Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

PROTECT

FEBRUARY 2014

LEGAL NOTICE: THIS PUBLICATION HAS BEEN PRODUCED BY THE DEFENCE SIGNALS DIRECTORATE (DSD), ALSO KNOWN AS THE AUSTRALIAN SIGNALS DIRECTORATE (ASD). ALL REFERENCES TO ASD SHOULD BE TAKEN TO BE REFERENCES TO DSD.

Strategies to Mitigate Targeted Cyber Intrusions

Introduction

1. Australian computer networks are being targeted by adversaries seeking access to sensitive information.

2. 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.

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

Mitigation Strategies

4. ASD's list of mitigation strategies, first published in February 2010, is revised for 2014 based on ASD's most recent analysis of cyber intrusions across the Australian Government. This document provides a summary of key changes for 2014.

5. While no single strategy can prevent malicious activity, the effectiveness of implementing the Top 4 strategies remains very high. At least 85% of the cyber intrusions that ASD responds to involve adversaries using unsophisticated techniques that would have been mitigated by implementing the Top 4 mitigation strategies as a package.

6. Implementing the Top 4 mitigation strategies can be achieved gradually, firstly on workstations of users who are most likely to be targeted by cyber intrusions, and then implementing them on all workstations and servers. Once this is achieved, organisations can selectively implement additional mitigation strategies to address security gaps until an acceptable level of residual risk is reached.

7. This document provides information about comparative mitigation implementation costs and user resistance levels to help organisations select the best set of strategies for their requirements.

8. These strategies complement the guidance provided in the *Australian Government Information Security Manual* (ISM) available on ASD's website.

Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

Strategies to Mitigate Targeted Cyber Intrusions

Originally published 18 February 2010, updated for February 2014

Mitigation Strategy Effectiveness Ranking for 2014 (and 2012)	Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)	Helps Detect Intrusions	Helps Prevent Intrusion Stage 1: Code Execution	Helps Contain Intrusion Stage 2: Network Propagation	Helps Contain Intrusion Stage 3: Data Exfiltration
1 (1)	**Application whitelisting** of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers.	Essential	Medium	High	Medium	Yes	Yes	Yes	Yes
2 (2)	**Patch applications** e.g. Java, PDF viewer, Flash, web browsers and Microsoft Office. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications.	Essential	Low	High	High	No	Yes	Possible	No
3 (3)	**Patch operating system vulnerabilities**. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP.	Essential	Low	Medium	Medium	No	Yes	Possible	No
4 (4)	**Restrict administrative privileges** to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.	Essential	Medium	Medium	Low	No	Possible	Yes	No

Once organisations have effectively implemented the Top 4 mitigation strategies, firstly on workstations of users who are most likely to be targeted by cyber intrusions and then on all workstations and servers, additional mitigation strategies can then be selected to address security gaps until an acceptable level of residual risk is reached.

