OCTOBER 2012

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 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

4. DSD's list of mitigation strategies, first published in February 2010, is revised for 2012 based on DSD's most recent analysis of incidents across the Australian Government. Further details on the mitigation strategies are available at the DSD web page http://www.dsd.gov.au.

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 intrusions that DSD responded to in 2011 involved adversaries using unsophisticated techniques that would have been mitigated by implementing the Top 4 mitigation strategies as a package.

6. Implementing the Top 4 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.

7. This document provides information about mitigation implementation costs and user resistance 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 DSD's web site.

Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

Strategies to Mitigate Targeted Cyber Intrusions

Originally published 18 February 2010, last updated 10 October 2012

Mitigation Strategy Effectiveness Ranking for 2012 (and 2011)		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	(4)	**Application whitelisting** of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files e.g. using Microsoft AppLocker.	Essential	Medium	High	Medium	Both	Yes	Yes	Yes
2	(1)	**Patch applications** e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate "extreme risk" vulnerabilities within two days. Avoid Adobe Reader prior to version X.	Essential	Low	High	High	Prevent	Yes	Possible	No
3	(2)	**Patch operating system** vulnerabilities. Patch or mitigate "extreme risk" vulnerabilities within two days. Avoid continuing to use Microsoft Windows XP or earlier versions.	Essential	Low	Medium	Medium	Prevent	Yes	Possible	Possible
4	(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.	Essential	Medium	Medium	Low	Prevent	Possible	Yes	Possible

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	(17)	**Disable local administrator accounts** to prevent network propagation using compromised local administrator credentials that are shared by several computers.	Excellent	Low	Medium	Low	Prevent	No	Yes	No
6	(16)	**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	Prevent	No	Yes	No
7	(15)	**Network segmentation and segregation** into security zones to protect sensitive information and critical services such as user authentication and user directory information.	Excellent	Low	High	Medium	Prevent	Possible	Yes	Possible
8	(13)	**Application based workstation firewall**, configured to deny traffic by default, to protect against malicious or otherwise unauthorised **incoming** network traffic.	Excellent	Low	Medium	Medium	Prevent	Yes	Yes	No
9	(14)	**Application based workstation firewall**, configured to deny traffic by default, that whitelists which applications are allowed to generate **outgoing** network traffic.	Excellent	Medium	Medium	Medium	Both	No	Yes	Yes
10	(22)	**Non-persistent virtualised trusted operating environment**, hosted within the organisation's Internet gateway, for risky activities such as reading email and web browsing.	Excellent	High	High	Medium	Prevent	No	Yes	Possible
11	(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
12	(24)	**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	Detect	Possible	Possible	Possible
13	(23)	**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	Detect	Possible	Possible	Possible
14	(6)	**Whitelisted email content filtering**, only allowing business related attachment types. Preferably analyse/convert/sanitise hyperlinks, PDF and Microsoft Office attachments.	Excellent	High	High	Medium	Prevent	Yes	No	Possible
15	(9)	**Web content filtering** of incoming and outgoing traffic, using web content whitelisting, behavioural analysis, reputation ratings, heuristics and signatures.	Excellent	Medium	Medium	Medium	Prevent	Yes	No	Possible
16	(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
17	(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
18	(26)	**Workstation application security configuration hardening** e.g. disable unrequired features in PDF viewers, Microsoft Office applications, and web browsers.	Excellent	Medium	Medium	Medium	Prevent	Yes	No	No
19	(7)	**Block spoofed emails** using Sender ID or Sender Policy Framework to check 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
20	(8)	**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	Both	Possible	No	No
21	(20)	**Operating system exploit mitigation mechanisms** such as Data Execution Prevention (DEP) and Address Space Layout Randomisation (ASLR).	Good	Low	Low	Low	Prevent	Yes	No	No
22	(25)	**Computer configuration management** based on a hardened Standard Operating Environment with unrequired operating system functionality disabled e.g. IPv6 and autorun.	Good	Medium	Medium	Low	Prevent	Yes	Yes	Possible
23	(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
24	(19)	**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.	Good	Low	Low	Low	Both	Possible	No	Yes
25	(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
26	(12)	**Workstation inspection of Microsoft Office files** for abnormalities e.g. using the Microsoft Office File Validation feature.	Good	Low	Low	Low	Prevent	Yes	No	No
27	(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
28	(27)	**Restrict access to Server Message Block (SMB) and NetBIOS** services running on workstations and on servers where possible.	Good	Low	Medium	Low	Prevent	Yes	Yes	No
29	(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	(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	(31)	**Disable LanMan** passphrase support and cached credentials on workstations and servers, to make it harder for adversaries to crack passphrase hashes.	Good	Low	Low	Low	Prevent	No	Yes	No
32	(32)	**Block attempts to access web sites by their IP address** instead of by their domain name, to force the adversary to obtain a domain name.	Good	Low	Low	Low	Both	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	Both	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	Both	Yes	No	Yes
35	(35)	**Selected network traffic capture** to perform post-incident analysis of successful intrusions, storing network traffic for at least seven days if storage space permits.	Average	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

Further Information

9. Additional supporting advice is available on the DSD website:

   a. *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details*

   b. *Top 4 Mitigation Strategies to Protect Your ICT System*

   c. *Implementing DSD's Top 4: For a Windows Environment*

   d. *Application Whitelisting Explained*

   e. *Assessing Security Vulnerabilities and Patches*

   f. *Minimising Administrative Privileges Explained*

   g. *Malicious Email Mitigation Strategies Guide*

   h. *Multi-factor Authentication*

   i. *Detecting Socially Engineered Emails*

   j. *Mitigating Spoofed Emails – Sender Policy Framework (SPF) Explained*

   k. *Network Segmentation and Segregation*.

10. DSD has also released a non-technical publication and accompanying video for user education which explain the cyber threat and how organisations can mitigate targeted cyber intrusion techniques in simple terms. The Top 4 *Strategies to Mitigate Targeted Cyber Intrusions* are simplified to ***Catch*** malicious software with a whitelist, ***Patch*** all applications and operating systems with updates and ***Match*** the right people with the right access.

Contact Details

Australian government customers with questions regarding this advice should contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

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.