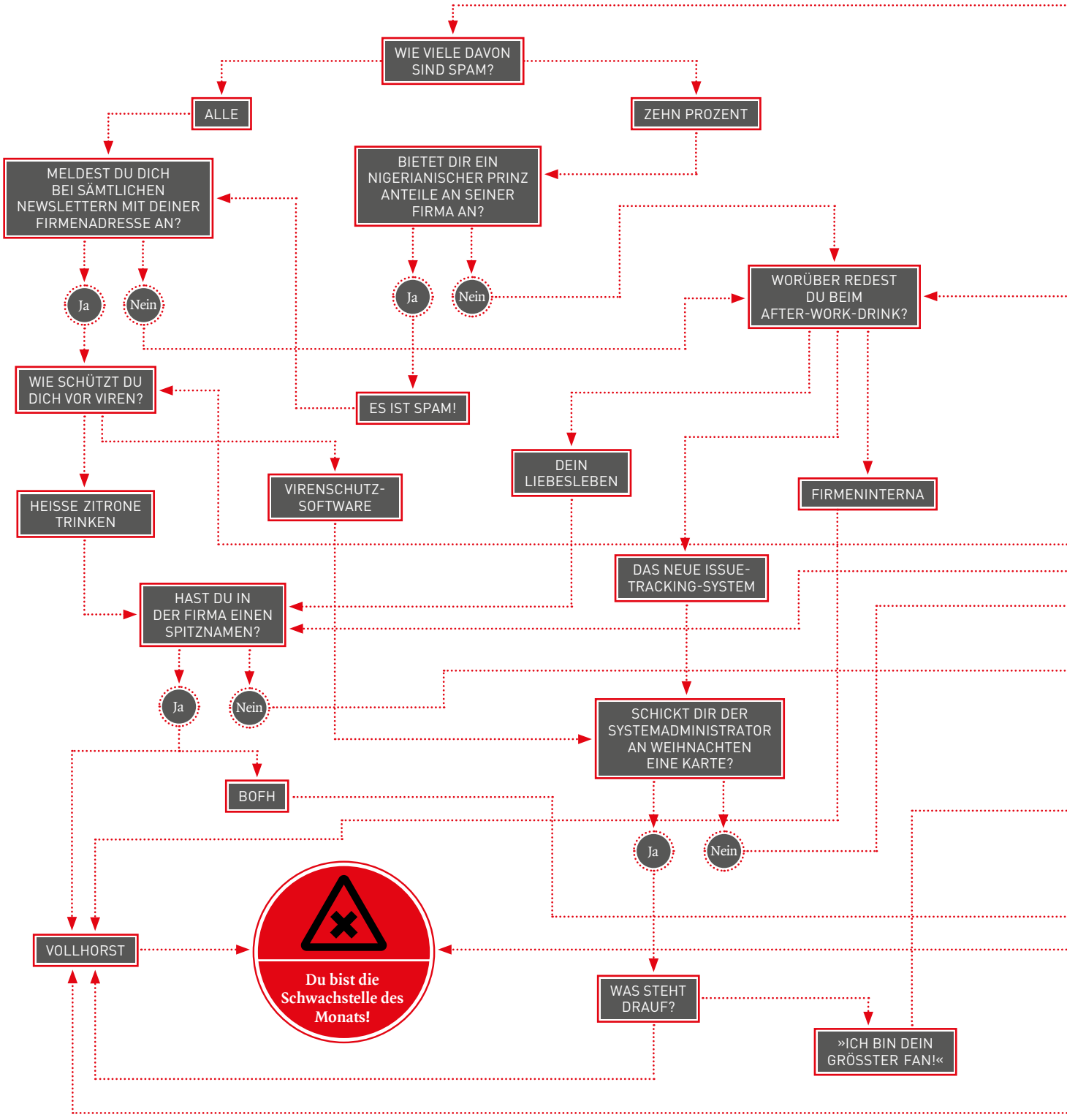
WEITBLICK

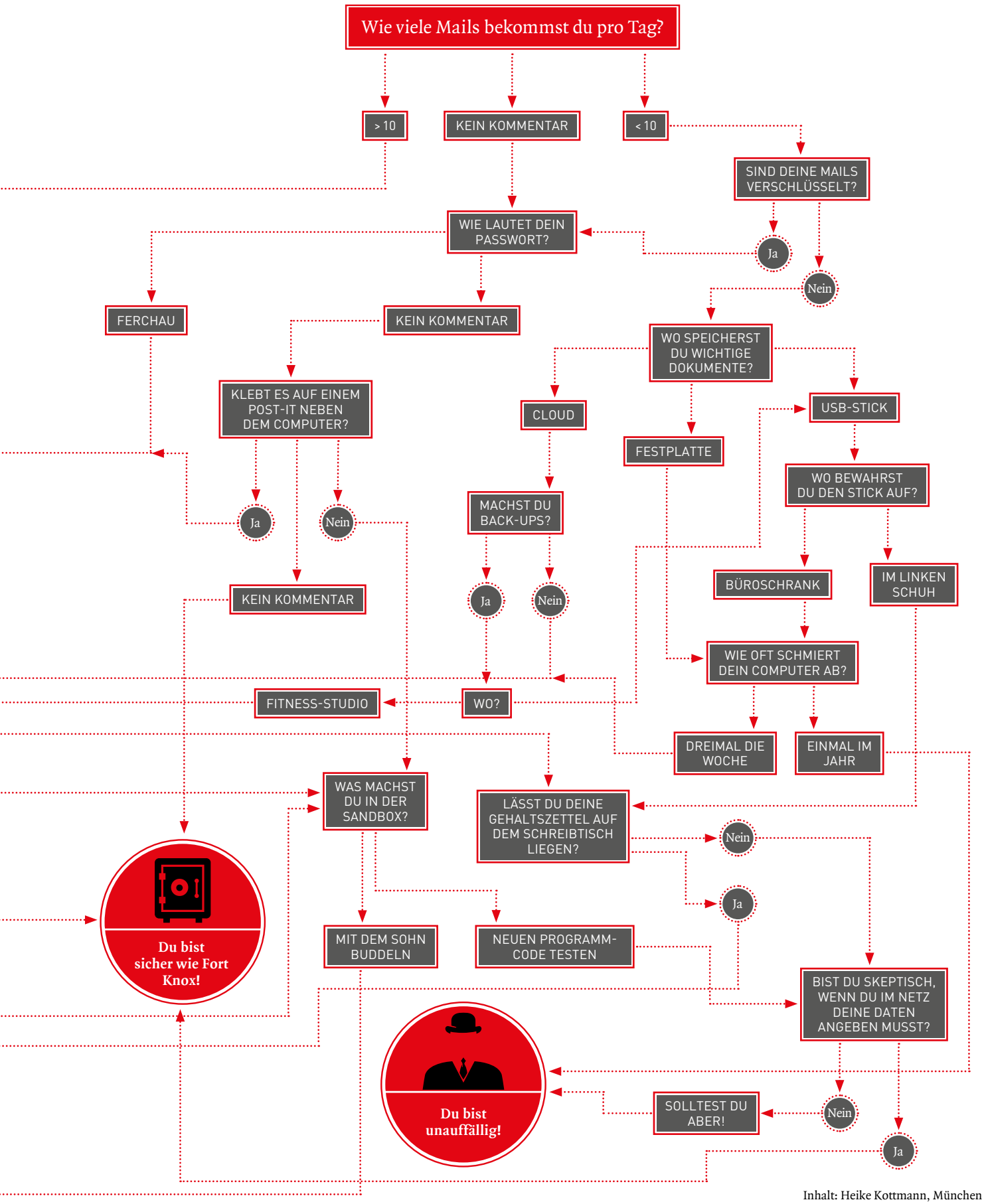
Neue Triebwerkgeneration

Im Gegensatz zu konventionellen Turbofan-Triebwerken ist die neue PurePower®-Familie von Pratt & Whitney mit einem Untersetzungsgetriebe (Planetengetriebe 3:1) zwischen Niederdruckturbine und Fan ausgestattet. Durch diese Entkopplung der beiden Module kann der vergrößerte Fan langsamer und die Niederdruckturbine schneller laufen als bisher. Auf diese Weise erreichen beide Module ihr jeweiliges Leistungsoptimum. Verbrauchswerte, Emissionen und Geräuschpegel werden dadurch reduziert. Auf einer Strecke von München nach London soll sich hiermit rund eine halbe Tonne Kerosin sparen lassen. Überdies sinken die Instandhaltungskosten um 20 Prozent. Laut dem Branchenmagazin »Flugrevue« (November 2015) haben die PurePower®-Triebwerke 20.000 Teststunden, davon 6.000 in der Luft, und 36.000 Zyklen absolviert.

Baum der Erkenntnis

BIN ICH EIN SICHERHEITSRISIKO?





