The Essential 8 Strategies to Mitigate Cybersecurity Incidents

Red Piranha

When deciding on how to implement Security for your business, it is critical to adopt a risk management framework, and there are many which often vary by industry. The Australian Signals Directorate's Australian Cyber Security Centre has published the Essential Eight, outlining recommendations for Cyber Security Risk Mitigation.

What is the Essential 8?

The Essential 8 (E8) is a prioritised subset of 'Strategies to Mitigate Cyber Security Incidents', outlining the eight most essential mitigation strategies. This baseline has been created to allow organisations, particularly small to medium businesses to focus on improving security controls to reduce the risk of a cybersecurity incident occurring.

Why does it exist?

Cybersecurity controls can be overwhelming, and for small, medium and large businesses without CISOs, dedicated cybersecurity professionals or existing information security management system frameworks. Choosing where to focus efforts on risk reduction and mitigation strategies is a difficult task. A simple set of controls that can be implemented, enforced through policy and procedures that cover the most likely vectors of compromise, pivoting and escalation and recovery from cybersecurity incidents is a valuable tool for organisations at risk. As Benjamin Franklin famously said, "an ounce of prevention is worth a pound of cure".

The cost to implement such controls is significantly lower on average than the cost to recover from a cybersecurity incident.

In fact, "A 2019 ACSC Small Business Cyber Security Survey showed 62 per cent of small businesses reported they had previously been a victim of a cybersecurity incident."

And according to "Stay Smart Online" the average cost of a cybercrime attack to a small business in Australia is $276,323.00

How do I measure my businesses implementation?

Alongside the Essential 8, the ACSC released 'The Essential Eight Maturity Model', a document outlining the maturity model for the Essential 8, with three levels of implementation that businesses can use to determine and improve upon their cybersecurity posture.

Of the more than 2 million businesses in Australia, less than 100 have appointed a CISO. Reasons cited are the cost and availability of CISO, the price and availability of experts the CISO would then hire to integrate multiple disparate vendor technologies, and the lack of awareness that Security spans the whole organisation, not being solely an IT function. Globally, the primary accreditation from the International Standards Organisation is ISO 27000. This is becoming a mandatory accreditation for companies to be part of a supply chain. In Singapore, as an example, to sell to Government, you must have ISO 27000 accreditation. In the Australian context, Red Piranha is one of only a few hundred companies who have this accreditation, can help companies to achieve it, and can provide auditing services for customers who increasingly appreciate the benefits and requirements of ISO 27000 compliance.

Red Piranha offers both vCISO services and eCISO services. vCISO is a Virtual CISO which provides under contract the services from its resources, that would otherwise be performed by an in house CISO. eCISO takes advantage of the high degree of automation, eliminating the need to integrate multiple vendor systems, which are often not compatible with each other and is backed by Red Piranha's team of experts, to provide Governance, Compliance and Reporting functions to a customer, blended with some on-site services such as reporting at Board meetings. This is an efficient and effective way for companies to access a CISO like capability without having an in house CISO. These services can manage and audit a range of strategies, including the implementation of frameworks such as ISO 2700 and the Essential Eight.

This article will outline each of the Essential 8 strategies, why they exist and how they relate to cybersecurity incidents as well as mitigation strategies.

The Essential 8

Application Whitelisting/Application Control

The first control, and therefore the control considered the most important of the eight defined mitigation strategies, is the prevention of execution of unapproved/malicious applications.

The execution of unapproved code including PowerShell, MSHTA, DLLs and installers is associated with a vast number of threat actors as a method of execution after initial access through methods such as phishing or exploitation of public-facing applications.

This step is important for attackers to install payloads on target networks which may be otherwise not vulnerable through the exploitation of public-facing applications, to establish persistence through command and control systems, escalate privileges and even encrypt filesystems for ransom.

Relevant ISM controls:

- Security Control: 0843; Revision: 8; Updated: Apr-20; Applicability: O, P, S, TS

Application control is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set.

- Security Control: 1490; Revision: 2; Updated: Apr-20; Applicability: O, P, S, TS

Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set.

- Security Control: 1544; Revision: 1; Updated: Apr-20; Applicability: O, P, S, TS

Microsoft's latest recommended block rules are implemented to prevent application control bypasses.

Mitre ATT&CK for Enterprise:

- Execution – Mshta, PowerShell, Rundll32, Scripting, User Execution, InstallUtil

Mitigations:

Scripts (Powershell, VBscript, MSHTA, etc)

- Code Signing - Set PowerShell execution policy to execute only signed scripts
- Disable or Remove Feature or Program - It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment since it could be in use for many legiti mate purposes and administrative functions
- Disable/restrict the WinRM Service - helps prevent uses of PowerShell for remote execution
- Privileged Account Management - When PowerShell is necessary, restrict PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration
- End-point Anti-malware solution – May be able to detect malicious code and prevent execution.

Executables (EXE, DLL, MSI etc)

- Disable or Remove Feature or Program – InstallUtil may not be necessary within a given environment
- Execution Prevention – Use application whitelisting to block execution of InstallUtil.exe
- End-point Anti-malware solution – May be able to detect malicious code and prevent execution.

Crystal Eye

- Enable web proxy and gateway anti-malware scanning
- Enable logging of executable downloading through IDS/IPS application
- Setup and configure Application Whitelisting Application to restrict the ability for unapproved applications to communicate with other hosts on the internet.

Training

- Cybersecurity awareness training – improve the ability for staff to identify and react accordingly to potentially malicious files.

Application Patching

Another common method of initial compromise, more commonly seen in targeted attacks but also seen with increasing frequency in automated attacks is the exploitation of public-facing applications. An attacker uses software, data or commands to take advantage of weaknesses of an application that is accessible to the external internet. There is an industry-standard dictionary for publicly disclosed vulnerabilities and exposures known as Common Vulnerabilities and Exposure (CVE) which is sponsored by the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA).

Most software vendors provide updates and patches to applications with publicly identified vulnerabilities, with best practice being that a patch or update is made available before the vulnerability is disclosed to the public. There are situations, however where software developers do not adequately respond to vulnerabilities or software is no longer supported (for example Windows 7), and a publicly disclosed vulnerability never receives a patch.

Relevant ISM Controls:

- Security Control: 1144; Revision: 9; Updated: Sep-18; Applicability: O, P, S, TS

Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.

- Security Control: 1497; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS

An automated mechanism is used to confirm and record that deployed application and driver patches or updates have been installed, applied successfully and remain in place.

- Security Control: 0304; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS

Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.

Mitre ATT&CK for Enterprise:

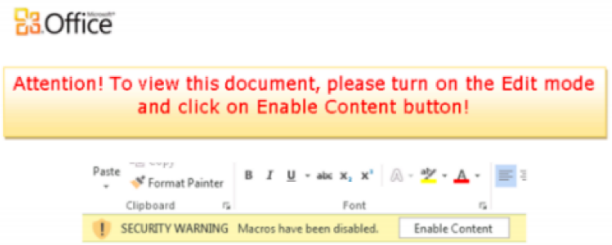
- Initial Access – Exploit Public-Facing Application

Mitigations:

- Remove any unnecessary applications
- Remove any unsupported or abandoned applications
- Maintain, monitor and apply application updates regularly with a recommendation of 48 hours to fix an 'extreme risk' vulnerability.

Configure Office Macros

A common method of executing malicious code on a victim machine is to attach a word document with malicious code that executes through macros, often with filenames such as invoice and recently COVID-19. A frequently used technique by attackers to encourage users to execute the code is to place what appears to be a genuine Microsoft message instructing the user to enable Add-ins, content and/or editing.



Relevant ISM Controls:

- Security Control: 1487; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS

Microsoft Office macros are only allowed to execute in documents from Trusted Locations where write access is limited to personnel whose role is to vet and approve macros.

