Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details

INTRODUCTION

1. This document provides further information regarding DSD's list of strategies to mitigate targeted cyber intrusions, including references to controls in the DSD Information Security Manual (ISM) available at http://www.dsd.gov.au/infosec/ism/index.htm

2. Readers are strongly encouraged to visit the web page http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm for the latest version of this document as well as subsequently added additional information about implementing the 35 mitigation strategies.

MOST LIKELY TARGETS

3. The phrase "Most Likely Targets" describes users who are most likely to be targeted as part of the first stage of a targeted cyber intrusion, and includes:

- senior executives and their assistants;
- help desk staff, system administrators, and other users with administrative privileges or privileged access;
- all users who have access to sensitive information;
- users with remote access; and,
- users whose job role involves interacting with unsolicited emails from members of the public and other unknown Internet users, for example the human resources team reading email attachments such as job applications.

STAGES OF AN INTRUSION

4. No single strategy can prevent a targeted cyber intrusion, and organisations should ensure that the strategies they select address all three high level stages of such intrusions:

- Stage 1 – An adversary performs reconnaissance to select a target user, and sends this user a malicious email. This reconnaissance is easier if the user's email address is readily available via agency web sites, social networking web sites, or if the user uses their email address for purposes unrelated to work. Malicious code is executed on the user's workstation and is typically configured to persist by automatically executing every time the user restarts their computer and/or logs on. The malicious code is remotely controlled by the adversary, enabling the adversary to access any information that is accessible to the user.

- Stage 2 – The adversary moves through the network to access information on other workstations and servers. Such information typically includes Microsoft Office files, PDF files as well as information stored in databases. Adversaries also typically access system information including computer and network configuration details, as well as details about users including organisation hierarchy and usernames and passphrases (including for remote access). Although passphrases might be stored as cryptographic hashes to frustrate adversaries, cracking such passphrase hashes to derive the passphrases may be fast, cheap and easy unless all users have selected very strong passphrases that are appropriately hashed. The appropriate use of multi-factor authentication may hinder adversaries.
- Stage 3 – The adversary exfiltrates information from the network using network protocols and ports allowed by the organisation, such as HTTPS, HTTP, or in some cases DNS and email. The adversary typically leaves behind several compromised computers as a backdoor to facilitate further exfiltration of information in the future.

RATIONALE FOR IMPLEMENTING MITIGATION STRATEGIES

5. Australian organisations with access to sensitive information, including all Australian federal government agencies, have a high likelihood of being compromised by successful intrusions of low sophistication which the organisation may not have the ability to immediately detect. In addition to the damage done to Australia's economic wellbeing and thereby to all Australian citizens, such compromises damage the reputation of affected organisations, undermine public confidence in the Australian Government, and unnecessarily consume scarce money and staff resources to continually cleanup such low and moderately sophisticated compromises.

6. In addition to implementing mitigation strategies, organisations require an incident response plan and associated capabilities so that when an intrusion is discovered, the damage can be contained, the adversary eradicated, the system restored from backups where appropriate to a trusted state, and the root cause identified and fixed to prevent similar incidents from occurring. Organisations need to regularly test and update their incident response plan and capabilities.

7. Organisations should perform continuous monitoring to test and measure the effectiveness of the mitigation strategies implemented. Missing patches, other known system weaknesses, and detected intrusion attempts should be regularly and systematically reported so that senior managers understand the level of risk that they are accepting.

DETAILS OF MITIGATION STRATEGIES

8. The concept of whitelisting is a key theme of the mitigation strategies, whereby activity such as network communication or program execution is denied by default, and only activity explicitly permitted by the business is allowed to occur. The traditional blacklisting approach only blocks a small amount of activity known to be undesirable, and this approach is reactive, time-consuming and provides weak security.

9. **Mitigation Strategy #1 - Patch applications**

- especially PDF viewer, Flash Player, Microsoft Office, Java, web browser and web browser plugins such as ActiveX.
- Maintain an inventory of software installed on each computing device.
- Apply patches or mitigation within two days for high risk vulnerabilities such as vulnerabilities enabling unauthorised code execution by an adversary using the Internet.
- Use the latest version of applications, which typically incorporate newer security technologies such as sandboxing.
- A supplementary document about patching is scheduled to be available at http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- ISM controls 774, 790, 297-298, 300, 303-304, 940-941, 1143-1144, 382, 1035, 1049.

