Strategies Simplified

macquarie GOVERNMENT

‘Essential 8’ strategies to mitigate cyber security incidents.

Australian Signals Directorate

FORTINET

macquarie GOVERNMENT

Introduction.

The Australian Signals Directorate's (ASD) 'Essential 8' strategies to mitigate cyber security incidents represent a set of cyber security best practices that, when implemented successfully, will provide your agency, with a baseline cyber security posture.

The essential 8 expand upon the 'Top 4' mitigation strategies, part of the government's Protective Security Policy Framework, which have been mandatory for federal agencies since 2014. ASD had stated that implementing the top 4 mitigation strategies will be able to prevent over 85% of unauthorised intrusions.

The essential 8 mitigation strategies have been developed to protect your data, applications and users by keeping adversaries from inserting malware into your network to minimise impact of incident and data loss. Malware – viruses, worms, ransomware, spyware and more - can compromise or exfiltrate data, disrupt operations or propagate into connected networks. It can cause operational disruptions, loss of critical or sensitive data and unwanted publicity. And that can be expensive. According to the EMC Global Data Protection Index, data loss and downtime cost Australian businesses AUD $65.5 billion in 2014. These mitigation strategies can help you avoid malware infections and their associated costs.

"The eight strategies will help protect businesses from ransomware, malicious insiders, business email compromise, threats to industrial control systems and adversaries with destructive intent."

Dan Tehan
the Minister Assisting the Prime Minister for Cyber Security

macquarie GOVERNMENT

The essential 8 strategies.

The top 4 mitigation strategies are mandatory for Australian government agencies. Here is a quick recap. First and foremost is application white listing. This feature allows only trusted applications to execute on your network. Pokemon Go which is subjected to malware intrusions, for instance, have no business running on a government network.

Two of the top 4 strategies revolve around patching applications and operating systems. Every day new vulnerabilities and exploits are uncovered and software vendors are continuously issuing patches to remedy the situation. Keeping your software updated should be one of your most important tasks.

The remaining four essential 8 mitigation strategies are not yet mandatory. However, they are essential for securing your networks.

Web browsers and Microsoft Office macros are widely-used productivity tools for many government agencies. Two of the essential 8 strategies focus on configuring browsers to restrict unauthorised apps from running and tightly controlling the use of macros and user applications.

Multi-factor authentication and daily back-ups complete the essential 8 mitigation strategy list. Tokens, biometrics and dual passwords are essential to secure traffic beyond the firewall. And backups are absolutely critical, especially to minimise the impact from ransomware. Every agency, as well as every business and home user, should perform regular backups and have 'full-metal' restore and disaster recovery strategies in place.

The top 4.

- Application whitelisting
- Patching applications
- Restrict administrative privileges
- Patching operating systems

Use it wisely

Tightly managing administrator privileges rounds out the top 4 strategies; Administrators have great power – but it comes with great responsibility.

Additional 4 that make up essential 8.

- Disable untrusted MS Office macros
- Harden user applications
- Use multi-factor authentication
- Backup important data daily.

macquarie GOVERNMENT

Why the essential 8?

Why another set of guidelines? There are any number of cyber security approaches that can secure networks. These essential 8 mitigation strategies have been developed specifically to provide Australian government agencies with a baseline of security operations that, if implemented and tied together, can protect networks, users, applications and data from all but the most persistent threats. The following points illustrate why these mitigation strategies make sense.

Defence in Depth

These strategies are designed to work together. Individually they are all powerful tools to protect individual components and operations of your network. Together they represent a multi-level approach that provides comprehensive protection, even if adversaries do manage to break one of the defensive measures.

Accessible to All

None of these strategies are 'state-of-the art' nor bleeding edge. They are all tried and true. There is virtually no risk in adopting these strategies if implemented correctly. Indeed, performing back-ups for important data has been an essential rule for IT managers since day one. The real benefit of the ASD essential 8 is that they provide a baseline cyber security posture and provide a quantifiable benchmark to meet ASD recommendations.

