Australian Government
Department of Defence
Intelligence and Security

PROTECT

CYBER SECURITY OPERATIONS CENTRE

FEBRUARY 2014

Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details

Australian Signals Directorate | Reveal Their Secrets – Protect Our Own

Table of Contents

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.

Introduction

This document provides further information regarding ASD'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.asd.gov.au/infosec/ism/index.htm. Annex A contains a summary of the key changes made to this documentation suite since the previous release in 2012.

Readers are strongly encouraged to visit the ASD website for the latest version of this document and additional information about implementing the mitigation strategies, available at: http://www.asd.gov.au/infosec/top35mitigationstrategies.htm.

This document focuses primarily on defending user workstations and servers. The underpinning principles highlighted by the guidance in this document are applicable to broader ICT security activities. ASD's guidance to securely use mobile devices, such as tablets and smartphones, is available at http://www.asd.gov.au/publications/csocprotect/enterprise_mobility_bring_your_own_device_byod_paper.htm in addition to ASD's device-specific hardening guides.

Stages of a Targeted Cyber Intrusion

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	Action	Methodology
Stage 1	Reconnaissance to select target user, execution of malicious software (malware) through the selected intrusion technique.	Creation of a malicious website, compromise of a legitimate website ("watering hole" or "drive by download") or sending a "spear-phishing" e-mail with a malicious hyperlink or content.
Stage 2	Network propagation	Use of compromised account credentials or exploitable vulnerabilities.
Stage 3	Data exfiltration	Extraction of data through RAR/ZIP archive files, potentially exfiltrated via a Virtual Private Network (VPN) or other remote access connection.

Stage 1 – Code Execution

Cyber adversaries perform reconnaissance to select a target user, and either create a malicious website or compromise a legitimate website that the user visits, referred to as a targeted "drive by download" or "watering hole" technique. Alternatively, cyber adversaries send the user a malicious "spear phishing" email containing either a hyperlink to a website with malicious content, or a malicious email attachment such as a PDF file or Microsoft Office document which might be in a RAR/ZIP archive file.

This reconnaissance is made easier for cyber adversaries if the user's name and email address are readily available via their employer's website, social networking websites, or if the user uses their work email address for purposes unrelated to work.

Malware is then executed on the user's workstation and is often configured to persist by automatically executing every time the user restarts their workstation and/or logs on. The malware communicates with the network infrastructure controlled by cyber adversaries, usually downloading additional malware, enabling cyber adversaries to remotely control the user's workstation and perform any action or access any information that the user can.

Stage 2 – Network Propagation

Cyber adversaries commonly use compromised account credentials or exploitable vulnerabilities in an organisation's other workstations and servers to propagate (laterally move) throughout 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 workstations or servers 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. Cyber adversaries typically access:

- details about users including organisation hierarchy, usernames and passphrases including remote access credentials
- system information including configuration details of workstations, servers and the network.

Although passphrases might be stored as cryptographic hashes to frustrate cyber adversaries, freely available software and a single workstation or publicly available cloud computing service might 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, cyber adversaries might use the "pass the hash" technique, avoiding the need to crack passphrase hashes[1].

The use of single sign-on authentication in an organisation might significantly benefit cyber adversaries. In contrast, the appropriate use of multi-factor authentication helps to hinder cyber adversaries, especially if implemented for remote access or for when a user is about to perform a privileged action such as administering a workstation or server, or accessing a sensitive information repository.

Stage 3 – Data Exfiltration

Cyber adversaries usually use RAR/ZIP archive files to compress and encrypt a copy of an organisation's sensitive information.

Cyber adversaries exfiltrate this information from the network, sometimes from a single "staging" workstation or server on the organisation's network. Cyber adversaries use available network

[1] https://blogs.technet.com/b/security/archive/2012/12/11/new-guidance-to-mitigate-determined-adversaries-favorite-attack-pass-the-hash.aspx

protocols and ports allowed by an organisation's gateway firewall, such as encrypted HTTPS/SSL, HTTP, or in some cases DNS or email.

Cyber adversaries might obtain VPN or other remote access account credentials and use this encrypted network connection for exfiltrating information, with the aim of defeating network based monitoring.

Cyber adversaries typically have several compromised workstations or servers on the organisation's network, as well as compromised VPN or other remote access accounts, maintained as backdoors to facilitate further collection and exfiltration of information in the future.

Sensitive Information

As part of a risk assessment performed by business representatives and security staff, organisations need to identify the type and location of their sensitive information stored electronically. For the purpose of this document, sensitive information refers to either unclassified or classified information identified as requiring protection. Such information might reside in various locations including 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 the intelligence goals of cyber adversaries can provide insight into which of an organisation's users, based on their access to specific information, are likely to be targeted as part of a cyber intrusion. In some cases, targeting will coincide with a significant upcoming meeting or other business event of relevance to cyber adversaries.

Most Likely Targets

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 and network administrators, and other users who have administrative privileges to operating systems or applications such as databases
- all users who have access to sensitive information, including information which could provide a foreign government or organisation with a strategic or economic advantage
- 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.

Rationale for Implementing the Mitigation Strategies

Australian organisations with access to sensitive information, including all Australian federal government agencies, have a high likelihood of being compromised by cyber intrusions of low sophistication if the organisation's security posture is inadequate. In addition to the damage caused 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 monetary and staff resources to continually clean-up cyber intrusions of low sophistication.

Most organisations have finite monetary and staff resources, requiring their senior management to commit to the importance of protecting the organisation's sensitive information. The Top 4 mitigation strategies, when implemented as a package, address all three high level stages of a cyber intrusion and are the "sweet spot" of providing a large increase in security posture for a relatively small investment of time, effort and money.

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.

In addition to implementing mitigation strategies, organisations require an incident response plan and associated operational capabilities, including regularly performed and tested offline backups to recover from cyber intrusions. Developing and implementing these capabilities requires support from technical staff and business representatives, including data owners, corporate communications, public relations and legal staff.

When a cyber intrusion is identified, it needs to be understood to a reasonable extent prior to remediation. Otherwise, the organisation plays "whack a mole", cleaning compromised workstations and servers, as well as blocking network access to Internet infrastructure known to be controlled by cyber adversaries, while the same adversaries simply compromise additional workstations and servers using different malware and different Internet infrastructure to avoid detection.

For cyber intrusions of higher sophistication, ASD can assist Australian government agencies to develop a strategic plan to contain and eradicate the cyber intrusion, and improve the agency's security posture in preparation for the likelihood that cyber adversaries will immediately attempt to regain access to the agency's workstations and servers.

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 cyber intrusion.

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 information, workstations and servers 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 information. Missing patches, other known weaknesses in workstations and servers, and detected cyber intrusion attempts should be regularly and systematically reported so that senior managers understand the threat and can make appropriate risk treatment decisions.

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

Details of Mitigation Strategies

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 system and network administrators to meet business requirements 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.

Mitigation Strategy #1 – Application whitelisting

Mitigation

Application whitelisting of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers, implemented at least on workstations used by Most Likely Targets.

Rationale

An appropriately configured implementation of application whitelisting helps to prevent the undesired execution of software regardless of whether the software was downloaded from a website, clicked on as an email attachment, or introduced via a USB memory stick or CD/DVD.

Implementing application whitelisting on important servers such as Active Directory and other authentication servers can help prevent cyber adversaries from running malware that obtains passphrase hashes or otherwise provides cyber adversaries with additional privileges.

Implementation Guidance

The ability of application whitelisting to provide a reasonable barrier for low to moderately sophisticated cyber 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.