Inhalt: Heike Kottmann, München

atFERCHAU-Gewinnspiel

IPAD PRO: ZUM WEGLEGEN ZU LEICHT

Es ist der vielleicht smarteste Handschmeichler unter den Gadgets überhaupt: das iPad Pro. Trotz des 12,9"-Displays ist es gerade mal 6,9 mm dünn und wiegt 713 Gramm. Herzstück ist der neue A9X, die dritte Generation des Chips mit 64-Bit-Desktoparchitektur. Er liefert eine bis zu 1,8-fache CPU-Performance und die doppelte Grafikleistung des iPad Air 2. Apple verspricht neun Stunden Laufzeit. Sie wollen das persönlich überprüfen und ein iPad Pro in Space Grau mit 32 GB gewinnen? Dann loggen Sie sich ein unter: **ferchau.com/go/it-gewinnspiel** und beantworten Sie folgende Frage: Auf wie viele US-Dollar Jahresumsatz wird der Markt für E-Sport geschätzt? Tipp: aufmerksam die Seite 21 lesen. Einsendeschluss ist der 24.3.2016. Viel Glück!

Gewinner der Apple Watch der letzten Ausgabe ist: Herr Andreas Firla von der ContiTech Vibration Control GmbH in Hannover. Herzlichen Glückwunsch!

ferchau.com/go/it-gewinnspiel

Jubiläum: 50 Jahre FERCHAU

ALS 1860 DEUTSCHER MEISTER WURDE

2016 feiert FERCHAU sein 50-jähriges Bestehen. Während Computer 1966 noch ganze Räume füllten – mit weniger Power als ein heutiges Smartphone –, schreitet der technische Fortschritt weiter mit immensem Tempo voran. Was bringt die Zukunft in Sachen IT?

Als Heinz Ferchau im Jahr 1966 ein Ingenieurbüro gründete – die FERCHAU Konstruktion GmbH –, wurde der TSV 1860 München gerade das erste und bisher einzige Mal deutscher Fußballmeister. Und die Nationalmannschaft verlor wenig später das WM-Finale gegen Gastgeber England – nicht zuletzt aufgrund des legendären Wembley-Tors – mit 2:4 nach Verlängerung. Ganz ohne Torlinientechnik, Sensoren in den Schienbeinschützern und am Rechner optimierte Taktiken.

In der Welt der Informationstechnik fiel 1966 der Startschuss für die dritte Rechnergeneration. Die Entwicklung der integrierten Schaltungen, der sogenannten Mikrochips, hatte begonnen. Erste Kleincomputer wurden gebaut, erste Netzwerke gebildet. Alles kleine Schritte, die die Grundlage für unsere heutige Welt der Technik bildeten. Laptops, Tablets, Smartphones, Smartwatches – die Geräte werden immer kleiner und können immer mehr. Wohin führt uns der technische Fortschritt?

1966-1974
Dritte Rechnergeneration: integrierte Schaltungen (Mikrochips), erste Kleinrechner und Netzwerke.

1969
Das »ARPANET«, das erste Computernetz der Welt, wird in Amerika in Betrieb genommen.

1974-1982
Vierte Rechnergeneration: hochintegrierte Schaltungen, Halbleiterspeicher, erste Super-Computer.

1981
»Osborne 1« ist der erste portable Computer. IBM bringt seinen IBM Personal Computer auf den Markt.

1984
Apple stellt den ersten Personal Computer mit einer grafischen Benutzeroberfläche vor.

1988
Der erste Internet-Wurm richtet großen Schaden an: 6.000 Rechner sind betroffen.

1968
Friedrich L. Bauer gründet an der TU München den ersten Informatik-Studiengang in Deutschland.

1971
Ray Tomlinson schreibt das erste E-Mail-Programm. Intel verkauft den ersten Mikroprozessor, den 4004.

1977
Das erste Infopaket wird mittels »TCP« über einen Radiosender, ein Kabelnetz und eine Satellitenverbindung verschickt.

1983
Das TCP/IP-Protokoll wird offizieller Standard für das Internet.

1985
Microsoft Windows 1.0 als grafische Oberfläche für MS/DOS wird schrittweise zum eigenständigen Betriebssystem ausgebaut.

1989
Die erste Anti-Viren-Software wird vorgestellt.

FERCHAU auf der CeBIT 2016

MITMACHEN, GESTALTEN UND ERFOLGREICH SEIN

Der Hype um die Digitalisierung und Industrie 4.0 bleibt ungebrochen. Doch was bedeutet die digitale Transformation konkret für Wirtschaft und Gesellschaft? Antworten soll die CeBIT in Hannover geben, die in diesem Jahr mit dem Leitmotto »d!conomy: join – create – succeed« an den Start geht. Auch FERCHAU ist vom 14. bis 18. März 2016 mit einem Stand auf der weltweit größten IT-Messe präsent.