Cost-effective

The essential eight strategies can go a long way into protecting your agencies from security breaches and potentially damaging malware for a comparatively modest financial investment. While implementing these strategies will entail an investment of staff time and possible hardware / software upgrades, the costs involved will be considerably lower than cleaning up in the wake of a compromise.

Deployment

Whilst your agency can implement these mitigation strategies in an ad hoc manner, basing your security posture on a single comprehensive framework has many benefits. With a comprehensive security fabric, you would be able to manage most of the strategies – such as whitelisting, patching, admin privileges – from a centralised console. Additionally, you'll be able to apply consistent and appropriate enforcement of policy across all users, applications and devices whether on premise, remote, cloud or hybrid cloud.

Automation

Many of these mitigation strategies can be automated to reduce management overheads whilst ensuring compliance. Most security solutions can be set up with thresholds and alerts to monitor network traffic so that any anomalous activity can be quickly identified and investigated. Massive unauthorised downloads, such as the Panama Papers leak, wouldn't have happened with the right mitigation strategies in place.

macquarie GOVERNMENT

Application whitelisting.

Top Mitigation Strategy Number One.

Application whitelisting restricts users from accessing any applications other than ones explicitly allowed (eg, programs, software libraries, scripts and installers) by your agency's appropriate use policy.

Application whitelisting protects against unauthorised or malicious code executing on a system regardless of whether the software was downloaded from a website, clicked on as an email attachment or introduced via removable storage media. In addition to preventing the execution and spread of malicious code, application whitelisting can also prevent the installation or use of unauthorised applications.

Application whitelisting is controlled by the vendor product chosen, configuration settings and permissions controlling which directories a user (and therefore malware) can write to and execute from. Endpoint protection or anti-malware software from some vendors includes application whitelisting functionality. Be aware that application whitelisting products may conflict with anti-malware software from a different vendor.

It's important that an application whitelisting solution does not replace antivirus and other internet security software already in place. Using multiple security solutions together can contribute to an effective defence-in-depth approach to preventing the compromise of systems.

Hint Deploying application whitelisting is easier if the organisation has detailed visibility of what software is installed on computers. Such visibility can be obtained by maintaining an inventory of software installed and implementing a robust change management process.

Application whitelisting.

Function

Restricts access to trusted applications

Prevents

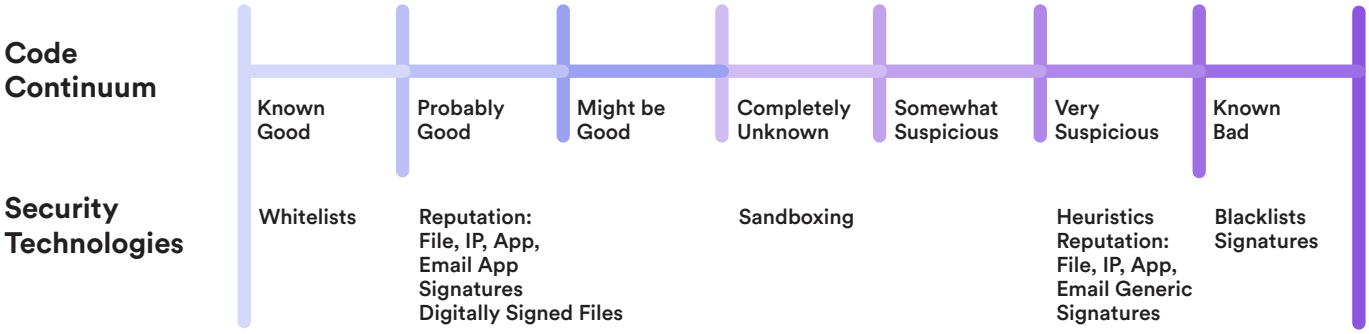
Malware from entering and executing inside your network

Enabler

Vendor-provided solutions, firewall, configurations, permissions, user training

In a recent study 30% of employees opened phishing email and 12% clicked on an infected document or link that allowed malware malicious code to damage targeted systems.

Source: Fortinet FortiGuard Labs



Addressing the unknown malicious codes.

macquarie GOVERNMENT

Patching applications.

Top Mitigation Strategy Number Two.

Applying patches – the latest updates - to applications and devices (as well as operating systems, strategy number 4) is critical to ensuring the security of systems. ASD currently rates this activity as one of the most effective security practices organisations can perform.

Patching protects networks from vulnerabilities not previously identified in the applications. Also known as exploits, these vulnerabilities enable adversaries to execute malicious code, which can result in significant consequences for the organisation. Exploits are so common that adversaries can buy or sell exploits on-line, for example in an open source tool like the Metasploit Framework or in a cybercrime exploit kit.

Time is important. Ideally you should apply patches within 48 hours of release as per ISM (Australian Government Information Security Manual) recommendation. When installing new applications, use the latest version since they typically incorporate 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.

Hint To obtain visibility of what software requires patching, maintain an inventory of software installed on every computer, especially devices that might only occasionally connect to the organisation's network such as spare or older machines, field laptops and handheld data capture devices.

406,887 Cryptowall ransomware attempts, 4,046 malware infections and 839 command and control URLs for servers, used by adversaries to send commands and receive data, have been responsible for an estimated US$325 million of damages in 2016.

Source: Cyber Threat Alliance

Patch applications.

Function

Updates applications to remedy previously unidentified vulnerabilities (exploits)

Prevents

Malware from entering and executing inside your network

Enabler

Vendor-provided software and threat updates

macquarie GOVERNMENT

Restrict administrative privileges.

Top Mitigation Strategy Number Three.

Restricting administrative privileges makes it more difficult for an adversary to spread its malicious code inside your network. As ASD calls it, the admin accounts are the keys to the kingdom and you don't want to hand over the keys at any time. If activated inside your network via an admin account, malicious codes can elevate its privileges, spread to other hosts, hide its existence, persist after reboot, obtain sensitive information or resist removal efforts.

Users with administrative privileges for operating systems and applications are able to make significant changes to their configuration and operation, bypass critical security settings and access sensitive information. Domain administrators have similar abilities for an entire network domain, which usually includes all of the workstations and servers on the network. If adversaries hijack these capabilities, there is virtually no end to the damage they can cause.

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.

An environment where administrative privileges are restricted is more stable, predictable and easier to administer and support, as fewer users can make significant changes to their operating environment, either intentionally or unintentionally.

Hint Privileged users should use a separate unprivileged account, and preferably a separate physical computer, for activities that are non-administrative or risky.

On average, FortiGuard Labs block 180,000 malicious websites, 220,000 Botnet attempts, and 733,000 network intrusion attempts per minute. They also set the industry record of 339 zero day threats discovered to date. Source: Fortinet FortiGuard Labs

Restrict admin privileges.

Function

Allows only trusted users to manage systems, install software and apply patches

Prevents

Unauthorised users and intruders from carrying out malicious activities

Enabler

Operating system and application configurations

macquarie GOVERNMENT

Patching operating systems.

Top Mitigation Strategy Number Four.

Applying patches (interim software upgrades) to operating systems and firmware (as well as applications, essential strategy number two) is critical to ensuring the security of systems. ASD currently rates this activity as one of the most effective security practices organisations can perform.

Patching operating systems and firmware significantly reduces the risks from zero-day threats which take advantage of exploits to install malware into your networks.

By maintaining a streamlined patch management strategy, organisations can position themselves to act swiftly upon security bulletin or patch releases. In doing so, organisations can dramatically reduce the time between noticing information on new security vulnerabilities, assessing the security vulnerabilities and applying patches or temporary workarounds where appropriate.

It is essential that security vulnerabilities are patched as quickly as possible. Once a vulnerability in an operating system, application or device is made public, it can be expected that malicious code will be developed by adversaries within 48 hours. In fact, there are cases in which adversaries have developed malicious code within hours of newly-discovered security vulnerabilities.

Hint Always 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.

Fortinet's research and response centre team have discovered 379 zero day vulnerabilities since 2006.

Source: Fortinet FortiGuard Labs

Patch operating systems.

Function

Updates applications to remedy any previously unidentified vulnerabilities (exploits)

Prevents

Malware from entering and executing inside your network

Enabler

Vendor-provided operating system, firmware and threat updates

macquarie GOVERNMENT

Disable Microsoft Office macro settings.

Top Mitigation Strategy Number Five.

Disabling or limiting Microsoft Office macros can prevent malicious code from entering your agency's network. Compromised macros can often evade basic email content filtering and application whitelisting.

Macros, embedded code written in the Visual Basic for Applications (VBA) programming language, are easily-created tools and greatly improve productivity. However, adversaries can also create and distribute macros to perform a variety of malicious activities. Out-of-date macros or macros downloaded from the internet may contain vulnerabilities that can be exploited by resulting in unauthorised access to sensitive information as part of a targeted cyber intrusion.

To manage the use of macros within an organisation, all macros created by users or third parties should be reviewed before being approved for use within the organisation. By understanding the business requirements for the use of macros, and applying the necessary mitigation strategies, organisations can effectively manage the risk of allowing macros in their IT environments.

Hint The best approach is 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.

Disable untrusted MS Office macros.

Function

Disables or restricts access to Microsoft Office macros

Prevents

Macro-borne malware from entering your network

Enabler

Microsoft Office configurations

macquarie GOVERNMENT

Harden user applications.

Top Mitigation Strategy Number Six.

Flash, Java, Acrobat Adobe and certain features in Microsoft Office (eg OLE), whilst useful for many business operations, can be vectors for malware or intruders to enter your network. Disabling these applications – and blocking online ads - removes any opportunity for adversaries to exploit these potentially disruptive tools. If your agency uses these applications, you can restrict which users may access these resources.

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 whitelisting by either exploiting an application's legitimate functionality or exploiting a security vulnerability for which a vendor patch is unavailable.

Online ads should be stopped due to the prevalent threat of adversaries using malicious advertising (malvertising) to compromise the integrity of legitimate websites. You can block them using web browser software and web content filtering at the gateway.

Hint Focus on hardening the configuration of applications used for online activities. For web browsers, disallow Adobe Flash (ideally uninstall it), ActiveX, Java, Silverlight and QuickTime for Windows. Whitelist trustworthy websites that require such web browser functionality for a specific business purpose.

Multiple zero day vulnerabilities (CVE-2017-2984, CVE-2017-2990, and CVE-2017-2991) discovered in Adobe Flash Player in November 2016 have resulted in Adobe-provided patches in February 2017, leaving organisations at risk for more than two months.

Source: Fortinet FortiGuard Labs

Harden user applications.

Function

Blocks or restricts access to potentially harmful online applications

Prevents

Malware from entering your network

Enabler

Operating system, firewall, third party applications

macquarie GOVERNMENT

Multi-factor authentication.

Top Mitigation Strategy Number Seven.

Multi-factor authentication is one of the most effective controls an organisation can implement to prevent an adversary from gaining access to a device or network and accessing sensitive information. When implemented correctly, multi-factor authentication can make it significantly more difficult for an adversary to steal legitimate credentials to facilitate further malicious activities on a network.

Multi-factor authentication should be used by all users accessing devices and sensitive information repositories, performing privileged operations and accessing networks via remote access. Using multi-factor authentication provides a secure authentication mechanism that is not as susceptible to brute force attacks that threaten traditional single-factor authentication like passwords.

Multi-factor authentication makes it significantly more difficult for an adversary to steal a complete set of credentials. They need physical access to a second factor that either they have (eg, a physical token, smartcard or software-based certificate) or are (eg, a fingerprint or iris scan). Without that second factor, they are stopped cold.

Ideally, multi-factor authentication should be implemented for all user logins including corporate computers in the office. But sometimes this isn't practicable. In these cases, ensure that user passwords for remote access are different from passwords used for office computers. However, adversaries could use a stolen password to access the network drives if someone who has access to the organisation's corporate network has been remotely compromised.

Hint Ensure mandatory multi-factor authentication for all administrative service accounts; other accounts that are unable to use multi-factor authentication should use strong passwords that contain a minimum of four random words, numeric and special characters.

Use multi-factor authentication.