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 #15 'Centralised and time-synchronised logging of successful and failed computer events'.

Simply preventing a user from installing new applications to their workstation's hard disk is not application whitelisting.

It is advisable to deploy application whitelisting in phases, instead of trying to deploy it to an entire organisation at once. For example, 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 users are Most Likely Targets who usually run a limited number of software applications such as Microsoft Office, an email program and a web browser. An additional benefit is that, when these users are made aware that they clicked on a malicious email attachment or visited a malicious website and application whitelisting mitigated the compromise, they might provide additional support for the deployment of application whitelisting to more user workstations 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 workstations and servers. Initially testing application whitelisting in “audit”/“logging only” mode helps organisations to develop an inventory of installed software. Once an inventory has been established, application whitelisting can be properly configured in “enforce” mode 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, might unacceptably slow down users logging into their workstations.

Installers, or installation packages, can install, modify or remove programs. Common installer frameworks include Windows Installer and InstallShield. Installers often contain installation information as well as files to be installed all within one package. Windows Installer package files have an MSI filename extension and are commonly referred to as MSI files. MSI files are commonly used for unattended installation or modification of programs in Microsoft Windows environments.

Endpoint protection or anti-malware software from some vendors includes application whitelisting functionality.

Further Information

Detailed guidance on the Top 4 mitigation strategies is available at:
http://www.asd.gov.au/infosec/top35mitigationstrategies.htm

ISM controls: 0843, 0845, 0846, 0848, 0849, 0851, 0955, 0956-0957.

Mitigation Strategy #2 – Patch applications

Mitigation

Patch applications especially Java, PDF viewer, Flash Player, Microsoft Office, web browsers and web browser plugins including ActiveX. Also patch server applications such as databases that store sensitive information as well as web server software that is Internet accessible. Patch or mitigate systems exposed to “extreme risk” vulnerabilities within two days.

Use the latest version of applications since they typically incorporate additional security technologies such as sandboxing and other anti-exploitation capabilities. For some vendor software, upgrading to the latest version is the only way to patch a vulnerability.

Rationale

“Extreme risk” vulnerabilities in software used by an organisation can enable unauthorised code execution by cyber adversaries using the Internet, which can result in significant consequences for the organisation. The level of risk might also be affected by whether exploit code for a vulnerability is available commercially or publicly, for example in an open source tool like the Metasploit Framework or in a cybercrime exploit kit.

Implementation Guidance

Approaches to patching

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 a subset of 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 percentage of workstations belonging to users from every business section, especially to users who are Most Likely Targets. If there are no complaints of broken functionality within a day, the patch is then deployed to all other workstations. This approach minimises an organisation’s exposure to the vulnerability while also minimising the cost of testing patches, at the risk of having to rollback a patch if it breaks business functionality.
- 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 an organisation significant amounts of money, and leave it vulnerable for weeks or months, the consequences of which might potentially be a higher cost than removing a patch that has broken a small percentage of workstations.
- A different approach involving more thorough testing is usually used for deploying patches to servers, as well as for deploying service packs that introduce additional functionality.

Patch management

To obtain visibility of what software requires patching, maintain an inventory of software installed on every workstation and server, especially laptops that might only occasionally connect to the organisation’s network, and include details about software version and patching history.

Use an automated mechanism to confirm and record that deployed patches have been installed and applied successfully and remain in place.

Using the latest version

Avoid using software which no longer receives vendor security patches for vulnerabilities. This is especially important for software that interacts with untrusted and potentially malicious data.

Avoid continuing to use Adobe Reader prior to version X, as well as versions of Internet Explorer prior to version 8 for accessing Internet websites.

Further Information

Detailed guidance on the Top 4 mitigation strategies is available at:
http://www.asd.gov.au/infosec/top35mitigationstrategies.htm

ISM controls: 0790, 0297, 0298, 0300, 0303, 0304, 0940, 0941, 1143, 1144, 1244, 1298, 1348-1349, 1350-1351, 1362, 1365-1366.

Mitigation Strategy #3 – Patch operating system vulnerabilities

Mitigation

Patch operating system vulnerabilities. Patch or mitigate systems exposed to “extreme risk” vulnerabilities within two days.

Use the latest operating system version that meets your organisation’s business requirements, since newer operating systems typically incorporate additional security technologies including anti-exploitation capabilities.

Rationale

“Extreme risk” vulnerabilities in software used by an organisation can enable unauthorised code execution by cyber adversaries using the Internet, which can result in significant consequences for the organisation. The level of risk might also be affected by whether exploit code for a vulnerability is available commercially or publicly, for example in an open source tool like the Metasploit Framework or in a cybercrime exploit kit.

Implementation Guidance

Refer to the implementation guidance provided for mitigation strategy #2 ‘Patch applications’.

Apply firmware patches to networking devices such as routers and switches, especially those devices that are Internet accessible.

Avoid using Microsoft Windows XP and earlier versions of Microsoft Windows.

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

Detailed guidance on the Top 4 mitigation strategies is available at:
http://www.asd.gov.au/infosec/top35mitigationstrategies.htm

Further information on additional security technologies contained in 64-bit versions of Microsoft Windows is available at:
http://support.microsoft.com/kb/946765.

ISM controls: 0790, 0297, 0298, 0300, 0303, 0304, 0940, 0941, 1143, 1144, 1244, 1298, 1348, 1365-1366.

Mitigation Strategy #4 – Restrict administrative privileges

Mitigation

Restrict administrative privileges to operating systems and applications based on user duties. Such users should use a separate unprivileged account, and preferably a separate physical workstation, for activities that are non-administrative or risky such as reading email, web browsing and obtaining files via Internet services such as instant messaging.

Such users should perform administrative activities using a workstation that implements at least the Top 4 mitigation strategies.

Rationale

The consequences of a compromise are reduced if malware runs as a low privileged user instead of a user with administrative privileges.

Implementation Guidance

This mitigation strategy applies to:

- users who have domain or local system administrative privileges, and equivalent administrative privileges in non-Windows operating systems
- users who have elevated operating system privileges[2] [3]
- users who have privileged access to applications such as a database[4]
- administrative accounts that permit vendors to perform remote access.

Further Information

Detailed guidance on the Top 4 mitigation strategies is available at:
http://www.asd.gov.au/infosec/top35mitigationstrategies.htm

ISM controls: 0405, 0434, 0445-0448, 0985, 0709, 1175, 0582-0583, 0987, 1380-1383, 1385-1388.

Mitigation Strategy #5 – User application configuration hardening

Mitigation

User application configuration hardening, disabling: running Internet-based Java code, untrusted Microsoft Office macros, and unneeded/undesired web browser and PDF viewer features.

Rationale

This mitigation strategy significantly helps to reduce the attack surface. Specifically, it helps mitigate cyber intrusions that involve malicious content attempting to evade application whitelisting by either

[2] http://technet.microsoft.com/en-us/library/dd349804(v=WS.10).aspx

[3] http://technet.microsoft.com/en-us/library/dd145442.aspx

[4] http://www.infoworld.com/print/218023

exploiting an application's legitimate functionality, or exploiting a vulnerability for which a vendor patch is unavailable.

Implementation Guidance

Focus on hardening the configuration of applications used to interact with content from the Internet. For web browsers, disallow ActiveX, Java and Flash except for whitelisted websites that require this specific functionality for business purposes (e.g. if Flash is required to use a website for business purposes, allow only Flash but not ActiveX or Java). Disallowing HTML inline frames and javascript, except for whitelisted websites, is ideal though challenging due to the large number of websites that require such functionality for business purposes.

