Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Strategies to Mitigate Cyber Security Incidents – Mitigation Details

FEBRUARY 2017

cyber.gov.au

ACSC Australian Cyber Security Centre

Table of contents

Introduction

This document, developed by the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), replaces the ***Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details*** publication and directly complements the ***Strategies to Mitigate Cyber Security Incidents*** publication.

Additional information is provided in this document to help organisations mitigate cyber security incidents caused by:

- targeted cyber intrusions (e.g. executed by advanced persistent threats such as foreign intelligence services) and other external adversaries who steal data
- ransomware denying access to data for monetary gain, and external adversaries who destroy data and prevent computers/networks from functioning
- malicious insiders who steal data such as customer details or intellectual property
- malicious insiders who destroy data and prevent computers/networks from functioning
- 'business email compromise'
- threats to industrial control systems.

Readers are strongly encouraged to visit the ACSC's website[1] for the latest version of this document and additional information about implementing the mitigation strategies.

The ACSC's website also has separate and specific guidance for mitigating denial of service[2], and securely using cloud computing[3] [4] [5] and enterprise mobility including personally owned computing devices[6] [7].

[1] https://www.cyber.gov.au/
[2] https://www.cyber.gov.au/publications/preparing-for-and-responding-to-denial-of-service-attacks
[3] https://www.cyber.gov.au/publications/cloud-computing-security-considerations
[4] https://www.cyber.gov.au/publications/cloud-computing-security-for-tenants
[5] https://www.cyber.gov.au/publications/cloud-computing-security-for-cloud-service-providers
[6] https://www.cyber.gov.au/publications/bring-your-own-device-for-executives
[7] https://www.cyber.gov.au/publications/risk-management-of-enterprise-mobility-including-bring-your-own-device

Threat overview

The following pages provide an overview of the threats of targeted cyber intrusions, ransomware and external adversaries who destroy data and prevent computers/networks from functioning, as well as malicious insiders.

Implementation guidance for associated mitigation strategies is provided later in this document, and a table summary of the associated mitigation strategies is provided in the complementary ***Strategies to Mitigate Cyber Security Incidents*** publication.

Targeted cyber intrusions

Overview

Targeted cyber intrusions involve external adversaries who steal data. This can damage the competitive advantages and reputation of affected organisations, damage a country's economic wellbeing, influence public opinion, negatively impact citizens due to the release of their private data, and unnecessarily consume scarce financial and staff resources to respond to such intrusions.

Organisations need to identify the type and location of their sensitive data stored electronically, as part of a security risk assessment performed to identify the level of protection that their assets require from various threats. For the purpose of this document, sensitive data refers to either unclassified or classified information identified as requiring protection. This protection is often focused on maintaining confidentiality of the data, although data integrity and availability are also important and are often overlooked. Such data might reside within organisations 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.

Stages of a targeted cyber intrusion

No single mitigation strategy can prevent a targeted cyber intrusion, and organisations should implement mitigation strategies that address all three high level stages of targeted cyber intrusions.

Stage 1 – Malicious software (malware) delivery and execution:

- Adversaries perform reconnaissance to select a target user, and commonly send the user a malicious 'spear phishing' email containing either a hyperlink to a website with malicious content or a malicious email attachment. Examples of such email attachments include an executable program, a Microsoft Office document containing a malicious macro, or a script file (e.g. JScript, VBScript, Windows Script File, HTML Application or PowerShell) – these files might be in a zip, RAR or other archive file. Alternatively, adversaries might compromise a legitimate website which the user is likely to visit, referred to as a 'watering hole' or 'strategic web compromise'.
- This reconnaissance is made easier for adversaries if the user's name and/or 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 computer and is often configured to persist by automatically executing every time the user restarts their computer and/or logs on. The malware communicates with 'command and control' internet infrastructure controlled by adversaries, usually downloading additional malware, enabling adversaries to remotely control the user's computer and perform any action or access any data that the compromised user account can.

Stage 2 – Network propagation:

- Adversaries could use compromised account credentials, or in some cases exploitable security vulnerabilities affecting other computers in the organisation, to propagate (laterally move) throughout the network in order to locate and access sensitive data. Network propagation can occur rapidly on networks with inadequate network access restrictions, especially when multiple computers share the same local administrator passphrase. Data accessed frequently includes Microsoft Office files, Outlook email files, PDF files as well as data stored in databases. Adversaries typically access details such as the organisation hierarchy, usernames and passphrases including remote access credentials, as well as system data including configuration details of computers and the network.
- Although passphrases might be stored as cryptographic hashes to frustrate adversaries, these hashes can often be extracted by the adversary. Depending on the cryptographic strength of the hashing algorithm, these hashes might be cracked to derive the associated passphrases by using freely available software and a single computer or a publicly available cloud computing service. Some mitigation is provided by requiring all users to select a strong passphrase that is appropriately hashed using a cryptographically strong algorithm. Alternatively, adversaries might use a keystroke logger or the 'pass the hash' technique, avoiding the need to crack passphrase hashes[8].
- The use of single sign-on authentication in the organisation might significantly benefit adversaries. In contrast, the appropriate use of multi-factor authentication helps to hinder adversaries, especially if implemented for remote access, as well as for when users perform privileged actions such as administering a computer, and for when users access an important (sensitive or high-availability) data repository.

Stage 3 – Data exfiltration:

- Adversaries often use zip, RAR or other archive files to compress and encrypt a copy of the organisation's sensitive data.
- Adversaries exfiltrate this data from the network, using available network protocols and ports allowed by the organisation's gateway firewall, such as HTTPS, HTTP, or in some cases DNS or email.
- Adversaries might obtain Virtual Private Network (VPN) or other remote access account credentials, especially in the absence of multi-factor authentication, and use this encrypted network connection for exfiltrating data, with the aim of defeating network-based monitoring.
- Adversaries typically have several compromised computers 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 data in the future.

Most Likely Targets

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

- senior executives and their executive 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 data, including data that 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 people communicating via the internet – this includes users who handle Freedom of Information requests, media

[8] https://www.microsoft.com/en-au/download/details.aspx?id=36036

and public relations staff, the human resources team whose job includes reading email attachments such as job applications, and finance teams that receive invoices or tender documents.

Understanding the goals of adversaries can provide insight into which other users are likely to be targeted based on their access to sensitive data. Targeting might occur just prior to a significant upcoming meeting or other business event of relevance to adversaries.

Ransomware and external adversaries with destructive intent

Overview

Ransomware denies access to data, typically by encrypting it, until a monetary ransom is paid within a specified time period. Ransomware can delete accessible backups, sometimes spreads to other computers, and encrypts all accessible data including data stored on local hard drives, network drives (file shares) and removable storage media such as USB drives. Ransomware can prevent computers from functioning, for example if operating system files or configuration data are encrypted. 'Lockers' are related malware that focus on preventing computers from functioning until a ransom is paid.

Some adversaries target specific organisations, for example hospitals are highly motivated to pay the ransom if lives are at risk, and educational institutions typically depend on access to their data. Such compromises might occur by adversaries sending spear phishing emails, by exploiting security vulnerabilities in internet-accessible computers such as websites and associated databases, or by using brute-force passphrase guessing to remotely access computers exposed to the internet via Remote Desktop Protocol (RDP). Additional techniques used by adversaries to motivate victims to pay the ransom include threatening to either delete files or publicly publish sensitive files on the internet.

A limited number of ransomware variants have cryptographic weaknesses or their master decryption key has been disclosed, enabling files to be decrypted in limited cases using free tools[9].

Paying a ransom has ethical implications and doesn't guarantee that encrypted files will be decrypted. Adversaries might not be honest and trustworthy[10], the ransomware might not have the technical capability to decrypt data[11], or the data might be encrypted/deleted by multiple adversaries[12].

External adversaries who destroy data and prevent computers/networks from functioning, often motivated by political goals, could delete or corrupt data in a variety of ways. This includes deleting or corrupting user data, applications, operating system files, boot firmware accessed via BIOS/UEFI and other firmware, or configuration settings of computers and other network devices which prevent them from booting their operating system or otherwise operating normally.

Malicious insiders

Overview

Malicious insiders motivated by money or in some cases coercion, ideology, ego or excitement, might steal data such as customer details or intellectual property.

Malicious insiders motivated by revenge or disgruntlement due to reasons such as a negative job performance review, a denied promotion or involuntary termination of employment, might destroy data and prevent computers/networks from functioning.

[9] https://www.nomoreransom.org/en/index.html
[10] https://blog.talosintelligence.com/2016/07/ranscam.html
[11] http://www.zdnet.com/article/247000-killdisk-ransomware-demands-a-fortune-forgets-to-unlock-files/
[12] https://krebsonsecurity.com/2017/01/extortionists-wipe-thousands-of-databases-victims-who-pay-up-get-stiffed/

For the purpose of this document, the definition of the malicious insider threat excludes non-malicious employees who unintentionally and inadvertently facilitate a cyber security incident, for example by interacting with malicious emails sent by external adversaries – in this case the employee is not the threat, rather they are a weakness that the external threat is exploiting.

Some industry commentators suggest that malicious insiders who steal data can be mitigated using the same mitigation strategies, implemented in the same prioritised order, as for a targeted cyber intrusion that compromises an employee's computer account to access and exfiltrate data. However, there is a difference in mitigating these two threats since malicious insiders who steal data usually already have an account and access to data, so therefore don't need to use malware to obtain initial access. Also, malicious insiders have the option of using removable storage media such as USB drives to exfiltrate data. This typically isn't a viable low-risk exfiltration option for a targeted cyber intrusion where adversaries are in a physically distant location such as a foreign country.