- Security Control: 1488; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS

Microsoft Office macros in documents originating from the internet are blocked.

- Security Control: 1489; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS

Microsoft Office macro security settings cannot be changed by users.

Mitre ATT&CK for Enterprise:

- Persistence – Office Application Startup: Office Template Macros

Mitigations:

- Follow Office macro security best practices suitable for your environment. Disable Office VBA macros from executing through group policy.
- Disable Office add-ins. If they are required, follow best practices for securing them by requiring them to be signed and disabling user notification for allowing add-ins.

Application Hardening

The ACSC recommends hardening end-point systems by locking down, uninstalling and disabling unnecessary features and applications. The effect of this is that the attack surface and management required for updates are reduced. Examples given by the ACSC include flash content, web advertisements, java running in web browsers and OLE packages. This can be extended to include the disabling of Mshta, network scans, RDP, screensavers, scripts and powershell, autorun, developer utilities and Windows Remote Management.

Why: The listed applications to be restricted are common vectors of initial compromise, used to deliver and execute malicious code on a system, along with this the management required for updates is reduced, saving time and money.

Relevant ISM Controls:

- Security Control: 1484; Revision: 1; Updated: Jan-19; Applicability: O, P, S, TS

Web browsers are configured to block or disable support for Flash content.

- Security Control: 1485; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS

Web browsers are configured to block web advertisements.

- Security Control: 1486; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS

Web browsers are configured to block java from the internet.

- Security Control: 1541; Revision: 0; Updated: Jan-19; Applicability: O, P, S, TS

Microsoft Office is configured to disable support for Flash content.

- Security Control: 1542; Revision: 0; Updated: Jan-19; Applicability: O, P, S, TS

Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.

Mitre ATT&CK for Enterprise:

- Mitigations – Disable or Remove Feature or Program

Mitigations:

- Establish a standard operating environment (SOE)
- Configure Windows end-point systems through group policy to disable Adobe Flash, Java, and harden Microsoft Office, web browsers and PDF viewers.

Restrict Administrator Privileges

The ACSC recommends restricting administrator privileges to Operating Systems and applications based upon user duties, with regular audits to revalidate the requirement of these privileges. Along with this, privileged accounts (such as SYSTEM, Administrator or root) should not be used for any activities outside their intended purpose, such as web browsing or reading emails.

Why: Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems. Enforcing proper management of privileged accounts mitigates several common adversary techniques such as account manipulation, credential dumping, exploitation of remote services, pass the hash, process injection and service execution.

Relevant ISM Controls:

- Security Control: 1507; Revision: 1; Updated: Sep-19; Applicability: O, P, S, TS

Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis.

- Security Control: 1508; Revision: 1; Updated: Sep-19; Applicability: O, P, S, TS

Privileged access to systems, applications and data repositories is limited to that required for personnel to undertake their duties.

- Security Control: 1175; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS

Technical security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.

Mitre ATT&CK for Enterprise:

- Mitigations – Privileged Account Management

Mitigations:

- Determine and document all privileged accounts existing within systems.
- Determine the access requirements for staff and provide minimal access.
- Disable local administrator accounts on Windows end-points.
- Ensure password hashes and secrets are not stored in locations accessible by lower privileged accounts.
- Enforce a strong password policy.
- Regularly audit administrative accounts.
- Ensure staff are educated on the proper use of privileged accounts.

Patch Operating Systems

Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.

Why: Security vulnerabilities in operating systems can be used to further the compromise of systems.

Relevant ISM Controls:

- Security Control: 1494; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS

Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.

- Security Control: 1500; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS

An automated mechanism is used to confirm and record that deployed operating system and firmware patches or updates have been installed, applied successfully and remain in place.

- Security Control: 1501; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS

Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.

