Australian Government
Department of Defence
Intelligence and Security

PROTECT

CYBER SECURITY OPERATIONS CENTRE
OCTOBER 2012

# 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 *Australian Government Information Security Manual (ISM)* which is 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 and additional information about implementing the 35 mitigation strategies.

## Most Likely Targets

3. The phrase "Most Likely Targets" describes users in an organisation 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, including information which could provide a foreign government or company with a strategic or economic advantage.
    - As part of a risk assessment performed by business representatives and security staff, organisations need to identify the type and location of sensitive information that they hold. Such information may reside in government ministerial submissions and other documents detailing government intentions, strategic planning documents, business proposals, tenders, meeting minutes, financial and accounting reports, legal documents, and intellectual property holdings.
    - Contemplating an adversary's intelligence goals may provide insight into which of the organisation's employees, based on their access to specific information, are likely to be targeted as part of an intrusion. In some cases, targeting will coincide with a significant upcoming meeting or other business event of relevance to the adversary.
- users with remote access.
- users whose job role involves interacting with unsolicited emails from members of the public and other unknown Internet users. This includes users handling Freedom of Information requests, media and public relations staff, as well as 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 cyber intrusions:

- Stage 1 – An adversary performs reconnaissance to select a target user, and either compromises a legitimate website that the user visits, referred to as a targeted "drive by download" or "watering hole" technique, or alternatively sends this user a malicious "spear phishing" email. The email might contain a hyperlink to a malicious file, possibly in a zip archive file. Alternatively, the email might contain a malicious attachment such as a PDF file

or Microsoft Office document, possibly in a zip archive file. This reconnaissance is made easier for the adversary if the user's name and email address are readily available via their employer's web site, social networking web sites, or if the user uses their work email address for purposes unrelated to work. Malicious code is then 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 communicates with the adversary's network infrastructure, usually downloading additional malicious code, enabling the adversary to remotely control the user's workstation and perform any action or access any information that the user can.

- Stage 2 – The adversary commonly uses compromised account credentials and exploitable vulnerabilities in the organisation's other computers to propagate (laterally move) across the network in order to locate and access sensitive information. Such network propagation can occur rapidly on networks with inadequate segmentation and segregation, especially when multiple computers share the same local administrator passphrase. Information accessed frequently includes Microsoft Office files, Outlook email .pst 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, freely available software and a single commodity computer or publicly available cloud computing service may be able to quickly and cheaply crack these hashes to derive the passphrases, unless all users have selected very strong passphrases that are appropriately hashed using a cryptographically strong algorithm.
  - Alternatively, the adversary might use the "pass the hash" technique, avoiding the need to crack passphrase hashes.
  - Organisations using single sign-on authentication may significantly help the adversary. In contrast, the appropriate use of multi-factor authentication, especially for when a user is about to perform a privileged action such as administer a system or access a sensitive information repository, may significantly hinder the adversary.
- Stage 3 – The adversary usually uses RAR/zip archive files to compress and encrypt a copy of sensitive information.
  - The adversary exfiltrates this information from the network, often from a single "staging" computer on the organisation's network. The adversary uses available network protocols and ports allowed by the organisation's gateway firewall, such as encrypted HTTPS/SSL, HTTP, or in some cases DNS or email.
  - The adversary may obtain Virtual Private Network (VPN) or other remote access account credentials and use this encrypted network connection for exfiltrating information, with the aim of defeating network based monitoring.
  - The adversary typically has several compromised computers on the organisation's network, as well as compromised VPN/remote access accounts, maintained as a backdoor to facilitate further collection and 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 targeted with intrusions of low sophistication that will succeed if the organisation's security posture is inadequate. 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 unsophisticated compromises.

6. Most organisations have finite funding and staff resources, requiring their senior management to commit to the importance of protecting the organisation's sensitive information. The top four mitigation strategies, when implemented as a package, address all three high level stages of an intrusion and are the "sweet spot" of providing a large increase in security posture for a relatively small investment of time, effort and money. Australian government agencies implementing the top four mitigation strategies have witnessed their network becoming defendable, making the job of adversaries significantly harder. Once an organisation has implemented the top four mitigation strategies, especially on the computers used by employees most likely to be targeted, and then for all users, a selection of additional mitigation strategies can then be implemented.