Relevance of mitigation strategies to additional threats

The complementary ***Strategies to Mitigate Cyber Security Incidents*** publication doesn't explicitly provide mitigation guidance for the threat of 'business email compromise' or threats to industrial control systems. Nevertheless, non-exhaustive guidance is provided for these threats on the following pages to highlight how the existing mitigation strategies are relevant and can be leveraged as a baseline for mitigating these threats.

Business email compromise

Overview

'Business email compromise' involves adversaries using social engineering or targeted cyber intrusion techniques to abuse the trust in the target organisation's business processes with the typical goal of committing fraud. Examples include conducting unauthorised transfers of money or in some cases obtaining personnel details to commit tax fraud[13].

Sometimes adversaries compromise a legitimate email account or create an email account with a similar email address, which is then used to interact with the target. Adversaries might change bank account numbers and contact details on invoices so that the adversaries are inadvertently paid[14].

Adversaries might compromise the email account of the target's CEO or senior executive, or send 'spoofed' emails that appear to come from a CEO or senior executive. These techniques are also referred to as 'CEO fraud', 'senior executive impersonation' and 'business email spoofing'.

Mitigation guidance

Mitigation guidance for 'business email compromise' includes:

- Educate employees who can perform money transfers about spear phishing emails and the business processes to telephone the requester (avoiding using phone numbers in the email) to verify requests that are unusual such as asking for more money than a threshold amount, applying pressure seeking immediate action or requesting secrecy to circumvent business processes. Avoid publicly disclosing the contact details of such employees and details of when executives are unable to be contacted, for example because they are travelling on a plane.
- Block spoofed emails:
  - use Sender Policy Framework (SPF) or Sender ID to check incoming emails
  - configure DNS records for the organisation's domain to add a 'hard fail' SPF TXT record as well as a Domain-based Message Authentication, Reporting and Conformance (DMARC) record
  - reject incoming emails that have the organisation's domain as the email sender but do not originate from email servers approved by the organisation
  - preferably register domains that look very similar to the organisation's domain when letters such as 'l' and 'o' are replaced by digits such as '1' and '0'.
- Implement at least the four 'essential' mitigation strategies to 'prevent malware delivery and execution', particularly on computers used by the finance and human resources teams, senior executives and their assistants.

[13] https://www.ic3.gov/media/2016/160614.aspx
[14] https://www.brisbanetimes.com.au/national/queensland/townsville-also-targeted-by-scam-as-state-put-on-alert-20160819-gqw9x2.html

Industrial control systems

Overview

Industrial control systems (ICS) leverage operational technology (OT) environments, which include components such as electronic sensors as well as systems such as networked computing hardware. This equipment is often used to monitor or control industrial equipment typically to support operational reliability and safety functions.

OT environments are special-purpose and are designed to be in production for decades. This extended asset lifecycle, characterised by infrequent upgrades and replacements, extends the period of time that OT assets are vulnerable to cyber threats and creates additional complexity over time with respect to applying mitigation strategies. Security solutions need to support the high reliability and availability requirements of OT environments and the infrequent opportunities for scheduled outages.

OT environments are distinct from the information technology (IT) environments common to many organisations, which are used for general purpose functions (e.g. email, writing documents and web browsing) and are designed to be in production typically for one to three years before being refreshed, with regular opportunities for scheduled outages.

Mitigation guidance

Prioritise the protection of OT assets (including supporting computers) which are critical to the organisation's ability to deliver essential services.

Mitigation guidance for OT environments includes:

- restrict network connectivity with IT environments and with the internet – noting that completely air gapping OT environments might be impractical, limit remote access from the internet, and where remote access is used implement network-level encryption such as a VPN, multi-factor authentication and a strong passphrase policy
- ensure that only authorised code can be introduced to OT environments and run, by controlling removable storage media and connected devices, implementing application control where possible, and considering the use of code signing
- use vendor-supported applications and operating systems, and patch associated security vulnerabilities in a timely manner as soon as possible within the constraints of system uptime requirements – note the lack of availability of patches for a proportion of security vulnerabilities specific to OT assets which are deemed too difficult to fix or the associated equipment is no longer supported by the vendor
- refer to additional guidance available from US Government authorities[15] [16] [17].

Mitigation guidance for IT environments includes implementing the mitigation strategies listed in the ***Strategies to Mitigate Cyber Security Incidents*** for both targeted cyber intrusions as well as for ransomware and external adversaries with destructive intent, especially focusing on the computers that administer OT environments, develop software for OT environments, or otherwise can interact with OT environments.

[15] https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/seven-steps-to-effectively-defend-ics.cfm
[16] https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf
[17] https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

Overarching considerations when implementing mitigation strategies

Control of application and network activities

The concept of allowing only approved applications or network communications is a key theme of the mitigation strategies. In such cases, activities such as application execution or network communication is denied by default and only activity explicitly approved of by system administrators and network administrators to meet business requirements is allowed to occur.

The traditional approach of blocking the limited subset of applications or network communication that is known to be malicious is a very reactive approach that provides limited security[18] [19] [20].

Vendor products increasingly advertise alternative approaches to determine whether applications, network communication, computer behaviour or associated logs exhibit indications of malicious activity. Example alternatives include leveraging threat intelligence consisting of more than just indicators of compromise, big data analytics, heuristics, machine learning, artificial intelligence and maths/statistics. Several of these alternative approaches assume that normal behaviour of users and computers can be accurately baselined to identify anomalies while avoiding false positives. Organisations need to critically assess the value of such approaches before purchasing such vendor products, noting that the value is likely to vary depending on each vendor's implementation.

Effectiveness of network-based mitigation strategies

The effectiveness of network-based mitigation strategies continues to decrease due to evolutions in the architecture of IT infrastructure. For example, the network perimeter continues to be eroded due to the increasing use of external computer infrastructure such as cloud computing services as well as mobile computing devices used by employees. Also, it is increasingly infeasible to backhaul or otherwise steer network traffic to a single bottleneck location to implement network-based mitigation strategies such as 'Network-based intrusion detection/prevention system' and 'Capture network traffic'. These evolutions also impact the ability to implement the mitigation strategy 'Deny corporate computers direct internet connectivity'.

Cyber insurance

Paying for cyber insurance isn't a substitute for investing in cyber security protection by implementing these mitigation strategies, although cyber insurance might encourage organisations to implement these mitigation strategies to reduce the cost of their cyber insurance premium.

Even if a cyber security incident is covered by the cyber insurance policy, an insurance payout might not be able to repair damage such as stolen intellectual property and the associated loss of long term competitive advantages, damage to the organisation's reputation, lost customer loyalty, and citizens dealing with the consequences of their private data being compromised and used for malicious purposes such as identity theft and fraud.

[18] https://www.darkreading.com/partner-perspectives/intel/botnet-to-cybersecurity-catch-me-if-you-can/a/d-id/1319919
[19] https://www.darkreading.com/attacks-breaches/sophisticated-malvertising-campaign-targets-us-defense-industry-/d/d-id/1316753
[20] https://www.securityweek.com/angler-exploit-kit-uses-domain-shadowing-evade-detection

Mitigation strategies to prevent malware delivery and execution

Application control

Mitigation strategy

Application control to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTML Applications) and installers.

Rationale

An appropriately configured implementation of application control 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 CD/DVD/USB removable storage media.

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

Implementation guidance

The following examples are not application control:

- simply preventing a user from installing new applications to their computer's hard disk
- using a 'next-generation' firewall in an attempt to identify whether network traffic is generated by an approved application
- using 'next-generation' cyber security software, or any other vendor product, that decides whether an application should be allowed to execute based on factors other than the system administrator's pre-configured list of approved applications.

The ability of application control to provide a reasonable barrier for low to moderately sophisticated cyber security incidents depends on the solution chosen to implement application control, 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.

Ensure that application control prevents unapproved programs running regardless of their file extension.

A very basic implementation to mitigate some unsophisticated malware from running involves using application control or filesystem permissions to block execution from user profile directories. Such directories include %AppData%, %LocalAppData%, their subdirectories, as well as %TEMP%. Additionally, to prevent malicious scripts from running when clicked on by users, the notepad program can be associated with script file extensions such as .hta, .js, .jse, .vbs, .vbe, .wsf and .ps1.

Organisations that don't require the use of Windows Script Host are strongly advised to disable it[21], while other organisations should use application control to allow only approved scripts to run.

After performing testing to confirm that there is no significant business impact, deny typical low-privileged users the ability to run all script execution engines shipped with Microsoft Windows including Windows Script Host (cscript.exe

[21] https://docs.microsoft.com/en-au/previous-versions/tn-archive/ee198684(v=technet.10)

and wscript.exe which run JScript and VBScript including Windows Script Files), powershell.exe, powershell_ise.exe, cmd.exe, wmic.exe and where possible Microsoft HTML Application Host (mshta.exe).

The ACSC urges organisations to exercise caution when using publisher certificate rules to allow operating system files and other applications to execute. There is a security risk of inadvertently allowing applications that are digitally signed by the same publisher which can be used for legitimate purposes or malicious purposes such as network propagation and running malicious programs. To help mitigate this security risk, ensure that publisher certificate rules specify the 'Product Name' in addition to the 'Publisher Name'.

Where possible, prevent users (and therefore malware running on the user's behalf) from running system executables commonly used for malicious purposes as listed in mitigation strategy 'Continuous incident detection and response'. Note the exception for regsvr32.exe and rundll32.exe – these are required for legitimate functionality but can be abused to circumvent application control, which can be mitigated by configuring rules in Microsoft's Enhanced Mitigation Experience Toolkit (EMET).

