Strategies to Mitigate Targeted Cyber Intrusions

INTRODUCTION

1. Australian computer networks are being targeted by adversaries seeking access to sensitive information. A commonly used technique is social engineering, where malicious "spear phishing" emails are tailored to entice the reader to open them. Users may be tempted to open malicious email attachments or follow embedded links to malicious websites. Either action can compromise the network and disclose sensitive information.

2. The Defence Signals Directorate (DSD) has developed a list of strategies to mitigate targeted cyber intrusions. The list is informed by DSD's experience in operational cyber security, including responding to serious cyber incidents and performing vulnerability assessments and penetration testing for Australian government agencies.

MITIGATION STRATEGIES

3. DSD's list of mitigation strategies, first published in February 2010, is revised for 2011 based on DSD's most recent analysis of incidents across the Australian Government. This revised version combines several similar strategies and adds new ones. A detailed list of changes is available at the DSD web page mentioned below.

4. While no single strategy can prevent this type of malicious activity, the effectiveness of implementing the top four strategies remains unchanged. Implemented as a package, these strategies would have prevented at least 70% of the intrusions that DSD analysed and responded to in 2009, and at least 85% of the intrusions responded to in 2010.

5. Implementing the top four strategies can be achieved gradually, starting with computers used by the employees most likely to be targeted by intrusions, and eventually extending them to all users. Once this is achieved, organisations can selectively implement additional mitigation strategies based on the risk to their information.

6. This document provides information about mitigation implementation costs and user acceptance to help organisations select the best set of strategies for their requirements.

7. These strategies complement the guidance provided in the Australian Government Information Security Manual (ISM) available at DSD's web site http://www.dsd.gov.au

CONTACT DETAILS

8. This document and additional information about implementing the 35 mitigation strategies is available at http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

9. Australian government agencies seeking clarification about this document can contact DSD via assist@dsd.gov.au

10. Australian businesses and other Australian private sector organisations seeking further information should contact CERT Australia via info@cert.gov.au

Australian Government
Department of Defence
Intelligence & Security

Strategies to Mitigate Targeted Cyber Intrusions

Originally published 18 February 2010, last updated 18 July 2011

CYBER SECURITY OPERATIONS CENTRE

Mitigation Strategy Effectiveness Ranking	Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)	Designed to Prevent or Detect an Intrusion	Helps Mitigate Intrusion Stage 1: Code Execution	Helps Mitigate Intrusion Stage 2: Network Propagation	Helps Mitigate Intrusion Stage 3: Data Exfiltration
1	**Patch applications** e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate within two days for high risk vulnerabilities. Use the latest version of applications.	Excellent	Low	High	High	Prevent	Yes	No	No
2	**Patch operating system** vulnerabilities. Patch or mitigate within two days for high risk vulnerabilities. Use the latest operating system version.	Excellent	Low	Medium	Medium	Prevent	Yes	Possible	Possible
3	**Minimise the number of users with domain or local administrative privileges**. Such users should use a separate unprivileged account for email and web browsing.	Excellent	Medium	Medium	Low	Prevent	Possible	Yes	Possible
4	**Application whitelisting** to help prevent malicious software and other unapproved programs from running e.g. by using Microsoft Software Restriction Policies or AppLocker.	Excellent	Medium	High	Medium	Both	Yes	Yes	Yes

Once organisations have implemented the top four mitigation strategies, firstly on computers used by employees most likely to be targeted by intrusions and then for all users, additional mitigation strategies can then be selected to address system security gaps to reach an acceptable level of residual risk.

