Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Essential Eight Maturity Model

JULY 2019

Introduction

The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies, in the form of the ***Strategies to Mitigate Cyber Security Incidents***, to help organisations mitigate cyber security incidents caused by various cyber threats. The most effective of these mitigation strategies are known as the Essential Eight.

Maturity levels

To assist organisations in determining the maturity of their implementation of the Essential Eight, three maturity levels have been defined for each mitigation strategy. The maturity levels are defined as:

- Maturity Level One: Partly aligned with the intent of the mitigation strategy
- Maturity Level Two: Mostly aligned with the intent of the mitigation strategy
- Maturity Level Three: Fully aligned with the intent of the mitigation strategy.

What maturity level to aim for

As a baseline organisations should aim to reach Maturity Level Three for each mitigation strategy. However, some organisations are constantly targeted by highly skilled adversaries, or otherwise operate in a higher risk environment. Where the ACSC believes an organisation requires a maturity level above that of Maturity Level Three, the ACSC will provide tailored advice to meet the specific needs of the organisation.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents.

Contact details

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

Essential Eight Maturity Model

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Application whitelisting	An application whitelisting solution is implemented on all workstations to restrict the execution of executables to an approved set. An application whitelisting solution is implemented on all servers to restrict the execution of executables to an approved set.	An application whitelisting solution is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set. An application whitelisting solution is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set.	An application whitelisting solution is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set. An application whitelisting solution is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set. Microsoft's latest recommended block rules are implemented to prevent application whitelisting bypasses.
Patch applications	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within two weeks of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	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. 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. Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.
Configure Microsoft Office macro settings	Microsoft Office macros are allowed to execute, but only after prompting users for approval. Microsoft Office macro security settings cannot be changed by users.	Only signed Microsoft Office macros are allowed to execute. Microsoft Office macros in documents originating from the Internet are blocked. Microsoft Office macro security settings cannot be changed by users.	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. Microsoft Office macros in documents originating from the Internet are blocked. Microsoft Office macro security settings cannot be changed by users.
User application hardening	Web browsers are configured to block or disable support for Flash content.	Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block web advertisements. Web browsers are configured to block Java from the Internet.	Web browsers are configured to block or disable support for Flash content. Web browsers are configured to block web advertisements. Web browsers are configured to block Java from the Internet. Microsoft Office is configured to disable support for Flash content. Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.
Restrict administrative privileges	Privileged access to systems, applications and information is validated when first requested. Policy security controls are used to prevent privileged users from reading emails, browsing the Web and obtaining files via online services.	Privileged access to systems, applications and information is validated when first requested and revalidated on an annual or more frequent basis. Policy security controls are used to prevent privileged users from reading emails, browsing the Web and obtaining files via online services.	Privileged access to systems, applications and information is validated when first requested and revalidated on an annual or more frequent basis. Privileged access to systems, applications and information is limited to that required for personnel to undertake their duties. Technical security controls are used to prevent privileged users from reading emails, browsing the Web and obtaining files via online services.
Patch operating systems	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within one month of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. 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.	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within two weeks of the security vulnerabilities being identified by vendors, independent third parties, system managers or users. 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.	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. 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. 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.
Multi-factor authentication	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication uses at least two of the following authentication factors: passwords with six or more characters, Universal 2nd Factor security keys, physical one-time password tokens, biometrics, smartcards, mobile app one-time password tokens, SMS messages, emails, voice calls or software certificates.	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication is used to authenticate all privileged users and any other positions of trust. Multi-factor authentication uses at least two of the following authentication factors: passwords with six or more characters, Universal 2nd Factor security keys, physical one-time password tokens, biometrics, smartcards or mobile app one-time password tokens.	Multi-factor authentication is used to authenticate all users of remote access solutions. Multi-factor authentication is used to authenticate all privileged users and any other positions of trust. Multi-factor authentication is used to authenticate all users when accessing important data repositories. Multi-factor authentication uses at least two of the following authentication factors: passwords with six or more characters, Universal 2nd Factor security keys, physical one-time password tokens, biometrics or smartcards.
Daily backups	Backups of important information, software and configuration settings are performed monthly. Backups are stored for between one to three months. Partial restoration of backups is tested on an annual or more frequent basis.	Backups of important information, software and configuration settings are performed weekly. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for between one to three months. Full restoration of backups is tested at least once. Partial restoration of backups is tested on a bi-annual or more frequent basis.	Backups of important information, software and configuration settings are performed at least daily. Backups are stored offline, or online but in a non-rewritable and non-erasable manner. Backups are stored for three months or greater. Full restoration of backups is tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur. Partial restoration of backups is tested on a quarterly or more frequent basis.