7. In addition to implementing mitigation strategies, organisations require an incident response plan and associated operational capabilities, as determined and supported by technical staff and business representatives including data owners, corporate communication, public relations and legal staff.

- When an intrusion is discovered, the intrusion needs to be understood to a reasonable extent prior to remediation. Otherwise, the organisation plays "whack a mole", cleaning compromised systems and blocking network access to the adversary's Internet infrastructure, while the adversary simply compromises additional systems using different malicious tools and different Internet infrastructure to avoid detection.
- For higher sophisticated intrusions, DSD can assist Australian government agencies to develop a strategic plan to contain and eradicate the adversary's malware and improve the agency's security posture in preparation for the likelihood that the adversary will immediately attempt to regain access to the agency's systems.
- Organisations need to regularly test and update their incident response plan and capabilities, focusing on decreasing the duration of time needed to detect and respond to the next intrusion.

8. Organisations should perform continuous monitoring and mitigation, using automated techniques to test and measure the effectiveness of the mitigation strategies implemented, and implement additional mitigation strategies as required to protect the data and systems that the organisation has identified as critical assets. Organisations that have implemented Data Loss Prevention solutions have usually already identified the location of their most sensitive data. 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.

9. Proactive organisations invest in *discovering* new intrusions instead of simply waiting for and relying on security products to *detect* intrusions. Leveraging access to information about adversary tradecraft and indicators of compromise, as provided to Australian government agencies via the OnSecure web portal, can assist with identifying intrusions.

## Details of Mitigation Strategies

10. 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.

11. **Mitigation Strategy #1 - Application whitelisting**

- of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files e.g. using Microsoft AppLocker, implemented at least on computers used by Most Likely Targets. Subsequently implementing application whitelisting on important servers such as Active Directory and other authentication servers can help prevent the adversary from running malicious programs, such as tools that obtain passphrase hashes or otherwise provide the adversary with additional privileges.
- Robust implementations of application whitelisting help to prevent the undesired execution of software regardless of whether the software was downloaded from a web site, clicked on as an email attachment, or introduced via a USB memory stick or CD/DVD. 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.
- It is advisable to deploy application whitelisting in phases, instead of trying to deploy it to the entire organisation at once.
    - After fully testing and understanding the application whitelisting mechanism to avoid false positives, one approach is to deploy application whitelisting to the workstations used by senior executives and their assistants. Such staff usually run a limited number of software applications such as Microsoft Office, an email program and a web browser. When these staff are made aware that they clicked on a malicious email attachment or visited a malicious web site and application whitelisting mitigated the compromise, they are likely to provide additional support for the deployment of application whitelisting to more users in the organisation.
- Deploying application whitelisting is easier if the organisation has a good change management process and therefore understands what software is installed on user workstations. Additionally, an option is to deploy application whitelisting in "logging only" mode, to develop an inventory of software installed on user workstations, before configuring application whitelisting to prevent unapproved programs from running.

- When installing new software, avoid creating hashes for added files that aren't of an executable nature. Otherwise if every new file is whitelisted, the whitelist is likely to become too large and if distributed via group policy, may unacceptably slow down users logging into their workstations.
- Configure the application whitelisting mechanism to prevent the running of unapproved programs regardless of their file extension.
- Where possible, prevent users (and therefore malware running on the user's behalf) from running system executables commonly used for reconnaissance as listed in mitigation strategy "Centralised and time-synchronised logging of successful and failed computer events".
- The ability of application whitelisting to provide a reasonable barrier for low to moderately sophisticated intrusions depends on the vendor product chosen to implement application whitelisting, combined with its configuration settings, as well as the file permissions controlling which directories a user (and therefore malware) can write to and execute from.
- Further guidance is available at: http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- ISM controls 0843-0851, 0955-0957.