10. **Mitigation Strategy #2 - Patch operating system vulnerabilities.**

- Apply patches or mitigation within two days for high risk vulnerabilities such as vulnerabilities enabling unauthorised code execution by an adversary using the Internet.
- Use the latest operating system version, which typically incorporates newer security technologies.
- A supplementary document about patching is scheduled to be available at http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- ISM controls 774, 790, 297-298, 300, 303-304, 940-941, 1143-1144, 382, 1035, 1049.

11. **Mitigation Strategy #3 - Minimise the number of users with domain or local administrative privileges**

- to reduce the consequences of a compromise.

- Such users should use a computer with a trusted operating environment that at least implements the top four mitigations.
- Such users should use a separate unprivileged account, and preferably a non-persistent virtualised environment or separate sacrificial physical computer, for activities that are non-administrative or risky such as reading email and web browsing.
- A supplementary document about administrative privileges is available at http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- ISM controls 404-405, 444-448, 985, 709.

12. **Mitigation Strategy #4 - Application whitelisting**

- to help prevent malicious software and other unapproved programs from running, by using solutions such as Microsoft Software Restriction Policies or AppLocker, implemented at least on computers used by Most Likely Targets.
- Simply preventing users from installing new applications to their workstation's hard disk is not application whitelisting.
- Some antivirus products are evolving into converged endpoint security products that incorporate application whitelisting functionality.
- A supplementary document about application whitelisting is available at http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- ISM controls 843-851, 955-957.

13. **Mitigation Strategy #5 - Host-based Intrusion Detection/Prevention System**

- to identify anomalous behaviour such as process injection, keystroke logging, driver loading and call hooking.
- Some antivirus products are evolving into converged endpoint security products that incorporate HIDS/HIPS functionality.
- ISM controls 575-576, 1034.

14. **Mitigation Strategy #6 - Whitelisted email content filtering**

- allowing only attachments that are file types required for business functionality.
- Preferably convert/sanitise PDF and Microsoft Office attachments to disable malicious content.
    - An example plugin for Microsoft Exchange that sanitises PDF files is scheduled to be available at http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

- Disallow content that cannot be inspected such as passphrase protected .zip files.
- Preferably archive PDF and Microsoft Office attachments and virus scan them again after a month.
- Preferably quarantine attachments and disable hyperlinks in emails from webmail providers that provide free email addresses to anonymous Internet users, since intrusions commonly use such email addresses due to the lack of attribution.
- Preferably use technology that automatically opens email attachments in a sandbox to detect anomalous behaviour such as network traffic or changes to the file system or registry.
- ISM controls 561, 1042, 1057.

15. **Mitigation Strategy #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.
- Alternative implementations include Sender ID and DomainKeys Identified Mail.
- Reject emails from the Internet that have your organisation's domain as the email sender.
- ISM controls 574, 1151-1152, 861, 1025-1027, 561.

16. **Mitigation Strategy #8 - User education**

- especially for Most Likely Targets, about Internet threats such as identifying spear phishing socially engineered emails or unexpected duplicate emails, and reporting such emails and suspicious phone calls to the security team.
- User education needs to be tailored to the job role of the user.
- Educate users to avoid:
    - selecting weak passphrases;
    - reusing the same passphrase on the same system;
    - using the same passphrase in several different places;
    - unnecessarily exposing their email address and other personal details;
    - visiting web sites unrelated to work; and,
    - using USB devices and other IT equipment not corporately provided.

- Educate users why following IT security policies helps them to protect and appropriately handle the sensitive information they have been entrusted to handle.
- The success of a user education program may be measured by a reduction in the frequency and severity of incidents (including incidents resulting from penetration tests) that involved users performing an action that facilitated the incident.
- ISM controls 735, 763-764, 785, 890, 58, 151, 251-253, 255-257, 922, 575-576, 609-610, 421-422.

17. **Mitigation Strategy #9 - Web content filtering**

- of incoming and outgoing traffic, using signatures, reputation ratings and other heuristics. Whitelist allowed types of web content, preferably blocking all executable content by default and use a process to enable individual selected access if a business justification exists.
- Preferably disallow ActiveX, Java, Flash Player, HTML inline frames and javascript except for whitelisted web sites.
- Preferably use a solution that can similarly inspect SSL traffic for malicious content, especially SSL communications with unfamiliar web sites.
- Preferably use technology that automatically opens downloaded files in a sandbox to detect anomalous behaviour such as network traffic or changes to the file system or registry.
- ISM control 963.