5	**Host-based Intrusion Detection/Prevention System** to identify anomalous behaviour such as process injection, keystroke logging, driver loading and call hooking.	Excellent	Low	Medium	Medium	Both	Yes	No	Possible
6	**Whitelisted email content filtering** allowing only attachment types required for business functionality. Preferably convert/sanitise PDF and Microsoft Office attachments.	Excellent	High	High	Medium	Prevent	Yes	No	Possible
7	**Block spoofed emails** using Sender Policy Framework checking of incoming emails, and a "hard fail" SPF record to help prevent spoofing of your organisation's domain.	Excellent	Low	Low	Low	Prevent	Yes	No	No
8	**User education** e.g. Internet threats and spear phishing socially engineered emails. Avoid: weak passphrases, passphrase reuse, exposing email addresses, unapproved USB devices.	Excellent	Medium	High	Medium	Both	Possible	No	No
9	**Web content filtering** of incoming and outgoing traffic, using signatures, reputation ratings and other heuristics, and whitelisting allowed types of web content.	Excellent	Medium	Medium	Medium	Prevent	Yes	No	Possible
10	**Web domain whitelisting for all domains**, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.	Excellent	High	High	Medium	Prevent	Yes	No	Yes
11	**Web domain whitelisting for HTTPS/SSL domains**, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.	Excellent	Medium	Medium	Medium	Prevent	Yes	No	Yes
12	**Workstation inspection of Microsoft Office files** for abnormalities e.g. using the Microsoft Office File Validation feature.	Excellent	Low	Low	Low	Prevent	Yes	No	No
13	**Application based workstation firewall**, configured to deny traffic by default, to protect against malicious or otherwise unauthorised **incoming** network traffic.	Good	Low	Medium	Medium	Prevent	Yes	Yes	No
14	**Application based workstation firewall**, configured to deny traffic by default, that whitelists which applications are allowed to generate **outgoing** network traffic.	Good	Medium	Medium	Medium	Both	No	Yes	Yes
15	**Network segmentation and segregation** into security zones to protect sensitive information and critical services such as user authentication and user directory information.	Good	Low	High	Medium	Prevent	Possible	Yes	Possible
16	**Multi-factor authentication** especially implemented for when the user is about to perform a privileged action, or access a database or other sensitive information repository.	Good	Medium	High	Medium	Prevent	No	Possible	No
17	**Randomised local administrator passphrases** that are unique and complex for all computers. Use domain group privileges instead of local administrator accounts.	Good	Low	Medium	Low	Prevent	No	Yes	No
18	**Enforce a strong passphrase policy** covering complexity, length, and avoiding both passphrase reuse and the use of dictionary words.	Good	Medium	Medium	Low	Prevent	No	Yes	No
19	**Border gateway** using an IPv6-capable firewall to prevent computers directly accessing the Internet except via a split DNS server, an email server, or an authenticated web proxy.	Good	Low	Low	Low	Both	Possible	No	Yes
20	**Data Execution Prevention** using hardware and software mechanisms for all software applications that support DEP.	Good	Low	Low	Low	Prevent	Yes	No	No
21	**Antivirus software** with up to date signatures, reputation ratings and other heuristic detection capabilities. Use gateway and desktop antivirus software from different vendors.	Good	Low	Low	Low	Both	Yes	No	No
22	**Non-persistent virtualised trusted operating environment** with limited access to network file shares, for risky activities such as reading email and web browsing.	Good	High	High	Medium	Prevent	No	Yes	Possible
23	**Centralised and time-synchronised logging** of allowed and blocked **network activity**, with regular log analysis, storing logs for at least 18 months.	Good	Low	High	High	Detect	Possible	Possible	Possible
24	**Centralised and time-synchronised logging** of successful and failed **computer events**, with regular log analysis, storing logs for at least 18 months.	Good	Low	High	High	Detect	Possible	Possible	Possible
25	**Standard Operating Environment** with unrequired operating system functionality disabled e.g. IPv6, autorun and Remote Desktop. Harden file and registry permissions.	Good	Medium	Medium	Low	Prevent	Yes	Yes	Possible
26	**Workstation application security configuration hardening** e.g. disable unrequired features in PDF viewers, Microsoft Office applications, and web browsers.	Good	Medium	Medium	Medium	Prevent	Yes	No	No
27	**Restrict access to NetBIOS** services running on workstations and on servers where possible.	Good	Low	Medium	Low	Prevent	Yes	Yes	No
28	**Server application security configuration hardening** e.g. databases, web applications, customer relationship management and other data storage systems.	Good	Low	High	Medium	Prevent	Yes	No	Yes
29	**Removable and portable media control** as part of a Data Loss Prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.	Good	High	Medium	Medium	Prevent	Yes	Possible	Yes
30	**TLS encryption between email servers** to help prevent legitimate emails being intercepted and used for social engineering. Perform content scanning after email traffic is decrypted.	Good	Low	Low	Low	Prevent	Possible	No	No
31	**Disable LanMan** password support and cached credentials on workstations and servers, to make it harder for adversaries to crack password hashes.	Good	Low	Low	Low	Prevent	No	Yes	No
32	**Block attempts to access web sites by their IP address** instead of by their domain name.	Good	Low	Low	Low	Both	Yes	No	Yes
33	**Network-based Intrusion Detection/Prevention System** using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	Average	Low	High	High	Both	Possible	Possible	Possible
34	**Gateway blacklisting** to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous Internet users.	Average	Low	Low	High	Both	Yes	No	Yes
35	**Full network traffic capture** to perform post-incident analysis of successful intrusions, storing network traffic for at least the previous seven days.	Minimal	Low	High	Low	Detect	No	No	No

This document and additional information about implementing the 35 mitigation strategies is available at http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm