Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Essential Eight Explained

JANUARY 2019

Introduction

The ***Strategies to Mitigate Cyber Security Incidents*** is a prioritised list of mitigation strategies to assist organisations in protecting their systems against a range of adversaries. The mitigation strategies can be customised based on each organisation's risk profile and the adversaries they are most concerned about.

The Essential Eight

While no single mitigation strategy is guaranteed to prevent cyber security incidents, organisations are recommended to implement eight essential mitigation strategies as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems. Furthermore, implementing the Essential Eight proactively can be more cost-effective in terms of time, money and effort than having to respond to a large-scale cyber security incident.

Before implementing any of the mitigation strategies, organisations should perform the following activities:

- identify which systems require protection (i.e. which systems store, process or communicate sensitive information or other information with a high availability requirement)
- identify adversaries most likely to target their systems (e.g. nation-states, cyber criminals or malicious insiders)
- identify what level of protection is required (i.e. selecting mitigation strategies to implement based on the risks to business activities from specific adversaries).

There is a suggested implementation order for each adversary to assist organisations in building a strong cyber security posture for their systems. Once organisations have implemented their desired mitigation strategies to an initial level, they should focus on increasing the maturity of their implementation such that they eventually reach full alignment with the intent of each mitigation strategy.

Further information

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

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at https://www.acsc.gov.au/infosec/mitigationstrategies.htm.

The ***Essential Eight Maturity Model*** complements the advice in the ***Strategies to Mitigate Cyber Security Incidents***. It can be found at https://www.acsc.gov.au/publications/protect/Essential_Eight_Maturity_Model.pdf.

Mitigation Strategies to Prevent Malware Delivery and Execution	
Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.	**Patch applications** e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
Why: All non-approved applications (including malicious code) are prevented from executing.	**Why:** Security vulnerabilities in applications can be used to execute malicious code on systems.
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.	**User application hardening.** Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
Why: Microsoft Office macros can be used to deliver and execute malicious code on systems.	**Why:** Flash, ads and Java are popular ways to deliver and execute malicious code on systems.
Mitigation Strategies to Limit the Extent of Cyber Security Incidents	
Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.	**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: Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.	**Why:** Security vulnerabilities in operating systems can be used to further the compromise of systems.
Multi-factor authentication including 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.	
Mitigation Strategies to Recover Data and System Availability	
Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.	
Why: To ensure information can be accessed following a cyber security incident (e.g. a ransomware incident).	