5 (18)	**User application configuration hardening**, disabling: running Internet-based Java code, untrusted Microsoft Office macros, and unneeded/undesired web browser and PDF viewer features.	Excellent	Medium	Medium	Medium	No	Yes	No	No
6 (N/A)	**Automated dynamic analysis** of email and web content run in a sandbox to detect suspicious behaviour including network traffic, new or modified files, or other configuration changes.	Excellent	Low	Medium	Low	Yes	Yes	No	Possible
7 (21)	**Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).	Excellent	Low	Medium	Low	Possible	Yes	Possible	No
8 (11)	**Host-based Intrusion Detection/Prevention System** to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence.	Excellent	Low	Medium	Medium	Yes	Yes	No	Possible
9 (5)	**Disable local administrator accounts** to prevent network propagation using compromised local administrator credentials that are shared by several workstations.	Excellent	Low	Medium	Low	No	No	Yes	No
10 (7)	**Network segmentation and segregation** into security zones to protect sensitive information and critical services such as user authentication by the Microsoft Active Directory service.	Excellent	Low	High	Medium	Yes	No	Yes	Possible
11 (6)	**Multi-factor authentication** especially implemented for remote access, or when the user is about to perform a privileged action or access a sensitive information repository.	Excellent	Medium	High	Medium	No	No	Possible	No
12 (8)	**Software-based application firewall, blocking incoming network traffic** that is malicious or otherwise unauthorised, and denying network traffic by default.	Excellent	Low	Medium	Medium	Yes	Yes	Yes	No
13 (9)	**Software-based application firewall, blocking outgoing network traffic** that is not generated by a whitelisted application, and denying network traffic by default.	Excellent	Medium	Medium	Medium	Yes	No	Yes	Yes
14 (10)	**Non-persistent virtualised sandboxed trusted operating environment**, hosted outside of the organisation's internal network, for risky activities such as web browsing.	Excellent	High	High	Medium	Possible	No	Yes	Possible
15 (12)	**Centralised and time-synchronised logging of successful and failed computer events**, with automated immediate log analysis, storing logs for at least 18 months.	Excellent	Low	High	High	Yes	No	Possible	Possible
16 (13)	**Centralised and time-synchronised logging of allowed and blocked network activity**, with automated immediate log analysis, storing logs for at least 18 months.	Excellent	Low	High	High	Yes	No	Possible	Possible
17 (14)	**Email content filtering**, allowing only whitelisted business related attachment types. Preferably analyse/convert/sanitise hyperlinks, PDF and Microsoft Office attachments.	Excellent	High	High	Medium	Yes	Yes	No	Possible
18 (15)	**Web content filtering** of incoming and outgoing traffic, whitelisting allowed types of web content and using behavioural analysis, cloud-based reputation ratings, heuristics and signatures.	Excellent	Medium	Medium	Medium	Yes	Yes	No	Possible
19 (16)	**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	Yes	Yes	No	Yes
20 (19)	**Block spoofed emails** using Sender ID or Sender Policy Framework (SPF) to check incoming emails, and a "hard fail" SPF record to help prevent spoofing of your organisation's domain.	Excellent	Low	Low	Low	Possible	Yes	No	No
21 (22)	**Workstation and server configuration management** based on a hardened Standard Operating Environment, disabling unneeded/undesired functionality e.g. IPv6, autorun and LanMan.	Good	Medium	Medium	Low	Possible	Yes	Yes	Possible
22 (25)	**Antivirus software using heuristics and automated Internet-based reputation ratings** to check a program's prevalence and its digital signature's trustworthiness prior to execution.	Good	Low	Low	Low	Yes	Yes	No	No
23 (24)	**Deny direct Internet access from workstations** by using an IPv6-capable firewall to force traffic through a split DNS server, an email server, or an authenticated web proxy server.	Good	Low	Low	Low	Yes	Possible	No	Yes
24 (23)	**Server application configuration hardening** e.g. databases, web applications, customer relationship management, finance, human resources and other data storage systems.	Good	Low	High	Medium	Possible	Yes	No	Possible
25 (27)	**Enforce a strong passphrase policy** covering complexity, length, expiry, and avoiding both passphrase reuse and the use of a single dictionary word.	Good	Medium	Medium	Low	Possible	No	Yes	No
26 (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	No	Yes	Possible	Yes
27 (28)	**Restrict access to Server Message Block (SMB) and NetBIOS** services running on workstations and on servers where possible.	Good	Low	Medium	Low	No	Yes	Yes	No
28 (20)	**User education** e.g. Internet threats and spear phishing socially engineered emails. Avoid: weak passphrases, passphrase reuse, exposing email addresses, unapproved USB devices.	Good	Medium	High	Medium	Possible	Possible	No	No
29 (26)	**Workstation inspection of Microsoft Office files** for potentially malicious abnormalities e.g. using the Microsoft Office File Validation or Protected View feature.	Good	Low	Low	Low	Possible	Yes	No	No
30 (25)	**Signature-based antivirus software** that primarily relies on up to date signatures to identify malware. Use gateway and desktop antivirus software from different vendors.	Good	Low	Low	Low	Possible	Possible	No	No
31 (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	No	No	No	No
32 (32)	**Block attempts to access websites by their IP address** instead of by their domain name, e.g. implemented using a web proxy server, to force cyber adversaries to obtain a domain name.	Average	Low	Low	Low	Yes	Yes	No	Yes
33 (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	Possible	Possible	Possible	Possible
34 (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	Possible	Yes	No	Yes
35 (35)	**Capture network traffic** to/from internal critical asset workstations and servers as well as traffic traversing the network perimeter, to perform post-intrusion analysis.	Average	Low	High	Low	No	No	No	No

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

Summary of Key Changes for 2014

9. The *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details* document includes an annex of key changes for 2014. A summary of the most significant changes are as follows.

10. Mitigation strategy #4 'Restrict administrative privileges' has been amended to clarify that the goal of this strategy is to ensure that the only users who have administrative privileges to operating systems and applications such as databases, are those users who require such privileges based on their job role and duties.

11. Mitigation strategy 'User application configuration hardening' has moved from #18 to #5 to address intrusions that exploit the prevalence of Java vulnerabilities or involve malicious macro code in Microsoft Office files. Additional technical guidance is provided to enable organisations to continue using Java for business purposes while minimising their risk.

12. The newly introduced mitigation strategy #6 'Automated dynamic analysis' extracts the behavioural analysis functionality from the existing two mitigation strategies 'Email content filtering' and 'Web content filtering'. Additional technical guidance is provided to enable organisations to select an appropriate vendor product.

13. Mitigation strategy 'Operating system generic exploit mitigation' has moved from #21 to #7 due to the increased support and proven effectiveness of Microsoft's free "Enhanced Mitigation Experience Toolkit" (EMET) software tool at mitigating vulnerabilities that were not publicly known at the time.

14. The previous 'Antivirus software' mitigation strategy has been divided into two separate mitigation strategies, to highlight the difference between less effective signature-based antivirus software and more effective heuristic/anomaly-based antivirus software.

15. Mitigation strategy 'User education' has moved from #20 to #28 due to the increase in intrusions using techniques that an educated user would not detect.

Further Information

16. Additional supporting advice is available on the ASD website at http://www.asd.gov.au/infosec/top35mitigationstrategies.htm.

Contact Details

Australian government customers with questions regarding this advice should contact ASD Advice and Assistance at asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.