Mitre ATT&CK for Enterprise:

- Persistence – Office Application Startup: Office Template Macros

Mitigations:

- Ensure an operating system patching process is in place.
- Audit updates regularly.
- Perform vulnerability scans to determine the presence of any outdated systems that identify their version number.
- Utilise an operating system update management system such as WSUS (Windows Server Update Services), or Windows Update for Business through an MDM solution such as Microsoft Intune.
- Utilise end-point agents such as osquery to query for and communicate software versions to a management system.

Multi-Factor Authentication

Multi-factor authentication provides additional steps to authorise access to systems compared to traditional single-factor authentication such as passwords or PINs. The ACSC recommends applying multi-factor authentication for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.

Why: Stronger user authentication makes it harder for adversaries to access sensitive information and systems.

Relevant ISM Controls:

- Security Control: 1173; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS

Multi-factor authentication is used to authenticate all privileged users and any other positions of trust.

- Security Control: 1504; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS

Multi-factor authentication is used to authenticate all users of remote access solutions.

- Security Control: 1505; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS

Multi-factor authentication is used to authenticate all users when accessing important data repositories.

- Security Control: 1401; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS

Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics or smartcards.

Mitre ATT&CK for Enterprise:

- Mitigations – Multi-Factor Authentication

Mitigations:

- Enable multi-factor authentication on VPN, RDP, SSH and other remote access systems
- Enforce multi-factor authentication for privileged actions or access to sensitive/high-availbility data repositories

Daily Backups

Daily backups are crucial for recovery from data-loss situations such as malware (particularly ransomware) infection, system crashes, hardware failures and destruction by malicious attackers. The ACSC recommends incremental or differential backups of relevant new/changed data, software and configuration settings, with offsite or disconnected storage and a retention period of at least three months. Further recommendations are given to test the backup process whenever significant, or related changes are made to infrastructure or systems. According to a survey by BackBlaze, the number of users who back up their data daily was only 9%, with 20% never backing up and 25% only performing backups yearly.

Why: To ensure information can be accessed and recovered following a cybersecurity incident (e.g. a ransomware incident).

Relevant ISM Controls:

- Security Control: 1511; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS

Backups of important information, software and configuration settings are performed at least daily.

- Security Control: 1512; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS

Backups are stored offline, or online but in a non-rewritable and non-erasable manner.

- Security Control: 1514; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS

Backups are stored for three months or greater.

- Security Control: 1515; Revision: 1; Updated: Jul-19; Applicability: O, P, S, TS

Full restoration of backups is tested at least once when initially implemented, and each time fundamental information technology infrastructure changes occur.

- Security Control: 1516; Revision: 1; Updated: Jul-19; Applicability: O, P, S, TS

Partial restoration of backups is tested on a quarterly or more frequent basis.

Mitre ATT&CK for Enterprise:

- Mitigations – Data Backup

Mitigations:

- Establish a daily differential/incremental backup strategy
- Establish a backup rotation and storage process
- Test and replace backup infrastructure as required
- Test the backup process regularly to ensure recovery as needed

References

The Essential Eight Explained (ACSC) – https://www.cyber.gov.au/publications/essential-eight-explained

The Essential Eight Maturity Model (ACSC) – https://www.cyber.gov.au/publications/essential-eight-maturity-model

Strategies to Mitigate Cyber Security Incidents (ACSC) – https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents

The Australian Government Information Security Manual (ISM) – https://www.cyber.gov.au/ism

BackBlaze Survey of Backups – https://www.backblaze.com/blog/more-people-than-ever-backing-up-according-to-our-survey/

Updates to the Essential Eight – https://www.cyber.gov.au/news/updates-essential-eight-maturity-model

The Essential Eight for MSPs – https://www.cyber.gov.au/news/msp-e8

Protecting Small Businesses against Cyber Attacks – https://www.cyber.gov.au/news/protecting-small-business-against-cyber-attacks-during-covid-19

Stay Smart Online Stats – https://www.staysmartonline.gov.au/sites/default/-files/Cost%20of%20cybercrime_INFOGRAPHIC_WEB_published_08102015.pdf