A variety of approaches can be used to mitigate running malicious Java code located on the Internet, including:

- uninstalling Java if there is no business requirement to use it
- configuring Java to disable "Java content in the browser"[5]
- applying web browser specific configuration settings that disable Java in the web browser[6]
- using a separate web browser that can only run Java code located on the organisation's internal systems
- using the Deployment Rule Set[7] [8] feature to whitelist Java applets and Java Web Start applications
- using web content filtering to provide defence in depth mitigation, including providing an exception for whitelisted Internet websites that require the use of Java for business purposes.

Further Information

ISM controls: 0380, 0961.

Mitigation Strategy #6 – Automated dynamic analysis

Mitigation

Perform 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.

Rationale

Dynamic analysis uses behaviour-based detection capabilities instead of relying on the use of signatures, enabling organisations to detect malware that has yet to be identified by vendors.

[5] http://java.com/en/download/help/disable_browser.xml

[6] http://blogs.technet.com/b/srd/archive/2013/05/29/java-when-you-cannot-let-go.aspx

[7] https://blogs.oracle.com/java-platform-group/entry/introducing_deployment_rule_sets

[8] http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/deployment_rules.html

Implementation Guidance

Analysis could be performed in an instrumented sandbox located either in an organisation's gateway, on a user's workstation, or in the cloud subject to concerns about data sensitivity, privacy, and security of the communications channel.

Preferably use an implementation that:

- is able to perform analysis of decrypted email and web content that is otherwise encrypted by SSL/TLS when in transit over the Internet
- analyses emails before delivering them to users, to avoid users being exposed to malicious content
- rapidly and effectively mitigates web content that has already been delivered to users and has subsequently been identified as malicious. Mitigation might include blocking the workstation's access to the Internet infrastructure that the malicious content communicates with, or otherwise quarantining the user's workstation
- enables the sandbox to be customised to match the operating systems, applications and configuration settings of workstations used throughout your organisation.

Use an implementation that is regularly updated by the vendor to mitigate evolving evasion techniques that challenge the effectiveness of this mitigation strategy. Avoid using implementations that are easily circumvented by cyber adversaries using evasion techniques such as:

- manipulating network traffic using approaches historically used to evade intrusion detection systems
- performing malicious actions only:
    - after a period of time or specified date has elapsed
    - after the user has interacted with the workstation, such as clicked a mouse button
    - if the malware considers the workstation to be a real user's workstation and not a virtual machine or honeypot.

Further Information

ISM control: 1389.

Mitigation Strategy #7 – Operating system generic exploit mitigation

Mitigation

Apply operating system generic exploit mitigation technologies e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET). Security-Enhanced Linux (SELinux) and grsecurity are examples of exploit mitigation mechanisms for Linux operating systems.

Rationale

These technologies provide system-wide measures to help mitigate techniques used to exploit vulnerabilities, including for applications which EMET is specifically configured to protect, even in cases where the existence and details of vulnerabilities are not publicly known.

Implementation Guidance

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.

Further Information

Further information about EMET is available at:

- http://www.microsoft.com/emet
- http://krebsonsecurity.com/2013/06/windows-security-101-emet-4-0/
- http://blogs.technet.com/b/security/archive/2012/08/08/microsoft-s-free-security-tools-enhanced-mitigation-experience-toolkit.aspx

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

ISM control: 0380.

Mitigation Strategy #8 – Host-based Intrusion Detection/Prevention System

Mitigation

Implement a Host-based Intrusion Detection/Prevention System (HIDS/HIPS) to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and call hooking. Suspicious behaviour also includes software attempting to persist after the workstation or server is rebooted, for example by modifying or adding registry settings and files such as computer services.

Rationale

HIDS/HIPS uses behaviour-based detection capabilities instead of relying on the use of signatures, enabling organisations to detect malware that has yet to be identified by vendors.

Implementation Guidance

Configure the HIDS/HIPS capability to achieve an acceptable balance between identifying malware, while avoiding negatively impacting users and your organisation's incident response team due to false positives.

Endpoint protection or anti-malware software from some vendors includes HIDS/HIPS functionality.

Further Information

ISM controls: 0576, 1034, 1341, 1184-1185.

Mitigation Strategy #9 – Disable local administrator accounts

Mitigation

Disable local administrator accounts to prevent cyber adversaries from easily propagating throughout an organisation’s network using compromised local administrator credentials that are shared by several workstations.

Rationale

Disabling local administrator accounts helps to prevent cyber adversaries from propagating throughout an organisation’s network as part of the second stage of a cyber intrusion.

Implementation Guidance

In cases where it is not feasible to disable the local administrator account on servers such as the Active Directory authentication server, ensure that the local administrator account has a passphrase that meets ISM requirements. Appropriately protect records of the passphrases used for such servers.

Further Information

ISM controls: 0383, 0445.

Mitigation Strategy #10 – Network segmentation and segregation

Mitigation

Segment and segregate networks into security zones to protect sensitive information and critical services, such as user authentication by the Microsoft Active Directory service.

Network segmentation involves partitioning the network into smaller networks. Network segregation involves developing and enforcing a ruleset controlling which workstations and servers are permitted to communicate with which other workstations and servers. For example, on most corporate networks, direct network communication between user workstations should not be required or permitted.

Rationale

Network segmentation and segregation helps to prevent cyber adversaries from propagating throughout an organisation’s network as part of the second stage of a cyber intrusion.

If implemented correctly, it can make it significantly more difficult for cyber adversaries to locate and gain access to an organisation’s most sensitive information.

Implementation Guidance

Network segmentation and segregation should be based on the connectivity required, user job role, business function, trust boundaries and sensitivity of information stored.

Network controls that can assist with implementing network segmentation and segregation include switches, virtual LANs, enclaves, data diodes, firewalls, routers and Network Access Control.

Constrain VPN and other remote access, wireless connections, as well as user-owned laptops, smartphones and tablets which are part of a “Bring Your Own Device” implementation.

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, might 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, 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.

Sensitive servers such as Active Directory and other authentication servers should only be able to be administered from a limited number of intermediary servers referred to as “jump servers”. Jump servers should be closely monitored, be well secured, limit which users and network devices are able to connect to them, and typically have no Internet access. Some jump servers might require limited Internet access if they are used to administer defined workstations or servers located outside of the organisation’s local network.

Organisations with critically sensitive information might choose to store and access it using air-gapped workstations and servers that are not accessible from the Internet. Security patches and other data can be transferred to and from such air gapped workstations and servers in accordance with a robust media transfer policy and process.

Further Information

Further guidance on network segmentation and segregation is available at:
http://www.asd.gov.au/publications/csocprotect/network_segmentation_segregation.htm

Information specifically pertaining to mobility solutions is available at:
http://www.asd.gov.au/publications/csocprotect/enterprise_mobility_bring_your_own_device_byod_paper.htm

ISM controls: 1346, 1181, 1182, 1385.

Mitigation Strategy #11 – Multi-factor authentication

Mitigation

Implement multi-factor authentication, especially for Most Likely Targets, remote access, and when the user is about to perform a privileged action (including system administration) or access a 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.

Rationale

Multi-factor authentication helps to prevent cyber adversaries from propagating throughout an organisation’s network as part of the second stage of a cyber intrusion.

If implemented correctly, multi-factor authentication can make it significantly more difficult for cyber adversaries to steal legitimate credentials to facilitate further malicious activities on the network.