18. **Mitigation Strategy #10 - Web domain whitelisting for all domains**

- since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.
- An example implementation is available at http://whitetrash.sourceforge.net
- ISM controls 263, 995, 958.

19. **Mitigation Strategy #11 - Web domain whitelisting for HTTPS/SSL domains**

- since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.
- An example implementation is available at http://whitetrash.sourceforge.net
- ISM controls 263, 995.

20. **Mitigation Strategy #12 - Workstation inspection of Microsoft Office files**
    - for abnormalities e.g. using the Microsoft Office File Validation feature.
    - ISM control 1156.
21. **Mitigation Strategy #13 - Application based workstation firewall**
    - configured to deny traffic by default, to protect against malicious or otherwise unauthorised **incoming** network traffic.
    - Some antivirus products are evolving into converged endpoint security products that incorporate application based workstation firewall functionality.
    - ISM controls 380, 1017.
22. **Mitigation Strategy #14 - Application based workstation firewall**
    - configured to deny traffic by default, that whitelists which applications are allowed to generate **outgoing** network traffic.
    - Some antivirus products are evolving into converged endpoint security products that incorporate application based workstation firewall functionality.
    - ISM controls 380, 1017.
23. **Mitigation Strategy #15 - Network segmentation and segregation**
    - into security zones to protect sensitive information and critical services such as user authentication and user directory information.
    - Network controls include switches, virtual LANs, data diodes, firewalls, routers and Network Access Control.
    - Data controls include file permissions and Information Rights Management.
    - Segregation should be based on connectivity required, user job role, business function, trust boundaries and sensitivity of information stored.
    - Constrain VPN and other remote access, wireless connections, as well as employee-owned laptops, smartphones and tablet computing devices.
    - ISM controls 637-639, 693-694.
24. **Mitigation Strategy #16 - Multi-factor authentication**
    - especially for Most Likely Targets, particularly implemented for when the user is about to perform a privileged action, or access a database or other sensitive information repository.

- Secure computers that store user authentication data and perform user authentication since such computers are targeted by adversaries.
- ISM control 1039.

25. **Mitigation Strategy #17 - Randomised local administrator passphrases**
    - that are unique and complex for all computers.
    - Use domain group privileges instead of local administrator accounts.
    - ISM control 384.
26. **Mitigation Strategy #18 - Enforce a strong passphrase policy**
    - covering complexity, length, and avoiding both passphrase reuse and the use of dictionary words.
    - An example plugin for Microsoft Windows that assists users to select a strong passphrase is scheduled to be available at http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
    - ISM controls 421-422.
27. **Mitigation Strategy #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.
    - The firewall should only allow approved networking ports and protocols.
    - Preferably use a web proxy that can inspect SSL traffic for malicious content, especially SSL communications with unfamiliar web sites.
    - Configure workstations with a non-routing network capture device as the default route to help detect malware attempting to directly communicate with the Internet.
    - ISM controls 569, 260-261, 996, 263, 841-842, 385, 953, 628, 631.
28. **Mitigation Strategy #20 - Data Execution Prevention**
    - using hardware and software mechanisms for all software applications that support DEP.
    - Information on DEP and other generic mitigation technologies is available at http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=26788
    - ISM control 380.

29. **Mitigation Strategy #21 - Antivirus software**

- with up to date signatures, reputation ratings and other heuristic detection capabilities.
- Scan files when they are accessed and on a scheduled basis.
- Use gateway and desktop antivirus software from different vendors.
- ISM controls 380, 1033.

30. **Mitigation Strategy #22 - Non-persistent virtualised trusted operating environment**

- with limited access to network file shares, for risky activities such as reading email and web browsing.