12. **Mitigation Strategy #2 - Patch applications**

- especially PDF viewer, Flash Player, Microsoft Office, Java, web browser and web browser plugins such as ActiveX. Also patch server applications, especially server applications such as databases that store sensitive information, and server applications such as web server software that are Internet accessible. Patch or mitigate "extreme risk" vulnerabilities as soon as possible and certainly within two days.
- "Extreme risk" vulnerabilities in software used by an organisation enable likely unauthorised code execution by an adversary using the Internet, that can result in significant consequences for the organisation.
- Preferably use the latest version of applications such as Adobe Reader X and later, which generally incorporate newer security technologies such as sandboxing. For some vendor software, upgrading to the latest version is the only way to patch a vulnerability.
  - Avoid continuing to use Adobe Reader prior to version X.
  - Avoid continuing to use versions of Internet Explorer prior to version 8 for accessing Internet web sites.
- Maintain an inventory of software installed on each computing device, including details about software version and patching history.
- There are a variety of approaches to deploying patches to applications and operating systems running on workstations, based on an organisation's risk tolerance, as well as how many applications an organisation uses where the applications are legacy, unsupported, developed in-house, or poorly designed.
  - Some organisations use a balanced approach involving waiting a few hours after a patch has been released to enable the vendor to recall the patch if it has been reported to break business functionality. The organisation then deploys the patch to a few workstations

belonging to system administrators or similar technically skilled users. If no broken functionality has been identified within a day, the organisation then deploys the patch to a small fraction of workstations belonging to users from every business section, especially to users who are most likely to be targeted by an intrusion. If there are no complaints of broken functionality within a day, the patch is then deployed to all other workstations. This approach aims to reduce the organisation's exposure to the vulnerability by applying patches within a reasonable timeframe, while reducing the risk of a patch breaking business functionality and reducing the cost of testing patches.

  - Some organisations spend a significant amount of time testing workstation patches prior to deployment. Although this minimises the likelihood that a deployed patch will break business functionality, such testing can cost the organisation significant amounts of money, and leave the organisation vulnerable for weeks or months, the consequences of which may potentially be a higher cost than removing a patch that has broken a small fraction of workstations.
  - Some organisations deploy workstation patches to all workstations either immediately, or after a few hours of a patch being released to enable the vendor to recall the patch if it has been reported to break business functionality. This approach minimises the organisation's exposure to the vulnerability and minimises the cost of testing patches, at the risk of having to rollback a patch if it breaks business functionality.

- A different approach involving more thorough testing is used for deploying patches to servers, as well as for deploying service packs that introduce additional functionality.
- Further guidance is available at: http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- ISM controls 0790, 0297-0298, 0300, 0303-0304, 0940-0941, 1143-1144, 1049, 1244, 1298, 1348-1351.

13. **Mitigation Strategy #3 - Patch operating system vulnerabilities.**

- Patch or mitigate "extreme risk" vulnerabilities as soon as possible and certainly within two days. "Extreme risk" vulnerabilities in software used by an organisation enable likely unauthorised code execution by an adversary using the Internet that can result in significant consequences for the organisation.
- Preferably use the latest operating system version that meets the organisation's business requirements, since newer operating systems generally incorporate newer security technologies.
  - Avoid continuing to use Microsoft Windows XP or earlier versions.
  - Preferably use a 64-bit version of Microsoft Windows instead of a 32-bit version, since the 64-bit version contains additional security technologies. Further information is available at http://support.microsoft.com/kb/946765
- Further guidance is available at: http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- ISM controls 0790, 0297-0298, 0300, 0303-0304, 0940-0941, 1143-1144, 1049, 1244, 1298, 1348.

14. **Mitigation Strategy #4 - 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 mitigation strategies.
- 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.
- Further guidance is available at: http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- ISM controls 0405, 0445-0448, 0985, 0709, 1175, 0582-0583, 0987.

15. **Mitigation Strategy #5 - Disable local administrator accounts**

- to prevent an adversary from easily propagating around the organisation's network using compromised local administrator credentials that are shared by several computers.
- To administer a computer, use domain accounts with local administrative privileges but without domain administrator privileges.
  - Remote administration could be performed via a Remote Desktop mechanism.
  - Ideally, a separate domain account per computer could be used to limit the scope of compromise if the adversary obtains access to credentials used for computer administration. However, this may introduce undesirable overhead in managing the different domain accounts.
- For systems where disabling the local administrator account is not feasible, such as the Active Directory authentication server, ensure that the local administrator account has a unique and complex passphrase. Appropriately protect records of the passphrases used for such systems.
- ISM controls 0383, 0445.

16. **Mitigation Strategy #6 - Multi-factor authentication**

- especially for Most Likely Targets, particularly implemented for remote access, or when the user is about to perform a privileged action (including system administration), or access a database or other sensitive information repository.
- Multi-factor authentication involves users verifying their identity by using at least any two of the following three mechanisms:
  - Something the user knows, such as a passphrase or PIN.
  - Something the user has, such as a physical token or software certificate.
  - Something the user is, such as their fingerprint.
- Preferably use a physically separate token, involving a time-based value, that is not physically connected to the computer. If a user's computing device is compromised, an adversary may be able to hijack a VPN/remote access session established by the user. Multi-factor authentication using physically separate tokens and a time-based value helps prevent the adversary from establishing their own VPN/remote access session.

- Smart cards may be a less secure option, depending on their use and implementation including whether the smart card is left connected to the computer, and also to what degree software running on the computer can interact with the smart card.
- Software based certificates that are stored and protected by the operating system are an even less secure option since they might be copied by an adversary who has obtained administrative privileges on the target user's computer.
- Software based certificates that are stored as a file without additional protection are an even less secure option since they might be easily copied by an adversary without requiring administrative privileges.

- The use of multi-factor authentication for remote access does not fully mitigate users entering their passphrase on a compromised computing device. An adversary may obtain a user's passphrase when it is entered into a less trustworthy computing device used for remote access. The adversary may then use this passphrase as part of a subsequent intrusion, for example by either gaining physical access to a corporate workstation and simply logging in as the user, or by using this passphrase to access sensitive corporate resources as part of a remote intrusion against the corporate network.
  - Mitigations include using multi-factor authentication for all user logins including corporate workstations in the office, or ensuring that user passphrases for remote access are different to passphrases used for corporate workstations in the office.
- Secure servers that store user authentication data and perform user authentication since such computers are frequently targeted by adversaries.
- Ensure that administrative service accounts, and other accounts that are unable to use multi-factor authentication, have a long and complex passphrase.
- The use of single sign-on authentication may significantly help adversaries.
- Further guidance is available at: http://www.dsd.gov.au/publications/csocprotect/multi_factor_authentication.htm
- ISM controls 1039, 1265, 1173-1174, 0974.

17. **Mitigation Strategy #7 - Network segmentation and segregation**

- into security zones to protect sensitive information and critical services such as user authentication and user directory information.
- Network segmentation involves partitioning the network into smaller networks. Network segregation involves developing and enforcing a ruleset controlling which computing devices are permitted to communicate with which other computing devices. For example, on most corporate networks, direct network communication between user workstations should not be required or permitted.
- Network controls include switches, virtual LANs, enclaves, data diodes, firewalls, routers and Network Access Control.
  - Organisations using operating system virtualisation, (especially third party) cloud computing infrastructure, or providing users with "Bring Your Own Device" or remote access to the organisation's network, may require controls that are less dependent on the

physical architecture of the network. Such controls include personal firewalls and "IPsec Server and Domain Isolation".

- The use of IPsec provides flexible network segmentation and segregation. For example, the use of IPsec authentication can ensure that a specific network port or ports on a sensitive server can only be accessed by specific workstations such as those workstations belonging to administrators.

- Data controls include file permissions, Information Rights Management, and use of content management systems such as Microsoft SharePoint instead of prolific use of network file shares.
- Segregation should be based on connectivity required, user job role, business function, trust boundaries and sensitivity of information stored.
- Sensitive systems such as Active Directory and other authentication servers should only be able to be administered (e.g. by using RDP or MMC) from a limited number of intermediary computers referred to as "jump servers". Jump servers should be closely monitored, have no Internet access, be well secured, and limit which users and network devices are able to connect to them.
- Constrain VPN/remote access, wireless connections, as well as employee-owned laptops, smartphones and tablet computing devices used as part of a "Bring Your Own Device" implementation.
- Organisations with critically sensitive information may choose to store it on air gapped computers that are not accessible from the Internet. Security patches and other data can be transferred to and from such air gapped systems in accordance with a robust media transfer policy and process.
- Further guidance is available at:
  http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- ISM controls 1346, 1181-1182.