Implementation Guidance

Different multi-factor authentication mechanisms provide varying levels of security.

- A physically separate token with a time-based value, that is not physically connected to the workstation, might be the most secure option depending on its use and implementation. Multi-factor authentication using a physically separate token with a time-based value helps to prevent cyber adversaries from establishing their own VPN or other remote access connection to an organisation's network.
- A smart card might be a less secure option, depending on its use and implementation including whether the smart card is left connected to the workstation, and also to what degree software running on the workstation can interact with the smart card.
- A software based certificate that is stored and protected by the operating system is an even less secure option. It might be copied by cyber adversaries who have obtained administrative privileges on the target user's workstation.
- A software based certificate that is stored as a file without additional protection is an even less secure option. It might be easily copied by cyber adversaries without requiring administrative privileges.

Secure servers that store user authentication data and perform user authentication since such servers are frequently targeted by cyber adversaries.

The use of multi-factor authentication for remote access does not fully mitigate users entering their passphrase on a compromised computing device. Cyber adversaries might obtain a user's passphrase when it is entered into a compromised computing device used for remote access. This passphrase might then be used as part of a subsequent cyber intrusion, for example by cyber adversaries 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 cyber intrusion against the corporate network. Mitigations for this 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.

Ensure that administrative service accounts, and other accounts that are unable to use multi-factor authentication, use a passphrase that meets ISM requirements.

Further Information

Further guidance on multi-factor authentication is available at:
http://www.asd.gov.au/publications/csocprotect/multi_factor_authentication.htm

ISM controls: 1039, 1265, 1173, 0974, 1384, 1357.

Mitigation Strategy #12 – Software-based application firewall, blocking incoming network traffic

Mitigation

Implement a software-based application firewall, blocking incoming network traffic that is malicious or otherwise unauthorised, and denying network traffic by default.

Rationale

Blocking unnecessary network connections reduces the potential attack surface by limiting exposure to network services running on workstations and servers, as well as reducing the ability of cyber adversaries to propagate throughout an organisation's network as part of the second stage of a cyber intrusion.

Implementation Guidance

Endpoint protection or anti-malware software from some vendors includes software-based application firewall functionality.

Further Information

ISM controls: 0380, 0941, 1017.

Mitigation Strategy #13 – Software-based application firewall, blocking outgoing network traffic

Mitigation

Implement a software-based application firewall, blocking outgoing network traffic that is not generated by a whitelisted application, and denying network traffic by default.

Rationale

Blocking outgoing network traffic that is not generated by a whitelisted application helps to prevent cyber adversaries from propagating throughout an organisation's network as part of the second stage of a cyber intrusion, and from exfiltrating the organisation's data as part of the third stage of a cyber intrusion.

Implementation Guidance

Endpoint protection or anti-malware software from some vendors includes software-based application firewall functionality.

Further Information

ISM controls: 0380, 0941, 1017.

Mitigation Strategy #14 – Non-persistent virtualised sandboxed trusted operating environment

Mitigation

Implement a non-persistent virtualised sandboxed trusted operating environment, hosted outside of your organisation’s internal network, for risky activities such as web browsing.

Rationale

Cyber adversaries who compromise a user’s non-persistent virtualised workstation, which is located outside of an organisation’s internal network, will have a significantly reduced ability to persist as part of the first stage of a cyber intrusion, and to propagate throughout the organisation’s network as part of the second stage of a cyber intrusion.

Implementation Guidance

Network segmentation and segregation should be implemented to mitigate the risk of a compromised virtualised operating environment accessing an organisation’s sensitive information.

The non-persistent nature of this mitigation strategy helps to automatically restore a compromised system to a known good state. However, it will also remove some forensic evidence related to the cyber intrusion, highlighting the importance of organisations performing centralised logging as discussed in mitigation strategies #15 and #16.

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.

Further Information

Implementation options are included in ASD’s guidance on network segmentation and segregation, available at:
http://www.asd.gov.au/publications/csocprotect/network_segmentation_segregation.htm

ISM controls: 1181, 1345, 1346.

Mitigation Strategy #15 – Centralised and time-synchronised logging of successful and failed computer events

Mitigation

Perform 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 VPN and other remote access connections.

Rationale

Centralised and time-synchronised logging and timely log analysis will increase an organisation’s ability to rapidly identify patterns of suspicious behaviour and correlate logged events across multiple workstations and servers, as well as enabling easier and more effective investigation and auditing if a cyber intrusion occurs.

Implementation Guidance

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 users.

Perform regular log analysis focusing on:

- Most Likely Targets, especially users who have administrative privileges to operating systems or applications such as databases
- application whitelisting logs revealing attempted but blocked program execution, as well as logs generated by other security products
- gaps in logs where there should be periodic activity. For example, an absence of expected daily antivirus or security product logs usually generated by workstations of users who are in the office and are believed to be using their workstations, potentially indicating that cyber adversaries have disabled the security products
- user actions outside of business hours, noting that malware compromising a user's account might 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
- access to critical asset workstations and servers that store or process sensitive data
- access 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, powershell, at, schtasks, tasklist, rundll32, gpresult and systeminfo
- user authentication and use of account credentials.

When performing log analysis of user authentication and use of account credentials, especially focus on:

- user authentication from a user who is currently on holiday or other leave
- user authentication from workstations other than the user's usual workstation, especially if from workstations that are located outside of the user's geographical location
- VPN and other remote access connections from countries that the associated user is not located in
- a single IP address attempting to authenticate as multiple different users
- VPN and other remote access connections 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 workstations or servers
- 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.

Further Information

ISM controls: 0120, 0670, 0790, 0380, 0957, 0261, 0109, 0580, 0582-0583, 0584, 0585, 0586, 0587, 0859, 0987, 0988, 0991, 1032, 0631, 0634, 1176, 1305.

Mitigation Strategy #16 – Centralised and time-synchronised logging of allowed and blocked network activity

Mitigation

Perform 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 an organisation's network, and metadata such as Network Flow data.

Rationale

Centralised and time-synchronised logging and timely log analysis will increase an organisation's ability to rapidly identify patterns of suspicious behaviour and correlate logged events across multiple workstations and servers, as well as enabling easier and more effective investigation and auditing if a cyber intrusion occurs.

Implementation Guidance

Perform regular log analysis focusing on connections and the 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 your 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 is yet to be registered by cyber adversaries
- DNS lookups for domain names that resolve to a localhost IP address such as 127.0.0.1, indicating malware that cyber adversaries are not ready to communicate with
- large amounts of traffic

- traffic outside of business hours
- long lived connections.

Maintain a network map and an inventory of devices connected to the network to help baseline normal behaviour on the network and highlight anomalous network activity.

Further Information

ISM controls: 0120, 0670, 0790, 0380, 0957, 0261, 0109, 0580, 0582-0583, 0584, 0585, 0586, 0587, 0859, 0987, 0988, 0991, 1032, 0631, 0634, 1176, 1305.

Mitigation Strategy #17 – Email content filtering

Mitigation

Implement email content filtering, allowing only whitelisted attachments with a file type and file extension that are required for business functionality.

Rationale

Email content filtering helps to prevent the compromise of user workstations via cyber adversaries using malicious emails.

Implementation Guidance

Preferably analyse/convert/sanitise hyperlinks, PDF and Microsoft Office attachments to disable malicious content.

Disallow or quarantine content that cannot be inspected such as passphrase protected ZIP archive files.

Reject emails from the Internet that have your organisation’s domain as the email sender.

Preferably archive PDF and Microsoft Office attachments, and virus scan them again every month for several months.