It is advisable to deploy application control in phases, instead of trying to deploy it to an entire organisation at once. For example, after fully testing and understanding application control to avoid false positives, one approach is to deploy application control to the computers used by senior executives and their executive 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 control mitigated the compromise, they might provide additional support for the deployment of application control to more computers in the organisation.

Deploying application control is easier if the organisation has detailed visibility of what software is installed on computers. Such visibility can be obtained by using a Standard Operating Environment, maintaining an inventory of software installed and implementing a robust change management process. Initially testing application control in 'audit'/'logging only' mode helps organisations to develop an inventory of installed software, while taking care to avoid including existing malware in the inventory. Once an inventory has been established, application control 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 hashed, the list of hashes is likely to become too large and if distributed via Group Policy, might unacceptably slow down users logging into their computers. Additionally, note that installing new software can create subdirectories in allowed paths that provide users (and therefore malware) with write and execute permissions, enabling arbitrary unapproved or malicious programs to run. Organisations need to verify the effectiveness of application control periodically and especially after installing new software.

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/MSP filename extension and are commonly used to perform installation or modification of programs in Microsoft Windows environments.

Endpoint protection or anti-malware software from some vendors includes application control functionality. The ACSC has witnessed application control conflict with anti-malware software from a different vendor that launched itself with a random filename in an attempt to hide from malware.

Windows Defender Application Control, introduced in Microsoft Windows 10 and Microsoft Windows Server 2016, is application control that uses virtualisation to help protect itself from being disabled either by malicious administrators or by malware that runs with administrative privileges which has already circumvented application control (somewhat negating the malware's need to disable application control).

Further information

Further guidance, including applicability for operating systems other than Microsoft Windows, is available at:

- https://www.cyber.gov.au/publications/implementing-application-control

- https://www.cyber.gov.au/publications/essential-eight-in-linux-environments
- https://docs.microsoft.com/en-au/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules.

Information about Windows Defender Application Control is available at https://docs.microsoft.com/en-au/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control-deployment-guide.

Patch applications

Mitigation strategy

Patch applications especially Adobe Flash, web browsers and web browser plug-ins/add-ons/extensions, Microsoft Office, Java and PDF viewers. Also patch server applications such as databases that store important (sensitive or high-availability) data as well as web server software that is internet-accessible.

Patch or mitigate computers exposed to 'extreme risk' security vulnerabilities within 48 hours of the security vulnerability being identified. The ACSC has developed guidance to facilitate a risk management approach to applying patches based on the severity and potential business impact of the associated security vulnerabilities.

Use the latest version of applications since they typically incorporate additional security technologies such as sandboxing and other anti-exploitation capabilities. For some vendor applications, upgrading to the latest version is the only way to patch a security vulnerability. Don't use application versions that are no longer vendor-supported with patches for security vulnerabilities.

Rationale

'Extreme risk' security vulnerabilities in software used by the organisation can enable adversaries to execute malicious code, which can result in significant consequences for the organisation. The level of security risk might also be affected by whether exploit code for a security 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 user computers, based on the organisation's risk tolerance, as well as how many applications the 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 computers belonging to a subset of system administrators or similar technically skilled users, optionally testing the ability to rollback the patch to remove it. If no broken functionality has been identified within a day, the organisation then deploys the patch to a small percentage of computers 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 user computers. This approach minimises the organisation's exposure to the security 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 patches for user computers prior to deployment. Although this approach facilitates change management and minimises the likelihood that a deployed patch will break business functionality, a lengthy patch testing process has associated financial costs and leaves the organisation vulnerable until the patch is deployed or a workaround is implemented.

A different approach involving more thorough testing is usually used for deploying patches to servers, as well as for deploying upgrades that introduce significant additional features and capabilities.

Patch management

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

Prioritise patching security vulnerabilities in software used to interact with content from the internet, as well as software which runs with elevated privileges such as anti-malware software and third party video drivers.

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

Using the latest version

Don't use software which is no longer vendor-supported with patches for security vulnerabilities. This is especially important for software that interacts with untrusted and potentially malicious data.

Don't use Adobe Reader prior to version X, or unsupported Internet Explorer versions (currently version 10 and older) especially when accessing the internet.

Further information

Further guidance is available at https://www.cyber.gov.au/publications/assessing-security-vulnerabilities-and-applying-patches.

Microsoft's guidance for improving patch management practices is available at https://blogs.msdn.microsoft.com/govtech/2015/04/21/if-you-do-only-one-thing-to-reduce-your-cybersecurity-risk/.

Configure Microsoft Office macro settings

Mitigation strategy

Configure Microsoft Office macro settings to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.

Rationale

This mitigation strategy addresses adversaries using Microsoft Office macros in an attempt to run malicious code while evading basic email content filtering and application control.

Implementation guidance

When configuring the new security feature added to Microsoft Office to block macros from the internet, also configure the Microsoft Windows Attachment Manager to prevent users from removing zone information to circumvent this security feature.

For organisations with a business requirement to run Microsoft Office macros, configure Microsoft Office on a per-user and per-application basis to only run macros vetted as trustworthy and preferably placed in 'trusted location' directories which typical low-privileged users can't write to, or less preferably digitally signed by trusted publishers. Note that adversaries might attempt to purchase or steal a code signing certificate issued by a trusted certificate authority, and use it to sign a malicious macro – even if the certificate is associated with an untrusted publisher, the user might undesirably be provided with the decision and ability to run the macro.

Enforce the macro security configuration settings via Group Policy to prevent users from changing them to run a malicious or otherwise unapproved macro.

Further information

Detailed guidance on implementing this mitigation strategy is available at https://www.cyber.gov.au/publications/microsoft-office-macro-security.

Further information about the new security feature in Microsoft Office to block macros from the internet is available at https://www.microsoft.com/security/blog/2016/10/26/office-2013-can-now-block-macros-to-help-prevent-infection/.

User application hardening

Mitigation strategy

User application hardening. Configure web browsers to block Flash (ideally uninstall it if possible), advertisements and untrusted Java code on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.

Rationale

This mitigation strategy significantly helps to reduce the attack surface of user computers. It also helps to mitigate adversaries using malicious content in an attempt to evade application control by either exploiting an application's legitimate functionality, or exploiting a security 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, block Adobe Flash (ideally uninstall it), ActiveX, Java, Silverlight and QuickTime for Windows. Only allow trustworthy websites that require such web browser functionality for a specific business purpose, such as a legacy Flash application used on the organisation's intranet. Note that some web browsers have an embedded version of Flash.

Ideally uninstall Flash, since simply disabling Flash in the web browser doesn't mitigate all exploitation vectors such as via Microsoft Office or PDF viewers. Furthermore, web browser 'click-to-play' functionality provides limited mitigation since it relies on users to make correct security decisions. Some users might choose incorrectly, for example enabling a malicious Flash advertisement located on a legitimate website.

Block internet advertisements using web browser software (and web content filtering in the gateway), due to the prevalent threat of adversaries using malicious advertising (malvertising) to compromise the integrity of legitimate websites to compromise visitors to such websites. Some organisations might choose to support selected websites that rely on advertising for revenue by enabling just their ads and potentially risking compromise.

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

- uninstall Java if there is no business requirement to use it
- configure Java to disable 'Java content in the browser'[22]
- use a modern web browser which forbids running deprecated Java plugins[23]
- apply web browser specific configuration settings that disable Java in the web browser[24]

[22] https://java.com/en/download/help/disable_browser.xml
[23] https://blogs.oracle.com/java-platform-group/entry/moving_to_a_plugin_free
[24] https://msrc-blog.microsoft.com/2013/05/29/java-a-fix-it-for-when-you-cannot-let-go/

- use a separate web browser that can only run Java code located on the organisation's internal systems
- use the Deployment Rule Set[25] feature to allow only approved Java applets and Java Web Start applications
- use web content filtering to provide defence-in-depth mitigation, including providing an exception for approved websites that require the use of Java for business purposes.

Blocking JavaScript, except for approved websites, is ideal though challenging due to the large number of websites that require such functionality for legitimate purposes, and is difficult to implement in a large scale deployment.

Configure Microsoft Office to disable activation of object linking and embedding (OLE) packages[26].

Configure the Microsoft Office File Validation and Protected View features to inspect and validate Microsoft Office files for potentially malicious abnormalities.

Further information

Detailed guidance on configuring the Microsoft Office File Validation and Protected View features is available at https://www.cyber.gov.au/publications/hardening-microsoft-office-365-proplus-office-2019-and-office-2016.

Automated dynamic analysis of email and web content run in a sandbox

Mitigation strategy

Automated dynamic analysis of email and web content run in a sandbox, blocked if suspicious behaviour is identified (e.g. network traffic, new or modified files, or other system configuration changes).

Rationale

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

Implementation guidance

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

Preferably use a vendor product that:

- is able to decrypt and perform analysis of email and web content that was 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 user's computer from having access to the internet infrastructure that the malicious content communicates with, or otherwise quarantining the user's computer
- enables the sandbox to be customised to match the operating systems, applications and configuration settings of computers used throughout the organisation.

[25] https://blogs.oracle.com/java-platform-group/entry/introducing_deployment_rule_sets
[26] https://www.microsoft.com/security/blog/2016/06/14/wheres-the-macro-malware-author-are-now-using-ole-embedding-to-deliver-malicious-files/

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 adversaries using evasion techniques such as:

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

Email content filtering

Mitigation strategy

Email content filtering. Allow only approved attachment types (including in archives and nested archives[27]). Analyse/sanitise hyperlinks, PDF and Microsoft Office attachments. Quarantine Microsoft Office macros.

Rationale

Email content filtering helps to prevent the compromise of user computers via adversaries using malicious emails. Allowing only approved business-related attachment types is significantly more effective than attempting to identify and block a complete list of malicious file types and file extensions, including those increasingly leveraged by adversaries such as .lnk shortcut files, PowerShell and JScript files.

Implementation guidance

Block/quarantine content that can't be inspected such as passphrase-protected archive files (e.g. zip or RAR). Inspect archive files in a controlled manner to avoid denial of service via resource exhaustion.

Reject incoming emails that have the organisation's domain as the email sender but do not originate from email servers approved by the organisation.

One approach to sanitising approved business-related attachment types is to use 'Content Disarm and Reconstruction' software, which replaces an email attachment with a new file containing the same content but without potentially malicious code.

Preferably archive PDF and Microsoft Office attachments, and scan them again for malware 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 adversaries often use such email addresses due to the lack of attribution.

Further information

Further guidance on malicious email mitigation strategies is available at https://www.cyber.gov.au/publications/malicious-email-mitigation-strategies.

[27] https://threatpost.com/sage-and-satan-ransomware-double-trouble/123250/

Web content filtering

Mitigation strategy

Web content filtering. Allow only approved types of web content and websites with good reputation ratings. Block access to malicious domains and IP addresses, ads, anonymity networks and free domains.

Rationale

An effective web content filter reduces the security risk of malware being accessed, as well as making it more difficult for adversaries to communicate with their malware. Defining a list of approved types of web content will assist in removing one of the most common malware delivery techniques.

Implementation guidance

Preferably block all executable content by default and use a process to enable selected users to access specific executable content 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.

Ideally block Flash, ActiveX and Java, except for approved websites that require such functionality for legitimate purposes. However, the administrative resources required to analyse legitimate business requirements in larger organisations could be significant.

Implement a solution that inspects HTTPS traffic for malicious content, especially HTTPS communications with unfamiliar websites, noting that encrypted network traffic has become pervasive.

If the web content filter has the capability to inspect Microsoft Office files, quarantine such files if they contain macros, especially if they are downloaded from the internet rather than from the organisation's intranet.

Block internet advertisements using web content filtering in the gateway (and web browser software), due to the prevalent threat of adversaries using malicious advertising (malvertising) to compromise the integrity of legitimate websites to compromise visitors to such websites. Some organisations might choose to support selected websites that rely on advertising for revenue by enabling just their ads and potentially risking compromise.

Block outbound network connections to anonymity networks such as Tor, Tor2web and I2P, to help mitigate malware that uses such networks for command and control as well as for data exfiltration. Some organisations might choose to support inbound network connections from anonymity networks to the organisation's public internet-accessible websites, to cater to website visitors who wish to remain anonymous for privacy reasons.

Cyber security incidents often 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 confirming that the organisation does not access any legitimate websites using these domains.

Where possible, block attempts to access websites by their IP address instead of by their domain name, to force adversaries to obtain a domain name which can contribute to an audit trail that can assist with identifying related cyber security incidents.

The effectiveness of this mitigation strategy is reduced by adversaries using legitimate websites, which are required for business purposes, for malware delivery, command and control, and exfiltration. Such websites include web forums, social networking websites, cloud computing services, legitimate but temporarily compromised websites and a range of other web infrastructure.

Deny corporate computers direct internet connectivity

Mitigation strategy

Deny corporate computers direct internet connectivity. Use a gateway firewall to require use of a split DNS server, an email server and an authenticated web proxy server for outbound web connections.

Rationale

A gateway firewall limits external adversaries from accessing corporate computers running vulnerable network services, and serves as a logging and choke point for incoming and outgoing network traffic.

Malware of lower sophistication might fail to exfiltrate data and operate correctly if it expects direct internet connectivity and is unable to traverse the organisation's internet gateway, resulting in the internet gateway detecting and blocking such unauthorised network communication.

Implementation guidance

The firewall should be configured to only allow approved networking ports and protocols required for business functionality, and should be capable of handling IPv6 traffic.

Implement a web proxy that decrypts and inspects encrypted HTTPS traffic for malicious content, especially HTTPS communications with unfamiliar websites.

Preferably configure computers 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.

Servers should have a very restricted ability, and ideally no ability, to browse websites and access emails from the internet.

This mitigation strategy should not be interpreted that internet users visiting the organisation's public internet-accessible websites need to be authenticated by a web proxy.

Operating system generic exploit mitigation

Mitigation strategy

Operating system generic exploit mitigation e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET)[28].

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 security vulnerabilities, including for applications which EMET is specifically configured to protect, even in cases where the existence and details of security vulnerabilities are not publicly known.

[28] https://support.microsoft.com/en-au/help/2458544/the-enhanced-mitigation-experience-toolkit

Implementation guidance

Configure DEP hardware and software mechanisms to apply to all operating system programs and other software applications that support DEP.

Configure ASLR for all operating system programs and other software applications that support ASLR.

In addition to configuring system-wide EMET rules, configure EMET rules for applications that interact with potentially untrusted content, for example web browsers, Microsoft Office and PDF viewers.

Configure EMET rules to mitigate the legitimate Microsoft Windows operating system files regsvr32.exe and rundll32.exe being abused to circumvent application control.

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

Microsoft note that their Microsoft Windows 10 operating system and Edge web browser natively implement many of EMET's features and mitigations, making EMET less relevant for Microsoft Windows 10. EMET is most useful to help protect previous operating system versions, legacy applications and third party software:

- https://msrc-blog.microsoft.com/2016/02/02/enhanced-mitigation-experience-toolkit-emet-version-5-5-is-now-available/
- https://insights.sei.cmu.edu/cert/2016/11/windows-10-cannot-protect-insecure-applications-like-emet-can.html.

Server application hardening

Mitigation strategy

Server application hardening especially internet-accessible web applications (sanitise input and use TLS not SSL) and databases, as well as other server applications that access important (sensitive or high-availability) data (e.g. customer, finance, human resources and other data storage systems).

Rationale

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

Implementation guidance

OWASP guidance helps to mitigate web application security vulnerabilities such as SQL injection, and covers 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

The ACSC has developed guidance for securing content management systems running on web servers, as part of the ACSC responding to cyber security incidents involving adversaries compromising internet-accessible web servers and using 'web shells' which can facilitate remote access, administration and pivoting to the organisation's internal systems.

Further guidance on protecting web applications is available at https://www.cyber.gov.au/publications/protecting-web-applications-and-users.

Further guidance on securing content management systems is available at https://www.cyber.gov.au/publications/securing-content-management-systems.

Operating system hardening

Mitigation strategy

Operating system hardening (including for network devices) based on a Standard Operating Environment (SOE), disabling unneeded functionality (e.g. RDP, AutoRun, LanMan, SMB/NetBIOS, Link-Local Multicast Name Resolution (LLMNR) and Web Proxy Auto-Discovery (WPAD)).

Rationale

Benefits of computers and network devices having a consistent managed SOE configuration include:

- system administrators performing configuration management and knowing what software is running on computers thereby facilitating implementing application control and patching security vulnerabilities
- the ability to detect anomalous software running by monitoring for deviations from the standard baseline – implementing application control, even if configured in 'audit'/'logging only' mode, can provide this ability
- network administrators knowing what software is running on network devices thereby facilitating patching security vulnerabilities, as well as knowing what software is allowed to communicate on the network thereby facilitating baselining expected network activity
- the ability to quickly restore compromised computers and network devices to a known clean state.

Implementation guidance

Harden file and Windows Registry permissions, for example where possible, prevent users (and therefore malware running on the user's behalf) from running system executables commonly used for malicious purposes as listed in mitigation strategies 'Application control' and 'Continuous incident detection and response'.

Configure the Windows Task Scheduler service to prevent user computers 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 via DLL search order hijacking techniques[29].

Disable Server Message Block (SMB) and NetBIOS services running on computers where possible, especially to help mitigate internal reconnaissance and network propagation.

Disabling LLMNR and associated name resolution services such as NetBIOS Name Service where possible, helps to mitigate adversaries on the organisation's network from responding to name queries performed by the organisation's other computers and collecting their authentication credentials.

Organisations should create a WPAD DNS record in their internal DNS server and/or in the 'hosts' file of user computers. Organisations that don't use Proxy Auto-Configuration should disable this feature in web browsers.

Configuring file extensions to be displayed assists users to understand a file's type, otherwise an email attachment called 'file.txt.exe' could appear as 'file.txt' making the user think it is a harmless text file.

[29] https://support.microsoft.com/en-au/help/2264107/a-new-cwdillegalindllsearch-registry-entry-is-available-to-control-the

The scarcity of unused and available publicly routable IPv4 address results in an increasing need for IPv6 to be used by computers that directly connect to the internet. However, IPv6 might not be needed by computers on an organisation's internal network which use IPv4 addresses in the reserved range.

Antivirus software using heuristics and reputation ratings

Mitigation strategy

Antivirus software using heuristics and reputation ratings to check a file's prevalence and digital signature prior to execution. Use antivirus software from different vendors for gateways versus computers.

Specifically, this includes checking the prevalence of a questionable file among the vendor's user base, and ideally also checking whether a digitally signed file uses a reputable vendor certificate that hasn't been revoked and wasn't expired when the digital signature was added to the file.

Rationale

Antivirus software helps to detect 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 the organisation's incident response team due to false positives.

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

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

Control removable storage media and connected devices

Mitigation strategy

Control removable storage media and connected devices. Block unapproved CD/DVD/USB storage media. Block connectivity with unapproved smartphones, tablets and Bluetooth/Wi-Fi/3G/4G/5G devices.

Rationale

Using removable storage media and connected devices in a controlled and accountable manner reduces the security risk of malware execution and unauthorised data exposure.

USB flash storage devices infected with malware might be deliberately provided to targeted users as a gift, and have been inadvertently distributed by major vendors at several Australian cyber security conferences. Additionally, adversaries might scatter USB flash storage devices, CDs and DVDs containing malicious content in the car park of targeted users.

Implementation guidance

Follow a robust storage media transfer policy and process when using removable storage media to transfer data between computers, especially if they are located on different networks or in different security domains. Ideally, an alternative corporately approved method of data transfer should be established which avoids the need to use removable storage media.

Computers without a need to use removable storage media or connected devices can be configured to help prevent such connectivity by removing associated drivers from the operating system, using third party solutions to allow and

block access to specific classes of devices, configuring computer BIOS/UEFI settings to disable access to associated hardware, and physically removing or disabling associated hardware used for external data storage or external device connectivity.

Block spoofed emails

Mitigation strategy

Block spoofed emails. Use Sender Policy Framework (SPF) or Sender ID to check incoming emails. Use 'hard fail' SPF TXT and DMARC DNS records to mitigate emails that spoof the organisation's domain.

Rationale

SPF, or alternative implementations such as Sender ID, reduce the likelihood of spoofed emails being delivered to the targeted user.

Implementation guidance

Configure 'hard fail' SPF TXT DNS records for the organisation's domains and subdomains, and configure a wildcard SPF TXT DNS 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) enables a domain owner to specify a policy stating what action the recipient's email server should take if it receives an email that has failed an SPF check and/or a DKIM check. DMARC also contains a reporting feature which enables a domain owner to obtain some visibility of whether their domain is being spoofed in emails sent by adversaries.

Configure a DMARC DNS record for the organisation's domain, specifying that emails from the organisation's domain and subdomains should be rejected if they fail SPF checks (and/or DKIM checks if DKIM is configured for the organisation's domain). In the absence of a DMARC DNS record, the ACSC responded to a cyber security incident involving a major free webmail provider that delivered a spoofed email to the recipient's inbox even though the email failed SPF checks.

Organisations can conservatively deploy DMARC if they are concerned about legitimate emails sent from their domain being incorrectly rejected.

Reject incoming emails that have the organisation's domain as the email sender but do not originate from email servers approved by the organisation.

Further information

Further guidance on spoofed email mitigation strategies is available at https://www.cyber.gov.au/publications/how-to-combat-fake-emails.

User education

Mitigation strategy

User education. Avoid phishing emails (e.g. with links to login to fake websites), weak passphrases, passphrase reuse, as well as corporately unapproved removable storage media, connected devices and external IT services such as cloud computing including webmail.

Educate users, especially Most Likely Targets, about internet threats such as identifying spear phishing emails or unexpected duplicate emails, and reporting such emails to the organisation's IT security team. Users should also report potential cyber security incidents, including suspicious phone calls such as unidentified callers attempting to solicit details about the organisation's IT environment. Finally, users should avoid using weak passphrases, reusing passphrases, using unapproved removable storage media and connected devices, and exposing their email addresses for example via social networking.

User 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 an attempted compromise, implementing a technical mitigation strategy (such as application control 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 a compromise.

The ACSC is aware of some spear phishing emails that use clever tradecraft and are believable such that no amount of user education would have helped to prevent or detect a compromise.

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 'drive by download', 'watering hole' or 'strategic web compromise', including where malvertising runs malicious software without requiring user interaction. Visiting such a website might compromise the user's computer without any obvious indications of compromise for the user to detect.

Implementation guidance

Educate users to avoid:

- logging into fake websites by visiting hyperlinks in emails that arrived from the internet[30] [31] [32] [33]
- sharing passphrases with other users
- selecting weak passphrases
- reusing a previously used passphrase
- using the same passphrase in several different places
- storing their passphrases unencrypted in files
- using removable storage media and other IT equipment not corporately provided
- performing work using corporately unapproved external IT services such as cloud computing including webmail
- unnecessarily exposing their email address and personal details (e.g. via public social networking platforms)
- visiting websites unrelated to work.

[30] https://www.darkreading.com/threat-intelligence/fbi-dhs-report-implicates-cozy-bear-fancy-bear-in-election-related-hacks/d/d-id/1327811
[31] https://www.wordfence.com/blog/2017/01/gmail-phishing-data-uri/
[32] https://threatpost.com/experts-warn-of-novel-pdf-based-phishing-scam/122896/
[33] https://isc.sans.edu/diary/Phishing+Campaign+with+Blurred+Images/21207

Educate users as to why following cyber security policies helps them to protect and appropriately handle the sensitive data they have been entrusted to handle. Share with users the anecdotal details of previous cyber security incidents affecting the organisation and similar organisations, highlighting the impact that such incidents 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 security 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 cyber security and adversary techniques
- educate senior business representatives to understand the security risks of rushing to complete a project with inadequate security design and testing, as well as the security 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:

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

Further information

Further guidance for users on detecting socially engineered emails is available at https://www.cyber.gov.au/publications/detecting-socially-engineered-messages.

Antivirus software with up-to-date signatures

Mitigation strategy

Antivirus software with up-to-date signatures to identify malware, from a vendor that rapidly adds signatures for new malware. Use antivirus software from different vendors for gateways versus computers.

Rationale

Antivirus software helps to detect 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.

TLS encryption between email servers

Mitigation strategy

TLS encryption between email servers to help prevent legitimate emails being intercepted and subsequently leveraged for social engineering. Perform content scanning after email traffic is decrypted.

Rationale

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

Implementation guidance

Perform content scanning after email traffic is decrypted.

Mitigation strategies to limit the extent of cyber security incidents

Restrict administrative privileges

Mitigation strategy

Restrict administrative privileges to operating systems and applications based on user duties. Validate the requirement for users to be granted administrative privileges, and revalidate this requirement at least annually and preferably monthly.

Privileged users should use a separate unprivileged account, and preferably a separate physical computer, for activities that are non-administrative or risky such as reading email, web browsing and obtaining files via internet services such as instant messaging or social networking – technical controls should be implemented to block all privileged user accounts from performing such activities.

Rationale

The consequences of a compromise are reduced if users (and therefore malware running on the user's behalf) have low privileges instead of administrative privileges.

Implementation guidance

This mitigation strategy applies to:

- users who have domain or local system administrative privileges, and equivalent administrative privileges in operating systems other than Microsoft Windows
- users who have elevated operating system privileges[34] [35]
- users who have privileged access to applications such as a database
- administrative accounts that allow vendors to perform remote access.

Further information

Further guidance is available at https://www.cyber.gov.au/publications/restricting-administrative-privileges.

Patch operating systems

Mitigation strategy

Patch operating systems. Patch or mitigate computers (including network devices) exposed to 'extreme risk' security vulnerabilities within 48 hours of the security vulnerability being identified. The ACSC has developed guidance to facilitate a risk management approach to applying patches based on the severity and potential business impact of the associated security vulnerabilities.

[34] https://docs.microsoft.com/en-au/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd349804(v=ws.10)
[35] https://docs.microsoft.com/en-au/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd145442(v=ws.11)

Use the latest version of operating systems since they typically incorporate additional security technologies such as anti-exploitation capabilities. Don't use operating system versions that are no longer vendor-supported with patches for security vulnerabilities.

Rationale

'Extreme risk' security vulnerabilities in operating systems used by the organisation can enable adversaries to perform actions such as elevating their privileges, which can result in significant consequences for the organisation. The level of security risk might also be affected by whether exploit code for a security 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 'Patch applications'.

Apply firmware patches, including for network devices such as routers, switches and firewalls, and especially for those devices that are internet-accessible.

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

Further guidance is available at https://www.cyber.gov.au/publications/assessing-security-vulnerabilities-and-applying-patches.

Microsoft's guidance for improving patch management practices is available at https://blogs.msdn.microsoft.com/govtech/2015/04/21/if-you-do-only-one-thing-to-reduce-your-cybersecurity-risk/.

Multi-factor authentication

Mitigation strategy

Multi-factor authentication especially for Most Likely Targets, VPNs, RDP, SSH and other remote access capabilities, and for all users when they perform a privileged action (including system administration) or access an important (sensitive or high-availability) data 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-based certificate
- something the user is, such as their fingerprint or iris.

Rationale

If implemented correctly, multi-factor authentication can make it significantly more difficult for adversaries to use stolen user credentials to facilitate further malicious activities against the organisation, including establishing their own VPN or other remote access connection to the organisation's network.

Implementation guidance

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

- A physically separate token with a time-based value, that is not physically connected to the computer, might be the most secure option depending on its use and implementation.
- 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 computer, and also to what degree software running on the computer 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 adversaries who have obtained administrative privileges on such a computer, noting that marking such certificates as non-exportable provides some mitigation.
- 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 adversaries without requiring administrative privileges.

Servers that store user authentication data and perform user authentication are frequently targeted by adversaries, therefore additional effort needs to be invested to secure such servers.

The use of multi-factor authentication for remote access does not fully mitigate users entering their passphrase on a compromised computing device. Adversaries who have obtained a user's passphrase could gain physical access to a corporate computer and simply log in as the user. Mitigations for this include using multi-factor authentication for all user logins including corporate computers in the office, or ensuring that user passphrases for remote access are different to passphrases used for corporate computers in the office. Furthermore, adversaries could use a stolen passphrase to access the user's network drives once any other user who has access to the organisation's corporate network has been remotely compromised.

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

Multi-step authentication using a single factor is not multi-factor authentication, for example, a user accessing the organisation's remote access VPN by authenticating using just a single factor, and then accessing the organisation's internal email or other internal server application by authenticating using just a single factor, even if the first factor is different to the second factor (e.g. two different passphrases).