18. **Mitigation Strategy #8 - 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 0380, 0941, 1017.

19. **Mitigation Strategy #9 - 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 0380, 0941, 1017.

20. **Mitigation Strategy #10 - Non-persistent virtualised trusted operating environment**

- hosted within the organisation's Internet gateway, for risky activities such as reading email and web browsing.
- Network segmentation and segregation should be implemented to mitigate a compromised virtualised operating environment from accessing the organisation's sensitive information.
- A robust policy and process should be used to enable data to be transferred from the virtualised operating environment to the user's local environment.
- The non-persistent nature of this mitigation strategy helps to automatically restore a compromised system to a known good state, however unfortunately it will also remove forensic evidence of how the intrusion occurred.
- Implementation options are in *Network Segmentation and Segregation* guidance available at: http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- ISM controls 1181, 1345-1346.

21. **Mitigation Strategy #11 - Host-based Intrusion Detection/Prevention System**

- to identify anomalous behaviour such as process injection, keystroke logging, driver loading and call hooking. Suspicious behaviour also includes software attempting to persist after the computer is rebooted, for example by modifying or adding registry settings and files such as computer services.
- Configure the HIDS/HIPS capability to achieve an acceptable balance between identifying malware, while avoiding negatively impacting users due to false positives.
- Some antivirus products are evolving into converged endpoint security products that incorporate HIDS/HIPS functionality.
- ISM controls 0576, 1034, 1341, 1184-1185.

22. **Mitigation Strategy #12 - Centralised and time-synchronised logging**

- of successful and failed **computer events**, with automated immediate real-time log analysis, storing logs for at least 18 months. Important logs include logs generated by security products, as well as Active Directory event logs and other logs associated with user authentication including access via VPN/remote access.
- Event logs that store evident changes to the normal behaviour of a network, system or user, must be retained for 7 years as required by the *Archives Act 1983* and specifically in accordance with the National Archives of Australia's *Administrative Functions Disposal Authority*.
- **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 account credentials, especially:
    - user authentication from a user who is currently on holiday or other leave.

        - user authentication from computers other than the user's usual computer, especially if from computers outside of the user's geographical location.
        - VPN/remote access from countries that the associated user is not located in.
        - a single IP address attempting to authenticate as multiple different users.
        - VPN/remote access by a user from two different IP addresses concurrently.
        - failed login attempts for accounts with administrative privileges.
        - user accounts that become locked out because of too many incorrect passphrase attempts.
        - administrative service accounts unexpectedly logging into other computers.
        - creation of user accounts, or disabled accounts being re-enabled, especially accounts with administrative privileges.
        - modifications to user account properties, such as "Store password using reversible encryption" or "Password never expires" configuration options being activated.
    - user actions outside of business hours, noting that malware compromising a user's account may appear in logs as though the malware's actions are the user's actions.
    - 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.
    - unauthorised attempts to access or modify event logs.
    - use of reconnaissance and network propagation tools such as the system executables: ipconfig, net, net1, netstat, reg, wmic, at, schtasks, tasklist, rundll32, gpresult and systeminfo.
- Use a Security Information and Event Management solution to aggregate and correlate logs from multiple sources to identify patterns of suspicious behaviour, including behaviour that deviates from the baseline of typical patterns of system usage by employees.
- ISM controls 0120, 0670, 0790, 0380, 0957, 0261, 0109, 0580, 0582-0587, 0859, 0987-0989, 0991, 1032, 0631, 0634, 1229, 1176, 1305.

23. **Mitigation Strategy #13 - Centralised and time-synchronised logging**

- of allowed and blocked **network activity**, with automated immediate real-time log analysis, storing logs for at least 18 months. Important logs include DNS server, web proxy logs containing connection details including user-agent values, DHCP leases, firewall logs detailing traffic entering and leaving the organisation's network, and Network Flow data.
- Event logs that store evident changes to the normal behaviour of a network, system or user, must be retained for 7 years as required by the *Archives Act 1983* and specifically in accordance with the National Archives of Australia's *Administrative Functions Disposal Authority*.

- 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.
  - HTTP traffic with a "User-Agent" header value that is not associated with legitimate software used by the organisation's users.
  - DNS lookups for domain names that don't exist and aren't an obvious user typo, indicating malware communicating to a domain that the adversary is yet to register.
  - DNS lookups for domain names that resolve to a localhost IP address such as 127.0.0.1, indicating malware that the adversary is not ready to communicate with.
  - large amounts of traffic.
  - traffic outside of business hours.
  - long lived connections.
- ISM controls 0120, 0670, 0790, 0380, 0957, 0261, 0109, 0580, 0582-0587, 0859, 0987-0989, 0991, 1032, 0631, 0634, 1176, 1229, 1305.

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

- allowing only attachments with a file type and file extension that are required for business functionality.
- Preferably analyse/convert/sanitise hyperlinks, PDF and Microsoft Office attachments to disable malicious content.
  - An example plugin for Microsoft Exchange that sanitises PDF files is 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/runs email attachments in a virtualised sandbox to detect anomalous behaviour such as network traffic or changes to the file system or registry.
- Further guidance is available at: http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- ISM controls 0561, 1057, 1234, 1284-1285, 1288, 0649-0652.

25. **Mitigation Strategy #15 - Web content filtering**

- of incoming and outgoing traffic, using web content whitelisting, behavioural analysis, reputation ratings, heuristics and signatures. 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 block access to web sites that the web content filter considers to be "uncategorised" or in a category that is not required for business purposes.
- 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/runs downloaded files in a virtualised sandbox to detect anomalous behaviour such as network traffic or changes to the file system or registry.
- Further guidance is available at: http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- ISM controls 0963, 0961, 1237.

26. **Mitigation Strategy #16 - 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
- Further guidance is available at: http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- ISM controls 0263, 0995, 0958.

27. **Mitigation Strategy #17 - 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
- Further guidance is available at: http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- ISM controls 0263, 0995, 0958.

28. **Mitigation Strategy #18 - Workstation application security configuration hardening**

- such as disabling unrequired script/macro features in PDF viewers and Microsoft Office applications, disabling unrequired Microsoft Office file converters, 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.

- Focus on hardening the configuration of applications used to interact with content from the Internet.
- ISM controls 0380, 0961.

29. **Mitigation Strategy #19 - 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.
- Sender ID is an alternative version of Sender Policy Framework that checks the legitimacy of the sender's email address that is displayed to the email recipient.
- Additional implementations include DomainKeys Identified Mail.
- Reject emails from the Internet that have your organisation's domain as the email sender.
- Further guidance is available at: http://dsd.gov.au/publications/csocprotect/spoof_email_sender_policy_framework.htm
- ISM controls 0574, 1151-1152, 0861, 1025-1027, 0561, 1183.

30. **Mitigation Strategy #20 - 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. Such education should focus on influencing user behaviour.
- 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.
  - 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. Share with users the anecdotal details of previous intrusion attempts targeting the organisation and similar organisations, highlighting the impact that intrusions have to the organisation and to the user. Such education may reduce the level of user resistance to the implementation of mitigation strategies. For example, users may be less likely to resist the removal of their unnecessary administrative privileges if they understand why the mitigation strategy is required.
- The success of a user education program may be measured by a reduction in the frequency and severity of incidents, including incidents resulting from phishing exercises and penetration tests, that involved users performing an action that facilitated the incident.
- User education can complement technical mitigation strategies. User awareness can help to *detect* a spear phishing email, including when users notice and report unexpected behaviour such as a suspicious email, or a blank document or irrelevant document content being

displayed when an email attachment is opened. However, to *prevent* and *automatically detect* an intrusion, implementing a technical mitigation strategy (such as application whitelisting configured to log and report violations) is preferable to relying on user education.

- Putting users in the position of making a security related decision and hoping that they are all educated to always choose correctly, is likely to result in some users choosing incorrectly resulting in compromise.
- DSD is aware of some spear phishing emails that use clever tradecraft and are believable such that no amount of user education would help to prevent or detect the intrusion attempt.
- No amount of user education will prevent a user's workstation from silently getting compromised due to a drive by download when the user visits a legitimate web site that has temporarily been compromised. An adversary might choose to compromise a legitimate web site that the target user is known to visit, resulting in a more targeted intrusion referred to as a "watering hole" technique.

- User education needs to be tailored to the job role of the user. Additional specialised education is useful for employees with specific roles, for example:
  - Educate inhouse software developers to write secure code.
  - Educate inhouse software testers about common vulnerabilities to look for.
  - Educate staff who have a technical administrative role (such as system administrators, network administrators and database administrators) about IT security as well as about adversary techniques.
  - Educate senior business representatives to understand the risks of rushing to complete a project with inadequate security design and testing, as well as the risks of favouring business functionality over security instead of integrating security with business functionality.
  - Educate help desk staff to have a healthy level of suspicion, for example when handling a passphrase reset request from a user who can't adequately verify their identity. The psychological desire of employees to be helpful should not override documented business processes, policies, or common sense.
- Further guidance is available at: http://www.dsd.gov.au/publications/csocprotect/socially_engineered_email.htm
- ISM controls 0058, 0251-0253, 0255-0257, 0266, 0413, 0817-0821, 0922, 0576, 0609-0610, 1339-1340, 1083, 1147, 1298.

31. **Mitigation Strategy #21 - Operating system exploit mitigation mechanisms**

- such as Data Execution Prevention (DEP) and Address Space Layout Randomisation (ASLR).
- Configure DEP hardware and software mechanisms to apply to all operating system programs and other software applications that support DEP.
- Configure ASLR to apply to all operating system programs and other software applications that support ASLR.

- Information on DEP, ASLR and other generic mitigation technologies such as SEHOP is available at http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=26788
- Information about the Microsoft Enhanced Mitigation Experience Toolkit is available at:
  http://blogs.technet.com/b/security/archive/2012/08/08/microsoft-s-free-security-tools-enhanced-mitigation-experience-toolkit.aspx
  as well as
  http://support.microsoft.com/kb/2458544
- ISM control 0380.

32. **Mitigation Strategy #22 - Computer configuration management**

- based on a hardened Standard Operating Environment with unrequired operating system functionality disabled e.g. IPv6, autorun and Remote Desktop.
- Benefits of user workstations having a consistent managed configuration include:
  - the ability to detect anomalous software on user workstations based on monitoring for deviations from the standard baseline. Implementing application whitelisting, even if configured in "logging only" mode, can provide this ability.
  - network administrators knowing what software is used on the network, helping to baseline expected network activity.
  - assisting with assessing the severity of a newly announced vulnerability.
  - the ability to quickly re-image a compromised computer to a known clean state.
- Harden file and registry permissions, for example where possible, prevent users (and therefore malware running on the user's behalf) from running system executables commonly used for reconnaissance as listed in mitigation strategy "Centralised and time-synchronised logging of successful and failed computer events".
- Limit or preferably eliminate the storing of cached credentials, to help mitigate adversary techniques such as using "pass the hash" for reusing passphrase hashes without having to crack them.
- Configure the Windows Task Scheduler service to prevent user workstations from creating scheduled tasks (especially on servers) to execute malicious programs.
- ISM controls 0380, 0382-0383, 0341.

33. **Mitigation Strategy #23 - 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 0401, 0971, 1244-1278.

34. **Mitigation Strategy #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.
- The firewall should only allow approved networking ports and protocols required for business functionality.
- 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 0569, 0260-0261, 0996, 0263, 0841-0842, 0385, 0953, 0628, 0631, 0639, 1193.