Preferably quarantine attachments and disable hyperlinks in emails from webmail providers that provide free email addresses to anonymous Internet users, since cyber intrusions commonly involve the use of such email addresses due to the lack of attribution.

Further Information

Refer to mitigation strategy #6 ‘Automated dynamic analysis of email and web content run in a sandbox’ for details about detecting email content exhibiting suspicious behaviour such as network traffic or changes to the file system or registry.

An example plugin for Microsoft Exchange that sanitises PDF files is available at:
http://www.asd.gov.au/infosec/top35mitigationstrategies.htm

Further guidance on malicious email mitigation strategies is available at:
http://www.asd.gov.au/publications/csocprotect/malicious_email_mitigation.htm

ISM controls: 0561, 1057, 1234, 1284-1285, 1288, 0649-0650, 0651-0652, 1389.

Mitigation Strategy #18 – Web content filtering

Mitigation

Implement web content filtering of incoming and outgoing traffic, whitelisting allowed types of web content and using behavioural analysis, Internet-based reputation ratings, heuristics and signatures.

Rationale

An effective web content filter reduces the risk of a malware infection or other inappropriate content from being accessed, as well as making it more difficult for cyber adversaries to communicate with their malware. Defining a whitelist will assist in removing one of the most common data delivery and exfiltration techniques used by malware.

Implementation Guidance

Preferably block all executable content by default and use a process to enable individual selected access if a business justification exists.

Preferably block access to websites that the web content filter considers to be “uncategorised” or in a category that is not required for business purposes.

Disallow ActiveX, Java and Flash except for whitelisted websites that require this specific functionality for business purposes (e.g. if Flash is required to use a website for business purposes, allow only Flash but not ActiveX or Java).

Disallowing HTML inline frames and javascript, except for whitelisted websites, is ideal though challenging due to the large number of websites that require such functionality for business purposes.

Implement a solution that inspects SSL traffic for malicious content, especially SSL communications with unfamiliar websites.

Further Information

Refer to mitigation strategy #6 ‘Automated dynamic analysis of email and web content run in a sandbox’ for details about detecting web content exhibiting suspicious behaviour such as network traffic or changes to the file system or registry.

ISM controls: 0963, 0961, 1237, 1389, 1390.

Mitigation Strategy #19 – Web domain whitelisting for all domains

Mitigation

Implement web domain whitelisting for all domains, since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.

Rationale

Defining a whitelist will assist in removing one of the most common data delivery and exfiltration techniques used by malware.

Implementation Guidance

To minimise the user resistance and the administrative overhead potentially associated with this mitigation strategy, implement a streamlined process for users to easily and quickly add domains to the whitelist.

Further Information

An example implementation is available at:
http://whitetrash.sourceforge.net

ISM controls: 0263, 0995, 0958.

Mitigation Strategy #20 – Block spoofed emails

Mitigation

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.

Rationale

SPF, or alternative implementations such as Sender ID, aid in the detection of spoofed emails and therefore reduce the success rate of such cyber intrusion methods.

Implementation Guidance

Configure SPF records for your organisation's domains and subdomains, and configure a wildcard SPF record to match non-existent subdomains.

Sender ID is an alternative version of SPF that checks the legitimacy of the sender's email address that is displayed to the email recipient. Additional implementations include DomainKeys Identified Mail (DKIM).

Domain-based Message Authentication, Reporting and Conformance (DMARC) standardises how email receivers perform email authentication using the SPF and DKIM mechanisms.

Reject emails from the Internet that have your organisation's domain as the email sender.

Further Information

Further guidance on spoofed email mitigation strategies is available at:
http://www.asd.gov.au/publications/csocprotect/spoof_email_sender_policy_framework.htm

ISM controls: 0574, 1151-1152, 0861, 1025-1027, 0561, 1183.

Mitigation Strategy #21 – Workstation and server configuration management

Mitigation

Perform workstation and server configuration management based on a hardened Standard Operating Environment, disabling unneeded/undesired functionality e.g. IPv6, autorun and LanMan.

Rationale

Benefits of workstations and servers having a consistent managed configuration include:

- the ability to detect anomalous software on workstations and servers by monitoring for deviations from the standard baseline – implementing application whitelisting, even if configured in "audit"/"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 restore a compromised workstation or server to a known clean state.

Implementation Guidance

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 #15 'Centralised and time-synchronised logging of successful and failed computer events'.

Configure the Windows Task Scheduler service to prevent user workstations from creating scheduled tasks (especially on servers) to execute malicious programs.

Configure the DLL search path algorithm to help mitigate malicious DLL files being loaded[9].

Further Information

Australian government agencies can access a Microsoft Windows 7 SP1 Standard Operating Environment build guideline as part of the Australian Government Common Operating Environment at: http://agict.gov.au/policy-guides-procurement/common-operating-environment-coe-policy

ISM controls: 0380, 0382, 0383, 0341, 1055.

Mitigation Strategy #22 – Antivirus software using heuristics and automated Internet-based reputation ratings

Mitigation

Implement 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. Specifically, this includes checking the prevalence of a questionable file among the Internet user base, and checking whether a digitally signed file uses a reputable vendor certificate that hasn't expired or been revoked.

Rationale

Antivirus software helps to prevent, detect and remove malware that includes computer viruses, worms, Trojans, spyware and adware.

Implementation Guidance

Configure the heuristic behaviour analysis capability to achieve an acceptable balance between identifying malware, while avoiding negatively impacting users and your organisation's incident response team due to false positives.

[9] http://support.microsoft.com/kb/2264107

Scan files when they are accessed and on a scheduled basis.

Endpoint protection or anti-malware software from some vendors includes heuristics and automated Internet-based reputation rating functionality.

Further Information

ISM controls: 0380, 1033, 1288, 1390.

Mitigation Strategy #23 – Deny direct Internet access from workstations

Mitigation

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.

Rationale

Malware used in cyber intrusions of low sophistication can fail to exfiltrate data and operate correctly if it expects direct Internet connectivity and is therefore unable to traverse an organisation's Internet gateway, resulting in the Internet gateway detecting and blocking such unauthorised attempts to directly access the Internet.

Implementation Guidance

The firewall should only allow approved networking ports and protocols required for business functionality.

Implement a web proxy that inspects SSL traffic for malicious content, especially SSL communications with unfamiliar websites.

Preferably configure workstations with a non-routing network capture device as the default route to help detect malware attempting to directly communicate with the Internet, noting that some legitimate applications or operating system functionality might generate false positives.

Further Information

ISM controls: 0569, 0260-0261, 0996, 0263, 0841-0842, 0385, 0953, 0628, 0631, 0639.

Mitigation Strategy #24 – Server application configuration hardening

Mitigation

Perform server application configuration hardening e.g. databases, web applications, customer relationship management, finance, human resources and other data storage systems.

Rationale

Server application configuration hardening helps an organisation to conduct its business with a reduced risk of malicious data access, theft, exposure, corruption and loss.

Implementation Guidance

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.

Further Information

Further guidance on protecting web applications is available at:
http://www.asd.gov.au/publications/csocprotect/protecting_web_apps.htm

ISM controls: 0401, 0971, 0393, 1244-1253, 1254-1278.

Mitigation Strategy #25 – Enforce a strong passphrase policy

Mitigation

Enforce a strong passphrase policy covering complexity, length, expiry, and avoiding both passphrase reuse and the use of a single dictionary word.

This is especially important for service accounts and all other accounts with administrative privileges.