»Die Digitalisierung ist kein kurzfristiges Phänomen, sondern bietet langfristig große Chancen«, sagt Oliver Frese, Vorstand der Deutschen Messe AG. Dennoch stellen sich vor allem kleinere und mittelgroße Unternehmen bisher nur zögerlich den Herausforderungen der Digitalisierung. Zwar müssen die großen und politischen Rahmenbedingungen – zum Beispiel hinsichtlich der Datensicherheit – erst noch gestaltet und neue Geschäftsmodelle, Produktionsprozesse sowie Kommunikations- und Arbeitsformen entwickelt werden. Doch klar ist: »Wer sich auch künftig in einem hochdynamischen Marktumfeld behaupten will, muss die Chancen der digitalen Transformation ergreifen«, meint Frese. Die Informationen, Innovationen und Inspirationen dazu liefere die CeBIT.

Partnerland der IT-Messe ist in diesem Jahr übrigens die Schweiz, eines der innovativsten Länder der Welt und international anerkannte Drehscheibe für Forschung und Entwicklung. Ein Land, das beim Einsatz digitaler Technologien im weltweiten Vergleich führend ist und das laut Digitalverband BITKOM zu den Top-10-Handelspartnern für deutsche IT- und Telekommunikationsunternehmen gehört.

Wer sich über Einstiegsmöglichkeiten, Karrierechancen und Weiterbildungsmöglichkeiten sowie über das gesamte Leistungsportfolio von FERCHAU informieren möchte, ist an unserem CeBIT-Stand genau richtig. Einer unserer Schwerpunkte bleibt Industrie 4.0, ergänzt durch Produktentwicklung in den Bereichen Mobility, Health Care und Power. Sprechen Sie mit unseren IT-Consultants vor Ort.

CeBIT 2016

Besuchen Sie uns in
HALLE 11,
STAND B17

CeBIT

14.–18.03.2016

Im Roman »Germany 2064« des schottischen Schriftstellers Martin Walker ist Deutschland im Jahr 2064 zweigeteilt: in High-Tech-Städte unter staatlicher Kontrolle und in selbstverwaltete freie Gebiete, naturnah und weitgehend technologiefrei. Wenig überraschend fahren die Autos in den Städten automatisch, und Roboter erledigen die meisten Aufgaben. Viele der Dinge im Roman sind Weiterentwicklungen von Geräten und Technologien, die es teilweise heute schon gibt.

Einen ähnlichen, wenn auch weiteren Blick in die Zukunft wirft der Physiker Michio Kaku. In seinem Buch »Die Physik der Zukunft« trifft er Vorhersagen über das Leben in 100 Jahren. Dazu hatte er zuvor 300 führende Wissenschaftler befragt. Die Antworten reichen von medizinischen Diagnosegeräten à la Raumschiff Enterprise, mit denen Patienten berührungslos untersucht werden, über selbst fahrende Magnetautos, Telefongespräche mit Gesprächspartnern, die als 3D-Hologramme erscheinen, bis hin zu Computerchips, die in jedem Gegenstand installiert sind und durch unsere Gedanken gesteuert werden. Kakus Ansicht nach werden die technischen Neuerungen dazu führen, dass der Wohlstand im 22. Jahrhundert gleichmäßiger verteilt wird und sich die Ländergrenzen langsam auflösen. Dann wird FERCHAU Engineering schon 150 Jahre alt sein.

1990
Das World Wide Web wird samt HTML und Browser von Tim Berners-Lee und Robert Cailliau am CERN präsentiert.

1991
Der Mathematiker Phil Zimmerman führt die digitale Verschlüsselungstechnik »Pretty Good Privacy« (PGP) ein.

1994
Festplatten erreichen erstmals eine Kapazität von 1 Gigabyte. Die Suchmaschine »Google« geht online.

1997
Die ersten LCD-Bildschirme werden vorgestellt. Es sind rund sechs Millionen Computer mit dem Internet verbunden.

1998
Die Internet Corporation for Assigned Names and Numbers (ICANN) wird gegründet.

1999
Die einmillionste .de-Domain wird registriert.

2007
Die Spam-Quote bei E-Mails erreicht 90 Prozent. Apple führt mit dem iPhone seine erfolgreiche Smartphone-Reihe ein.

2010
Erstmals wird ein Rechner im Weltraum mit dem Internet verbunden. Apples iPad sorgt für den Durchbruch der Tablets.

2012
Google stellt seine »Datenbrille« Google Glass vor, einen am Kopf getragenen Miniaturcomputer.

2015
Microsoft veröffentlicht Windows 10 als einheitliches Betriebssystem für verschiedenste Geräteklassen.

2016
Gerüchte: Samsung präsentiert ein faltbares Smartphone, LG einen aufrollbaren Fernseher.

2020
Prognose: Die ersten selbst fahrenden Autos kommen in Serienreife auf den Markt.

JAHRE