35. **Mitigation Strategy #25 - Antivirus software**

- with up to date signatures, reputation ratings, and other heuristic detection capabilities such as checking the prevalence of a questionable file among the Internet user base, as well as whether the questionable file has been digitally signed with a reputable vendor certificate that hasn't been revoked.
- Scan files when they are accessed and on a scheduled basis.
- Use gateway and desktop antivirus software from different vendors.
- Some antivirus products have been evolving into anti-malware products, further evolving into converged endpoint security products that incorporate functionality to perform application whitelisting, HIDS/HIPS, and application based workstation firewalling.
- ISM controls 0380, 0847, 1033, 1288.

36. **Mitigation Strategy #26 - Workstation inspection of Microsoft Office files**

- for abnormalities e.g. using the Microsoft Office File Validation feature.
- ISM controls 1284-1285.

37. **Mitigation Strategy #27 - Enforce a strong passphrase policy**

- covering complexity, length, and avoiding both passphrase reuse and the use of dictionary words.
- This is especially important for service accounts and other accounts with administrative privileges.
- ISM controls 0417, 0421-0426.

38. **Mitigation Strategy #28 - Restrict access to Server Message Block (SMB) and NetBIOS services**

- running on workstations and on servers where possible.
- ISM controls 0520, 1182.

39. **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.

- USB flash storage devices infected with malware have been inadvertently distributed by major vendors at several Australian IT security conferences. Additionally, penetration testers have been known to scatter malicious USB flash storage devices, CDs and DVDs in the car park of targeted users.
- Transferring data from one system or network to another using portable media must be done in accordance with a robust media transfer policy and process.
- ISM controls 0161-0162, 0322-0323, 0325, 0330-0338, 0341-0348, 0831-0832, 1059, 0350-0354, 0356-0360, 0835-0836, 0947, 1065-1068, 0361-0364, 0366, 0368, 0370-0373, 0838-0840, 1160, 1069, 0329, 0374-0375, 0378, 0159, 1169, 1347.

40. **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 0572, 0263.

41. **Mitigation Strategy #31 - Disable LanMan passphrase support**

- and cached credentials on workstations and servers, to make it harder for adversaries to crack passphrase hashes.
- Preferably force a passphrase change for all accounts, so that existing LanMan passphrase hashes are less useful to an adversary.
- ISM control 1055.

42. **Mitigation Strategy #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.
- ISM control 1171.

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

- using signatures and heuristics to identify anomalies listed in mitigation strategy “Centralised and time-synchronised logging of allowed and blocked network activity”, as well as traffic crossing perimeter boundaries that contains keywords such as classification markings indicating sensitive data, noting that adversaries usually compress and/or encrypt such data in an attempt to defeat scanning for classification markings.
- ISM controls 0576-0578, 1028-1031, 1184-1185.

44. **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.
- An example implementation is available at: http://www.sans.org/windows-security/2010/08/31/windows-dns-server-blackhole-blacklist

- DSD accepts no liability for the accuracy of the example list of dynamic domains available at: http://www.malware-domains.com/files/dynamic_dns.zip
- ISM controls 0959-0960, 1236.

45. **Mitigation Strategy #35 - Selected network traffic capture**

- to perform post-incident analysis of successful intrusions, to determine the adversary's techniques and assess the extent of damage.
- Ensure that employees are aware that network traffic on the organisation's network is monitored for security purposes.
- Store network traffic for at least seven days if storage space permits, noting that the high upfront cost of this mitigation strategy might make it impractical for some organisations that will instead need to rely on logs. When a successful intrusion occurs, retain a copy of network traffic for several days prior to remediation, as well as for several days following remediation during which time the adversary is likely to attempt to regain access to the organisation's network.
- Focus on capturing traffic from computers on internal networks containing sensitive information. Preferably also capture traffic from the network perimeter for at least seven days if storage space permits, noting that its usefulness is diminished by exfiltrated data being encrypted and being sent to a computer that can't be attributed to the adversary.
- Metadata relating to network connections can complement logging, and consumes less storage space than network packets.
- ISM control 1213.

## Further Reading

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

47. A complementary publication regarding mitigation strategies is the 20 *Critical Security Controls* available from SANS at http://www.sans.org/critical-security-controls

## Contact Details

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

49. 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.