Rationale

It is more challenging for cyber adversaries to crack passphrase hashes and propagate throughout an organisation’s network as part of the second stage of a cyber intrusion if passphrases are complex, long and hashed with a cryptographically strong algorithm.

Implementation Guidance

The use of an appropriately configured and secured passphrase vault can assist with storing and managing many complex passphrases.

Further Information

ISM controls: 0417, 0421-0422, 0423-0426.

Mitigation Strategy #26 – Removable and portable media control

Mitigation

Control removable and portable media as part of a Data Loss Prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.

Rationale

Using media in a controlled and accountable manner reduces the risk of malware execution and unauthorised data exposure. 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.

Implementation Guidance

Follow a robust media transfer policy and process when using portable media to transfer data between workstations or servers, especially if they are located on different networks or in different security domains.

Further Information

ISM controls: 0161-0162, 0322-0323, 0325, 0330-0335, 0336, 0337-0338, 0341-0345, 0346, 0347, 0348, 0831-0832, 1059, 0350, 0351-0353, 0354, 0356-0357, 0358-0360, 0835, 0836, 0947, 1065-1068, 0361, 0362, 0363-0364, 0366, 0368, 0370-0373, 0838, 0839-0840, 1160, 1360, 1361, 1069, 0329, 0374, 0375, 0378, 0159, 1169, 1347, 1359.

Mitigation Strategy #27 – Restrict access to Server Message Block (SMB) and NetBIOS

Mitigation

Restrict access to Server Message Block (SMB) and NetBIOS services running on workstations and on servers where possible.

Rationale

This mitigation strategy primarily helps to mitigate internal reconnaissance and network propagation as part of the second stage of a cyber intrusion.

Implementation Guidance

Access to these services can be restricted by using a firewall or by disabling unneeded services.

Further Information

ISM controls: 0520, 1182.

Mitigation Strategy #28 – User education

Mitigation

Educate users, especially Most Likely Targets, about Internet threats such as identifying spear phishing socially engineered emails or unexpected duplicate emails, and reporting such emails to the IT security team. Users should also report suspicious phone calls, such as unidentified callers attempting to solicit details about the organisation’s IT environment. Such education should focus on influencing user behaviour.

Rationale

User education can complement technical mitigation strategies. Users can 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. This can assist in detecting spear phishing emails as an intrusion vector. However, to *prevent* and *automatically detect* a cyber 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.

ASD 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 cyber intrusion attempt.

User education won't prevent a user from visiting a legitimate website that has been temporarily compromised to serve malicious content as part of a "watering hole" or "drive by download". Visiting such a website might compromise the user's workstation without any obvious indications of compromise for the user to detect.

Implementation Guidance

Educate users to avoid:

- selecting weak passphrases
- reusing the same passphrase on the same workstation
- using the same passphrase in several different places
- unnecessarily exposing their email address and other personal details
- visiting websites unrelated to work
- using USB flash storage devices and other IT equipment not corporately provided.

Educate users as to 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 cyber intrusion attempts targeting the organisation and similar organisations, highlighting the impact that cyber intrusions have to the organisation and to the user. Such education might reduce the level of user resistance to the implementation of mitigation strategies. For example, users might be less likely to resist the removal of their unnecessary administrative privileges if they understand why the mitigation strategy is required.

User education needs to be tailored to the job role of the user. Additional specialised education is useful for users with specific roles, for example:

- educate in-house software developers to write secure code
- educate in-house software testers about common vulnerabilities to look for
- educate staff who have a technical role (such as system administrators, network administrators, database administrators, enterprise architects, IT project engineers and systems integrators) about IT security as well as about cyber 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 to be helpful should not override documented business policies, processes, or common sense.

The success of educating users needs to be measured using evidence such as whether user education contributed to:

- a reduction in the frequency and severity of successful compromises, including compromises resulting from phishing exercises and penetration tests, that involved users performing an action that facilitated the compromise
- an increased proportion of spear phishing emails and other indicators of malicious activity that users detect and report to their IT security team.

Further Information

Further guidance for users on detecting socially engineered emails is available at: http://www.asd.gov.au/publications/csocprotect/socially_engineered_email.htm

ISM controls: 0058, 0251-0253, 0255-0256, 0266, 0413, 0817-0820, 0821, 0922, 0576, 0609-0610, 1340, 1083, 1147, 1298.

Mitigation Strategy #29 – Workstation inspection of Microsoft Office files

Mitigation

Perform workstation inspection of Microsoft Office files for potentially malicious abnormalities.

Rationale

Inspection and validation of Microsoft Office files can assist with identifying malformed content, thereby enabling potentially malicious content to be blocked.

Implementation Guidance

Inspection and validation of Microsoft Office files can be performed using the Microsoft Office File Validation[10] or Protected View[11] feature[12].

Further Information

ISM controls: 1284-1285.

[10] http://www.cert.org/blogs/certcc/2011/05/effectiveness_of_microsoft_off.html

[11] http://office.microsoft.com/en-au/excel-help/what-is-protected-view-HA010355931.aspx

[12] http://technet.microsoft.com/en-us/library/ee857084.aspx

Mitigation Strategy #30 – Signature-based antivirus software

Mitigation

Use signature-based antivirus software that primarily relies on up to date signatures to identify malware. Use gateway and desktop antivirus software from different vendors.

Rationale

Antivirus software helps prevent, detect and remove malware that includes computer viruses, worms, Trojans, spyware and adware.

However, signature-based antivirus software is a reactive approach that has difficulty protecting against targeted malware that is not yet known to the antivirus vendor.

Implementation Guidance

Scan files when they are accessed and on a scheduled basis.

Further Information

ISM controls: 0380, 1033, 1288.

Mitigation Strategy #31 – TLS encryption between email servers

Mitigation

Use TLS encryption between email servers.

Rationale

Enabling TLS encryption on both the originating and accepting email servers helps to prevent legitimate emails being intercepted in transit and subsequently being used for social engineering.

Implementation Guidance

Perform content scanning after email traffic is decrypted.

Further Information

ISM controls: 0572, 0263.

Mitigation Strategy #32 – Block attempts to access websites by their IP address

Mitigation

Block attempts to access websites by their IP address instead of by their domain name.

Rationale

This mitigation strategy forces cyber adversaries to obtain a domain name, resulting in an audit trail that can assist with identifying related cyber intrusions.

Implementation Guidance

A web proxy server can be used to implement this mitigation strategy.

Further Information

ISM control: 1171.

Mitigation Strategy #33 – Network-based Intrusion Detection/Prevention System

Mitigation

Implement a network-based Intrusion Detection/Prevention System (IDS/IPS) using signatures and heuristics to identify anomalies listed in mitigation strategy #16 'Centralised and time-synchronised logging of allowed and blocked network activity'.

Rationale

A network-based IDS/IPS, when configured correctly, kept up to date with signatures, and supported by appropriate processes, assists with identifying and responding to known cyber intrusion profiles.

Implementation Guidance

Inspect traffic crossing perimeter boundaries for keywords such as classification markings that indicate sensitive information, noting that cyber adversaries usually compress and/or encrypt exfiltrated data in an attempt to defeat such inspection.

Further Information

ISM controls: 0576, 0577, 0578, 1028-1029, 1030, 1031, 1184-1185.

Mitigation Strategy #34 – Gateway blacklisting

Mitigation

Implement gateway blacklisting to block access to known malicious domains and IP addresses.

Rationale

Gateway blacklisting reduces the risk of users connecting to domains and IP addresses known to be controlled by cyber adversaries.