Function
Adds another layer of security for remote logins

Prevents
Unauthorised access into your network

Enabler
Operating system, firewall, third party applications

Using cloud-based password cracking tools, attackers can attempt 300 million different passwords in only 20 minutes at a cost of less than USD$20. Adversaries can easily compromise even a strong alpha-numeric password with special characters during a typical lunch hour. Multi-factor authentication eliminates this particular threat.

Source: Fortinet FortiGuard Labs

macquarie GOVERNMENT

Daily backups.

Top Mitigation Strategy Number Eight.

Data is your most important digital asset. Protect your data with daily back-ups. Similarly, back up your software and configuration settings every time they change. Store back-ups offsite, if possible, and retain for three months as recommended by the ISM. Test as appropriate.

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.

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.

Hint 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; use corporate file servers and ASD certified cloud services.

Ransomware attacks more than doubled in 2016, with upwards of 4,000 attacks occurring daily that infected an average of 30,000 to 50,000 devices each month. The amount of ransom paid last year increased thirty-fivefold—skyrocketing from US$24 million to US$850 million. Ransom demands also expanded—jumping from an average of US$294 in 2015 to US$679 last year.

Source: Fortinet FortiGuard Labs

Backup important data daily.

Function

Provides clean, up-to-date and recoverable copy of your data and configurations

Prevents

Disruption from loss or corruption of data from ransomware

Enabler

Third-party vendors

macquarie GOVERNMENT

Conclusion.

The ASD essential 8 mitigation strategies, if implemented correctly as an integral component of your overall security fabric, provide a baseline cyber security posture for your agency to ensure that your security defences are working together to provide baseline protection. You owe it to your stakeholders, users and the public to assure them that you are doing everything within your power to protect sensitive data and critical applications from prying eyes, leaks or disruption.

These guidelines provide an excellent opportunity for you to systematically examine your complete network infrastructure and ensure that every component is correctly configured and that you have installed the basic security features and procedures to ensure business continuity.

The ASD's essential 8 mitigation strategies, along with the other 29 strategies, provide an excellent blueprint for security best practices. At the very least you should download the checklist and do a quick stock-take on which ones you already employ, which ones are on your 'to-do' list, which ones are for later and which ones you hadn't considered. Indeed, the top four have been mandatory for Australian government agencies since 2014.

While the full set of 37 strategies are not yet mandatory, not adopting these guidelines can lead to problems if indeed your network gets compromised due to lack of following the ASD recommendations. Governing boards especially should be aware of these guidelines and ensure that they are being followed or planned.

More work? Probably. More expense? Possibly. More protection? Absolutely. Safer outcomes? Most definitely.

The Australian Signals Directorate has recognised the cyber security threats and responded with Essential 8 mititgation strategies. Are you doing all you can to protect your agency, people, data and applications? You owe it to your stakeholders – and the public - to ensure that these mitigation strategies are implemented and maintained.

macquarie GOVERNMENT

About Macquarie Government.

As a part of ASX listed Macquarie Telecom Group (ASX: MAQ), Macquarie Government is Australian specialist in cyber security, secure cloud and data centres solutions. Currently 42% of Federal Government agencies trust and use Macquarie Government's security and cloud services.

About Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider and government organisations around the world. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 290,000 customers trust Fortinet to protect their businesses.

fortinet.com

FORTINET

References:

[1] High-level overview of the 'essential 8' http://www.asd.gov.au/publications/protect/essential-eight-explained.htm

[2] Nicely organised overview of all the strategies with the rationale, implementation guidance and links to further information. Also available as a PDF http://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-details.htm

[3] Somewhat older overview of mitigation strategies with more comprehensive details on the 'top 4' strategies http://www.asd.gov.au/infosec/mitigationstrategies.htm

[4] For the latest on zero day threat research http://fortiguard.com/advisoryupcoming

Let's talk.
Canberra Level 7, 54 Marcus Clarke St, Canberra ACT 2600, Tel 02 6257 6277
Sydney Level 15, 2 Market St, Sydney NSW 2000, Tel 02 8221 7777

Want to know more?
Visit macquariegovernment.com