Further information

Further guidance on multi-factor authentication is available at https://www.cyber.gov.au/publications/implementing-multi-factor-authentication.

Disable local administrator accounts

Mitigation strategy

Disable local administrator accounts or assign passphrases that are random and unique for each computer's local administrator account to prevent adversaries from easily propagating throughout the organisation's network using compromised local administrator credentials that are shared by several computers.

Rationale

Disabling local administrator accounts or assigning random unique passphrases helps to prevent adversaries from propagating throughout the organisation's network.

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 strong passphrase. Appropriately protect records of the passphrases used for such servers.

Microsoft developed a free tool called 'Local Administrator Password Solution' (LAPS) to periodically change the passphrase of the local administrator account on every Microsoft Windows computer in the domain to a random value.

Further information

Further information about Microsoft LAPS is available at https://www.microsoft.com/en-au/download/details.aspx?id=46899.

Network segmentation

Mitigation strategy

Network segmentation. Deny traffic between computers unless required. Constrain devices with low assurance (e.g. 'Bring Your Own Device' (BYOD) and 'Internet of Things' (IoT)). Restrict user access to network drives and data repositories based on user duties.

Rationale

Network segmentation helps to prevent adversaries from propagating throughout the organisation's network. If implemented correctly, it can make it significantly more difficult for adversaries to locate and gain access to the organisation's important (sensitive or high-availability) data.

Implementation guidance

Restrict access based on the connectivity required, user job role, business function, trust boundaries and the extent to which data is important.

Develop and enforce a ruleset controlling which computers are allowed to communicate with other computers. For example, on most corporate networks, direct network communication between user computers should not be required or allowed.

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

Permissions on files and network drives (file shares) can be used to limit access to data.

Constrain VPN and other remote access, wireless connections, IoT devices, as well as user-owned laptops, smartphones and tablets which are part of a BYOD implementation.

Organisations using operating system virtualisation, (especially third party) cloud computing infrastructure, or providing users with BYOD 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 'micro-segmentation' firewalling implemented by the virtualisation platform layer, software-based firewalling implemented in individual computers and virtual machines, and 'IPsec Server and Domain Isolation'.

The use of IPsec authentication can ensure that a specific network port or ports on a sensitive server can only be accessed by specific computers such as those computers belonging to administrators.

Important 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 hosts' or 'jump boxes'. 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 computers located outside of the organisation's local network.

Organisations with critically important data might choose to store and access it using air-gapped computers that are not accessible from the internet. Security patches and other data can be transferred to and from such air gapped computers in accordance with a robust media transfer policy and processes.

Adversaries could propagate throughout the network by leveraging the organisation's existing systems used to distribute software such as patches for security vulnerabilities, login programs or scheduled tasks configured via Group Policy Objects, updated anti-malware detection engine software, or the computer Standard Operating Environment master image. Alternatively, adversaries could turn the organisation's intranet website into a watering hole to compromise users when they visit. Therefore, protect software distribution systems from modifications which are malicious or otherwise unauthorised, combined with implementing a robust change management process.

Further information

Further guidance on network segmentation is available at https://www.cyber.gov.au/publications/implementing-network-segmentation-and-segregation.

Information about BYOD and other enterprise mobility solutions is available at:

- https://www.cyber.gov.au/publications/bring-your-own-device-for-executives
- https://www.cyber.gov.au/publications/risk-management-of-enterprise-mobility-including-bring-your-own-device.

Protect authentication credentials

Mitigation strategy

Protect authentication credentials. Remove CPassword values (MS14-025). Configure WDigest (KB2871997). Use Credential Guard. Change default passphrases. Require long complex passphrases.

Rationale

It is more challenging for adversaries to obtain and crack passphrase hashes to propagate throughout the organisation's network if passphrases are unique, complex, long, hashed with a cryptographically strong algorithm and securely stored.

Implementation guidance

Ensure that Microsoft patch MS14-025 (CVE-2014-1812) has been applied. Most importantly, subsequently manually delete existing stored passphrases.

For Microsoft Windows operating systems prior to Microsoft Windows 8.1 and Microsoft Windows Server 2012 R2, ensure that Microsoft patch KB2871997 has been applied and configure the 'UseLogonCredential' Windows Registry value to 0 to help mitigate adversaries obtaining clear-text credentials stored in memory.

Configure the Credential Guard feature in Microsoft Windows 10 and Microsoft Windows Server 2016, noting Microsoft's stated limitations of this feature including it doesn't protect the Active Directory database running on Microsoft Windows Server 2016 domain controllers, and it doesn't prevent adversaries with malware running on a computer from using the privileges associated with any credential[36].

Enforce a strong passphrase policy covering complexity, length and expiry. This is especially important for service accounts and all other accounts with administrative privileges. Avoid passphrase reuse, use of a single dictionary word and unencrypted storage of passphrases.

[36] https://docs.microsoft.com/en-au/windows/security/identity-protection/credential-guard/credential-guard

Use an appropriately configured and secured passphrase manager program, sometimes referred to as a passphrase vault, to assist with storing and managing many complex passphrases. This helps to avoid users storing passphrases unencrypted in files, which assists adversaries to propagate throughout the organisation's network.

Avoid exposing passphrases via insecure communication, for example unencrypted remote administration or other unencrypted remote access.

Disable Link-Local Multicast Name Resolution (LLMNR) and associated name resolution services such as NetBIOS Name Service where possible as part of mitigation strategy 'Operating system hardening'. This helps to mitigate adversaries on the organisation's network from responding to name queries performed by the organisation's other computers and collecting their authentication credentials.

Further information

Further information about Microsoft patch MS14-025 is available at https://support.microsoft.com/en-au/help/2962486/ms14-025-vulnerability-in-group-policy-preferences-could-allow-elevati.

Further information about Microsoft patch KB2871997 is available at:

- https://msrc-blog.microsoft.com/2014/06/05/an-overview-of-kb2871997/
- https://support.microsoft.com/en-au/help/2871997/microsoft-security-advisory-update-to-improve-credentials-protection-a.

Information about Credential Guard is available at https://docs.microsoft.com/en-au/windows/security/identity-protection/credential-guard/credential-guard.

Information about configuring additional protection for the Local Security Authority (LSA) process to prevent code injection that could compromise credentials is available at https://docs.microsoft.com/en-au/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn408187(v=ws.11).

Non-persistent virtualised sandboxed environment

Mitigation strategy

Non-persistent virtualised sandboxed environment, denying access to important (sensitive or high-availability) data, for risky activities (e.g. web browsing, and viewing untrusted Microsoft Office and PDF files).

Rationale

Adversaries whose compromise is contained within a non-persistent virtualised sandboxed environment will have a reduced ability to persist and to propagate throughout the organisation's network.

Implementation guidance

There are several different approaches to implementing this mitigation strategy, with varying levels of security effectiveness, potential user resistance and cost.

One partial approach is to use applications that have been architected to run in an inbuilt sandbox, often leveraging operating system functionality to assist with the sandbox implementation. Applications such as web browsers[37] [38] and PDF viewers[39] from some vendors include such an inbuilt sandbox. This approach has lower potential user resistance and cost, although security vulnerabilities allowing sandbox escapes are periodically publicly disclosed.

[37] https://docs.microsoft.com/en-au/microsoft-edge/deploy/group-policies/security-privacy-management-gp
[38] https://chromium.googlesource.com/chromium/src/+/master/docs/design/sandbox.md
[39] https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/protectedmode.html

An alternative approach, which can be used in combination with the previous approach for increased security effectiveness, is to run applications in a non-persistent virtualised environment. This approach has higher potential user resistance and cost, though some vendor solutions reduce the cost by running the virtualised environment on the user's computer or in public cloud computing infrastructure to avoid the organisation having to build dedicated virtualised environments in their own data centre. The requirement for adversaries to exploit an additional security vulnerability to escape from the virtualised environment can increase the security effectiveness of this alternative approach, although hypervisor security vulnerabilities are occasionally publicly disclosed.

When implementing this alternative approach, the mitigation strategy 'Network segmentation' should also be implemented to mitigate the security risk of a compromised virtualised environment accessing the organisation's important data. Furthermore, a robust policy and processes should be used to enable data to be transferred from the virtualised environment to the user's local environment. Finally, although the non-persistent nature of this mitigation strategy helps to automatically restore a compromised system to a known good state, this will remove some forensic evidence related to the compromise, highlighting the importance of performing centralised logging.

Further information

Implementation options are included in the ACSC's guidance on network segmentation available at https://www.cyber.gov.au/publications/implementing-network-segmentation-and-segregation.

Software-based application firewall, blocking incoming network traffic

Mitigation strategy

Software-based application firewall, blocking incoming network traffic that is malicious or unauthorised, and denying network traffic by default (e.g. unneeded/unauthorised RDP and SMB/NetBIOS traffic).

Rationale

Blocking unneeded/unauthorised network traffic reduces the attack surface of computers by limiting exposure to network services, as well as reducing the ability of adversaries to propagate throughout the organisation's network.

Implementation guidance

Configure the firewall to restrict access to network services running on computers, especially to help mitigate internal reconnaissance and network propagation.

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

Software-based application firewall, blocking outgoing network traffic

Mitigation strategy

Software-based application firewall, blocking outgoing network traffic that is not generated by approved/trusted programs, and denying network traffic by default.

Rationale

Blocking outgoing network traffic that is not generated by approved/trusted programs helps to prevent adversaries from propagating throughout the organisation's network, and from exfiltrating the organisation's data.