Implementation Guidance

Cyber intrusions commonly involve the use of dynamic domains and other domains provided free to anonymous Internet users, due to the lack of attribution. Block access to such domains after checking that your organisation does not access any legitimate websites using these domains.

Further Information

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

An example list of dynamic domains (for which ASD accepts no liability) is available at: http://www.malware-domains.com/files/dynamic_dns.zip

ISM controls: 0959-0960, 1236.

Mitigation Strategy #35 – Capture network traffic

Mitigation

Capture network traffic to/from internal critical asset workstations and servers, as well as traffic traversing the network perimeter, to perform post-intrusion analysis.

Rationale

Capturing network traffic can assist an organisation to determine the techniques used by cyber adversaries, and to assess the extent of damage if a cyber intrusion occurs. Analysis after a successful cyber intrusion helps to ensure that the compromise has been remediated.

Implementation Guidance

Focus on capturing traffic from workstations and servers on internal networks that store or access sensitive information. Preferably also capture traffic from the network perimeter, noting that its usefulness is diminished by exfiltrated data typically being encrypted and sent to a computer that probably can't be attributed to cyber adversaries.

Ensure that users are aware that network traffic on the organisation's network is monitored for security purposes.

When a successful cyber 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 cyber adversaries are likely to attempt to regain access to the organisation's network.

Metadata relating to network connections can complement logging, and consumes less storage space than network packets.

Further Information

ISM control: 1213.

Further Reading

This document and additional information about implementing the Top 35 mitigation strategies, and the Top 4 in particular, is available at http://www.asd.gov.au/infosec/top35mitigationstrategies.htm

Alternative computer security guidance titled *The Critical Security Controls for Effective Cyber Defense* is available at http://www.counciloncybersecurity.org/practice-areas/technology.

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.

Annex A: Strategies to Mitigate Targeted Cyber Intrusions – Key Changes for 2014

This annex highlights the key changes made for the 2014 version of the *Strategies to Mitigate Targeted Cyber Intrusions* table and *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details* document. Specifically highlighted are the key changes to the mitigation strategy descriptors, rankings and overall security effectiveness, as well as key additional guidance provided in the body of this document.

Key Overarching Changes

Document & Section	Change & Reason
Strategies to Mitigate Targeted Cyber Intrusions, table.	**Change:** Amendment to text that separates the Top 4 mitigation strategies from the remaining mitigation strategies. **Reason:** To further clarify priority order of implementing the Top 4, and ensure implementation on servers is specifically referenced.
	Change: Amendments to table columns. ▪ Column 'Designed to Prevent or Detect an Intrusion' deleted. ▪ Column 'Helps Detect Intrusions' added. ▪ Column 'Helps Mitigate Intrusion Stage 1: Code Execution' retitled to 'Helps Prevent Intrusion Stage 1: Code Execution'. ▪ Column 'Helps Mitigate Intrusion Stage 2: Network Propagation' retitled to 'Helps Contain Intrusion Stage 2: Network Propagation'. ▪ Column 'Helps Mitigate Intrusion Stage 3: Data Exfiltration' retitled to 'Helps Contain Intrusion Stage 3: Data Exfiltration'. **Reason:** In the 2012 version, in some cases the word *prevent* was used to mean preventing the scope of an intrusion escalating to enable cyber adversaries to achieve their goals, rather than necessarily preventing initial malicious code execution. For example, using a non-persistent virtualised sandboxed trusted operating environment was listed as preventing an intrusion. However, the primary benefit of this mitigation strategy is to *contain* malicious code that has already executed, rather than preventing the malicious code from executing. The changes to the table columns are intended to clarify that to *prevent* an intrusion in the context of this document suite now specifically refers to preventing initial code execution. These wording changes are also the reason why the values in these columns have changed for a small number of mitigation strategies.
Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details, *Introduction*.	**Change:** Text added on document's applicability to mobile devices. **Reason:** To clarify that the primary focus of the *Strategies to Mitigate Targeted Cyber Intrusions* document suite is on defending user workstations and servers, as well as to refer to other available ASD guidance for advice on the secure use of mobile devices.
Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details, *Rationale for Implementing the Mitigation Strategies*.	**Change:** Additional text to reference the requirement for organisations to regularly perform and test offline backups. **Reason:** This guidance helps organisations to recover from cyber intrusions.

Key Changes to the Mitigation Strategies

Reasons for changes to the effectiveness ranking of mitigation strategies have not been provided in every instance. Such changes are, for the most part, due to other mitigation strategies being introduced, merged, or changing in ranking. Specific reasons are provided for mitigation strategies that have significantly changed in effectiveness.

Strategy	2014	↑↓	2012	Change & Reason
Application whitelisting	1	–	1	**Change:** Amendment to strategy descriptor and text added to *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details*. **Reason:** To address additional types of programs such as scripts and installers.
Patch applications	2	–	2	**Change:** Strategy descriptor amended to mention patching web browsers and using the latest version of applications. **Reason:** To reflect the prevalent exploitation of vulnerabilities in web browsers and Java, as well as the additional security technologies typically incorporated into newer versions of applications.
				Change: Text added to *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details.* **Reason:** To assist with patch management and assessing the risk of vulnerabilities.
Patch operating system vulnerabilities	3	–	3	**Change:** Text added to *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details.* **Reason:** To assist with patch management and assessing the risk of vulnerabilities.
Restrict administrative privileges	4	–	4	**Change:** Strategy descriptor amended and text added to *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details.* **Reason:** To highlight that administrative privileges need to be restricted based on user duties, and that this mitigation strategy applies to: ▪ users who have domain or local system administrative privileges, and equivalent administrative privileges in non-Windows operating systems ▪ users who have elevated operating system privileges ▪ users who have privileged access to applications such as a database ▪ administrative accounts that permit vendors to perform remote access.
User application configuration hardening	5	↑	18	**Change:** Ranking moved up to #5. Strategy descriptor amended and text added to *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details.* **Reason:** To assist with significantly reducing the attack surface, including mitigating intrusions that exploit the prevalence of Java vulnerabilities or leverage Microsoft Office macros.

Strategy	2014	↑↓	2012	Change & Reason
Automated dynamic analysis	6	N/A	N/A	**Change:** Behavioural analysis functionality has been extracted from the 'Email content filtering' and 'Web content filtering' mitigation strategies to create a new mitigation strategy. Text added to *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details.* **Reason:** There has been an increase in the availability and effectiveness of automated dynamic analysis technologies since the previous version of this document suite was published.
Operating system generic exploit mitigation	7	↑	21	**Change:** Ranking moved up to #7. The 'Overall Security Effectiveness' column value changed from *Good* to *Excellent*. Strategy descriptor amended and text added to *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details.* **Reason:** To reflect the proven effectiveness of Microsoft's Enhanced Mitigation Experience Toolkit (EMET) to help mitigate techniques used to exploit vulnerabilities, even in cases where the existence and details of vulnerabilities were not publicly known at the time. [13] [14] [15] [16] [17] [18] [19] [20] [21]
Host-based Intrusion Detection/Prevention System	8	↑	11	**Change:** Ranking moved up to #8.
Disable local administrator accounts	9	↓	5	**Change:** Ranking moved down to #9.
Network segmentation and segregation	10	↓	7	**Change:** Ranking moved down to #10. Minor amendment to strategy descriptor. **Reason:** To include a specific example of sensitive information and critical services requiring the protection provided by this strategy.
Multi-factor authentication	11	↓	6	**Change:** Ranking moved down to #11.