31. **Mitigation Strategy #23 - Centralised and time-synchronised logging**

- of allowed and blocked **network activity** especially at the DNS server and the web proxy, storing logs for at least 18 months. Preferably include Network Flow data.
- Maintain a network map and an inventory of devices connected to the network to help baseline normal behaviour on the network.
- **Perform regular log analysis** focusing on connections and amount of data transferred by Most Likely Targets to highlight abnormal internal network traffic such as suspicious reconnaissance enumeration of network shares and user information including honeytoken accounts. Also focus on abnormal external network traffic crossing perimeter boundaries such as:
    - periodic beaconing traffic;
    - HTTP sessions with an incorrect ratio of outgoing traffic to incoming traffic;
    - large amounts of traffic;
    - traffic outside of business hours; and,
    - long lived connections.
- ISM controls 781, 108, 790, 380, 957, 261, 109, 580, 582-587, 859, 986-991, 1032, 631, 634.

32. **Mitigation Strategy #24 - Centralised and time-synchronised logging**

- of successful and failed **computer events**, storing logs for at least 18 months.
- **Perform regular log analysis** focusing on
    - Most Likely Targets;
    - logs generated by antivirus software and other security products;

- attempted but blocked program execution;
- user authentication and use of credentials especially from computers other than the user's usual computer;
- creation of user accounts;
- new or changed services or registry keys used to automatically run programs on bootup or user login;
- new or changed files that are executable;
- accesses to databases;
- accesses to files on network shared group drives; and,
- use of reconnaissance tools such as the system executables: ipconfig, net, net1, reg, gpresult and systeminfo.

- Use a Security Information and Event Management solution to correlate logs from multiple sources to identify patterns of suspicious behaviour.
- ISM controls 781, 108, 790, 380, 957, 261, 109, 580, 582-587, 859, 986-991, 1032, 631, 634.

33. **Mitigation Strategy #25 - Standard Operating Environment**

- with unrequired operating system functionality disabled.
- Disable or restrict IPv6, autorun, and services such as Remote Desktop.
- Harden file and registry permissions.
- ISM controls 380, 382-384, 341.

34. **Mitigation Strategy #26 - Workstation application security configuration hardening**

- such as disabling unrequired script/macro features in PDF viewers and Microsoft Office applications, as well as disabling web browser features such as ActiveX and Java.
- Preferably disallow Flash Player, HTML inline frames and javascript except for whitelisted web sites.
- ISM controls 961-962.

35. **Mitigation Strategy #27 - Restrict access to NetBIOS services**

- running on workstations and on servers where possible.

36. **Mitigation Strategy #28 - Server application security configuration hardening**

- e.g. databases, web applications, customer relationship management and other data storage systems.
- OWASP guidelines help mitigate web application vulnerabilities such as SQL injection. These guidelines cover code review, data validation and sanitisation, user and session management, protection of data in transit and storage, error handling, user authentication, logging and auditing.
- ISM controls 401, 971.

37. **Mitigation Strategy #29 - Removable and portable media control**

- as part of a Data Loss Prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.
- ISM controls 322-323, 325, 330-336, 946, 337-338, 341-347, 831-832, 1059, 348, 350-354, 356-360, 835-836, 947, 949, 1065-1068, 361-366, 368, 370-373, 838-840, 1160, 1069, 329, 374-375, 378.

38. **Mitigation Strategy #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.
- ISM controls 572, 263.

39. **Mitigation Strategy #31 - Disable LanMan password support**

- and cached credentials on workstations and servers, to make it harder for adversaries to crack password hashes.
- ISM control 1055.

40. **Mitigation Strategy #32 - Block attempts to access web sites by their IP address**

- instead of by their domain name.

41. **Mitigation Strategy #33 - Network-based Intrusion Detection/Prevention System**

- using signatures and heuristics to identify anomalies listed in mitigation strategy #23, as well as traffic crossing perimeter boundaries that contains keywords such as classification markings indicating sensitive data.
- ISM controls 575-578, 1028-1031.

42. **Mitigation Strategy #34 - Gateway blacklisting**

- to block access to known malicious domains and IP addresses.
- Preferably include blocking of dynamic and other domains provided free to anonymous Internet users, after checking your organisation does not access any legitimate web sites using these domains, since intrusions commonly use such domains due to the lack of attribution.
- ISM controls 959-960.

43. **Mitigation Strategy #35 - Full network traffic capture**

- to perform post-incident analysis of successful intrusions, storing network traffic for at least the previous seven days. Such analysis helps to determine the adversary's techniques and assess the extent of damage.
- Capture traffic from both the network perimeter as well as computers on internal networks containing sensitive information.

CONTACT DETAILS

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

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

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