Implementation guidance

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

Outbound web and email data loss prevention

Mitigation strategy

Outbound web and email data loss prevention. Block unapproved cloud computing services including personal webmail. Log and report recipient, size and frequency of outbound emails. Block and log outgoing emails with sensitive keywords or data patterns deemed to be too sensitive for the recipient's email address.

Rationale

This mitigation strategy helps to identify and block the exfiltration of sensitive organisational data.

Implementation guidance

Note that adversaries might use encryption in an attempt to evade this mitigation strategy.

The effectiveness of this mitigation strategy is further reduced if the sensitive data is unstructured and therefore difficult to identify using keywords or data patterns such as regular expressions.

Mitigation strategies to detect cyber security incidents and respond

Continuous incident detection and response

Mitigation strategy

Continuous incident detection and response with automated immediate analysis of centralised time-synchronised logs of allowed and denied computer events, authentication, file access and network activity.

Rationale

Performing continuous incident detection and response increases the organisation's ability to rapidly detect and respond to cyber security incidents in a timely manner to minimise business impact.

General implementation guidance

Use a Security Information and Event Management (SIEM) solution to perform real-time automated aggregation and correlation of 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.

Modern SIEM solutions typically contain features to assist with interpreting, analysing and providing context to log data, prioritising alerts, incorporating incident response workflow and automating the process wherever possible, while using data storage structures that improve scalability and enable flexible data searches and queries that rapidly return their results.

When choosing a SIEM solution, determine what exactly the vendor means if they advertise their product as leveraging threat intelligence, big data analytics, heuristics, machine learning, artificial intelligence, maths/statistics, or baselining normal user and system behaviour.

Store logs for at least 18 months, or longer if required by regulatory compliance.

Regularly test the organisation's incident response plan, processes and technical capabilities.

To help make the most of limited staff resources, leverage automation and context to focus on high priority security events and avoid false positives.

Implementation guidance leveraging computer-related logs

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.

Perform timely log analysis focusing on:

- Most Likely Targets, especially users who have administrative privileges to operating systems or applications such as databases
- application control 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 security product logs usually generated by computers of users who are in the office and are believed to be using their computers, potentially indicating that 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 Windows Registry keys used to automatically run programs on bootup or user login
- new or changed files that are executable
- access to critical asset computers that store or process important (sensitive or high-availability) data
- access to files on network drives
- unauthorised attempts to access or modify event logs
- use of tools shipped with Microsoft Windows to perform code execution, reconnaissance and network propagation (e.g. cscript.exe, wscript.exe, cmd.exe, mshta.exe, ipconfig.exe, net.exe, net1.exe, netstat.exe, reg.exe, wmic.exe, powershell.exe, powershell_ise.exe, at.exe, schtasks.exe, tasklist.exe, regsvr32.exe, rundll32.exe, gpresult.exe and systeminfo.exe)[40] [41] [42]
- user authentication and use of account credentials.

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

- 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 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 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.

Implementation guidance leveraging network-related logs

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.

Important logs include DNS, web proxy logs containing connection details including User-Agent values, DHCP leases, firewall logs detailing network traffic entering and leaving the organisation's network as well as logs of (especially outbound) blocked network traffic, and metadata such as Network Flow data.

Perform timely 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 both network drives (file

[40] https://lolbas-project.github.io/
[41] https://thisissecurity.stormshield.com/2014/08/20/poweliks-command-line-confusion/
[42] https://www.microsoft.com/security/blog/2019/09/26/bring-your-own-lolbin-multi-stage-fileless-nodersok-campaign-delivers-rare-node-js-based-malware/

shares) and user data including honeytoken accounts. Also focus on abnormal external network traffic crossing perimeter boundaries such as:

- periodic beaconing traffic
- HTTP/HTTPS sessions with an unusual ratio of outgoing traffic to incoming traffic
- HTTP/HTTPS traffic with a 'User-Agent' header value that is not associated with legitimate software used by the organisation
- 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 adversaries
- DNS lookups for domain names that resolve to a localhost IP address such as 127.0.0.1, indicating malware that adversaries are not ready to communicate with
- large amounts of traffic
- traffic outside of business hours
- long lived connections.

Implementation guidance applicable to ransomware

Analyse and action real-time log alerts generated by file activity monitoring tools to identify suspicious rapid and numerous file changes reflecting unapproved data deletion or modification such as encryption.

Implementation guidance applicable to malicious insiders

Analyse and action real-time log alerts generated by file activity monitoring tools to identify suspicious rapid and numerous file copying or changes.

Logs should be analysed by staff who have no other privileges or job roles in order to help mitigate a malicious insider with administrative privileges ignoring or deleting logs of their own malicious actions.

Perform timely log analysis focusing on:

- use of removable storage media and connected devices especially USB storage devices
- computer usage outside of business hours
- data access and printing which is excessive compared to the normal baseline for a user and their peer colleagues
- data transfers to unapproved cloud computing services including personal webmail, as well as the use of unapproved VPNs from the organisation's network.

Implementation guidance applicable to incident response

Developing and implementing an incident response capability requires support from technical staff and business representatives, including data owners, corporate communications, public relations and legal staff. Organisations need to regularly test and update their incident response plan, processes and technical capabilities, focusing on decreasing the duration of time taken to detect cyber security incidents and respond to them.

When a targeted 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 computers, as well as blocking network access to internet infrastructure known to be controlled by adversaries, while the same adversaries simply compromise additional computers using different malware and different internet infrastructure to avoid detection.

For targeted cyber intrusions of higher sophistication, the ACSC can assist Australian government organisations with responding. This includes developing a strategic plan to contain and eradicate the intrusion, and providing guidance to

improve the organisation's cyber security posture in preparation for adversaries attempting to regain access to the organisation's computers.

Host-based intrusion detection/prevention system

Mitigation strategy

Host-based intrusion detection/prevention system (HIDS/HIPS) to identify anomalous behaviour during program execution (e.g. process injection, keystroke logging, driver loading and persistence). Such persistence involves malware attempting to persist after the computer is rebooted, for example by modifying or adding Windows 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 the cyber security community.

Implementation guidance

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

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

Endpoint detection and response software

Mitigation strategy

Endpoint detection and response (EDR) software on all computers to centrally log system behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry level option[43].

Rationale

EDR software typically generates an ongoing stream of system behaviour logs and other telemetry metadata. This facilitates timely incident detection based on known indicators of compromise and more importantly discovery of cyber security incidents without previously known indicators of compromise. Typical functionality enables organisations to perform investigation and response activities such as rapidly analysing multiple computers seamlessly, blocking specific network communication attempts and isolating a compromised computer from the network.

Implementation guidance

Configure the EDR software to achieve a balance between identifying malware, while avoiding negatively impacting users and the organisation's incident response team due to false positives.

The ACSC has witnessed the benefit of EDR software deployed to user computers, especially before a targeted cyber intrusion occurs, that logs which programs ran (including individual processes and DLL files), what changes were made to the Windows Registry and the file system, and what network connections were attempted and established.

Exercise due diligence before purchasing EDR software, especially due to the rapid innovation being performed by startup companies, and assess:

[43] https://docs.microsoft.com/en-au/sysinternals/downloads/sysmon

- whether the product generates logs and other telemetry metadata in a format that can easily be integrated into the organisation's existing tools for performing log aggregation and analysis
- whether the product supports searching for the presence of indicators of compromise specified by the organisation
- whether the product and the vendor will exist in 18 months
- how mature the product's functionality is, and whether the vendor's customer support team is responsive to adding key features that are currently missing
- how scalable the product is, and whether it avoids overwhelming the organisation's systems and network capacity
- whether the product generates enough useful data to enable cyber security incidents to be identified, without causing too many false positives which overwhelm the organisation's incident response team.

Some vendor EDR software products have additional functionality to assist with preventing cyber security incidents, covering other mitigation strategies such as application control, host-based intrusion detection/prevention system and application sandboxing/containerisation[44].

Hunt to discover incidents

Mitigation strategy

Hunt to discover cyber security incidents based on knowledge of adversary tradecraft. Leverage threat intelligence consisting of analysed threat data with context enabling mitigating action, not just indicators of compromise.

Rationale

Hunting is a very proactive and deliberate activity to discover cyber security incidents leveraging threat intelligence that provides an understanding of the adversary's goals, strategy, tactics, techniques, procedures and to a lesser extent tools. The focus is not on detecting cyber security incidents based on a list of known malicious domains, IP addresses, file hashes and other indicators of compromise which are similar to reactive signatures.

General implementation guidance

This mitigation strategy has a comparatively very high cost of skilled staff resources.

Threat intelligence assists with the hunting process, though organisations should critically assess whether an external threat intelligence feed is of value, based on whether:

- the organisation has already implemented mitigation strategies that have higher security effectiveness including 'Continuous incident detection and response', and leverages logs and threat intelligence already available to the organisation
- the organisation has the staff resources and the IT infrastructure capability to consume and action the threat intelligence

[44] https://www.darkreading.com/endpoint/microsoft-develops-next-generation-endpoint-security-offering/d/d-id/1324473

- the threat intelligence consists of more than simply domains, IP addresses, file hashes and other indicators of compromise which are similar to reactive signatures and have little relevance if changed regularly or per victim[45] [46] [47]
- the threat intelligence has context and ideally is tailored to the organisation (or at least to their business sector/industry) to provide a high signal-to-noise ratio with negligible false positives
- the threat intelligence is actionable by assisting the organisation to take informed action such as selecting and implementing mitigation strategies to prevent and identify cyber security incidents based on an awareness of the adversary's goals, strategy, tactics, techniques, procedures and to a lesser extent tools.