[13] https://isc.sans.edu/diary/Nuclear+Scientists%2C+Pandas+and+EMET+Keeping+Me+Honest/15890

[14] https://community.qualys.com/blogs/laws-of-vulnerabilities/2013/05/08/defense-for-the-0-day-in-ie8

[15] https://blogs.technet.com/b/srd/archive/2013/09/17/cve-2013-3893-fix-it-workaround-available.aspx

[16] https://blogs.technet.com/b/srd/archive/2013/07/10/running-in-the-wild-not-for-so-long.aspx

[17] https://blogs.technet.com/b/srd/archive/2012/12/29/new-vulnerability-affecting-internet-explorer-8-users.aspx

[18] https://blogs.technet.com/b/srd/archive/2013/06/11/ms13-051-get-out-of-my-office.aspx

[19] http://isc.sans.edu/diary.html?storyid=16985

[20] https://isc.sans.edu/diary/EMET+3.5%3A+The+Value+of+Looking+Through+an+Attacker's+Eyes/14797

[21] https://blogs.technet.com/b/srd/archive/2013/11/05/cve-2013-3906-a-graphics-vulnerability-exploited-through-word-documents.aspx

Strategy	2014	↑↓	2012	Change & Reason
Software-based application firewall, blocking incoming network traffic	12	↓	8	**Change:** Ranking moved down to #12. Minor amendment to strategy descriptor.
Software-based application firewall, blocking outgoing network traffic	13	↓	9	**Change:** Ranking moved down to #13. Minor amendment to strategy descriptor.
Non-persistent virtualised sandboxed trusted operating environment	14	↓	10	**Change:** Ranking moved down to #14. Minor amendment to strategy descriptor.
Centralised and time-synchronised logging of successful and failed computer events	15	↓	12	**Change:** Ranking moved down to #15. **Change:** Text added to *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details.* **Reason:** To provide additional guidance on where to focus log analysis activities.
Centralised and time-synchronised logging of allowed and blocked network activity	16	↓	13	**Change:** Ranking moved down to #16.
Email content filtering	17	↓	14	**Change:** Ranking moved down to #17. Amendments to strategy descriptor and *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details.* **Reason:** To reflect that cyber adversaries increasingly use spear phishing emails that either have an attachment type required for business purposes (and is therefore whitelisted), or have a hyperlink instead of an attachment. Also, the behavioural analysis component of this mitigation strategy is now covered in detail by the new 'Automated dynamic analysis' mitigation strategy.
Web content filtering	18	↓	15	**Change:** Ranking moved down to #18. Minor amendment to strategy descriptor. **Reason:** The behavioural analysis component of this mitigation strategy is now covered in detail by the new 'Automated dynamic analysis' mitigation strategy.
Web domain whitelisting for all domains	19	↓	16	**Change:** Ranking moved down to #19. **Reason:** To reflect that cyber adversaries are distributing and controlling malware by using legitimate (and therefore probably whitelisted) cloud computing services, as well as legitimate but temporarily compromised websites.[22] [23] [24]

[22] https://isc.sans.edu/diary/Challenges+of+Anti-Phishing+Advice%2C+the+Google+Docs+Edition/14731

Strategy	2014	↑↓	2012	Change & Reason
				Change: Now incorporates previous mitigation strategy #17 ‘Web domain whitelisting for HTTPS/SSL domains’. **Reason:** To reflect the significant increase in the number of websites that use HTTPS/SSL.
Block spoofed emails	20	↓	19	**Change:** Ranking moved down to #20. Text added to *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details.* **Reason:** To provide more complete guidance and help avoid misconfiguration of SPF records for subdomains and non-existent subdomains.
Workstation and server configuration management	21	↑	22	**Change:** Ranking moved up to #21. Minor amendment to strategy descriptor and text to help mitigate malicious DLL files being loaded added to *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details.* **Reason:** To reflect cyber intrusion tradecraft[25].
				Change: Now incorporates previous mitigation strategy #31 ‘Disable LanMan passphrase support’.
Antivirus software using heuristics and automated Internet-based reputation ratings	22	↑	25	**Change:** The ‘Antivirus software’ mitigation strategy (#25 in the previous version of this document) has been split into two mitigation strategies, creating this new mitigation strategy. Text added to *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details.* **Reason:** To reflect the difference in effectiveness between signature-based antivirus software and antivirus software that uses heuristics and automated Internet-based reputation ratings.
Deny direct Internet access from workstations	23	↑	24	**Change:** Ranking moved up to #23.
Server application configuration hardening	24	↓	23	**Change:** Ranking moved down to #24. Minor amendment to strategy descriptor.
Enforce a strong passphrase policy	25	↑	27	**Change:** Ranking moved up to #25.
				Change: Amendment to strategy descriptor and minor addition to *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details.* **Reason:** To note that use of an appropriately configured and secured passphrase vault can assist with storing and managing many complex passphrases.

[23] http://computerworld.com/s/article/9233831/Malware_uses_Google_Docs_as_proxy_to_command_and_control_server

[24] http://arstechnica.com/security/2013/06/vast-majority-of-malware-attacks-spawned-from-legit-sites/

[25] http://nakedsecurity.sophos.com/2013/02/27/targeted-attack-nvidia-digital-signature/

Strategy	2014	↑↓	2012	Change & Reason
Removable and portable media control	26	↑	29	**Change:** Ranking moved up to #26. Minor addition to *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details.*
Restrict access to Server Message Block (SMB) and NetBIOS	27	↑	28	**Change:** Ranking moved up to #27.
				Change: Minor addition to *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details.* **Reason:** To provide specific information on the risks this strategy primarily mitigates – internal reconnaissance and network propagation.
User education	28	↓	20	**Change:** Ranking moved down to #28. **Reason:** To reflect that user education will not prevent a user from visiting a legitimate website that has been temporarily compromised to serve malicious content as part of a "watering hole" or "drive by download". Visiting such a website might compromise the user's workstation without any obvious indications of compromise for the user to detect.
				Change: Minor addition to *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details.* **Reason:** To clarify the specific need to educate staff who have a technical role.
Workstation inspection of Microsoft Office files	29	↓	26	**Change:** Ranking moved down to #29. Minor amendment to strategy descriptor.
Signature-based antivirus software	30	↓	25	**Change:** Ranking moved down to #30. Amendments to strategy descriptor and *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details.* **Reason:** To reflect the difference in effectiveness between signature-based antivirus software and antivirus software that uses heuristics and automated Internet-based reputation ratings (as is now expressed through two distinct mitigation strategies - #22 and #30 - relating to antivirus software).
TLS encryption between email servers	31	↓	30	**Change:** Ranking moved down to #31.
Block attempts to access websites by their IP address	32	–	32	**Change:** Minor amendment to strategy descriptor. **Reason:** To provide implementation guidance.
				Change: The 'Overall Security Effectiveness' column value changed from *Good* to *Average*. **Reason:** To reflect that cyber adversaries who compromise a legitimate website automatically inherit a domain name. This mitigation strategy is also circumvented by cyber adversaries who obtain dynamic domains and other domains provided free to anonymous Internet users with minimal or no attribution.

Strategy	2014	↑↓	2012	Change & Reason
Network-based Intrusion Detection/Prevention System	33	–	33	**Change:** No changes.
Gateway blacklisting	34	–	34	**Change:** No changes.
Capture network traffic	35	–	35	**Change:** Minor amendment to strategy descriptor. **Reason:** To focus on capturing network traffic to/from internal critical asset workstations and servers, as well as traffic traversing the network perimeter.