As an example of actual threat intelligence consisting of more than just indicators of compromise, the ACSC provided an Australian organisation with threat intelligence about a specific adversary who was likely to send spear phishing emails to the organisation's employees during a specified one-month date range to obtain data about a specific topic. This enabled the organisation to take action by identifying which employees had access to such data, double checking that their user computers had already implemented key mitigation strategies, verifying that email content filtering would block such emails, and increasing logging and focusing on analysing logs associated with these employees.

Implementation guidance applicable to malicious insiders

Focus on users who are underperforming, about to be terminated or who intend to resign.

Search for hacking tools as well as assembled data repositories which await exfiltration.

Further information

An overview of hunting to discover cyber security incidents is available at:

- https://www.sans.org/reading-room/whitepapers/analyst/membership/36785
- https://www.sans.org/reading-room/whitepapers/analyst/membership/36882.

Network-based intrusion detection/prevention system

Mitigation strategy

Network-based intrusion detection/prevention system (NIDS/NIPS) using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.

Rationale

A NIDS/NIPS correctly configured with up-to-date signatures and supported by appropriate processes can provide some assistance with identifying cyber security incidents.

Implementation guidance

Inspect traffic crossing network perimeter boundaries for keywords such as classification markings that indicate sensitive data, noting that adversaries usually compress and/or encrypt exfiltrated data in an attempt to defeat such inspection. Additionally, adversaries use legitimate websites, which are required for business purposes, for malware

[45] https://www.darkreading.com/partner-perspectives/intel/botnet-to-cybersecurity-catch-me-if-you-can/a/d-id/1319919
[46] http://www.darkreading.com/attacks-breaches/sophisticated-malvertising-campaign-targets-us-defense-industry-/d/d-id/1316753
[47] http://www.securityweek.com/angler-exploit-kit-uses-domain-shadowing-evade-detection

delivery, command and control, and data exfiltration. Such websites include web forums, social networking websites, cloud computing services, as well as legitimate but temporarily compromised websites.

The pervasiveness of encrypted network traffic can limit the effectiveness of this mitigation strategy, requiring potentially complicated approaches to decrypt and inspect network traffic.

Capture network traffic

Mitigation strategy

Capture network traffic to and from corporate computers storing important data or considered as critical assets, and network traffic traversing the network perimeter, to perform incident detection and analysis.

Rationale

Capturing network traffic can assist the organisation to determine the techniques used by adversaries, perform a damage assessment and assist with remediating the compromise.

Implementation guidance

Focus on capturing traffic from computers on internal networks that store or access sensitive data.

Preferably also capture traffic from the network perimeter, noting that its usefulness is diminished if exfiltrated data is encrypted and sent to a computer that probably can't be attributed to adversaries.

To minimise the cost of storing complete network traffic captures, such data might need to be overwritten after a relatively short amount of time, with the security risk that by the time an incident is identified the associated captured network traffic has been deleted. Metadata relating to network connections, including network packet headers, can complement logging, and consumes less storage space than network packets.

When a significant cyber security incident occurs, retain a copy of network traffic for several days prior to remediation, as well as for several days following remediation during which time adversaries are likely to attempt to regain access to the organisation's network.

For privacy reasons, ensure that users are aware that the organisation's network traffic is monitored.

Mitigation strategies to recover data and system availability

Daily backups

Mitigation strategy

Daily backups of important new/changed data, software and configuration settings, stored disconnected and retained for at least three months. Test the restoration process when the backup capability is initially implemented, annually and whenever IT infrastructure changes.

Rationale

A recent backup of data and proven data restoration process are vital to mitigate data being encrypted, corrupted or deleted by ransomware or other destructive malware, malicious insiders, accidental mistakes by users, or non-malicious failure of storage hardware due to a range of causes including faulty equipment, wear, power outage, fire or flood.

Implementation guidance

Encourage users to avoid storing data on local storage media such as their computer's hard disk or USB storage media which is unlikely to be backed up, and instead use corporate file servers and corporately approved cloud storage services which are backed up.

Store backups offline or otherwise disconnected from computers and the network since ransomware, destructive malware and malicious insiders can encrypt, corrupt or delete backups that are easily accessible.

Some organisations might have an operational requirement to perform hourly or continuous backups[48]. If backups need to be stored online or otherwise connected to computers and the network, for example due to the use of continuous backup with cloud storage services, require the use of multi-factor authentication with human intervention to modify or delete backups.

Test the data restoration process to verify that the backups are comprehensive and that data can be restored successfully.

Customised scripts could be used to generate an alert following a daily backup if an unusually high number of files have been deleted, created or modified, especially if such created or modified files have a high degree of entropy (randomness) indicative of encryption[49].

Retain backups for at least three months and long enough to ensure that by the time a cyber security incident is identified, backups are available which contain undamaged copies of files. Implement a backup strategy that minimises or preferably eliminates dependencies so that a version of files can be restored even if other versions have been encrypted, corrupted or deleted. Finally, ensure that the organisation's incident response process identifies and restores all files that have been maliciously modified or deleted.

For example, in 2016 an Australian government organisation identified ransomware on a user computer and responded by simply reimaging the computer's hard drive. Three months later, the organisation's IT staff realised that thousands of files needed for legal proceedings and stored on a network drive (file share) had also been encrypted by the

[48] https://www.theregister.co.uk/2016/11/04/papworth_ransomware_dodge/
[49] https://isc.sans.edu/forums/diary/Using+File+Entropy+to+Identify+Ransomwared+Files/21351/

ransomware. Due to the amount of time that had elapsed, the organisation's backups contained encrypted copies of the files.

Business continuity and disaster recovery plans

Mitigation strategy

Business continuity and disaster recovery plans which are tested, documented and printed in hardcopy with a softcopy stored offline. Focus on the highest priority systems and data to recover.

Rationale

Robust business continuity and disaster recovery plans assist with enabling organisations to remain in business and continue providing critical services and products to customers and other stakeholders.

Implementation guidance

Document the criteria and thresholds at which operations are to be transitioned to the disaster recovery site, while avoiding internal and external staff involved in the incident response activity becoming exhausted and ineffective.

System recovery capabilities

Mitigation strategy

System recovery capabilities e.g. virtualisation with snapshot backups, remotely installing operating systems and applications on computers, approved enterprise mobility, and onsite vendor support contracts.

Rationale

System recovery capabilities assist with mitigating destructive malware, malicious insiders who are motivated to destroy systems, and non-malicious failures of critically important IT equipment.

Implementation guidance

Examples of system recovery capabilities implemented prior to a cyber security incident occurring include:

- virtualisation with snapshot backups to simplify recovering systems and limit the ability of malware to damage firmware – using outsourced cloud services provides spare hardware capacity, transfers the responsibility to fix damaged hardware to the cloud service provider, and enables users and incident responders to communicate via cloud-based email if the organisation's internal email servers are unavailable
- capabilities to rapidly install operating systems and applications on computers over the network to avoid having to physically visit computers to rebuild them, ensuring that the master copies of software are protected from deletion or malicious modifications
- enterprise mobility including virtual desktops, enabling users to access corporate data and applications via approved tablets, smartphones and laptops especially when other computers in the office are damaged and unusable
- contractual timely onsite vendor support to repair and replace damaged computers and network devices such as switches, routers and IP-based telephones.

Mitigation strategy specific to preventing malicious insiders

Personnel management

Mitigation strategy

Personnel management e.g. ongoing vetting especially for users with privileged access, immediately disable all accounts (especially remote access accounts) of departing users, and remind users of their security obligations and penalties.

Rationale

Personnel management assists to avoid employees having malicious intent, developing malicious intent, or carrying out their malicious intentions undiscovered until after damage has been done.

Some malicious insiders are motivated by money, coercion, ideology, ego or excitement, and might steal a copy of customer details or intellectual property. Other malicious insiders are motivated by revenge or disgruntlement due to reasons such as a negative job performance review, a denied promotion or involuntary termination of employment, and might cause damage such as destroying data and preventing computers/networks from functioning.

Implementation guidance

Perform pre-employment screening and ongoing vetting, consisting of verification of previous employment and education for all employees, as well as a criminal history background check at least for employees who have privileged access.

Immediately disable all accounts and require sanitisation or return of mobile computing devices for departing employees and remind them of their security obligations and penalties for violations. Require departing employees to also return items that could facilitate access to organisational computers and data, including their identification pass and keys used to access the organisation's buildings and IT facilities.

Educate employees to never share or otherwise expose their passphrase to other employees, including via 'shoulder surfing'. Educate employees to lock their computer screen whenever they are away from their computer.

Organisational executives and management can reduce some motivations for employees to become malicious insiders by facilitating a culture of appreciated and engaged employees who have fair remuneration and merit-based career advancement opportunities.

For the relatively small number of organisations where employees have access to highly classified data or other extremely sensitive data, a psychological assessment should be performed by qualified personnel to explore topics including allegiances and beliefs as well as character weaknesses which could be leveraged and manipulated by adversaries. Employees should be encouraged to advise the personnel security team of unusual behaviour exhibited by other employees as well as their own significant life changes such as financial, relationship and health problems.

Further information

Australian Government policy on personnel security is available at:
https://www.protectivesecurity.gov.au/personnel/Pages/default.aspx.

Further reading

This document and additional information about implementing the mitigation strategies is available at https://www.cyber.gov.au/.

The Center for Internet Security (CIS) publishes alternative guidance titled the ***CIS Critical Security Controls for Effective Cyber Defense*** which is available at: https://www.cisecurity.org/controls/.

Contact details

Organisations or individuals with questions regarding this advice can email asd.assist@defence.gov.au or call 1300 CYBER1 (1300 292 371).